

La Martinière Monplaisir

Cours de MPSI

26 août 2026

Table des matières

I	Trigonométrie et nombres imaginaires	7	V	Nombres complexes	81
1	Relation de congruence modulo un réel	8	1	L'inégalité triangulaire	82
2	Les fonctions sinus, cosinus et tangente	8	2	Propriétés supplémentaires de l'exponentielle complexe et des arguments	82
3	Modes de repérage dans le plan et angles orientés	10	3	Groupe $\mathbb{U}$ des nombres complexes de module 1	83
4	Trigonométrie	14	4	Équations du second degré	83
5	Nombres imaginaires	21	5	Racines énièmes.	85
II	Fonctions usuelles	29	6	Techniques de calcul	86
1	Rappels d'analyse.	30	7	L'exponentielle complexe	87
2	Effet d'une transformation sur le graphe.	34	8	Nombres complexes et géométrie plane	87
3	Composée de fonctions, réciproque.	36	VI	Équations différentielles linéaires	93
4	Fonction valeur absolue	39	1	Résultats d'analyse	94
5	Fonctions puissances entières, polynomiales et rationnelles	40	2	Équations linéaires du premier ordre.	100
6	Fonctions exponentielles, logarithmes et puissances quelconques	42	3	Équations différentielles du second ordre à coefficients constants.	103
7	Fonctions circulaires réciproques	45	VII	Théorie des ensembles	111
8	Fonctions hyperboliques	48	1	Définitions.	112
III	Un peu de calcul	51	2	Interprétation logique	117
1	Le symbole somme : Σ	52	VIII	Notion d'application	119
2	Le symbole produit : Π	56	1	Vocabulaire.	120
3	Quelques formules à connaître	56	2	Restriction, prolongement	121
4	Systèmes linéaires et pivot de Gauss	59	3	Composition d'applications	122
IV	Quelques fondamentaux	65	4	Injectivité, surjectivité, bijectivité	122
1	Propositions.	66	5	Image directe, tiré en arrière.	125
2	Connecteurs logiques.	66	IX	Calcul matriciel	129
3	Quantificateurs universel et existentiel.	69	1	Définitions élémentaires	130
4	Raisonnements par récurrence.	71	2	Systèmes linéaires	139
			X	Relations d'ordre et d'équivalence	143
			1	Relations binaires.	144

2	Relations d'équivalence.	144	1	$\mathbb{K}[X]$: définitions et résultats algébriques.	222
3	Relations d'ordre.	145	2	Décomposition.	229
4	Majorants, minorants et compagnie.	146	3	Dérivation des polynômes.	235
5	Relation d'ordre naturelle sur $\mathbb{N}$	149	4	Arithmétique de $\mathbb{K}[X]$	238
6	Relation d'ordre naturelle sur $\mathbb{R}$	149	5	Formule d'interpolation de Lagrange.	243
XI	Entiers relatifs et arithmétique de $\mathbb{Z}$	155	6	Annexe : construction de $\mathbb{K}[X]$	245
1	Divisibilité.	156	7	Annexe : fonctions polynomiales à valeurs dans un anneau	247
2	PGCD, PPCM.	157	XVII	Dérivabilité	249
3	Nombres premiers.	163	1	Définitions et premières propriétés.	250
XII	Suites réelles et complexes	167	2	Les grands théorèmes.	256
1	Vocabulaire.	168	3	Extension au cas des fonctions complexes.	262
2	Limite d'une suite réelle.	169	4	Convexité.	263
3	Résultats de convergence.	173	XVIII	Fractions rationnelles	271
4	Traduction séquentielle de certaines propriétés.	176	1	Corps des fractions rationnelles $\mathbb{K}(X)$	272
5	Suites particulières.	177	2	Étude locale d'une fraction rationnelle.	275
6	Suites définies par une relation de récurrence d'ordre 1.	181	3	Application au calcul intégral.	281
7	Suites à valeurs complexes.	182	XIX	Espaces vectoriels	283
8	Premiers exemples de séries numériques.	184	1	Espaces vectoriels et combinaisons linéaires.	284
XIII	Groupes, anneaux, corps	185	2	Sous-espaces vectoriels.	286
1	Lois de composition internes.	186	3	Translations, sous-espaces affines.	293
2	Structure de groupe.	188	XX	Analyse asymptotique	297
3	Anneaux	193	1	Comparaison asymptotique de suites.	298
4	Structure de corps.	196	2	Comparaison de fonctions.	301
XIV	Limite d'une fonction	197	3	Développements limités.	303
1	Préliminaires.	198	4	Théorèmes de comparaison pour les séries.	311
2	Définitions de la limite d'une fonction.	199	XXI	Familles de vecteurs et espaces vectoriels de dimension finie	315
3	Propriétés des limites de fonctions.	204	1	Familles de vecteurs.	316
4	Théorèmes d'existence.	206	2	Notion de dimension.	322
5	Cas des fonctions à valeurs complexes.	208	3	Sous-espaces vectoriels en dimension finie.	326
XV	Continuité	211	XXII	Intégration	331
1	Définitions et premières propriétés.	212	1	Continuité uniforme.	332
2	Les grands théorèmes.	215			
3	Extension au cas des fonctions à valeurs complexes.	219			
XVI	Polynômes	221			

2	Construction de l'intégrale.	333	5	Systèmes d'équations linéaires. . .	413
3	Le théorème fondamental du calcul différentiel.	338	6	Matrices semblables et trace. . .	414
4	Méthodes de calcul.	339	7	Matrices par blocs (HP).	417
5	Formules de Taylor.	340	XXVII Déterminants		423
6	Cas des fonctions à valeurs complexes.	341	1	Groupe symétrique.	424
7	Approximation d'intégrales. . .	341	2	Applications multilinéaires. . . .	428
8	Comparaison série-intégrale. . .	344	3	Déterminant d'une famille de vecteurs.	430
9	Annexes.	345	4	Déterminant d'un endomorphisme.	434
XXIII	Dénombrement	347	5	Déterminant d'une matrice carrée.	435
1	Cardinal d'un ensemble fini. . .	348	XXVIII Séries numériques		441
2	Dénombrement.	350	1	Prolégomènes	442
XXIV	Applications linéaires	355	2	Séries à termes réels positifs . .	444
1	Généralités.	356	3	Comparaison série-intégrale . . .	446
2	Applications linéaires en dimension finie.	362	4	Séries absolument convergentes .	447
3	Endomorphismes particuliers. .	365	5	Familles sommables	449
4	Formes linéaires et hyperplans. .	367	6	Annexe : compléments	457
XXV	Probabilités sur un univers fini	371	XXIX	Espaces euclidiens et préhilbertiens réels	459
1	Événements, probabilités.	372	1	Produit scalaire, norme et distance.	460
2	Variables aléatoires.	382	2	Orthogonalité.	463
XXVI	Matrices et algèbre linéaire	397	XXX	Fonctions de deux variables	469
1	Structure de $\mathcal{M}_{n,p}(\mathbb{K})$	398	1	Fonctions numériques à deux variables	470
2	Matrices, familles de vecteurs et applications linéaires.	399	2	Introduction au calcul différentiel	472
3	Matrices remarquables.	407			
4	Rang d'une matrice.	409			

Chapitre I

Trigonométrie et nombres imaginaires

Sommaire

1	Relation de congruence modulo un réel	8
2	Les fonctions sinus, cosinus et tangente	8
2.1	Définitions géométriques	8
2.2	Résultats admis	9
3	Modes de repérage dans le plan et angles orientés	10
3.1	Coordonnées cartésiennes	10
3.2	Angles orientés de vecteurs	11
3.3	Angles orientés de droites	12
3.4	Cercle trigonométrique	13
3.5	Coordonnées polaires	13
4	Trigonométrie	14
4.1	Angles remarquables	14
4.2	Propriétés élémentaires	15
4.3	Équations trigonométriques	16
4.4	Formules trigonométriques	16
4.5	Régularité des fonctions trigonométriques circulaires	19
5	Nombres imaginaires	21
5.1	Bref aperçu historique	21
5.2	Une définition géométrique	21
5.3	Écriture trigonométrique d'un complexe	23
5.4	Multiplication de deux complexes . . .	25
5.5	Conjugué et module d'un nombre complexe	26
5.6	Inverse d'un nombre complexe non nul	27
5.7	Technique de l'angle moitié	27

Nous nous placerons dans tout ce chapitre dans le plan $\mathbb{R}^2$, muni de son repère orthonormal canonique $(O, \vec{i}, \vec{j})$.

1 Relation de congruence modulo un réel

Définition 1.0.1.

Soit $\theta \in \mathbb{R}$. On dit que deux réels a et b sont *congrus modulo θ* s'il existe $k \in \mathbb{Z}$ tel que $a = b + k\theta$. On note alors $a \equiv b [\theta]$, ou aussi $a = b [\theta]$.

Exemple 1.0.2. • $\frac{\pi}{2}, -\frac{\pi}{2}$ et $\frac{5\pi}{2}$ sont congrus modulo π ;
• $\frac{\pi}{4}, \frac{9\pi}{4}$ et $-\frac{15\pi}{4}$ sont congrus modulo 2π .

Remarque 1.0.3.

La relation $a = b [\theta]$ se lit aussi « a et b sont égaux à un multiple de θ près ».

Proposition 1.0.4.

Soit $\theta \in \mathbb{R}$, et a, b, c, d quatre réels.

1. On a $a \equiv a [\theta]$ (on dit que la relation de congruence modulo θ est *réflexive*).
2. Si $a \equiv b [\theta]$, alors $b \equiv a [\theta]$ (on dit que la relation de congruence modulo θ est *symétrique*).
3. Si $a \equiv b [\theta]$ et $b \equiv c [\theta]$, alors $a \equiv c [\theta]$ (on dit que la relation de congruence modulo θ est *transitive*).
4. Si $a \equiv b [\theta]$ et $c \equiv d [\theta]$, alors $a + c \equiv b + d [\theta]$.
5. Si $a \equiv b [\theta]$, alors $a \equiv b [-\theta]$.
6. Si $n \in \mathbb{Z}$ et $a \equiv b [n\theta]$, alors $a \equiv b [\theta]$.
7. Si $a \equiv b [\theta]$, alors $ac \equiv bc [c\theta]$.

Une relation vérifiant les trois premiers points de cette proposition est appelée une *relation d'équivalence*.

Démonstration.

C'est immédiat en revenant à la définition.

1. On a $a = a + 0\theta$, donc $a \equiv a [\theta]$.
2. Soit $k \in \mathbb{Z}$ tel que $a = b + k\theta$, alors $b = a + (-k)\theta$, or $-k \in \mathbb{Z}$, donc $b \equiv a [\theta]$.

3. Soit $k, \ell \in \mathbb{Z}$ tels que $a = b + k\theta$ et $b = c + \ell\theta$, alors $a = c + (k + \ell)\theta$, or $k + \ell \in \mathbb{Z}$, donc $a \equiv c [\theta]$.
4. Soit $k, \ell \in \mathbb{Z}$ tels que $a = b + k\theta$ et $c = d + \ell\theta$, alors $a + c = b + d + (k + \ell)\theta$, or $k + \ell \in \mathbb{Z}$, donc $a + c \equiv b + d [\theta]$.
5. C'est un cas particulier du point suivant (avec $n = -1$).
6. Soit $k \in \mathbb{Z}$ tel que $a = b + kn\theta$, alors $a = b + (nk)\theta$, or $nk \in \mathbb{Z}$, donc $a \equiv b [\theta]$.
7. Soit $k \in \mathbb{Z}$ tel que $a = b + k\theta$, alors $ac = bc + k(c\theta)$, or $k \in \mathbb{Z}$, donc $ac \equiv bc [c\theta]$.

□

Exercice 1.0.5.

Parmi la famille de réels suivants, déterminer lesquels sont congrus entre eux modulus 2π . Même question pour $\pi, \frac{\pi}{2}$ et $\frac{2\pi}{3}$.

- $\alpha = 1$
- $\beta = 3\pi$
- $\gamma = 4\pi$
- $\delta = -\frac{\pi}{2}$
- $\varepsilon = \frac{5\pi}{6}$
- $\zeta = \frac{28\pi}{4}$

Au besoin, vous placerez les points/angles correspondants sur le cercle trigonométrique (voir partie 3.4).

Remarque 1.0.6 (Irrationalité de π).

Tout au long de cette année, vous pourrez utiliser le résultat suivant :

$$\pi \notin \mathbb{Q}.$$

Ce résultat sera démontrable en milieu d'année de MPSI.

2 Les fonctions sinus, cosinus et tangente

2.1 Définitions géométriques

Soit (ABC) un triangle du plan, rectangle en B . On suppose les trois points A, B, C deux à deux distincts. On note α l'angle (non orienté) $\widehat{BAC}$. Alors nous posons :

- $\cos \alpha = \frac{AB}{AC}$;
- $\sin \alpha = \frac{CB}{AC}$;
- $\tan \alpha = \frac{CB}{AB} = \frac{\sin \alpha}{\cos \alpha}$.

En particulier, dans le cas où $AC = 1$, grâce au théorème de Pythagore nous obtenons que :

$$\cos^2 \alpha + \sin^2 \alpha = AB^2 + CB^2 = AC^2 = 1.$$

Cette relation entre sinus et cosinus est la première formule de trigonométrie à connaître !

Vous connaissez ces définitions depuis la fin du collège. Elles sont bien sûr historiquement et géométriquement fondamentales, mais posent quelques problèmes théoriques : tout d'abord, qu'est-ce qu'un angle ? Comment définir cette notion ?

Ensuite, avec cette définition, tous les sinus et cosinus sont positifs. Pour obtenir des quantités algébriques, donc avec des signes, il faut *orienter* toutes les quantités en jeu : aussi bien les angles que les longueurs. Et cela oblige à quelques contorsions.

Enfin, comment définir le sinus et le cosinus d'un angle droit ?

Dans les mathématiques « modernes », les choses sont introduites différemment : les fonctions sinus et cosinus sont introduites grâce à la notion de *série entière*, que vous étudierez en seconde année. Et c'est à partir de ces fonctions que l'on peut définir ce qu'est un angle, et retrouver toutes les propriétés géométriques habituelles.

Nous allons dans la suite adopter ce point de vue : tout ce que nous admettrons, c'est qu'il existe deux fonctions réelles sinus et cosinus, dont nous admettrons quelques propriétés, en particulier que pour tout $t \in \mathbb{R}$, $\cos^2 t + \sin^2 t = 1$.

Finalement, en MPSI peu importe le point de vue, vous devrez uniquement connaître les liens entre angles et fonctions trigonométriques (vous les connaissez déjà pour la plupart).

2.2 Résultats admis

Nous admettons qu'il existe deux fonctions sinus et cosinus, dont les graphes sont représentés figure I.1, et vérifiant les propriétés suivantes :

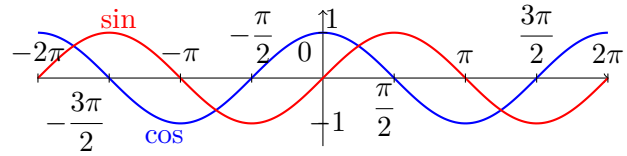


FIGURE I.1 – Fonctions cos et sin.

Proposition 2.2.1. 1. Les fonctions sinus (sin) et cosinus (cos) sont définies sur $\mathbb{R}$ et sont 2π -périodiques ;

2. La fonction cosinus est paire et la fonction sinus est impaire ;

3. La fonction cos est strictement décroissante sur $[0, \pi]$ établit une bijection de $[0, \pi]$ dans $[-1, 1]$; cela signifie que pour tout $x \in [-1, 1]$, il existe un unique réel $t \in [0, \pi]$ tel que $x = \cos t$;

4. Pour tout $t \in \mathbb{R}$, $\cos t = \sin\left(t + \frac{\pi}{2}\right)$ (le graphe de cos n'est donc que le translaté de celui de sin, et la connaissance d'une seule de ces deux fonctions permet de connaître l'autre) ;

5. Si $t \in \mathbb{R}$,

$$\cos t = 0 \quad \text{ssi} \quad t \equiv \frac{\pi}{2} [\pi]$$

$$\sin t = 0 \quad \text{ssi} \quad t \equiv 0 [\pi]$$

$$\cos t = 1 \quad \text{ssi} \quad t \equiv 0 [2\pi]$$

$$\cos t = -1 \quad \text{ssi} \quad t \equiv \pi [2\pi]$$

$$\sin t = 1 \quad \text{ssi} \quad t \equiv \frac{\pi}{2} [2\pi]$$

$$\sin t = -1 \quad \text{ssi} \quad t \equiv -\frac{\pi}{2} [2\pi]$$

6. Pour tout $t \in \mathbb{R}$, $\cos^2 t + \sin^2 t = 1$.

Nous pouvons alors démontrer le lemme suivant, fort utile :

Lemme 2.2.2.

Soit $a, b \in \mathbb{R}$ tels que $a^2 + b^2 = 1$. Alors il existe

$$t \in \mathbb{R} \text{ tel que } \begin{cases} a = \cos t \\ b = \sin t \end{cases}.$$

Démonstration.

Puisque $a^2 + b^2 = 1$, alors a^2 et b^2 appartiennent à l'intervalle $[0, 1]$, et donc $a, b \in [-1, 1]$. Ainsi il existe un réel t tel que $a = \cos t$. Dans ce cas : $b^2 = 1 - a^2 = 1 - \cos^2 t = \sin^2 t$. Par conséquent, $|b| = |\sin t|$. Si b et $\sin t$ sont de même signe, $b = \sin t$ et nous avons fini.

Sinon, $b = -\sin t = \sin(-t)$ puisque $\sin$ est impaire. Si nous posons $t' = -t$, alors $b = \sin t'$ et $a = \cos t = \cos(-t') = \cos t'$ car $\cos$ est paire. Nous avons donc bien démontré le résultat voulu. $\square$

Nous pouvons alors définir la fonction tangente :

Définition 2.2.3.

Notons A l'ensemble des points d'annulation de la fonction $\cos$, *i.e.* l'ensemble des réels congrus à $\frac{\pi}{2}$ modulo π :

$$\begin{aligned} A &= \left\{ x \in \mathbb{R} \mid \exists k \in \mathbb{Z} \ x = \frac{\pi}{2} + k\pi \right\} \\ &= \left\{ \frac{\pi}{2} + k\pi \mid k \in \mathbb{Z} \right\}. \end{aligned}$$

On appelle alors *fonction tangente*, notée $\tan$, la fonction :

$$\begin{array}{ccc} \tan : & \mathbb{R} \setminus A & \rightarrow \mathbb{R} \\ & t & \mapsto \frac{\sin t}{\cos t} \end{array}$$

Remarque 2.2.4.

On peut définir de la même manière la fonction *cotangente* :

Posons

$$B = \{ x \in \mathbb{R} \mid \exists k \in \mathbb{Z} \ x = k\pi \} = \pi\mathbb{Z}.$$

On appelle alors *fonction cotangente*, notée $\cotan$, la fonction :

$$\begin{array}{ccc} \cotan : & \mathbb{R} \setminus B & \rightarrow \mathbb{R} \\ & t & \mapsto \frac{\cos t}{\sin t} \end{array}$$



La fonction cotangente n'est pas égale à $\frac{1}{\tan}$. Pourquoi ?

Par parité du cosinus et imparité du sinus, la fonction tangente est impaire. Elle est aussi π -périodique, ce que nous allons montrer plus loin. Les autres propriétés des fonctions $\cos$, $\sin$ et $\tan$, qui sont appelées *fonctions trigonométriques circulaires*, vont être démontrées plus loin également. Elles nous permettront de tracer le graphe de la fonction tangente.

Nous allons d'abord effectuer quelques rappels de géométrie du plan.

3 Modes de repérage dans le plan et angles orientés

3.1 Coordonnées cartésiennes

Définition 3.1.1 (voir figure I.2). 1. Soit u un vecteur du plan. Il existe un unique couple $(a, b) \in \mathbb{R}^2$ tel que $u = a\vec{i} + b\vec{j}$. Ce couple est appelé couple des *coordonnées* de u dans la base $(\vec{i}, \vec{j})$. On note alors $u = \begin{pmatrix} a \\ b \end{pmatrix}$.

2. Soit M un point du plan. Soit (a, b) les coordonnées du vecteur $\overrightarrow{OM}$ dans la base $(\vec{i}, \vec{j})$. Ce couple est appelé couple des *coordonnées* de M dans le repère $(O, \vec{i}, \vec{j})$. On note alors $M = (a, b)$. Le réel a est l'abscisse du point M , le réel b est son ordonnée.

Remarque 3.1.2.

On identifiera fréquemment le point M avec le vecteur $\overrightarrow{OM}$. Notamment, on notera souvent $M = \begin{pmatrix} a \\ b \end{pmatrix}$ pour donner les coordonnées de M .

Rappelons maintenant une série de résultats que vous connaissez déjà :

Théorème 3.1.3 (Règles de calcul). 1. Soient u et u' deux vecteurs de coordonnées respectives (x, y) et (x', y') , et λ et λ' deux réels. Le vecteur $\lambda u + \lambda' u'$ a pour coordonnées le couple $(\lambda x + \lambda' x', \lambda y + \lambda' y')$.

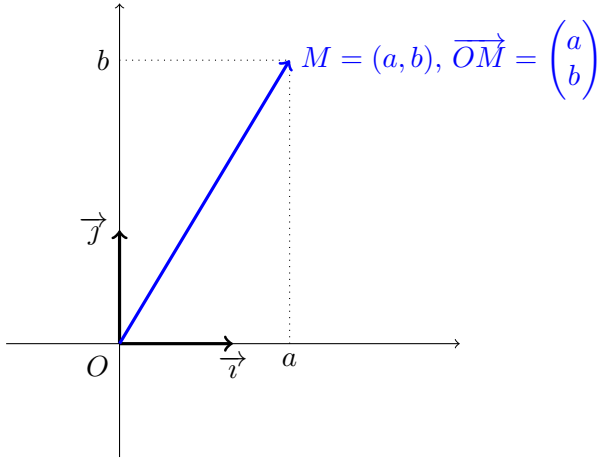


FIGURE I.2 – Repérage d'un point par ses coordonnées cartésiennes.

2. Soient A et B deux points de coordonnées respectives (x_A, y_A) et (x_B, y_B) . Le vecteur $\overrightarrow{AB}$ a pour coordonnées le couple $(x_B - x_A, y_B - y_A)$.

Définition 3.1.4. 1. Soit u un vecteur du plan de coordonnées (a, b) . La *norme (euclidienne)* du vecteur u est le réel $\|u\| = \sqrt{a^2 + b^2}$.

2. Soient A et B deux points de coordonnées respectives (x_A, y_A) et (x_B, y_B) . La *distance* AB est le réel

$$AB = \|\overrightarrow{AB}\| = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}.$$

On a immédiatement le résultat suivant.

Proposition 3.1.5.

Soit u un vecteur du plan, soit $\lambda \in \mathbb{R}$.

1. On a $\|u\| = 0 \Leftrightarrow u = \vec{0}$.
2. On a $\|\lambda u\| = |\lambda| \|u\|$.

Et pour finir, l'inégalité triangulaire, qui sera démontrée plus tard grâce aux nombres complexes :

Proposition 3.1.6 (Inégalité triangulaire).

1. Soit u, u' deux vecteurs. Alors

$$\left| \|u\| - \|u'\| \right| \leq \|u \pm u'\| \leq \|u\| + \|u'\|.$$

2. Soit A, B, C trois points du plan. Alors

$$|AB - BC| \leq AC \leq AB + BC.$$

3.2 Angles orientés de vecteurs

Dans toute la suite de ce chapitre et tout au long de l'année, nous allons parler d'*angle*. Mais qu'est-ce qu'un angle ? Observons tout d'abord qu'il s'agit de distinguer les angles orientés et les angles non orientés, ainsi que les angles entre droites et entre vecteurs.

Nous n'allons considérer que des angles orientés, et pour cela il faut *orienter* le plan : nous reviendrons plus tard dans l'année sur la définition précise d'orientation. Contentons-nous pour l'instant de considérer la base canonique $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$ comme étant directe, et les angles étant orientés *dans le sens trigonométrique* (ou *sens anti-horaire*), comme vous en avez pris l'habitude au lycée.

Dans le secondaire, vous n'avez jamais vraiment défini ce qu'était un angle. Mais vous avez vu une définition des fonctions cosinus et sinus à partir de la notion d'angle. Comme nous l'avons dit plus haut, nous pouvons faire l'inverse : définir la notion d'angle à partir des fonctions cosinus et sinus.

Il existe plusieurs manières de définir un angle entre deux vecteurs. Donnons une définition possible, qui ne figure pas au programme :

Définition 3.2.1 (voir figure I.3).

Soit u, v deux vecteurs **non nuls** du plan. Nous introduisons $u' = \frac{u}{\|u\|}$ et $v' = \frac{v}{\|v\|}$. Ces deux

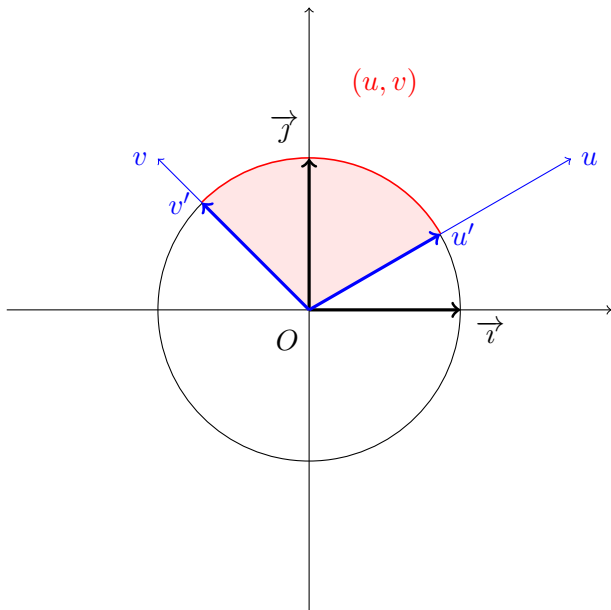


FIGURE I.3 – Angle entre deux vecteurs u et v .

vecteurs sont donc de norme 1, ou *unitaires*. Nous noterons $u' = \begin{pmatrix} a' \\ b' \end{pmatrix}$ et $v' = \begin{pmatrix} c' \\ d' \end{pmatrix}$.

On appelle *mesure de l'angle* (u, v) tout réel θ tel que

$$\begin{cases} c' &= \cos \theta & a' - \sin \theta & b' \\ d' &= \sin \theta & a' + \cos \theta & b' \end{cases}$$

Cette condition se note matriciellement

$$v' = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} u'.$$

Il existe une infinité de tels réels, mais si θ_0 est l'un d'entre eux, l'ensemble des mesures de l'angle (u, v) est l'ensemble de tous les réels congrus à θ_0 modulo 2π , *i.e.*

$$\{\theta_0 + 2k\pi, k \in \mathbb{Z}\}.$$

On note alors $(u, v) = \theta_0 [2\pi]$.

Remarque 3.2.2. • Par abus, on parle souvent de « l'angle (u, v) » plutôt que d'« une

mesure de l'angle (u, v) »¹.

- Il est important de retenir qu'un angle orienté de vecteurs se donne toujours modulo 2π .
- Géométriquement, l'angle (u, v) vaut θ si v' est l'image de u' par la rotation vectorielle d'angle θ .

Nous pourrions démontrer les résultats suivants plus tard dans l'année mais nous allons les admettre ici :

Proposition 3.2.3.

Soit $u, v, w \in \mathbb{R}^2$.

1. $(u, v) = -(v, u) [2\pi]$;
2. Relation de Chasles :

$$(u, v) + (v, w) = (u, w) [2\pi].$$

3.3 Angles orientés de droites

Il est aussi possible de définir l'angle orienté entre deux droites :

Définition 3.3.1.

Soit $\mathcal{D}$ et $\mathcal{D}'$ deux droites. On appelle *mesure de l'angle orienté* $(\mathcal{D}, \mathcal{D}')$ tout réel θ pour lequel il existe u un vecteur directeur de $\mathcal{D}$ et v un vecteur directeur de $\mathcal{D}'$ tel que θ est une mesure de l'angle (u, v) .

Il existe une infinité de tels réels, mais si θ_0 est l'un d'entre eux, l'ensemble des mesures de l'angle $(\mathcal{D}, \mathcal{D}')$ est l'ensemble de tous les réels congrus à θ_0 modulo π , *i.e.* $\{\theta_0 + k\pi, k \in \mathbb{Z}\}$.

On note alors $(\mathcal{D}, \mathcal{D}') = \theta_0 [\pi]$.

Remarque 3.3.2. • Par abus, on parle souvent de « l'angle $(\mathcal{D}, \mathcal{D}')$ » plutôt que d'« une mesure de l'angle (u, v) ».

- Il est important de retenir qu'un angle orienté de droites se donne toujours modulo π .

1. en toute rigueur l'angle (u, v) est l'ensemble de toutes les mesures de l'angle (u, v) : il s'agit d'une *classe d'équivalence* ; nous en reparlerons plus tard dans l'année

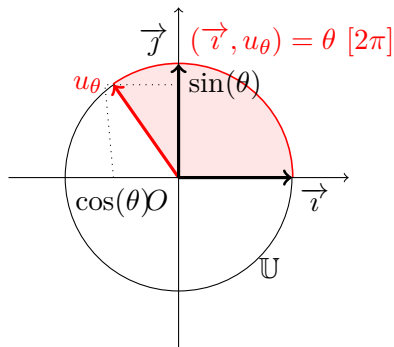


FIGURE I.4 – Cercle trigonométrique et vecteur u_θ .

Nous pourrions démontrer les résultats suivants plus tard dans l'année mais nous allons les admettre ici :

Proposition 3.3.3.

Soit $\mathcal{D}, \mathcal{D}', \mathcal{D}''$ trois droites du plan.

1. $(\mathcal{D}, \mathcal{D}') = -(\mathcal{D}', \mathcal{D}) [\pi]$;
2. Relation de Chasles : $(\mathcal{D}, \mathcal{D}') + (\mathcal{D}', \mathcal{D}'') = (\mathcal{D}, \mathcal{D}'') [\pi]$.

3.4 Cercle trigonométrique

Le cercle dit *trigonométrique*, souvent noté $\mathbb{U}$ (nous en reparlerons), est tout simplement le cercle de rayon 1 et de centre O .

Son utilité est principalement de représenter graphiquement les propriétés trigonométriques usuelles.

Le point de départ est le suivant : pour tout $\theta \in \mathbb{R}$, posons M_θ le point de coordonnées $(\cos \theta, \sin \theta)$: puisque $\cos^2 \theta + \sin^2 \theta = 1$, ce point est sur le cercle trigonométrique. Si nous posons $u_\theta = \overrightarrow{OM_\theta} = \begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix}$, alors $(\vec{i}, u_\theta) = \theta [2\pi]$ (voir figure I.4).

Mais réciproquement, tout point du cercle trigonométrique est de cette forme.

Théorème 3.4.1 (Représentation paramétrique du cercle trigonométrique).

Une représentation paramétrique du cercle trigonométrique est

$$\begin{cases} x = \cos t \\ y = \sin t \end{cases}, t \in \mathbb{R}.$$

Ou encore, $\mathbb{U} = \{(\cos t, \sin t), t \in \mathbb{R}\}$.

Démonstration.

L'inclusion $\mathbb{U} \subset \{(\cos t, \sin t), t \in \mathbb{R}\}$ se démontre directement grâce au lemme 2.2.2 $\square$

Remarque 3.4.2 (radians).

La longueur du cercle trigonométrique étant de 2π , par proportionnalité, la mesure d'un angle est la longueur de l'arc du cercle trigonométrique intersecté par ledit angle (voir figure I.3).

La mesure d'un angle « en radians » est le rapport entre la longueur de l'arc d'un cercle centré en O intersecté par ledit angle et le rayon de ce cercle, c'est donc une mesure sans dimension (du point de vue des physiciens). Le cercle trigonométrique étant de rayon 1, on obtient immédiatement que la mesure en radians d'un angle est la mesure donnée précédemment.

Remarque 3.4.3.

On retrouve sur ce cercle les relations « cosinus = côté adjacent sur hypoténuse », « sinus = côté opposé sur hypoténuse » et donc ensuite « tangente = côté opposé sur côté adjacent », puisqu'ici l'hypoténuse est de longueur 1.

3.5 Coordonnées polaires

Les coordonnées polaires ne sont plus au programme en mathématiques, mais vous pourrez les rencontrer en physique, et elles vous aideront à comprendre l'écriture trigonométrique des nombres complexes, que nous verrons dans la suite de ce chapitre.

Définition 3.5.1.

Soit M un point du plan. On appelle *couple de coordonnées polaires* de M tout couple $(r, \theta) \in \mathbb{R}^2$ tel que $\overrightarrow{OM} = ru_\theta$ et $r \geq 0$.

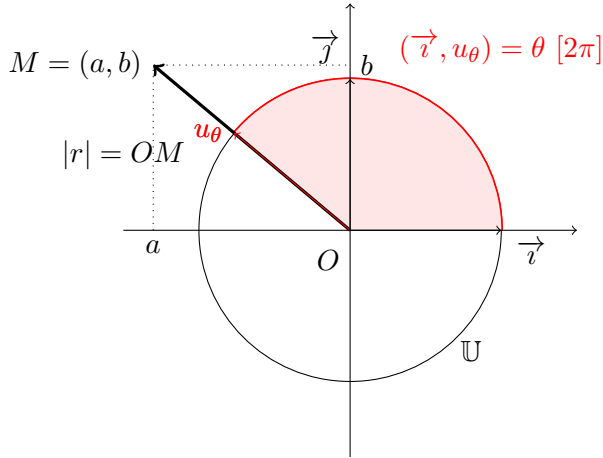


FIGURE I.5 – Coordonnées polaires (r, θ) de $M = (a, b)$.

Théorème 3.5.2.

Tout point admet une infinité de couples de coordonnées polaires.

Plus précisément :

- Les couples de coordonnées polaires de O sont tous les couples $(0, \theta)$ quand $\theta \in \mathbb{R}$;
- Si $M \neq O$, posons $\theta = (\vec{i}, \overrightarrow{OM}) [2\pi]$. Alors les couples de coordonnées polaires de M sont tous les couples $(OM, \theta + 2k\pi)$ quand $k \in \mathbb{Z}$.

Remarque 3.5.3.

On rencontre parfois une définition plus générale où r peut être négatif, mais nous l'éviterons. Cela dit, il faut remarquer que quel que soit le signe de r , $ru_\theta = -ru_{\theta+\pi}$. Il est donc toujours possible de se restreindre au cas r positif.

Exemple 3.5.4.

Si M est le point de coordonnées cartésiennes $(-1, 1)$, alors M admet $\left(\sqrt{2}, \frac{3\pi}{4}\right)$, $\left(\sqrt{2}, \frac{-5\pi}{4}\right)$ comme couples de coordonnées polaires. Le couple $\left(-\sqrt{2}, -\frac{\pi}{4}\right)$ est parfois accepté.

Remarque 3.5.5.

On passe facilement des coordonnées polaires aux coordonnées cartésiennes : si M a pour coordonnées polaires (r, θ) , posons $x = r \cos \theta$, $y = r \sin \theta$.

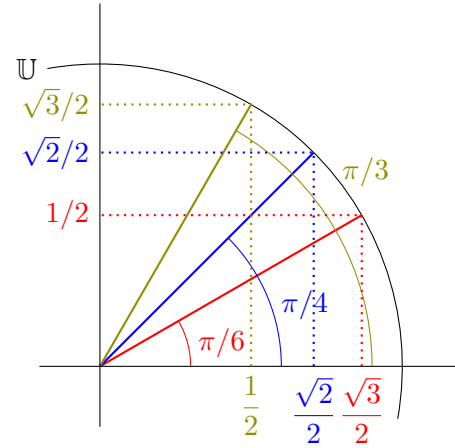


FIGURE I.6 – Angles usuels dans $\left]0, \frac{\pi}{2}\right[$.

Alors M a pour coordonnées cartésiennes le couple (x, y) .

Pour l'autre sens, il est nécessaire d'utiliser les fonctions trigonométriques circulaires inverses Arccos, Arcsin et Arctan, que nous définirons dans le chapitre sur les fonctions usuelles.

4 Trigonométrie

4.1 Angles remarquables

Vous devez connaître par cœur les valeurs des sinus, cosinus et tangentes pour les angles $0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}$, et tous leurs multiples. Ces valeurs sont données dans un tableau du formulaire de trigonométrie qui vous a été distribué en début d'année, vous les retrouverez dans la figure I.6.

Toutes ces valeurs se retrouvent sur le cercle trigonométrique, et peuvent se démontrer géométriquement. Faisons-le pour retrouver les valeurs des sinus et cosinus des angles $\frac{\pi}{4}$ (voir figure I.7) et $\frac{\pi}{3}$ (voir figure I.8).

Démonstration.

Comme $\frac{\pi}{4} \in \left]0, \frac{\pi}{2}\right[$, on a $\cos\left(\frac{\pi}{4}\right) > 0$ et $\sin\left(\frac{\pi}{4}\right) > 0$.

Si nous notons M, N, P les points de coordonnées respectives $(\cos \frac{\pi}{4}, \sin \frac{\pi}{4})$, $(\cos \frac{\pi}{4}, 0)$ et $(0, \sin \frac{\pi}{4})$, alors $ONMP$ est un carré dont la diagonale est de longueur 1. Ainsi, grâce au théorème de Pythagore, ses côtés sont de longueur $\frac{1}{\sqrt{2}}$, ou encore $\frac{\sqrt{2}}{2}$. Donc $\cos \frac{\pi}{4} = \sin \frac{\pi}{4} = \frac{\sqrt{2}}{2}$. $\square$

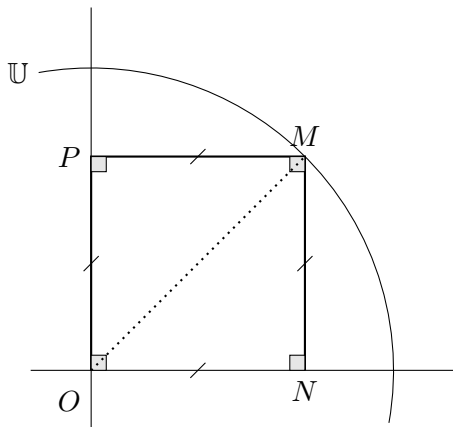


FIGURE I.7 – Détermination de $\cos\left(\frac{\pi}{4}\right)$.

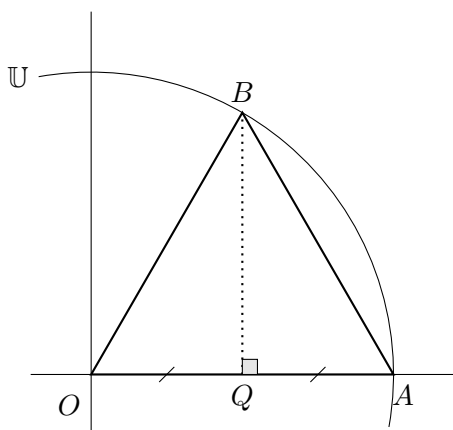


FIGURE I.8 – Détermination de $\cos\left(\frac{\pi}{3}\right)$.

Démonstration.

Comme $\frac{\pi}{3} \in \left]0, \frac{\pi}{2}\right[$, on a $\cos\left(\frac{\pi}{3}\right) > 0$ et $\sin\left(\frac{\pi}{3}\right) > 0$.

Si nous notons maintenant A, B les points de coordonnées respectives $(1, 0)$ et $(\cos \frac{\pi}{3}, \sin \frac{\pi}{3})$, alors OAB est équilatéral, de côtés de longueur 1. Ainsi, la médiatrice de $[O, A]$ passe par B . Si Q est le milieu de $[OA]$, alors $(QB) \perp (OA)$, donc Q a pour coordonnées $(\cos \frac{\pi}{3}, 0)$, donc $\cos \frac{\pi}{3} = \frac{1}{2}$. De plus, avec le théorème de Pythagore, $QB^2 = OB^2 - OQ^2 = 1 - \frac{1}{4}$. Ainsi $\sin \frac{\pi}{3} = QB = \frac{\sqrt{3}}{2}$. $\square$

Remarque 4.1.1 (⚠).

Il est fréquent d'hésiter dans les valeurs des sinus et cosinus des angles $\frac{\pi}{3}$ et $\frac{\pi}{6}$: encore une fois, au moindre doute, tracez un cercle trigonométrique.

Vous y verrez clairement que le point du cercle trigonométrique désigné par l'angle $\frac{\pi}{6}$ a une abscisse supérieure à celle du point correspondant à l'angle $\frac{\pi}{3}$. Donc $\cos \frac{\pi}{6} = \frac{\sqrt{3}}{2}$ et $\cos \frac{\pi}{3} = \frac{1}{2}$. Même méthode pour les sinus.

4.2 Propriétés élémentaires

Là encore, ces propriétés doivent se retrouver rapidement sur un cercle trigonométrique (voir exercice 4.2.3).

Proposition 4.2.1.

Les fonctions $\sin$ et $\cos$ sont 2π -périodiques sur $\mathbb{R}$.

La fonction $\tan$ est π -périodique sur son ensemble de définition.

De plus, pour tout réel α on a :

- $\cos(-\alpha) = \cos(\alpha)$
- $\sin(-\alpha) = -\sin(\alpha)$
- $\cos(\pi/2 - \alpha) = \sin(\alpha)$
- $\sin(\pi/2 - \alpha) = \cos(\alpha)$
- $\cos(\pi/2 + \alpha) = -\sin(\alpha)$
- $\sin(\pi/2 + \alpha) = \cos(\alpha)$
- $\cos(\pi - \alpha) = -\cos(\alpha)$
- $\sin(\pi - \alpha) = \sin(\alpha)$
- $\cos(\pi + \alpha) = -\cos(\alpha)$
- $\sin(\pi + \alpha) = -\sin(\alpha)$

Démonstration.

Il suffit d'utiliser les formules d'addition (voir la proposition 4.4.1). $\square$

Remarque 4.2.2.

Le dernier point permet de montrer que la fonction tangente est π -périodique.

Exercice 4.2.3.

Reproduire à main levée la figure I.9 et y placer tous les sinus et cosinus relevés, puis retrouver graphiquement les formules données par la proposition 4.2.1.

Exercice 4.2.4.

Ordonner les cosinus des angles suivants.

- $\alpha = \frac{\pi}{7}$
- $\delta = \frac{41\pi}{3}$
- $\beta = \frac{15\pi}{6}$
- $\varepsilon = \frac{31\pi}{6}$
- $\gamma = \frac{37\pi}{12}$
- $\zeta = \frac{112\pi}{5}$

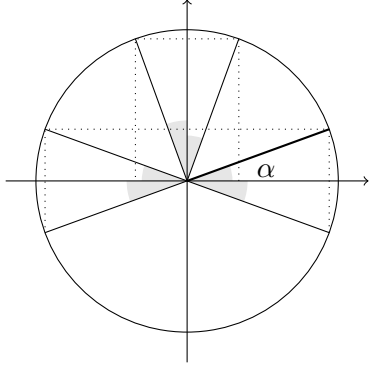


FIGURE I.9 – Formules sur les sinus et cosinus.

4.3 Équations trigonométriques

Proposition 4.3.1.

Soient a et b deux réels. Alors :

$$\begin{aligned} \cos(a) = \cos(b) & \text{ ssi } (a = b[2\pi] \text{ ou } a = -b[2\pi]) \\ \sin(a) = \sin(b) & \text{ ssi } (a = b[2\pi] \text{ ou } a = \pi - b[2\pi]) \\ \tan(a) = \tan(b) & \text{ ssi } a = b[\pi] \end{aligned}$$

On retrouve ces résultats sur un cercle trigonométrique, et en utilisant les propriétés élémentaires précédentes. Par exemple, pour résoudre $\sin x = \sin y$: on trace sur la droite d'équation $y = \sin a$. Elle coupe le cercle trigonométrique en deux points (ou éventuellement un seul si $\sin a = \pm 1$). Cela nous donne déjà deux solutions : a et $\pi - a$. Il faut ensuite considérer tous les réels congrus à ces deux solutions modulo 2π . Même chose pour résoudre $\cos a = \cos b$ en traçant la droite d'équation $x = \cos a$.

4.4 Formules trigonométriques

Les formules à partir desquelles on retrouve quasiment toutes les autres sont les suivantes :

Proposition 4.4.1 (formules d'addition).

Soit $a, b \in \mathbb{R}$. Alors :

1. $\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$;
2. $\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b)$.

Démonstration.

Notons M le point de coordonnées $(\cos(a + b), \sin(a + b))$ (voir figure I.10) : cela signifie que

$$\overrightarrow{OM} = \cos(a + b)\vec{i} + \sin(a + b)\vec{j} \quad (\text{I.1})$$

D'autre part, notons

$$\vec{u} = \begin{pmatrix} \cos(a) \\ \sin(a) \end{pmatrix} \text{ et } \vec{v} = \begin{pmatrix} -\sin(a) \\ \cos(a) \end{pmatrix}.$$

Comme

$$\begin{aligned} -\sin(a) &= 0 \times \cos(a) - 1 \sin(a) \\ &= \cos\left(\frac{\pi}{2}\right) \cos(a) - \sin\left(\frac{\pi}{2}\right) \sin(a) \end{aligned}$$

et comme

$$\begin{aligned} \cos(a) &= 0 \times \sin(a) + 1 \cos(a) \\ &= \cos\left(\frac{\pi}{2}\right) \sin(a) + \sin\left(\frac{\pi}{2}\right) \cos(a), \end{aligned}$$

on a

$$(\vec{u}, \vec{v}) = +\frac{\pi}{2}[2\pi].$$

On peut donc voir que $(\vec{u}, \vec{v})$ est la base obtenue à partir de $(\vec{i}, \vec{j})$ par la rotation vectorielle d'angle a .

Or, comme $(\vec{i}, \vec{u}) = a[2\pi]$ et $(\vec{i}, \overrightarrow{OM}) = a + b[2\pi]$, on a alors $(\vec{u}, \overrightarrow{OM}) = b[2\pi]$.

On peut donc écrire que

$$\overrightarrow{OM} = \cos(b)\vec{u} + \sin(b)\vec{v}.$$

Nous avons aussi par définition

$$\begin{aligned} \vec{u} &= \cos(a)\vec{i} + \sin(a)\vec{j} \\ \vec{v} &= -\sin(a)\vec{i} + \cos(a)\vec{j} \end{aligned}$$

Ainsi, on a

$$\begin{aligned} \overrightarrow{OM} &= \cos(b)[\cos(a)\vec{i} + \sin(a)\vec{j}] \\ &\quad + \sin(b)[- \sin(a)\vec{i} + \cos(a)\vec{j}] \\ &= (\cos(a)\cos(b) - \sin(a)\sin(b))\vec{i} \\ &\quad + (\sin(a)\cos(b) + \cos(a)\sin(b))\vec{j} \end{aligned}$$

Grâce à l'unicité des coordonnées d'un vecteur dans une base, il suffit d'utiliser l'expression trouvée en I.1 pour obtenir les formules demandées.

On peut aussi obtenir ces formules par un raisonnement géométrique élémentaire (voir figure I.11), dans le cas où a, b et $a + b$ sont dans $\left]0, \frac{\pi}{2}\right[$.

Notons M le point de coordonnées $(\cos(a + b), \sin(a + b))$, qui se situe sur $\mathbb{U}$ (on a donc $OM = 1$). Notons $\mathcal{D}_a$ la droite passant par O et faisant un angle de mesure a avec la droite $O\vec{i}$. Notons A le projeté orthogonal de M sur $\mathcal{D}_a$. Ainsi, le triangle OAM est rectangle en A . Notons J le projeté orthogonal de M sur la droite $O\vec{j}$. Ainsi, le triangle OJM est rectangle en J . Notons I le projeté orthogonal de A sur la droite $O\vec{i}$. Ainsi, le triangle OAM est rectangle en I .

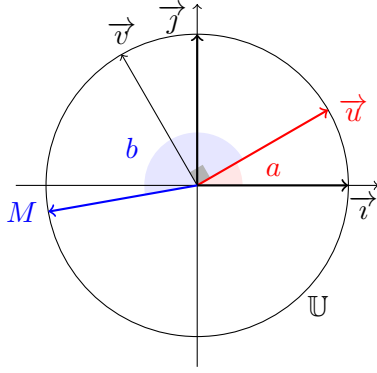


FIGURE I.10 – Formules d'addition : première preuve.

On a donc immédiatement, en utilisant $OM = 1$:

$$\begin{aligned} OJ &= \sin(a+b), \\ JM &= \cos(a+b), \\ OA &= \cos(b), \\ AM &= \sin(b), \\ AI &= \sin(a)\cos(b), \\ OI &= \cos(a)\cos(b). \end{aligned}$$

Comme les droites $(O\vec{v})$ et $(O, \vec{j})$ sont orthogonales, les droites (MB) et (AI) sont aussi orthogonales, donc sécantes : on note B leur point d'intersection. Ainsi, le triangle MAB est rectangle en B .

On admet que la somme des mesures des angles d'un triangle est égale à π , à un multiple de 2π près. Comme l'angle $\widehat{OIA}$ est droit, l'angle $\widehat{OAI}$ a pour mesure $\frac{\pi}{2} - a$. Comme $A \in (BI)$, l'angle $\widehat{IAB}$ est plat (donc de mesure π), or

$$(\vec{AI}, \vec{AB}) = (\vec{AI}, \vec{AO}) + (\vec{AO}, \vec{AM}) + (\vec{AM}, \vec{AB}) [2\pi].$$

On en déduit que l'angle $\widehat{BAM}$ a pour mesure a (ainsi, les triangles BAM et OAI sont semblables). Ainsi,

$$\begin{aligned} BA &= \cos(a)\sin(b) \\ BM &= \sin(a)\sin(b). \end{aligned}$$

Remarquons que $OJBI$ est un rectangle, donc $OJ = BI$ et $JB = OI$. On en déduit immédiatement la formule demandée.

Nous verrons à la fin de ce chapitre une méthode plus rapide pour retrouver ces formules, utilisant l'exponentielle complexe. $\square$

En jouant sur la parité de cosinus et l'imparité de sinus, nous avons bien sûr également, à partir de ces deux premières formules :

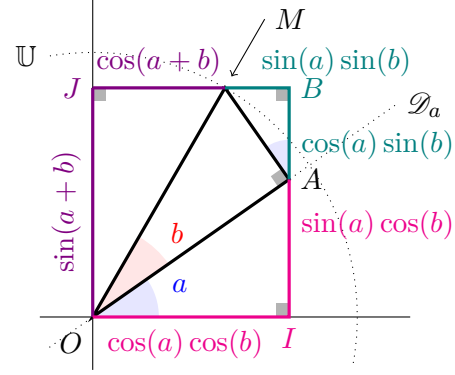


FIGURE I.11 – Formules d'addition : deuxième preuve.

Corollaire 4.4.2.

Soit $a, b \in \mathbb{R}$. Alors :

1. $\cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b)$;
2. $\sin(a-b) = \sin(a)\cos(b) - \cos(a)\sin(b)$.

On en tire les formules de duplication des angles, très utilisées aussi :

Corollaire 4.4.3 (formules de duplication).

Soit $a \in \mathbb{R}$. Alors

$$\begin{aligned} \cos(2a) &= \cos^2(a) - \sin^2(a) \\ &= 2\cos^2(a) - 1 \\ &= 1 - 2\sin^2(a) \end{aligned}$$

$$\text{et } \sin(2a) = 2\sin(a)\cos(a).$$

Viennent ensuite les formules d'addition de cosinus et sinus, et celles de produit :

Proposition 4.4.4.

Soit $a, b \in \mathbb{R}$. Alors :

1. $\cos(a) + \cos(b) = 2\cos\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right)$
2. $\sin(a) + \sin(b) = 2\sin\left(\frac{a+b}{2}\right)\cos\left(\frac{a-b}{2}\right)$
3. $\cos(a) - \cos(b) = -2\sin\left(\frac{a+b}{2}\right)\sin\left(\frac{a-b}{2}\right)$

4. $\sin(a) - \sin(b) = 2 \cos\left(\frac{a+b}{2}\right) \sin\left(\frac{a-b}{2}\right)$
5. $\cos(a) \cos(b) = \frac{1}{2}(\cos(a+b) + \cos(a-b))$
6. $\sin(a) \sin(b) = \frac{1}{2}(\cos(a-b) - \cos(a+b))$
7. $\sin(a) \cos(b) = \frac{1}{2}(\sin(a+b) + \sin(a-b))$.

Démonstration.

• Pour les quatre premières formules, il suffit de remarquer que $a = \frac{a+b}{2} + \frac{a-b}{2}$ et $b = \frac{a+b}{2} - \frac{a-b}{2}$, et d'appliquer les formules de base. Ainsi, pour la première formule :

$$\begin{aligned} \cos(a) + \cos(b) &= \cos\left(\frac{a+b}{2} + \frac{a-b}{2}\right) \\ &\quad + \cos\left(\frac{a+b}{2} - \frac{a-b}{2}\right) \\ &= \cos\left(\frac{a+b}{2}\right) \cos\left(\frac{a-b}{2}\right) \\ &\quad - \sin\left(\frac{a+b}{2}\right) \sin\left(\frac{a-b}{2}\right) \\ &\quad + \cos\left(\frac{a+b}{2}\right) \cos\left(\frac{a-b}{2}\right) \\ &\quad + \sin\left(\frac{a+b}{2}\right) \sin\left(\frac{a-b}{2}\right) \\ &= 2 \cos\left(\frac{a+b}{2}\right) \cos\left(\frac{a-b}{2}\right). \end{aligned}$$

Les trois formules suivantes s'obtiennent de même.

• Pour les deux dernières formules, on procède comme suit :

$$\cos(a+b) = \cos(a) \cos(b) - \sin(a) \sin(b) \quad (\text{I.2})$$

$$\cos(a-b) = \cos(a) \cos(b) + \sin(a) \sin(b) \quad (\text{I.3})$$

Nous obtenons immédiatement les deux formules de produit par demi-somme et demi-différence des lignes (I.2) et (I.3). $\square$

Pour finir, voici les formules de trigonométrie concernant la fonction tangente :

Proposition 4.4.5.

Soit $a, b \in \mathbb{R}$. Lorsque les tangentes qui suivent sont bien définies, nous avons les égalités suivantes :

1. $\tan(a+b) = \frac{\tan(a) + \tan(b)}{1 - \tan(a) \tan(b)} ;$
2. $\tan(a-b) = \frac{\tan(a) - \tan(b)}{1 + \tan(a) \tan(b)} ;$
3. $\tan(2a) = \frac{2 \tan(a)}{1 - \tan^2(a)} ;$

4. $\frac{1}{\cos^2(a)} = 1 + \tan^2(a) ;$
5. $\cos(2a) = \frac{1 - \tan^2(a)}{1 + \tan^2(a)} ;$
6. $\sin(2a) = \frac{2 \tan(a)}{1 + \tan^2(a)}.$

Démonstration.

1. On factorise :

$$\begin{aligned} \tan(a+b) &= \frac{\sin(a+b)}{\cos(a+b)} \\ &= \frac{\sin(a) \cos(b) + \sin(b) \cos(a)}{\cos(a) \cos(b) - \sin(a) \sin(b)} \\ &= \frac{\cos(a) \cos(b)}{\cos(a) \cos(b)} \times \frac{\tan(a) + \tan(b)}{1 - \tan(a) \tan(b)}. \end{aligned}$$

2. Utiliser le point précédent en utilisant l'impairité de la fonction tangente.
3. Utiliser le premier point en posant $b = a$.
4. $1 + \tan^2(a) = 1 + \frac{\sin^2 a}{\cos^2 a} = \frac{\cos^2 a + \sin^2 a}{\cos^2 a} = \frac{1}{\cos^2(a)}.$
- 5.

$$\begin{aligned} \cos(2a) &= 2 \cos^2 a - 1 \\ &= \frac{2}{1 + \tan^2 a} - 1 \\ &= \frac{2 - (1 + \tan^2 a)}{1 + \tan^2 a} \\ &= \frac{1 - \tan^2(a)}{1 + \tan^2(a)}. \end{aligned}$$

6.

$$\begin{aligned} \frac{2 \tan(a)}{1 + \tan^2(a)} &= 2 \tan(a) \cos^2(a) \\ &= 2 \sin(a) \cos(a) \\ &= \sin(2a) \end{aligned}$$

$\square$

Proposition 4.4.6 (Forme amplitude-phase).

Soit $a, b \in \mathbb{R}$. Alors il existe $A, \varphi \in \mathbb{R}$ tels que pour tout $t \in \mathbb{R}$, $a \cos(t) + b \sin(t) = A \cos(t - \varphi)$.

Démonstration.

Il s'agit de normaliser le vecteur $\begin{pmatrix} a \\ b \end{pmatrix}$ puis d'utiliser des formules de trigonométrie :

Si $a = b = 0$, il suffit de poser $A = 0$.

Sinon, posons $A = \left\| \begin{pmatrix} a \\ b \end{pmatrix} \right\| = \sqrt{a^2 + b^2}$. Ainsi $\left\| \begin{pmatrix} \frac{a}{A} \\ \frac{b}{A} \end{pmatrix} \right\| =$

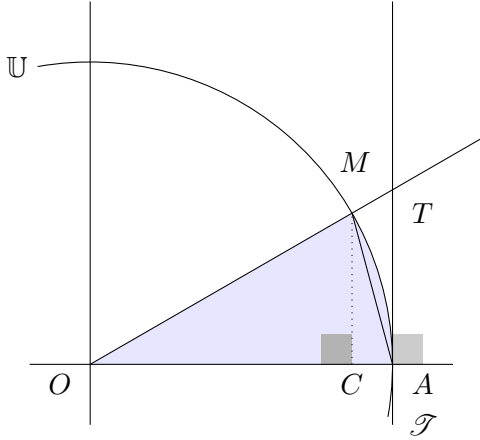


FIGURE I.12 – Preuve du lemme 4.5.1.

1. Par conséquent il existe $\varphi \in \mathbb{R}$ tel que $\frac{a}{A} = \cos \varphi$ et $\frac{b}{A} = \sin \varphi$. Alors, pour tout réel t :

$$\begin{aligned} a \cos(t) + b \sin(t) &= A \left(\frac{a}{A} \cos(t) + \frac{b}{A} \sin(t) \right) \\ &= A(\cos(\varphi) \cos(t) + \sin(\varphi) \sin(t)) \\ &= A \cos(t - \varphi) \end{aligned}$$

□

Remarque 4.4.7.

Ce résultat sera utilisé dans le chapitre sur les équations différentielles, pour exprimer sous une certaine forme les solutions de certaines équations.

4.5 Régularité des fonctions trigonométriques circulaires

Commençons par démontrer l'inégalité fondamentale suivante.

Lemme 4.5.1.

Si $0 < x < \frac{\pi}{2}$, alors

$$0 \leq x \cos(x) \leq \sin(x) \leq x.$$

Démonstration.

Soit $0 < x < \frac{\pi}{2}$, notons $A = (1, 0)$ et $M = (\cos(x), \sin(x))$ (voir figure I.12).

Remarquons que $\cos(x), \sin(x), \tan(x) \in \mathbb{R}_+^*$.

Notons $\mathcal{T}$ la perpendiculaire à (OA) passant par A et notons T le point d'intersection de $\mathcal{T}$ et (OM) , qui

existe bien car (OM) et $\mathcal{T}$ ne sont pas parallèles, vu l'encadrement sur x .

Notons C le projeté orthogonal de M sur (OA) : on a $C = (\cos(x), 0)$.

Par le théorème de Thalès, comme $CM = \sin(x)$, $OC = \cos(x)$ et comme $OA = OM = 1$, on a $AT = \tan(x)$.

Ainsi, le triangle OAM a pour aire $\frac{\sin(x)}{2}$.

Le disque unité a une aire de π et un périmètre de longueur 2π . La longueur de l'arc de cercle $\widehat{AM}$ est x . Par proportionnalité, la portion du disque unité comprise entre les segments OA et OM a pour aire $\frac{x}{2}$.

Enfin, le triangle OAT a pour aire $\frac{\tan(x)}{2}$.

Ces trois domaines sont inclus l'un dans l'autre (on l'admet), ce qui donne

$$0 \leq \sin(x) \leq x \leq \tan(x),$$

ce qui donne l'encadrement demandé. □

Proposition 4.5.2.

Les fonctions sinus et cosinus sont continues sur $\mathbb{R}$.

Démonstration.

Rappelons qu'une fonction f est continue en un point a lorsque $f(x) \xrightarrow{x \rightarrow a} f(a)$.

Commençons par démontrer la continuité en 0.

Si $0 < x < \frac{\pi}{2}$, alors $0 \leq \sin(x) \leq x$. Par encadrement, on obtient donc que $\sin(x) \xrightarrow{x \rightarrow 0^+} 0 = \sin(0)$. Mais imparité de $\sin$ et $x \mapsto x$, nous avons $x \leq \sin x \leq 0$ si $-\frac{\pi}{2} < x < 0$, donc encore par encadrement, $\sin(x) \xrightarrow{x \rightarrow 0^-} 0 = \sin(0)$. Les limites à gauche à droite valant $\sin(0)$, $\sin(x) \xrightarrow{x \rightarrow 0} \sin(0)$, d'où la continuité de $\sin$ en 0.

Pour le cosinus, il suffit d'observer que si $x \in \mathbb{R}$,

$$\cos(x) = \cos\left(2\frac{x}{2}\right) = 1 - 2\sin^2\left(\frac{x}{2}\right).$$

Il suffit d'utiliser la limite précédente pour obtenir que

$$\cos(x) \xrightarrow{x \rightarrow 0} 1 = \cos(0).$$

Ainsi $\cos$ est aussi continue en 0.

Étudions maintenant la continuité en un point $a \in \mathbb{R}$ quelconque : si $h \in \mathbb{R}$, $\sin(a+h) = \sin(a)\cos(h) + \cos(a)\sin(h) \xrightarrow{h \rightarrow 0} \sin(a)$. Donc $\sin(x) \xrightarrow{x \rightarrow a} \sin(a)$, et $\sin$ est continue en a . On procède de la même manière pour $\cos$. □

Donnons un dernier résultat intermédiaire, qui sera utilisé dans la démonstration du théorème suivant, mais dont le premier point est un résultat très important que vous réutiliserez souvent :

Proposition 4.5.3. 1. $\frac{\sin(x)}{x} \xrightarrow{x \rightarrow 0} 1$;

2. $\frac{\cos(x) - 1}{x} \xrightarrow{x \rightarrow 0} 0$.

Démonstration. 1. Par la continuité du cosinus, on a $\cos(x) \xrightarrow{x \rightarrow 0} 1$. Par le lemme 4.5.1, on a pour tout $0 < x < \frac{\pi}{2}$:

$$\cos(x) \leq \frac{\sin(x)}{x} \leq 1.$$

Par encadrement, on obtient que

$$\frac{\sin(x)}{x} \xrightarrow{x \rightarrow 0^+} 1,$$

Par imparité de $\sin$, $x \mapsto x \cos x$ et $x \mapsto x$, on obtient de la même manière $\frac{\sin(x)}{x} \xrightarrow{x \rightarrow 0^-} 1$, donc

$$\frac{\sin(x)}{x} \xrightarrow{x \rightarrow 0} 1.$$

Par les formules de duplication, on obtient

$$\cos(x) = \cos\left(2\frac{x}{2}\right) = 1 - 2\sin^2\left(\frac{x}{2}\right).$$

Ainsi,

$$\frac{\cos(x) - 1}{x} = -\frac{x}{2} \left(\frac{\sin\left(\frac{x}{2}\right)}{\frac{x}{2}} \right)^2 \xrightarrow{x \rightarrow 0} 0.$$

grâce au premier point. $\square$

Théorème 4.5.4. 1. La fonction cosinus est dérivable sur $\mathbb{R}$, est sa dérivée est $\cos' = -\sin$;

2. La fonction sinus est dérivable sur $\mathbb{R}$, est sa dérivée est $\sin' = \cos$;

3. La fonction tangente est dérivable là où elle est définie, et sa dérivée est

$$\tan' = 1 + \tan^2 = \frac{1}{\cos^2}.$$

Démonstration.

On rappelle qu'une fonction f est dérivable en un point a s'il existe $l \in \mathbb{R}$ tel que $\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a} l$. Dans ce cas, la dérivée de f en a est $f'(a) = l$.

Directement avec le premier point de la proposition 4.5.3, nous voyons que $\sin$ est dérivable et $\sin'(0) = 1$.

Et avec le second point de ce même lemme, $\cos$ est dérivable en 0 et $\cos'(0) = 0$.

1. Soit $a \in \mathbb{R}$, fixé. Posons $f : h \mapsto \sin(a + h)$ et $g : h \mapsto \sin(a) \cos(h) + \cos(a) \sin(h)$. Alors $f = g$. Puisque g est dérivable en 0, f l'est aussi, et $f'(0) = g'(0) = \sin(a) \cos'(0) + \cos(a) \sin'(0) = \cos(a)$.

$$\text{Donc } \frac{\sin(a+h) - \sin(a)}{h} \xrightarrow{h \rightarrow 0} \cos(a), \text{ ou encore } \frac{\sin(t) - \sin(a)}{t - a} \xrightarrow{t \rightarrow a} \cos(a).$$

Ainsi, la fonction sinus est dérivable en a et

$$\sin'(a) = \cos(a).$$

2. On procède de même pour le cosinus.

3. La fonction tangente est le quotient de deux fonctions dérivables là où elle est définie, donc elle est dérivable, et

$$\begin{aligned} \tan' &= \frac{\sin' \cos - \sin \cos'}{\cos^2} \\ &= \frac{\sin^2 + \cos^2}{\cos^2} \\ &= \frac{1}{\cos^2} \\ &= 1 + \tan^2. \end{aligned}$$

$\square$

Maintenant que nous voyons que la fonction tangente a une dérivée strictement positive, nous sommes en mesure d'affirmer qu'elle est strictement croissante sur chaque intervalle où elle est définie. Par composition de limites, pour tout $k \in \mathbb{Z}$, $\tan \xrightarrow{(\frac{\pi}{2} + k\pi)^-} +\infty$ et $\tan \xrightarrow{(\frac{\pi}{2} + k\pi)^+} -\infty$.

Enfin, $\tan'(k\pi) = 1$, ce qui nous permet de donner une allure du graphe de la fonction, qui est donné dans la figure I.13.

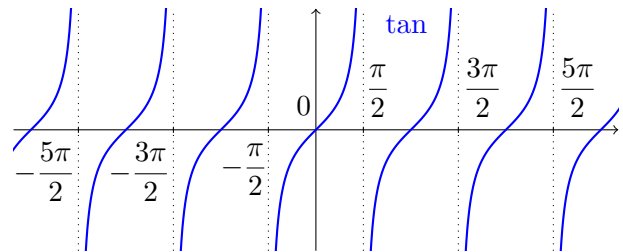


FIGURE I.13 – Fonction $\tan$.

Un dernier résultat, que la première partie de la démonstration précédente implique déjà sur $[-\frac{\pi}{2}, \frac{\pi}{2}]$:

Proposition 4.5.5.

Pour tout $x \in \mathbb{R}$, $|\sin x| \leq |x|$.

Démonstration.

Introduisons les fonctions $f : x \mapsto x - \sin(x)$ et $g : x \mapsto x + \sin(x)$, définies sur $\mathbb{R}_+$. Ces fonctions sont dérivables, et $f'(x) = 1 - \cos(x) \geq 0$. Ainsi f est croissante. Comme elle s'annule en 0, elle est donc positive sur $\mathbb{R}_+$. Avec un raisonnement analogue, g est positive également. Donc, pour tout $x \in \mathbb{R}_+ : -x \leq \sin x \leq x$, ou encore $-|x| \leq \sin x \leq |x|$ car $x \geq 0$. Finalement, $|\sin x| \leq |x|$ sur $\mathbb{R}_+$. Mais par parité de $x \mapsto |\sin x|$ et $x \mapsto |x|$, ce résultat est aussi valable sur $\mathbb{R}_-$, donc sur $\mathbb{R}$. $\square$

5 Nombres imaginaires

5.1 Bref aperçu historique

Au XVIème siècle, Cardan et Bombelli, deux mathématiciens italiens, s'intéressent à la résolution de certaines équations algébriques du troisième degré. Mais ils sont confrontés à un problème : ils ont besoin de la racine carrée d'un nombre réel négatif pour exprimer certaines solutions réelles qui existent bel et bien ! Ils « imaginent » alors que ces racines carrées existent.

Pendant trois siècles, des mathématiciens vont se pencher sur ces travaux, avec des points de vue divers. Pour certains, l'existence de ces « nombres imaginaires » n'a aucun sens. D'autres vont chercher à comprendre ces nombres. Il faudra attendre des travaux d'Euler à la fin du XVIIIème siècle pour que la situation s'éclaircisse et que les mathématiciens acceptent et utilisent ces nombres.

À partir du XIXème siècle, plusieurs mathématiciens vont proposer des définitions plus modernes et abouties de ces nombres alors appelés « complexes ». Il en existe plusieurs, ce qui fait l'intérêt et la richesse des nombres complexes : on peut les comprendre et les utiliser de plusieurs manières, et il existe des correspondances entre tous ces points de vue.

Les nombres complexes sont très importants. Vous les rencontrerez dans la plupart des chapitres de MPSI : dans les résolutions d'équations polynomiales, des équations différentielles, des suites récurrentes linéaires, en algèbre linéaire, et

en géométrie bien sûr. Vous les utiliserez aussi énormément en physique et en SI.

C'est pourquoi il est essentiel de bien les appréhender. Ne vous laissez pas influencer par leur dénomination de « complexes ». Ils doivent cet attribut à trois siècles d'assimilation difficile. Mais vous avez suivi une formation moderne, dans laquelle les nombres imaginaires (adjectif plus positif que complexes) vont trouver leur place facilement. Après tout, les nombres négatifs ont aussi mis plusieurs siècles à être acceptés, mais vous les maniez au moins depuis que vous avez 12 ans, parfois même bien avant.

Aucune construction des nombres complexes n'est au programme. Mais il faut bien les introduire, et nous allons le faire en gardant un point de vue géométrique. Tous les résultats sur les complexes s'interprètent géométriquement : ne l'oubliez pas, cela vous aidera à mieux vous les représenter, mieux mémoriser les résultats et élaborer vos raisonnements.

5.2 Une définition géométrique

À tout point du plan de coordonnées (a, b) , nous allons associer un nouvel objet noté $a + ib$, appelé un *nombre complexe*. À tout point il correspond exactement un nombre complexe. Ainsi, si a, a', b, b' sont quatre réels, $a + ib = a' + ib'$ ssi $(a, b) = (a', b')$ ssi $a = a'$ et $b = b'$.

La même construction peut être faite à partir de vecteurs : à tout vecteur $\begin{pmatrix} a \\ b \end{pmatrix}$, on associe le complexe $a + ib$.

Introduisons maintenant un peu de vocabulaire :

Définition 5.2.1 (voir figure I.14). 1. On note $\mathbb{C}$ l'ensemble des nombres complexes, c'est-à-dire que $\mathbb{C} = \{a + ib, a, b \in \mathbb{R}\}$.

2. Soit M un point du plan de coordonnées (a, b) . On appelle *affiche* de M le complexe $a + ib$.

3. Soit u un vecteur du plan de coordonnées $\begin{pmatrix} a \\ b \end{pmatrix}$. On appelle *affiche* de u le complexe $a + ib$.
4. Soit z un nombre complexe. Il existe donc un unique $(a, b) \in \mathbb{R}^2$ tel que $z = a + ib$. Le réel a est appelé la *partie réelle* de z . On le note $\operatorname{Re} z$. Le réel b est appelé la *partie imaginaire* de z . On le note $\operatorname{Im} z$.
5. Un complexe de partie réelle nulle est dit *imaginaire pur*. Les imaginaires purs s'écrivent donc sous la forme $0 + ib$, avec $b \in \mathbb{R}$, que nous écrirons plus simplement ib . Un complexe de partie imaginaire nulle est dit *réel*. Les réels s'écrivent donc sous la forme $a + i \cdot 0$, avec $a \in \mathbb{R}$, que nous écrirons plus simplement a .
6. Soit z un complexe de partie réelle a et de partie imaginaire b . On appelle *image* de z le point du plan de coordonnées (a, b) , ou le vecteur $\begin{pmatrix} a \\ b \end{pmatrix}$.

Remarque 5.2.2.

L'ensemble des *réels* correspond donc aux points du plan qui se trouvent sur l'axe des abscisses. D'une certaine manière, cela permet de voir $\mathbb{R}$ comme une partie de $\mathbb{R}^2$.

L'ensemble des imaginaires purs correspond quant à lui à l'axe des ordonnées.

Jusque-là, tout cela a peu d'intérêt : nous nous sommes contentés de « réécrire » les objets (a, b) et $\begin{pmatrix} a \\ b \end{pmatrix}$ sous une autre forme. Pour qu'un ensemble d'objets ait un intérêt, il faut pouvoir faire des opérations entre ces objets. Nous allons donc définir deux opérations, une addition et un produit externe, sur $\mathbb{C}$:

Définition 5.2.3. 1. Soit $z = a + ib$ et $z' = c + id$ deux complexes. On définit leur somme $z + z' = (a + c) + i(b + d)$. Ainsi $\operatorname{Re}(z + z') = \operatorname{Re}(z) + \operatorname{Re}(z')$ et $\operatorname{Im}(z + z') = \operatorname{Im}(z) + \operatorname{Im}(z')$.

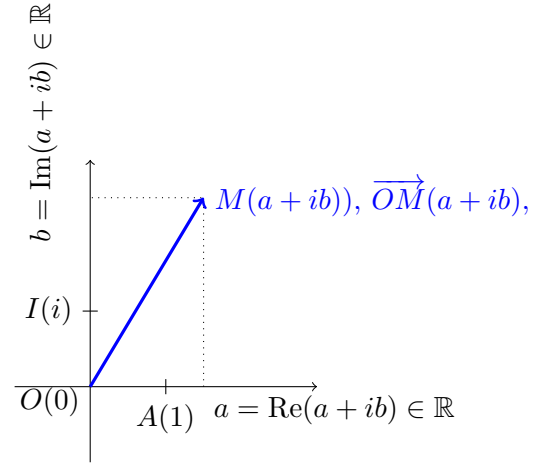


FIGURE I.14 – Repérage d'un point par ses coordonnées cartésiennes.

2. Soit $z = a + ib$ un complexe et $\lambda \in \mathbb{R}$. On définit le complexe $\lambda z = (\lambda a) + i(\lambda b)$. Ainsi $\operatorname{Re}(\lambda z) = \lambda \operatorname{Re}(z)$ et $\operatorname{Im}(\lambda z) = \lambda \operatorname{Im}(z)$.

Remarque 5.2.4.

Un complexe de partie imaginaire nulle est un réel. Mais alors pour les réels, nous disposons maintenant de deux additions : celle entre deux réels, que vous connaissez depuis toujours ; et celle entre complexes, que nous venons d'introduire. Mais, si a et b sont deux réels, nous pouvons les voir comme des complexes : $a = a + i \times 0$, et $b = b + i \times 0$. Si nous les additionnons comme des complexes, il vient : $a + b = a + i \times 0 + b + i \times 0 = (a + b) + i \times (0 + 0) = a + b$, cette dernière somme étant celle entre a et b vus comme des réels. Pour des réels, il n'y a donc aucune différence entre ces deux additions : on dit que l'addition des complexes *prolonge* celle des réels.

Nous pouvons alors aller plus loin dans les identifications point / complexe et vecteur / complexe :

Théorème 5.2.5 (Règles de calcul).

On a les propriétés suivantes :

- (i) Soient $\vec{u}$ et $\vec{u}'$ deux vecteurs d'affixes respectifs z et z' , et soit $\lambda \in \mathbb{R}$. Alors le vecteur

$\vec{u} + \lambda \vec{u}'$ a pour affixe $z + \lambda z'$. En particulier, pour tout couple de vecteurs, l'affixe de la somme de ces vecteurs est la somme des affixes et pour tout scalaire λ et tout vecteur $\vec{u}$ d'affixe z , l'affixe de $\lambda \vec{u}$ est λz .

- (ii) Soient A et B deux points d'affixes respectifs a et b . Alors le vecteur $\overrightarrow{AB}$ a pour affixe $b - a$.

Démonstration. (i) Notons a et b respectivement les parties réelle et imaginaire de z , et a' et b' celles de z' . Alors $\vec{u}$ (resp. $\vec{u}'$) a pour coordonnées (a, b) (resp. (a', b')). $\vec{u} + \lambda \vec{u}'$ a alors pour coordonnées $(a + \lambda a', b + \lambda b')$, donc pour affixe $(a + \lambda a') + i(b + \lambda b')$. Or on a

$$\begin{aligned} z + \lambda z' &= (a + ib) + \lambda(a' + ib') \\ &= (a + \lambda a') + i(b + \lambda b') \end{aligned}$$

Donc $\vec{u} + \lambda \vec{u}'$ a bien pour affixe $z + \lambda z'$.

Il suffit alors d'étudier les cas particuliers où $\lambda = 1$, où $\vec{u} = \vec{0}$ et où $\vec{u} = \vec{0}$ et $\lambda = -1$ pour conclure.

- (ii) Il suffit d'utiliser la relation fondamentale $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$ et le point précédent pour conclure. $\square$

Remarque 5.2.6.

Soit $b \in \mathbb{C}$. L'application

$$\begin{aligned} \mathbb{C} &\rightarrow \mathbb{C} \\ z &\mapsto z + b \end{aligned}$$

s'interprète géométriquement comme la translation de vecteur d'affixe b .

Mais cela est encore peu. Pour aller plus loin, nous voulons pouvoir multiplier des complexes entre eux.

5.3 Écriture trigonométrique d'un complexe

L'écriture précédente des complexes est appelée *écriture algébrique*. Nous pouvons remarquer qu'elle est très liée aux coordonnées cartésiennes. Et si nous utilisions les coordonnées polaires ?

Définition 5.3.1.

Soit un nombre complexe, que l'on écrit sous forme algébrique $z = a + ib$ (i.e. $a = \operatorname{Re}(z)$ et $b = \operatorname{Im}(z)$).

On appelle *module* de z le réel $\sqrt{a^2 + b^2}$. On le note $|z|$.

Notation 5.3.2.

On note $\mathbb{U}$ le cercle unité complexe :

$$\mathbb{U} = \{ z \in \mathbb{C} \mid |z| = 1 \},$$

Remarque 5.3.3. 1. Si $x \in \mathbb{R}$, on peut le voir comme un complexe. On se retrouve alors avec deux objets notés de la même manière, $|x|$: son module et sa valeur absolue. Mais $x = x + i \cdot 0$, donc son module est $\sqrt{x^2 + 0} = \sqrt{x^2}$: il est donc bien égal à sa valeur absolue. Là encore, le module prolonge sur $\mathbb{C}$ la valeur absolue réelle.

2. Si M (ou le vecteur u) est l'image de z , alors $|z|$ n'est autre que la distance OM (ou la norme $\|u\|$).
3. En particulier, soit a et z deux complexes et $R \geq 0$. Notons M et A les points du plans d'affixes respectives z et a . Alors $|z - a|$ est la distance AM . Et M appartient au cercle (resp. disque ouvert, resp. disque fermé) de centre A et de rayon R si et seulement si $|z - a| = R$ (resp. $|z - a| < R$, resp. $|z - a| \leq R$).
4. L'ensemble des affixes des points du cercle trigonométrique est donc $\mathbb{U}$. Nous identifierons donc ces deux objets.

Proposition 5.3.4.

Soit $z \in \mathbb{C}$

1. $|\operatorname{Re}(z)| \leq |z|$ et $|\operatorname{Im} z| \leq |z|$;
2. $|z| = 0$ ssi $z = 0$;
3. Si $\lambda \in \mathbb{R}$, alors $|\lambda z| = |\lambda| |z|$.

Démonstration.

Écrivons sous forme algébrique $z = a + ib$.

1. On a l'encadrement fondamental

$$0 \leq a^2 \leq a^2 + b^2,$$

donc par croissance de la racine carrée $0 \leq \sqrt{a^2} \leq \sqrt{a^2 + b^2}$, donc $0 \leq |a| \leq \sqrt{a^2 + b^2}$, ce qui est exactement le premier encadrement demandé.

On procède de même pour b .

2. Si $z = 0 = 0 + i0$, on a immédiatement $|z| = 0$.
Si $|z| = 0$, on a par l'encadrement précédent : $0 \leq a^2 \leq a^2 + b^2 = 0$, donc $a^2 = 0$, donc $a = 0$. On procède de même pour b , donc $z = 0$.
3. On a $\lambda z = (\lambda a) + i(\lambda b)$, or λa et λb sont des réels, donc

$$|\lambda z|^2 = (\lambda a)^2 + (\lambda b)^2 = \lambda^2(a^2 + b^2) = \lambda^2|z|^2.$$

Comme $|\lambda z|$ et $|z|$ sont positifs, on obtient bien le résultat demandé.

□

Corollaire 5.3.5.

Si $z \in \mathbb{C} \setminus \{0\}$, alors $\left| \frac{z}{|z|} \right| = 1$, i.e

$$\frac{z}{|z|} \in \mathbb{U}.$$

Démonstration.

Immédiat avec le dernier point de la proposition précédente.

□

Théorème 5.3.6 (Inégalité triangulaire).

Soit $z, z' \in \mathbb{C}$. Alors

$$\left| |z| - |z'| \right| \leq |z \pm z'| \leq |z| + |z'|.$$

Démonstration.

Ce résultat sera démontré dans le chapitre sur les complexes.

Mais nous allons ici montrer qu'il est équivalent à l'inégalité triangulaire vue dans le plan avec trois points ou deux vecteurs.

Soit deux vecteurs $\vec{u}$ et $\vec{v}$ d'axes respectifs z et z' . Alors l'axe de $\vec{u} \pm \vec{v}$ est $z \pm z'$, et nous avons les égalités $\|\vec{u}\| = |z|$, $\|\vec{v}\| = |z'|$, $\|\vec{u} \pm \vec{v}\| = |z \pm z'|$, donc directement

$$\begin{aligned} \left| \|\vec{u}\| - \|\vec{v}\| \right| &\leq \|\vec{u} \pm \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\| \\ \Leftrightarrow \left| |z| - |z'| \right| &\leq |z \pm z'| \leq |z| + |z'|. \end{aligned}$$

□

Définition 5.3.7.

Soit $\theta \in \mathbb{R}$. On appelle *exponentielle complexe* de $i\theta$ le complexe $e^{i\theta} = \cos \theta + i \sin \theta$.



L'écriture $e^{i\theta}$ n'est qu'une **notation** : en aucun cas il ne s'agit du réel e élevé à la puissance $i\theta$, ce qui n'a aucun sens.

Remarque 5.3.8.

Pour tout $\theta \in \mathbb{R}$, $|e^{i\theta}| = 1$, donc une exponentielle complexe, tout comme les exponentielles réelles, ne s'annule jamais.

Remarque 5.3.9.

Grâce à la représentation paramétrique du cercle trigonométrique, nous pouvons écrire que $\mathbb{U} = \{e^{i\theta}, \theta \in \mathbb{R}\}$.

Définition 5.3.10.

Soit $z \neq 0$. Alors $z/|z| \in \mathbb{U}$, donc il existe $\theta \in \mathbb{R}$ vérifiant $z/|z| = e^{i\theta}$, c'est-à-dire $z = |z|e^{i\theta}$.

Le réel θ est alors appelé **un argument** de z . Il existe à 2π près. Il existe alors un unique $\theta \in]-\pi, \pi]$ vérifiant $z = |z|e^{i\theta}$. Ce réel est appelé *l'argument principal* de z , et noté $\arg z$.

L'écriture « $z = |z|e^{i\theta}$ » est appelée *écriture trigonométrique* de z .

Remarque 5.3.11. 1. Attention à la non unicité de l'argument.

2. Le complexe 0 n'a pas d'argument ;
3. Pour tout z non nul, $(|z|, \arg z)$ est un couple de coordonnées polaires du point d'axe z ;
4. Il est simple de passer de l'écriture trigonométrique à l'écriture algébrique, de même qu'il est simple de passer des coordonnées polaires aux coordonnées cartésiennes : $re^{i\theta} = (r \cos \theta) + i(r \sin \theta)$. La réciproque nécessite là aussi l'utilisation des fonctions circulaires inverses, qui seront bientôt vues.

Exercice 5.3.12.

Mettre sous forme trigonométrique les nombres complexes suivants.

$$-3; -2i; 2\sqrt{3} - 2i; \sqrt{6} + i\sqrt{2}$$

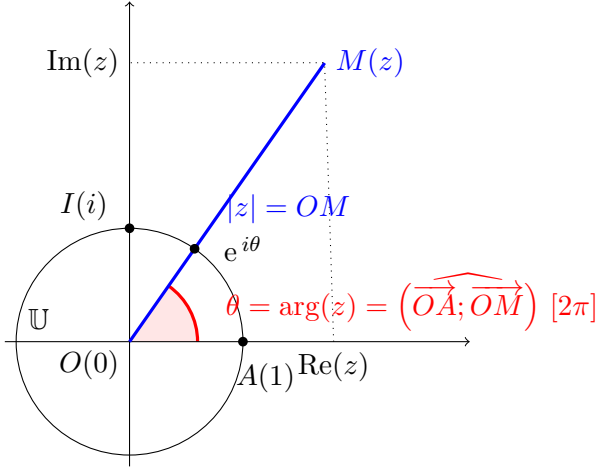


FIGURE I.15 – Interprétation géométrique du module et de l'argument de $z \in \mathbb{C}^*$.

5.4 Multiplication de deux complexes

Nous pouvons maintenant définir une multiplication sur $\mathbb{C}$:

Définition 5.4.1.

Soit $z, z' \in \mathbb{C}$. On définit leur produit $z \times z'$, ou plus simplement zz' , de la manière suivante :

Si z ou z' est nul, alors $zz' = 0$;

Sinon, on écrit z et z' sous forme trigonométrique, $z = re^{i\theta}$ et $z' = r'e^{i\theta'}$, et on pose $zz' = rr'e^{i(\theta+\theta')}$.

Remarque 5.4.2.

Multiplier un complexe z par $z' = re^{i\theta}$, c'est donc multiplier z par la constante réelle positive r (on appelle cette transformation une *homothétie* de rapport r), et ensuite appliquer la rotation d'angle θ au vecteur obtenu. On remarque que l'on peut aussi appliquer d'abord la rotation, puis l'homothétie : l'ordre n'importe pas, ces deux transformations *commutent* (voir figure I.16).

Le résultat suivant nous permet d'exprimer la multiplication entre deux complexes, cette fois-ci sous forme algébrique, et non pas sous forme trigonométrique :

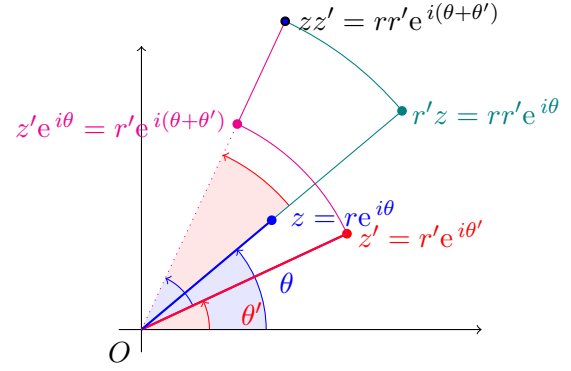


FIGURE I.16 – Produit zz' .

Proposition 5.4.3.

Pour tout $a, b, a', b' \in \mathbb{R}$,

$$(a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b).$$

Ou encore, si $z, z' \in \mathbb{C}$:

$$\begin{cases} \operatorname{Re}(zz') &= \operatorname{Re}(z) \operatorname{Re}(z') - \operatorname{Im}(z) \operatorname{Im}(z') \\ \operatorname{Im}(zz') &= \operatorname{Re}(z) \operatorname{Im}(z') + \operatorname{Im}(z) \operatorname{Re}(z') \end{cases}.$$

Démonstration.

Les deux formulations de l'énoncé sont équivalentes : démontrons la seconde.

Soit $z, z' \in \mathbb{C}$. Notons-les $z = re^{i\theta}$ et $z' = r'e^{i\theta'}$. Ainsi $zz' = rr'e^{i(\theta+\theta')}$. Nous avons donc :

$$\begin{aligned} \operatorname{Re}(zz') &= \operatorname{Re} [rr'(\cos(\theta + \theta') + i \sin(\theta + \theta'))] \\ &= rr' \cos(\theta + \theta') \\ &= rr' [\cos(\theta) \cos(\theta') - \sin(\theta) \sin(\theta')] \\ &= r \cos(\theta) r' \cos(\theta') - r \sin(\theta) r' \sin(\theta') \\ &= \operatorname{Re}(z) \operatorname{Re}(z') - \operatorname{Im}(z) \operatorname{Im}(z') \end{aligned}$$

De même :

$$\begin{aligned} \operatorname{Im}(zz') &= rr' \sin(\theta + \theta') \\ &= rr' [\cos(\theta) \sin(\theta') + \sin(\theta) \cos(\theta')] \\ &= r \cos(\theta) r' \sin(\theta') + r \sin(\theta) r' \cos(\theta') \\ &= \operatorname{Re}(z) \operatorname{Im}(z') + \operatorname{Im}(z) \operatorname{Re}(z') \end{aligned}$$

□

Remarque 5.4.4.

Nous voyons qu'additionner des complexes sous forme algébrique est très simple. Les multiplier sous forme trigonométrique l'est aussi. Multiplier

des complexes sous forme algébrique est déjà moins agréable. Quant à les additionner sous forme trigonométrique, nous verrons plus tard que cela n'est réalisable que si les deux complexes sont de même module, et même dans ce cas l'opération n'est pas immédiate.

Il convient donc de choisir l'écriture des complexes que vous utiliserez en fonction des opérations que vous voudrez effectuer.

Remarque 5.4.5.

Là encore, si $x, y \in \mathbb{R}$, nous pouvons les multiplier comme des complexes : $(x + i.0)(y + i.0) = (xy - 0) + i(0 + 0) = xy$. Nous obtenons le produit de x et y vus comme des réels : le produit sur $\mathbb{C}$ est donc un prolongement du produit sur $\mathbb{R}$.

Remarque 5.4.6.

L'identité « $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$ » est inoubliable ! Et à partir de cette identité, la démonstration précédente permet de retrouver les formules de trigonométrie de la proposition 4.4.1. Ce sera pour vous la technique à favoriser pour retrouver ces formules si besoin (mais insistons tout de suite : vous devriez normalement connaître ces formules par coeur).

Proposition 5.4.7 (règles de calcul).

Soit $a, b, c \in \mathbb{C}$, alors

1. $ab = ba$ (commutativité de la multiplication) ;
2. $(ab)c = a(bc)$ (associativité de la multiplication) ;
3. $a(b + c) = ab + ac$ (distributivité de $\times$ sur $+$) ;
4. $0 + a = a$ (0 est neutre pour $+$) ;
5. $a + (-1)a = 0$, i.e. $(-1)a = -a$;
6. $0a = 0$ (0 est absorbant pour $\times$) ;
7. $1a = a$ (1 est neutre pour $\times$) ;
8. $ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$.

Démonstration.

Il suffit d'écrire cela avec la définition 5.4.1, ou bien à partir des formules obtenues à la proposition 5.4.3. $\square$

Remarque 5.4.8.

Toutes ces propriétés des opérations $+$ et $\times$ sur $\mathbb{C}$,

font que $\mathbb{C}$ est appelé un *corps* : nous en reparlerons dans le chapitre sur les groupes, anneaux et corps.

Théorème 5.4.9.

On a $i^2 = -1$.



Remarque 5.4.10 (

Ce dernier résultat indique que la règle des signes n'est pas vraie sur $\mathbb{C}$. On ne peut donc prolonger la relation d'ordre $\leq$ de $\mathbb{R}$ à $\mathbb{C}$.

En résumé, on ne peut pas comparer deux complexes (non réels). Lorsque l'on travaille dans un cadre complexe, on ne peut donc utiliser aucune notion construite sur $\leq$ (ex : monotonie).

Comparer deux nombres complexes est une grave et lourde erreur !

5.5 Conjugué et module d'un nombre complexe

Définition 5.5.1.

On appelle *conjugué d'un complexe* z le complexe $\bar{z} = \text{Re}(z) - i \text{Im}(z)$.

Proposition 5.5.2 (Interprétation géométrique).

Soit $M(z)$ un point du plan. Alors $|z| = OM$ et $\bar{z}$ est le symétrique de M par rapport à l'axe $(O \vec{i})$ (voir figure I.17).

Démonstration.

Immédiat $\square$

Proposition 5.5.3.

Soit z un complexe non nul, écrit $z = re^{i\theta}$ sous forme trigonométrique. Alors $\bar{z} = re^{-i\theta}$.

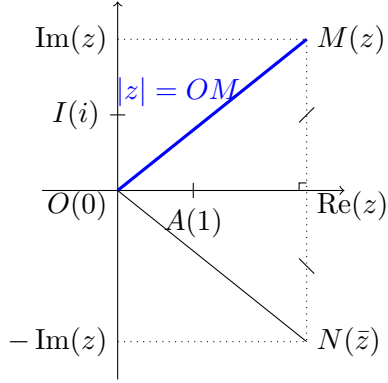


FIGURE I.17 – Interprétation géométrique du conjugué de $z \in \mathbb{C}$.

Proposition 5.5.4 (Règles de calcul).

Soit $(z, z') \in \mathbb{C}^2$, on a les identités suivantes.

$$\begin{aligned} \operatorname{Re}(z) &= \frac{z + \bar{z}}{2} & \operatorname{Im}(z) &= \frac{z - \bar{z}}{2i} \\ \overline{z + z'} &= \bar{z} + \bar{z}' & \overline{z \times z'} &= \bar{z} \times \bar{z}' \\ \overline{\bar{z}} &= z & z\bar{z} &= |z|^2 \\ |\bar{z}| &= |z| & |zz'| &= |z| \times |z'| \end{aligned}$$

Démonstration.

Ces identités sont élémentaires et se vérifient directement en posant $z = x + iy$, avec $(x, y) \in \mathbb{R}^2$. Celles qui ne font pas intervenir de somme sont même encore plus simple à démontrer sous forme trigonométrique.

Pour la dernière, remarquons aussi que, facilement, $|zz'|^2 = zz' \overline{zz'} = zz' \bar{z} \bar{z}' = z \bar{z} z' \bar{z}' = |z|^2 |z'|^2$. $\square$

Corollaire 5.5.5.

Soit $z \in \mathbb{C}$, on a

$$\begin{aligned} z \in \mathbb{R} &\Leftrightarrow \bar{z} = z, \\ z \in i\mathbb{R} &\Leftrightarrow \bar{z} = -z. \end{aligned}$$

5.6 Inverse d'un nombre complexe non nul

Proposition 5.6.1.

Soit $z \in \mathbb{C}$ tel que $z \neq 0$. Il existe un unique complexe z' tel que $zz' = 1$: on dit que z est *inversible* pour la multiplication, et que z' est son *inverse*. On notera ce dernier $\frac{1}{z}$ ou encore z^{-1} .

De plus : $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$.

Remarque 5.6.2.

Attention : 0 n'est pas inversible, et comme avec les réels, il est interdit d'écrire $\frac{1}{0}$. De manière générale, avant d'écrire une fraction (de complexes ou d'autre chose), on s'assurera que le dénominateur n'est pas nul.

Démonstration.

Pour l'existence, il suffit d'utiliser l'égalité $z\bar{z} = |z|^2$ vue précédemment. Si $z \neq 0$, alors $|z|^2$ est un réel non nul donc $z \times \frac{\bar{z}}{|z|^2} = 1$.

Pour l'unicité, si z'' est un autre inverse, alors $z'z'' = (z'z)z'' = 1.z'' = z''$ mais aussi $z'z'' = z'(zz'') = z'.1 = z'$, par associativité. $\square$

Nous pouvons compléter les règles de calcul précédentes :

Proposition 5.6.3 (Règles de calcul).

Soit $(z, z') \in \mathbb{C}^2$, tel que $z' \neq 0$. On a les identités suivantes :

$$\left| \frac{z}{z'} \right| = \frac{|z|}{|z'|} \quad \text{et} \quad \overline{\frac{z}{z'}} = \frac{\bar{z}}{\bar{z'}}.$$

Remarque 5.6.4.

L'inverse d'un complexe est donc

$$\frac{1}{a + ib} = \frac{a - ib}{a^2 + b^2}$$

Exercice 5.6.5.

Écrire $\frac{1 + 2i}{3 - 4i}$ sous forme algébrique.

5.7 Technique de l'angle moitié

La méthode suivante est indispensable : elle permet d'additionner deux complexes de même module, le tout sous forme trigonométrique.

Théorème 5.7.1 (technique de l'angle moitié).

Pour tout $(x, y) \in \mathbb{R}^2$, on a

$$\begin{aligned} e^{ix} + e^{iy} &= e^{i\frac{(x+y)}{2}} \left(e^{i\frac{(x-y)}{2}} + e^{-i\frac{(x-y)}{2}} \right) \\ &= 2e^{i\frac{(x+y)}{2}} \cos\left(\frac{x-y}{2}\right) \end{aligned}$$

Cette technique permet en particulier de montrer

Corollaire 5.7.2.

Soit $t \in \mathbb{R}$, alors

$$\begin{aligned} 1 + e^{it} &= 2e^{i\frac{t}{2}} \cos\left(\frac{t}{2}\right) \\ 1 - e^{it} &= -2e^{i\frac{t}{2}} i \sin\left(\frac{t}{2}\right) \end{aligned}$$

Démonstration.

Il suffit de remarquer que $1 = e^{i0}$ et d'appliquer la technique. $\square$

Exercice 5.7.3.

Mettre sous forme trigonométrique le nombre complexe $e^{3i\pi/5} + e^{4i\pi/9}$.

Chapitre II

Fonctions usuelles

Sommaire

1	Rappels d'analyse.	30
1.1	Régularité de fonctions.	30
1.2	Parité, imparité, périodicité.	31
1.3	Monotonie.	32
1.4	Lecture de tableaux de variations.	33
2	Effet d'une transformation sur le graphe.	34
3	Composée de fonctions, réciproque.	36
3.1	Rappels de dérivation.	36
3.2	Composée de deux fonctions.	36
3.3	Propriétés d'une composée.	37
3.4	Cas des bijections.	37
4	Fonction valeur absolue	39
5	Fonctions puissances entières, polynomiales et rationnelles	40
5.1	Fonctions puissances entières	40
5.2	Fonctions polynomiales et rationnelles	41
6	Fonctions exponentielles, logarithmes et puissances quelconques	42
6.1	Exponentielle et logarithme	42
6.2	Exponentielle de base quelconque	43
6.3	Racines énièmes.	44
6.4	Croissances comparées	45
7	Fonctions circulaires réciproques	45
7.1	Arccos et Arcsin	45
7.2	Arctangente	47
7.3	Coordonnées polaires	48
8	Fonctions hyperboliques	48
8.1	ch, sh et th	48
8.2	Fonctions hyperboliques inverses	50

Dans tout ce chapitre, A désigne une partie de $\mathbb{R}$ et f une fonction de A dans $\mathbb{R}$.

1 Rappels d'analyse.

On rappelle dans ce chapitre les notions fondamentales d'analyse réelle vues dans le secondaire.

1.1 Régularité de fonctions.

On rappelle succinctement ici les notions de continuité et de dérivabilité. Ces notions seront définies et travaillées en profondeur ultérieurement.

Définition 1.1.1 (Continuité).

Soit $f : A \rightarrow \mathbb{R}$, soit $a \in A$. La fonction f est continue en a si $f(x) \xrightarrow{x \rightarrow a} f(a)$.

La fonction f est continue sur A si f est continue en tout point de A .

Définition 1.1.2 (Dérivabilité).

Soit $f : A \rightarrow \mathbb{R}$, soit $a \in A$. La fonction f est dérivable en a si la quantité $\frac{f(x) - f(a)}{x - a}$ admet une limite finie en a . Cette limite est notée $f'(a)$, i.e. si f est dérivable en a ,

$$\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a} f'(a).$$

La fonction f est dérivable sur A si f est dérivable en tout point de A . La fonction f' est alors appelée *fonction dérivée de f* .

Si f est dérivable et si f' est dérivable, alors f est dite *deux fois dérivable*, et l'on note $f'' = (f')'$, que l'on appelle *fonction dérivée seconde de f* .

Remarque 1.1.3.

La quantité $\frac{f(x) - f(a)}{x - a}$ est la pente de la corde à la courbe de f reliant les points d'abscisses a et x .

Remarque 1.1.4.

On peut aussi dériver des expressions, avec le sym-

bole $\frac{d}{d[\text{variable}]}$. On pourra par exemple écrire

$$\frac{d}{dx}(x^{42}) = 42x^{41},$$

ou

$$\frac{d}{dt}(3t^2 + 1515) = 6t.$$



On s'interdira absolument d'écrire un $'$ sur une expression pour signifier sa dérivation. Ainsi, $(\sin x)'$ ou $(x^2 + x - 1)'$ sont des écritures incorrectes, et on écrira $\sin'(x)$ ou $\frac{d}{dx}(x^2 + x - 1)$.

Remarque 1.1.5.

Lorsque l'on dérive une expression dépendant de plusieurs variables x, y, z, t, α etc, on pourra utiliser les symboles $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}, \frac{\partial}{\partial t}, \frac{\partial}{\partial \alpha}$ etc, pour signifier que l'on dérive l'expression considérée par rapport à la variable notée, les autres variables étant supposées fixées (ce sont donc des constantes). On parle alors de *dérivation partielle* par rapport à une variable.

Bien entendu, il conviendra de se poser la question de la dérivabilité de ladite expression, par rapport à la variable considérée. Ces techniques seront détaillées en fin d'année.

Exemple 1.1.6.

Les deux dérivées partielles de l'expression $x^2y - e^{y-x}$ sont

$$\begin{aligned} \frac{\partial}{\partial x}(x^2y - e^{y-x}) &= 2xy + e^{y-x} \\ \frac{\partial}{\partial y}(x^2y - e^{y-x}) &= x^2 - e^{y-x} \end{aligned}$$

Exercice 1.1.7.

Déterminer les dérivées partielles suivantes. On se reportera au besoin à la partie 3 pour les rappels sur les formules de dérivation.

1. $\frac{\partial}{\partial x}(xe^{-(x^2+y^2)})$
2. $\frac{\partial}{\partial t}(3xt^2 - xyt + 2x \sin(y))$
3. $\frac{\partial}{\partial z}(xe^y + ye^z + ze^x)$
4. $\frac{\partial}{\partial x}(\alpha \sin(y + z))$

Proposition 1.1.8.

Une fonction dérivable en un point est continue en ce point. Une fonction dérivable est donc continue.

Remarque 1.1.9.

Comme le montrent les exemples des fonctions « valeur absolue » et « racine carrée », la réciproque est fautive : il existe des fonctions continues, et non dérivables.

Proposition 1.1.10.

Soit $f, g : A \rightarrow \mathbb{R}$ dérivables, soit $\lambda, \mu \in \mathbb{R}$.

1. La fonction $\lambda f + \mu g$ est dérivable et

$$(\lambda f + \mu g)' = \lambda f' + \mu g'.$$

2. La fonction fg est dérivable et

$$(fg)' = fg' + f'g.$$

Exemple 1.1.11.

$$\frac{d}{dx}(\cos(x) \sin(x)) = \cos^2(x) - \sin^2(x).$$

1.2 Parité, imparité, périodicité.

Définition 1.2.1.

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$.

1. On dit que f est *paire* si, pour tout $x \in A$,

$$-x \in A \quad \text{et} \quad f(-x) = f(x).$$

2. On dit que f est *impaire* si, pour tout $x \in A$,

$$-x \in A \quad \text{et} \quad f(-x) = -f(x).$$

Remarque 1.2.2 (Réduction du domaine d'étude).

Il suffit d'étudier une fonction paire ou impaire sur $\mathbb{R}_+ \cap A$ pour obtenir toutes les informations nécessaires sur cette fonction.



Une fonction n'est pas toujours paire ou impaire. Le contraire de « paire » n'est pas « impaire ».

Exemple 1.2.3.

Sur $\mathbb{R}$, $x \mapsto x^2$ est paire, $x \mapsto x^3$ est impaire et $x \mapsto x^2 + x$ n'est ni paire ni impaire.

Exercice 1.2.4.

Déterminer toutes les fonctions à la fois paires et impaires.

Remarque 1.2.5.

Une fonction impaire définie en 0 est forcément nulle en 0.

Proposition 1.2.6.

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$ dérivable.

1. Si f est paire, alors f' est impaire.
2. Si f est impaire, alors f' est paire.

Démonstration.

Dans le cas où f est impaire, on a, pour tout $x \in \mathbb{R}$, $f(x) = -f(-x)$.

La fonction f et la fonction $x \mapsto -f(-x)$ sont donc égales, et dérivables. Leurs dérivées sont donc égales. On dérive donc de part et d'autre : pour tout $x \in \mathbb{R}$, $f'(x) = -(-f'(-x)) = f'(-x)$.

On procède de même dans le cas où f est paire. $\square$

Définition 1.2.7.

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$, soit $T > 0$. On dit que f est T -périodique si, pour tout $x \in A$,

$$x + T \in A \quad \text{et} \quad f(x + T) = f(x).$$

Dans ce cas T est appelé **UNE** période de f .

La fonction f est périodique s'il existe $T > 0$ tel que f est T -périodique.

Remarque 1.2.8 (Réduction du domaine d'étude).

Si f est T -périodique et si $a \in A$, il suffit d'étudier f sur $A \cap [a, a + T]$ pour obtenir toutes les informations sur f .



Il n'y a jamais unicité de la période !

Exemple 1.2.9.

Les fonctions constantes, $\cos$, $\sin$, $\tan$, $x \mapsto x - \lfloor x \rfloor$, $\mathbb{R} \rightarrow \mathbb{R}$ sont périodiques.

La fonction $\mathbf{1}_{\mathbb{Q}}$, qui vaut 1 sur $\mathbb{Q}$ et 0 sur $\mathbb{R} \setminus \mathbb{Q}$, est périodique. Tout rationnel strictement positif est une période pour cette fonction.

Toute fonction constante admet tout réel strictement positif comme période.

Proposition 1.2.10.

Soit $A \subset \mathbb{R}$, $T > 0$ et soit $f : A \rightarrow \mathbb{R}$ dérivable et T -périodique.

Alors, f' est T -périodique.

Démonstration.

Il suffit d'écrire que, pour tout $x \in A$, $f(x) = f(x + T)$, puis de dériver de part et d'autre. $\square$

Exercice 1.2.11.

Déterminer l'allure de la fonction f paire, 4-périodique et telle que pour tout $x \in [0, 2]$, $f(x) = x$ (cela s'écrit $f|_{[0,2]} = \text{Id}_{[0,2]}$).

1.3 Monotonie.

Définition 1.3.1 (Monotonie au sens large).

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$.

1. On dit que f est *croissante* si, pour tout $x, y \in A$, :

$$x \geq y \Rightarrow f(x) \geq f(y).$$

2. On dit que f est *décroissante* si, pour tout $x, y \in A$, :

$$x \geq y \Rightarrow f(x) \leq f(y).$$

3. On dit que f est *monotone* si elle est croissante ou décroissante.

Définition 1.3.2 (Monotonie stricte).

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$.

1. On dit que f est *strictement croissante* si, pour tout $x, y \in A$, :

$$x < y \Rightarrow f(x) < f(y).$$

2. On dit que f est *strictement décroissante* si, pour tout $x, y \in A$, :

$$x < y \Rightarrow f(x) > f(y).$$

3. On dit que f est *strictement monotone* si elle est strictement croissante ou strictement décroissante.



Une fonction n'est pas toujours croissante ou décroissante. Le contraire de croissant n'est pas décroissant.

Exemple 1.3.3.

La fonction carré n'est ni croissante, ni décroissante.

Exercice 1.3.4.

Déterminer toutes les fonctions qui sont à la fois croissantes et décroissantes.

Remarque 1.3.5.

Une fonction monotone strictement l'est bien entendu au sens large.

À chaque fois que l'on vous demande d'étudier la monotonie d'une fonction, on attend le résultat le plus précis possible. Si la fonction est croissante strictement mais que vous n'établissez que sa croissance, votre réponse ne pourra être considérée comme complète.

Proposition 1.3.6 (Injectivité d'une fonction strictement croissante).

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$ strictement monotone. Alors, pour tout $x, x' \in A$, si $x \neq x'$, alors $f(x) \neq f(x')$. Ceci est équivalent à dire que, pour tout $x, x' \in A$, si $f(x) = f(x')$, alors $x = x'$.

Notamment, si $y \in \mathbb{R}$, il existe au plus un $x \in A$ vérifiant $y = f(x)$.

Démonstration.

On traite le cas strictement croissant (le cas strictement décroissant se traite de la même manière, ou bien en étudiant $-f$).

Soit $x, x' \in A$ tels que $x \neq x'$. On a soit $x < x'$, dans ce cas $f(x) < f(x')$ par croissance stricte de f , ou $x > x'$, dans ce cas $f(x) > f(x')$. Dans les deux cas, $f(x) \neq f(x')$.

On peut très bien en montrer la contraposée. Soit $x, x' \in A$ tels que $f(x) = f(x')$. On ne peut pas avoir $x < x'$ car

sinon on aurait $f(x) < f(x')$, par croissance stricte de f , ni $x > x'$ car sinon $f(x) > f(x')$. Ainsi $x = x'$. $\square$

Exemple 1.3.7.

La fonction cosinus est strictement croissante sur $[\pi, 3\pi/2]$.

1.4 Lecture de tableaux de variations.

Définition 1.4.1.

Un intervalle est une partie « sans trou » de $\mathbb{R}$ (plus formellement on appelle cela une partie *connexe*), i.e. c'est une partie I qui vérifie : pour tout $x, y \in I$, pour tout $t \in \mathbb{R}$,

$$x \leq t \leq y \Rightarrow t \in I.$$

Le théorème suivant permet de relier le tableau de signes de la dérivée d'une fonction au tableau de variations de la fonction.

Théorème 1.4.2.

Soit I un intervalle de $\mathbb{R}$, soit $f : I \rightarrow \mathbb{R}$ dérivable.

1. f est croissante (resp. décroissante) si et seulement si $f' \geq 0$ (resp. $f' \leq 0$).
2. La fonction f est constante si et seulement si $\forall x \in I, f'(x) = 0$.

Remarque 1.4.3.

On déduit de ce théorème que deux primitives d'une même fonction diffèrent d'une constante.



Il est essentiel que I soit un intervalle pour que l'implication de la droite vers la gauche soit vraie (en revanche pour l'autre implication ce n'est pas nécessaire).

Exercice 1.4.4. 1. Trouver une application f non croissante dérivable sur son ensemble de définition, de dérivée positive.

2. Trouver une application g non constante dérivable sur son ensemble de définition, de dérivée nulle.

3. Trouver une application h dérivable non décroissante sur son ensemble de définition, de dérivée négative.

Remarque 1.4.5.

Nous avons aussi : si f' est strictement positive (resp. négative), alors f est strictement croissante (resp. décroissante).

Attention, la réciproque est fautive ! Par exemple, la fonction $x \mapsto x^3$ est strictement croissante sur $\mathbb{R}$, bien que sa dérivée s'annule en 0.

Le théorème suivant traduit les flèches continues tracées dans les tableaux de variations.

Théorème 1.4.6 (Théorème de la bijection).

Soit $a < b$ deux réels, soit $f : [a, b] \rightarrow \mathbb{R}$ continue.

1. Si f est strictement croissante, pour tout $y \in [f(a), f(b)]$, il existe un unique $x \in [a, b]$ vérifiant $y = f(x)$. On dit que f réalise une bijection de $[a, b]$ sur $[f(a), f(b)]$.
2. Si f est strictement décroissante, pour tout $y \in [f(b), f(a)]$, il existe un unique $x \in [a, b]$ vérifiant $y = f(x)$. On dit que f réalise une bijection de $[a, b]$ sur $[f(b), f(a)]$.

On a des résultats analogues avec un intervalle semi-ouvert ou ouvert (de la forme $]a, b]$, $[a, b[$ ou $]a, b[$), même si a ou b valent $\pm\infty$, mais ces résultats font alors intervenir des limites.

Démonstration.

L'existence d'un tel x provient directement du théorème des valeurs intermédiaires : f est continue sur l'intervalle $[a, b]$, y est entre $f(a)$ et $f(b)$, donc il existe $x \in [a, b]$ tel que $y = f(x)$.

L'unicité provient de la monotonie stricte, par la proposition 1.3.6. $\square$

Exercice 1.4.7.

Écrire le théorème 1.4.6 dans le cas où $a \in \mathbb{R}$ et $b = +\infty$.

Justifier, sans faire intervenir la notion de dérivée, que pour tout $y \geq 0$, il existe un unique $x \geq 0$ vérifiant $y = x^2$.

Exercice 1.4.8.

Chercher un contre-exemple au théorème 1.4.6 pour chaque hypothèse que l'on enlève.

Remarque 1.4.9.

L'étude du signe d'une expression se fera systématiquement en la factorisant. Ensuite, si le signe de l'un des facteurs n'est pas évident, il conviendra d'étudier ce facteur (par une étude de fonctions).

Exercice 1.4.10.

Déterminer l'ensemble de définition de $x \mapsto \frac{(x+1)^2}{e^x - 1}$ puis tracer son tableau de variations.

2 Effet d'une transformation sur le graphe.

Soit $A \subset \mathbb{R}$. On considère une application $f : A \rightarrow \mathbb{R}$, dont on veut étudier les propriétés. Notamment, on peut vouloir représenter le graphe de cette fonction : c'est

$$\left\{ (x, y) \in \mathbb{R}^2 \mid x \in A \text{ et } y = f(x) \right\},$$

que l'on représente, lorsque c'est possible, par une « courbe ».

Proposition 2.0.1.

Soit $a \in \mathbb{R}_+^*$, on considère des graphes tracés dans le repère orthonormé direct $(O, \vec{i}, \vec{j})$.

- Le graphe de la fonction $x \mapsto f(x) + a$ s'obtient en translatant le graphe de f du vecteur $a\vec{j}$ (voir la figure II.1).
- Le graphe de la fonction $x \mapsto f(x + a)$ s'obtient en translatant le graphe de f du vecteur $-a\vec{i}$ (voir la figure II.2).
- Le graphe de la fonction $x \mapsto f(ax)$ s'obtient en dilatant le graphe de f suivant le vecteur $\vec{i}$ et par le rapport $\frac{1}{a}$ (voir la figure II.3).
- Le graphe de la fonction $x \mapsto af(x)$ s'obtient en dilatant le graphe de f suivant le vecteur $\vec{j}$ et par le rapport a (voir la figure II.4).
- Le graphe de la fonction $x \mapsto f(-x)$ s'obtient en prenant le symétrique du graphe de f par rapport à l'axe $O\vec{j}$ (voir la figure II.5).
- Le graphe de la fonction $x \mapsto -f(x)$ s'obtient en prenant le symétrique du graphe

de f par rapport à l'axe $O\vec{i}$ (voir la figure II.6).

- Le graphe de la fonction $x \mapsto -f(-x)$ s'obtient en prenant le symétrique du graphe de f par rapport au point O (voir la figure II.7).

Démonstration.

On montre le premier cas, les autres sont similaires. Notons Γ le graphe de f , Γ' celui de $x \mapsto f(x) + a$. Soit $(x, y) \in \mathbb{R}^2$, alors $(x, y) \in \Gamma' \Leftrightarrow (x, y - a) \in \Gamma$, ce qui est bien le résultat demandé. $\square$

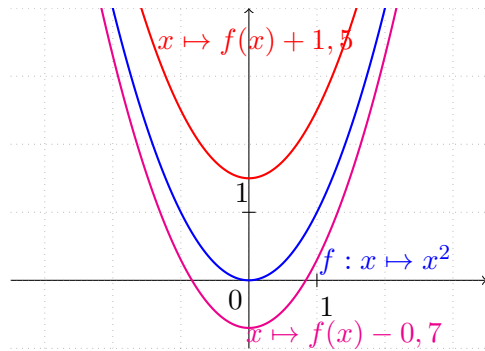


FIGURE II.1 – Translation verticale du graphe.

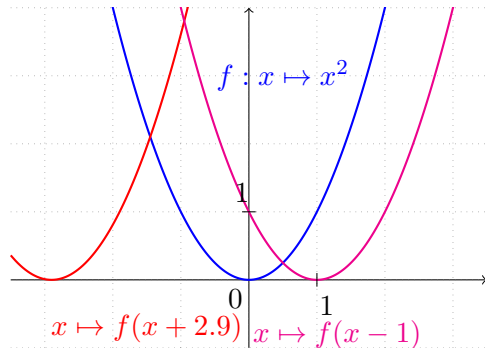


FIGURE II.2 – Translation horizontale du graphe.

Remarque 2.0.2.

Le graphe de la fonction $x \mapsto f(a - x)$ s'obtient donc

- soit en translatant le graphe de f du vecteur $a\vec{i}$ puis en prenant le symétrique par rapport à $O\vec{j}$;

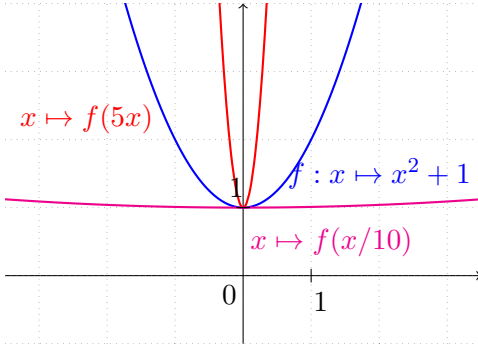


FIGURE II.3 – Dilatation horizontale du graphe.

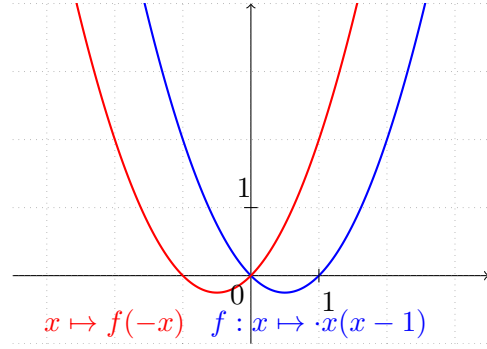


FIGURE II.5 – Symétrie du graphe par rapport à l'axe vertical.

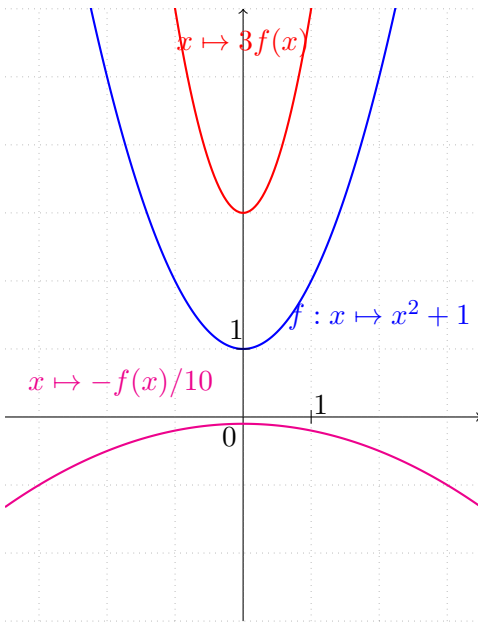


FIGURE II.4 – Dilatation verticale du graphe.

- soit en prenant le symétrique du graphe de f par rapport à $O\vec{j}$ puis en le translatant par le vecteur $-a\vec{i}$.

Proposition 2.0.3. 1. Le graphe d'une fonction paire présente une symétrie par rapport à l'axe des ordonnées.

2. Le graphe d'une fonction impaire présente une symétrie par rapport à l'origine.

3. Le graphe d'une fonction T -périodique présente un motif de longueur T se répétant

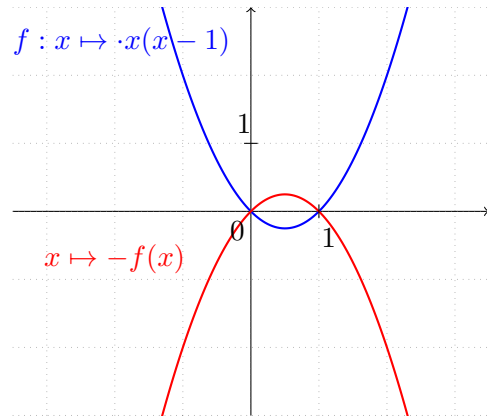


FIGURE II.6 – Symétrie du graphe par rapport à l'axe horizontal.

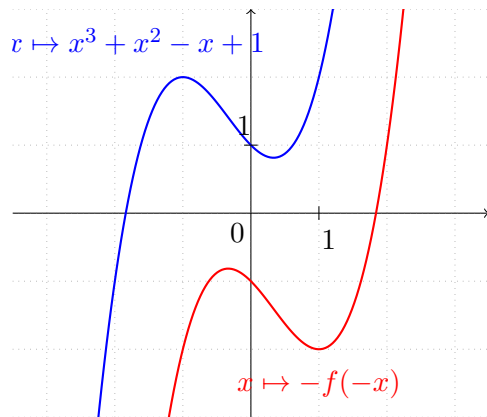


FIGURE II.7 – Symétrie du graphe par rapport à l'origine.

(plus formellement, il est invariant par la translation de vecteur $T\vec{v}$).

Exercice 2.0.4.

Quelle symétrie la courbe d'une fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ vérifiant, pour un $a \in \mathbb{R}$, $\forall x \in \mathbb{R} f(a-x) = f(x)$ présente-t-elle ?

3 Composée de fonctions, réciproque.

3.1 Rappels de dérivation.

On rappelle les formules de dérivation usuelles utilisées dans le secondaire.

Théorème 3.1.1.

Soit $A \subset \mathbb{R}$ et $u : A \rightarrow \mathbb{R}$ dérivable.

1. Soit n un entier strictement positif. La fonction $x \mapsto u^n(x)$ est dérivable sur A et, pour tout $x \in A$,

$$\frac{d}{dx}(u^n(x)) = nu'(x)u^{n-1}(x).$$

2. Soit n un entier strictement négatif. Si u ne s'annule pas, la fonction $x \mapsto u^n(x)$ est dérivable sur A et, pour tout $x \in A$,

$$\frac{d}{dx}(u^n(x)) = nu'(x)u^{n-1}(x).$$

3. Si u est strictement positive, la fonction $x \mapsto \sqrt{u(x)}$ est dérivable sur A et, pour tout $x \in A$,

$$\frac{d}{dx}(\sqrt{u(x)}) = \frac{u'(x)}{2\sqrt{u(x)}}.$$

4. La fonction $x \mapsto \exp(u(x))$ est dérivable sur A et, pour tout $x \in A$,

$$\frac{d}{dx}(\exp(u(x))) = u'(x) \exp(u(x)).$$

5. Si u est strictement positive, la fonction $x \mapsto \ln(u(x))$ est dérivable sur A et, pour tout $x \in A$,

$$\frac{d}{dx}(\ln(u(x))) = \frac{u'(x)}{u(x)}.$$

3.2 Composée de deux fonctions.

Définition 3.2.1.

Soit $A, B \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{R}$ et $g : B \rightarrow \mathbb{R}$.

Si, pour tout $x \in A$, $f(x) \in B$, alors on peut construire la fonction *composée* de f par g :

$$\begin{aligned} g \circ f : A &\rightarrow \mathbb{R} \\ x &\mapsto g(f(x)) \end{aligned}.$$

On pourra, pour s'aider, se rappeler du schéma de la figure II.8.

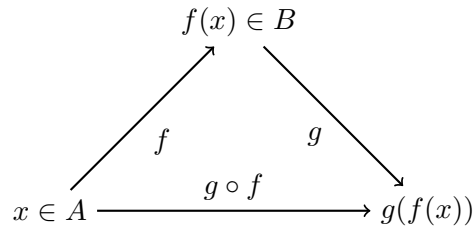


FIGURE II.8 – Diagramme de composition de fonctions.

Exemple 3.2.2.

On peut donc écrire, sous réserve de validité,

$$(\exp \circ u)' = u' \times \exp \circ u \quad \text{et} \quad (\ln \circ u)' = \frac{u'}{u}.$$

Remarque 3.2.3.

Pour déterminer le domaine de définition d'une composée $g \circ f$, il convient de déterminer dans l'ordre :

1. le domaine de définition de f , noté ici $\mathcal{D}_f$;
2. puis le domaine de définition de g , noté ici $\mathcal{D}_g$;
3. enfin, déterminer l'ensemble des $x \in \mathcal{D}_f$ pour lesquels $f(x) \in \mathcal{D}_g$.

En particulier, il est impossible de conclure sans avoir étudié l'ensemble d'arrivée de f !

Exercice 3.2.4.

Déterminer le domaine de définition de

$$x \mapsto \sqrt{x-2 - \frac{2}{x-3}}.$$

3.3 Propriétés d'une composée.

Théorème 3.3.1.

Soit $A, B \subset \mathbb{R}$, $f : A \rightarrow \mathbb{R}$ et $g : B \rightarrow \mathbb{R}$ telles que $g \circ f$ soit définie.

1. Si f et g sont continues, alors $g \circ f$ est continue sur A .
2. Si f et g sont dérivables, alors $g \circ f$ est dérivable sur A et

$$(g \circ f)' = f' \times g' \circ f.$$

Démonstration.

Cela sera démontré ultérieurement. $\square$

Exercice 3.3.2.

Dériver les expressions suivantes :

1. $\sin(3x^2 + 2)$;
2. $\sqrt{1 + \ln(\cos(t))}$.

Remarque 3.3.3.

Sous réserve de définition, on a donc de manière générale

$$\frac{d}{dx}(f(ax + b)) = af'(ax + b).$$

Proposition 3.3.4.

Soit $A, B \subset \mathbb{R}$, $f : A \rightarrow \mathbb{R}$ et $g : B \rightarrow \mathbb{R}$ telles que $g \circ f$ soit définie.

1. Si f est paire, $g \circ f$ est paire.
2. Si f est impaire et g est paire, $g \circ f$ est paire.
3. Si f et g sont impaires, $g \circ f$ est impaire.

Démonstration.

Soit $x \in A$. Si f est paire,

$$g \circ f(-x) = g(f(-x)) = g(f(x)) = g \circ f(x).$$

Si f est impaire et g paire,

$$g \circ f(-x) = g(f(-x)) = g(-f(x)) = g(f(x)) = g \circ f(x).$$

Si f et g sont impaires,

$$g \circ f(-x) = g(f(-x)) = g(-f(x)) = -g(f(x)) = -g \circ f(x).$$

$\square$

Proposition 3.3.5.

Soit $A, B \subset \mathbb{R}$, $f : A \rightarrow \mathbb{R}$ et $g : B \rightarrow \mathbb{R}$ tels que $g \circ f$ soit définie.

1. Si f et g sont de même monotonie, $g \circ f$ est croissante.
2. Si f et g sont de monotonies opposées, $g \circ f$ est décroissante.

On a les mêmes résultats dans les cas de monotonie stricte.

Démonstration.

On traite le cas où f est croissante et g décroissante. Les autres sont semblables.

Soit $x, y \in A$, supposons que $x \leq y$. Par croissance de f , on a $f(x) \leq f(y)$ puis, par décroissance de g , on a $g(f(x)) \geq g(f(y))$. Ainsi, $g \circ f$ est décroissante. $\square$

Exercice 3.3.6.

Déterminer sans calculs le sens de variations de la fonction

$$x \mapsto \ln(1 + e^{-2x}).$$

3.4 Cas des bijections.

Définition 3.4.1.

Soit $E \subset \mathbb{R}$. On définit la fonction *identité sur E* comme

$$\begin{aligned} \text{Id}_E : E &\rightarrow \mathbb{R} \\ x &\mapsto x \end{aligned}$$

On définit maintenant la réciproque d'une fonction dans le cadre restreint du théorème de la bijection. Nous étendrons cette notion ultérieurement.

Définition 3.4.2.

Soit $a < b$ deux réels, $f : [a, b] \rightarrow \mathbb{R}$ continue et strictement monotone. Soit x entre $f(a)$ et $f(b)$, il existe donc un unique $t \in [a, b]$ tel que $x = f(t)$. On note ce réel $t = f^{-1}(x)$.

La fonction f^{-1} est appelée *réciproque* de f .

On a des résultats analogues avec un intervalle semi-ouvert ou ouvert (de la forme $]a, b]$, $[a, b[$ ou $]a, b[$), même si a ou b valent $\pm\infty$, mais ces résultats font alors intervenir des limites.

Proposition 3.4.3.

Soit $a < b$ deux réels, $f : [a, b] \rightarrow \mathbb{R}$ continue et strictement croissante. On a alors

$$f^{-1} : [f(a), f(b)] \rightarrow [a, b]$$

et on a les propriétés suivantes :

1. $f \circ f^{-1} = \text{Id}_{[f(a), f(b)]}$;
2. $f^{-1} \circ f = \text{Id}_{[a, b]}$.

Dans le cas où f est strictement décroissante, on a les mêmes résultats en remplaçant $[f(a), f(b)]$ par $[f(b), f(a)]$.

On a des résultats analogues avec un intervalle semi-ouvert ou ouvert (de la forme $]a, b]$, $[a, b[$ ou $]a, b[$), même si a ou b valent $\pm\infty$, mais ces résultats font alors intervenir des limites.

Démonstration.

Le domaine de définition de f^{-1} et son image sont évidents, par la définition de f^{-1} .

1. Soit $x \in [f(a), f(b)]$. Posons $t = f^{-1}(x)$. Par définition, $f(t) = x$, donc $f(f^{-1}(x)) = x$, d'où le résultat.
2. Soit $t \in [a, b]$, posons $x = f(t)$. Par croissance stricte de f , il y a unicité du réel $u \in [a, b]$ vérifiant $x = f(u)$, donc par définition $t = f^{-1}(x)$. On a donc $t = f^{-1}(f(t))$, d'où le résultat.

□

Proposition 3.4.4.

Soit $a < b$ deux réels, $f : [a, b] \rightarrow \mathbb{R}$ continue et strictement monotone. Alors, le graphe de f^{-1} est le symétrique du graphe de f par rapport à la droite d'équation $y = x$ (aussi appelée *première bissectrice du plan*).

Démonstration.

Soit $x \in [a, b]$, soit y entre $f(a)$ et $f(b)$. On a alors $y = f(x)$ si et seulement si $x = f^{-1}(y)$. Ainsi, le point de coordonnées (x, y) appartient au graphe de f si et seulement si celui de coordonnées (y, x) appartient au graphe de f^{-1} . Or, l'application qui échange les coordonnées est la symétrie par rapport à la première bissectrice du plan, d'où le résultat. □

Le résultat suivant permet notamment d'obtenir le tableau de variations de la réciproque d'une fonction.

Théorème 3.4.5.

Soit I un intervalle de $\mathbb{R}$ et $f : I \rightarrow \mathbb{R}$ continue et strictement monotone.

1. La fonction f^{-1} est strictement monotone, de même monotonie que f .
2. Si f est impaire, alors f^{-1} est aussi impaire..
3. La fonction f^{-1} est continue.
4. Si f dérivable et si f' ne s'annule pas, alors f^{-1} est aussi dérivable et $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$.

Démonstration.

On ne démontre que les deux premiers points.

1. Dans le cas où f est strictement décroissante. Soit x, y des images par la fonction f , posons $a = f^{-1}(x)$ et $b = f^{-1}(y)$, de sorte que $a, b \in I$, $x = f(a)$ et $y = f(b)$.

Supposons que $x < y$. Si $a \leq b$, alors, par décroissance de f , $f(a) \geq f(b)$, i.e. $x \geq y$: c'est impossible. Ainsi, $f^{-1}(x) > f^{-1}(y)$, donc f^{-1} est strictement décroissante.

2. Soit x une image par la fonction f , on a par imparité de f

$$f(-f^{-1}(x)) = -f(f^{-1}(x)) = -x.$$

Ainsi, par définition, $f^{-1}(-x) = -f^{-1}(x)$, donc f^{-1} est impaire.

□

Remarque 3.4.6.

Une fois que l'on sait que f^{-1} est dérivable, la dernière formule peut se retrouver en dérivant $f \circ f^{-1} = \text{Id}$, ce qui donne :

$$(f^{-1})' \times f' \circ f^{-1} = 1.$$

Remarque 3.4.7.

Avec quelques considérations de limites, le théorème précédent permet de relier les tableaux de variations d'une fonction et de sa réciproque (voir figure II.9 dans le cas où f est strictement décroissante).

Remarque 3.4.8.

Plus précisément, si $f'(x) = 0$, alors f^{-1} ne sera pas dérivable en $y = f(x)$.

En effet, le graphe de f possède une tangente horizontale au point de coordonnées (x, y) , donc par symétrie celui de f^{-1} possède une tangente verticale au point de coordonnées (y, x) .

x	a	b
$f(x)$	c	d
x	d	c
$f^{-1}(x)$	b	a

FIGURE II.9 – Tableaux de variations d’une fonction et de sa réciproque.

Exemple 3.4.9.

On peut observer tous ces résultats sur les fonctions carré et racine carrée (voir figure II.10).

La fonction carré est strictement croissante sur $\mathbb{R}_+$ (mais pas sur $\mathbb{R}$), est continue, $0^2 = 0$ et $x^2 \xrightarrow{x \rightarrow +\infty} +\infty$. Ainsi, la fonction carré réalise une bijection de $\mathbb{R}_+$ sur $\mathbb{R}_+$. On appelle sa réciproque la fonction *racine carrée*, notée $\sqrt{\cdot}$: si $x \geq 0$, $\sqrt{x}$ est l’unique réel $t \geq 0$ vérifiant $t^2 = x$. La fonction racine carrée est donc strictement croissante et $\sqrt{x} \xrightarrow{x \rightarrow +\infty} +\infty$.

On a, pour tout $x \geq 0$, $\frac{d}{dx}(x^2) = 2x$, qui s’annule exactement en 0. La fonction racine carrée est donc dérivable sur $\mathbb{R}_+^*$, mais pas en 0, et pour tout $x > 0$,

$$\frac{d}{dx}(\sqrt{x}) = \frac{1}{2\sqrt{x}}.$$

4 Fonction valeur absolue

Définition 4.0.1.

Soit $x \in \mathbb{R}$. On appelle *valeur absolue* de x le réel $|x| = \sqrt{x^2}$. Il vaut x si $x \geq 0$ et $-x$ sinon (voir la figure II.11).

Proposition 4.0.2.

C’est une fonction paire, continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R}_-^*$ et $\mathbb{R}_+^*$, mais pas en 0. Si $x > 0$, on

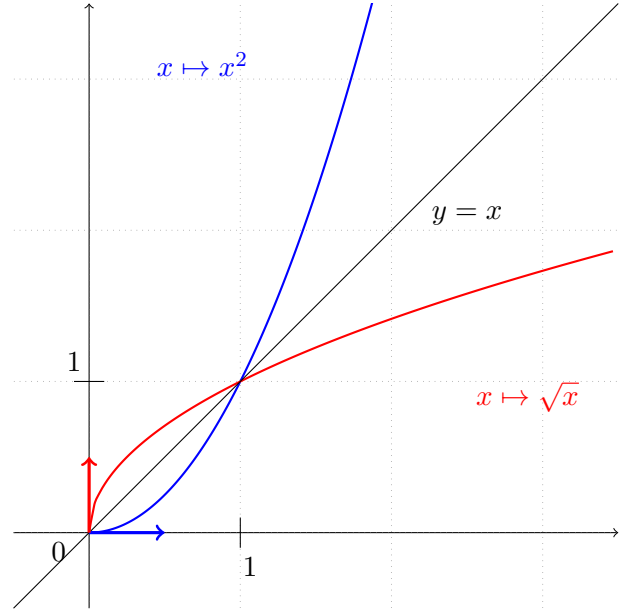


FIGURE II.10 – Fonctions carré et racine carrée.

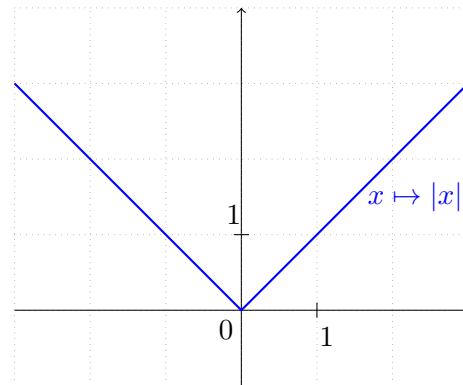


FIGURE II.11 – Fonction valeur absolue.

$$\text{a } \frac{d}{dx}(|x|) = 1 \text{ et si } x < 0, \frac{d}{dx}(|x|) = -1.$$

Remarque 4.0.3.

Pour tout réel x , $|x| \geq 0$, et $|x| = 0$ si et seulement si $x = 0$.

Remarque 4.0.4.

Pour tout $x, y \in \mathbb{R}$, $|x \cdot y| = |x| \cdot |y|$.

Théorème 4.0.5.

Soit $x, y \in \mathbb{R}$. Alors, $|x| \leq y$ si et seulement si $-y \leq x \leq y$.

Démonstration.

Il suffit de discuter selon les signes de x et de y . □

Proposition 4.0.6 (Inégalité triangulaire).

Soit $x, y \in \mathbb{R}$, alors :

1. $|x + y| \leq |x| + |y|$;
2. $||x| - |y|| \leq |x + y|$;
3. enfin, $|x + y| = |x| + |y|$ si et seulement si x et y sont de même signe.

Remarque 4.0.7.

L'*inégalité triangulaire* est celle du premier point, mais on trouve souvent sous cette appellation les deux premiers points résumés dans l'encadrement $||x| - |y|| \leq |x + y| \leq |x| + |y|$. Le troisième point est le *cas d'égalité de l'inégalité triangulaire*.

Le cas d'égalité du second point existe également : $||x| - |y|| = |x + y|$ si et seulement si x et y sont de signe opposés.

On retrouvera ces résultats pour les nombres complexes, car la valeur absolue et le module complexe coïncident sur $\mathbb{R}$. Le premier point sera démontré dans le chapitre correspondant. Le second point en découle facilement et peut être démontré dès maintenant. Nous donnons cependant une démonstration élémentaire des points (i) et (iii), valable uniquement pour des réels.

Démonstration. 1.

$$\begin{aligned} (|x| + |y|)^2 - |x + y|^2 &= (|x| + |y|)^2 - (x + y)^2 \\ &= 2(|xy| - xy) \\ &\geq 0, \end{aligned}$$

donc $|x + y|^2 \leq (|x| + |y|)^2$. On conclut par positivité de $|x + y|$ et de $|x| + |y|$.

3. Dans le raisonnement précédent, il y a égalité si et seulement si $|xy| = xy$, ce qui est équivalent à $xy \geq 0$, ce qui est bien équivalent à « x et y sont de même signe ».
2. En appliquant le premier point, $|x| = |(x + y) + (-y)| \leq |x + y| + |y|$ donc $|x| - |y| \leq |x + y|$. En permutant les rôles de x et y , nous avons également $|y| - |x| \leq |x + y|$, ce qui permet de conclure. □

Remarque 4.0.8 (Interprétation en terme de distance).

Si $x, y \in \mathbb{R}$, $|x - y|$ est la distance entre x et y . On peut alors écrire, avec $(x, \varepsilon) \in \mathbb{R}^2$, les intervalles

$$\begin{aligned} [x - \varepsilon, x + \varepsilon] &= \{ y \in \mathbb{R} \mid |y - x| \leq \varepsilon \}, \\]x - \varepsilon, x + \varepsilon[&= \{ y \in \mathbb{R} \mid |y - x| < \varepsilon \}. \end{aligned}$$

5 Fonctions puissances entières, polynomiales et rationnelles

5.1 Fonctions puissances entières

Définition 5.1.1.

Soit $x \in \mathbb{R}$, $n \in \mathbb{N}$. On appelle x *puissance n* le réel $x \times \dots \times x$ (n fois), noté x^n .

Par convention $x^0 = 1$ pour tout $x \in \mathbb{R}$, même 0.

Si n est un entier strictement négatif, et si $x \neq 0$, on pose $x^n = \frac{1}{x^{-n}}$.

Remarque 5.1.2.

Cela peut se définir rigoureusement par récurrence.

Proposition 5.1.3.

Soit $m, n \in \mathbb{Z}$, de manière générale :

$$\begin{aligned} x^{m+n} &= x^m x^n, \\ x^{mn} &= (x^m)^n, \\ (xy)^n &= x^n y^n, \\ \frac{x^n}{y^n} &= \left(\frac{x}{y} \right)^n. \end{aligned}$$

De plus, $x \mapsto x^n$ a la même parité que n . C'est une fonction continue, dérivable, de dérivée $x \mapsto nx^{n-1}$.

Les allures des courbes dans tous les cas (n pair, impair, positif, négatif) sont données dans les figures II.12 et II.13.

Proposition 5.1.4 (Comparaisons de puissances).

Soit $x \in]0, 1]$, alors

$$0 < x^4 \leq x^3 \leq x^2 \leq x \leq 1 \leq 1/x \leq 1/x^2 \dots$$

Plus formellement, la suite $(x^n)_{n \in \mathbb{Z}}$ est décroissante (strictement si $0 < x < 1$).

Soit $x \in [1, +\infty[$, la suite $(x^n)_{n \in \mathbb{Z}}$ est croissante (strictement si $x > 1$).

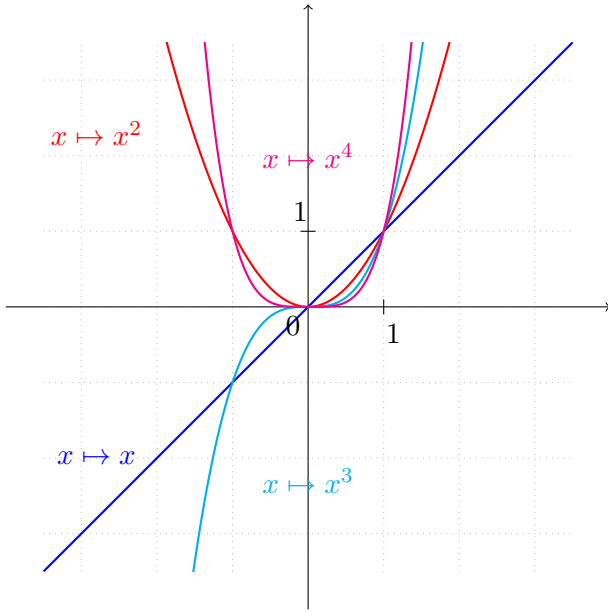


FIGURE II.12 – Quelques fonctions puissance, exposants positifs.

5.2 Fonctions polynomiales et rationnelles

Définition 5.2.1.

On appelle fonction polynomiale toute fonction de la forme

$$f : \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \underbrace{a_0 + a_1x + a_2x^2 + \dots + a_nx^n}_{\sum_{k=0}^n a_k x^k}$$

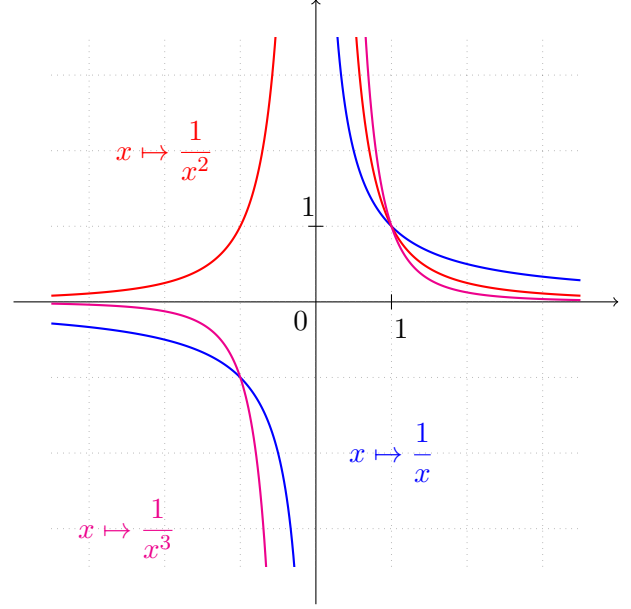


FIGURE II.13 – Quelques fonctions puissance, exposants négatifs.

où $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{R}$ et où $a_n \neq 0$.

Dans ce cas, n est appelé le degré de f , a_n est le coefficient dominant (ou de plus haut degré) de f et a_0 est le coefficient constant de f . Le terme $a_n x^n$ est le monôme dominant de f .

Proposition 5.2.2.

Toute fonction polynomiale est continue et dérivable sur $\mathbb{R}$.

De plus, avec les notations précédentes, $f(x)$ et $a_n x^n$ ont même limite en $\pm\infty$.

Démonstration.

On factorise $a_n x^n$:

$$f(x) = a_n x^n \left(\frac{a_0}{a_n x^n} + \frac{a_1}{a_n x^{n-1}} + \dots + \frac{a_{n-1}}{a_n x} + 1 \right) \\ = a_n x^n \left(1 + \sum_{k=0}^{n-1} \frac{a_k}{a_n x^{n-k}} \right).$$

Il suffit de voir que, si $0 \leq k \leq n-1$,

$$\frac{a_k}{a_n x^{n-k}} \xrightarrow{x \rightarrow \pm\infty} 0.$$

□

Définition 5.2.3.

On appelle *fonction rationnelle* toute fonction de la forme $f : x \mapsto \frac{g(x)}{h(x)}$ où g et h sont des fonctions polynomiales. Si $a_n x^n$ et $b_m x^m$ sont les monômes dominants de g et h , alors $f(x)$ et $\frac{a_n x^n}{b_m x^m}$ ont même limite en $\pm\infty$.

Remarque 5.2.4.

L'ensemble de définition d'une telle fonction est au moins inclus dans l'ensemble des réels sur lesquels h ne s'annule pas. Nous l'étudierons précisément dans le chapitre dédié aux fractions rationnelles. Sur cet ensemble, toute fraction rationnelle est continue et dérivable.

6 Fonctions exponentielles, logarithmes et puissances quelconques

6.1 Exponentielle et logarithme

Définition 6.1.1.

On appelle *logarithme népérien* la primitive, notée $\ln$, de $x \mapsto \frac{1}{x}$ sur $\mathbb{R}_+^*$ valant 0 en 1.

Proposition 6.1.2.

La fonction $\ln$ est continue, dérivable sur $\mathbb{R}_+^*$, strictement croissante (donc injective) et bijective de $\mathbb{R}_+^*$ dans $\mathbb{R}$.

$$\text{Si } x \in \mathbb{R}_+^*, \text{ on a } \ln'(x) = \frac{1}{x}.$$

Démonstration.

Les outils pour cela seront vus plus tard, mais il suffit de dire que c'est la primitive d'une fonction continue et positive. $\square$

Définition 6.1.3.

On appelle fonction *exponentielle* notée $\exp$ la réciproque de $\ln$. On a donc $\exp : \mathbb{R} \rightarrow \mathbb{R}_+^*$.

Proposition 6.1.4.

La fonction $\exp$ est continue, dérivable sur $\mathbb{R}$, et égale à sa dérivée.

Démonstration.

Utiliser les propriétés de la réciproque. $\square$

- Graphes : voir la figure II.14.

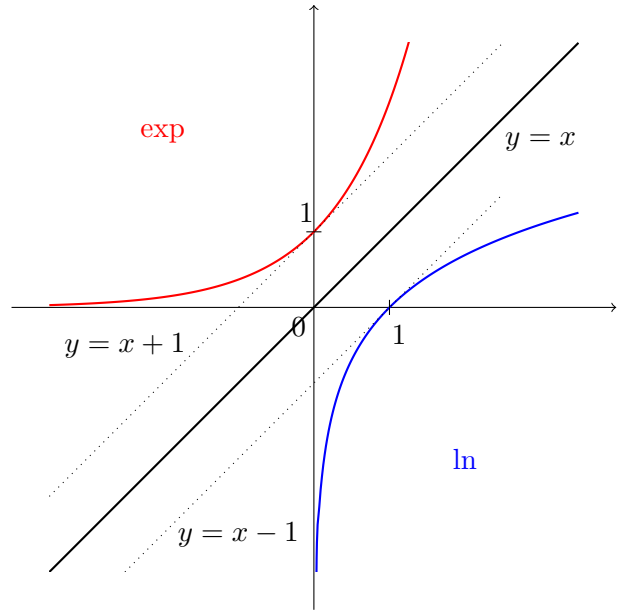


FIGURE II.14 – Logarithme et exponentielle.

Proposition 6.1.5.

L'exponentielle est partout strictement positive, elle est strictement croissante et bijective de $\mathbb{R}$ dans $\mathbb{R}_+^*$.

Démonstration.

Utiliser les propriétés de la réciproque. $\square$

Proposition 6.1.6.

Pour tout $x, y \in \mathbb{R}_+^*$, $\ln(xy) = \ln(x) + \ln(y)$.

Pour tout $x, y \in \mathbb{R}$, $\exp(x + y) = \exp(x)\exp(y)$.

Démonstration.

Soit $y \in \mathbb{R}_+^*$, étudions $f_y : \mathbb{R}_+^* \rightarrow \mathbb{R}$, $x \mapsto \ln(xy)$. C'est une fonction dérivable, comme composée de fonctions dérivables, et si $x \in \mathbb{R}_+^*$, $f_y'(x) = y \left(\frac{1}{xy} \right) = \frac{1}{x}$. Ainsi, f_y est

une primitive de $x \mapsto \frac{1}{x}$, donc diffère de $\ln$ d'une constante. Avec $x = 1$, on obtient cette constante : pour tout $x > 0$, on a bien $\ln(xy) = \ln x + \ln y$.

L'autre identité s'en déduit en observant que $\exp$ est la réciproque de $\ln$:

$$\begin{aligned}\ln(\exp(x)\exp(y)) &= \ln(\exp(x)) + \ln(\exp(y)) \\ &= x + y.\end{aligned}$$

Par définition de l'exponentielle, $\exp(x + y) = \exp(x)\exp(y)$. $\square$

Exemple 6.1.7.

En particulier, $\exp(-x) = \frac{1}{\exp(x)}$, $\ln(1/x) = -\ln x$ et $\ln(x^n) = n \ln x$.

Remarque 6.1.8.

On définit $e = \exp(1)$, dont une valeur approchée à 10^{-3} près est 2,718.

Proposition 6.1.9 (inégalités fondamentales).
Pour tout $x \in \mathbb{R}$,

$$e^x \geq 1 + x$$

et pour tout $x > -1$,

$$\ln(1 + x) \leq x.$$

Démonstration.

Il suffit d'étudier les fonctions $x \mapsto e^x - 1 - x$ et $x \mapsto \ln(1 + x) - x$, en dressant leurs tableaux de signes/variations. $\square$

Remarque 6.1.10.

Ces inégalités s'observent aisément sur la figure II.14.

Elles découlent immédiatement de la propriété de convexité de l'exponentielle et de la propriété de concavité du logarithme.

Remarque 6.1.11.

Les dérivées de l'exponentielle en 0 et du logarithme en 1 donnent les limites suivantes, fort utiles :

$$\begin{aligned}\frac{\exp(x) - 1}{x} &\xrightarrow{x \rightarrow 0} 1, \\ \frac{\ln(1 + x)}{x} &\xrightarrow{x \rightarrow 0} 1.\end{aligned}$$

6.2 Exponentielle de base quelconque

Définition 6.2.1.

Soient $x \in \mathbb{R}_+^*$ et $a \in \mathbb{R}$. On appelle « x puissance a » (ou exponentielle de base x), noté x^a , le réel $x^a = \exp(a \ln x)$.



x^a n'est qu'une notation pour $\exp(a \ln x)$.



x^a n'est pas défini avec $x \leq 0$, avec cette définition.

Remarque 6.2.2.

- Si $a \in \mathbb{N}$, cette définition coïncide avec la définition donnée précédemment.
- On a alors pour tout $x > 0$, $\exp(x) = e^x$. La notation e^x est alors utilisée pour tout $x \in \mathbb{R}$ pour désigner $\exp(x)$.

Cas particuliers :

1. $a \in \mathbb{N}$: x^a défini sur $\mathbb{R}$.
2. $a \in \mathbb{Z}$: x^a défini sur $\mathbb{R}^*$.
3. $a \in \mathbb{R}^+$: prolongeable en 0 par continuité.
4. $a = \frac{1}{q} \in \mathbb{Q}$, $q > 0$: définie sur $\mathbb{R}_+$, donc prolongeable en zéro, comme réciproque de la fonction $x \mapsto x^q$. Et même prolongeable sur $\mathbb{R}$ si q impair.

- Pour traiter un exercice avec des puissances quelconques, il faut quasiment toujours repasser par l'écriture exponentielle.

Proposition 6.2.3.

Soit $x, x' \in \mathbb{R}_+^*$ et $y, y' \in \mathbb{R}$, on a :

1. $(xx')^y = x^y \cdot x'^y$.
2. $x^{y+y'} = x^y \cdot x^{y'}$.
3. $x^{(yy')} = (x^y)^{y'}$.
4. $x^{-y} = \frac{1}{x^y} = \left(\frac{1}{x}\right)^y$.

Démonstration.

Revenir à la définition via l'exponentielle. $\square$

- On peut dériver x^a en utilisant directement sa définition. On remarquera notamment que

$$\frac{\partial}{\partial x}(x^a) \neq \frac{\partial}{\partial a}(x^a).$$



On n'utilisera jamais le symbole ' pour dériver une expression, mais plutôt $\frac{d}{d\heartsuit}$ ou $\frac{\partial}{\partial\heartsuit}$, où $\heartsuit$ est la variable par rapport à laquelle on dérive l'expression (les autres étant fixées).

Exemple 6.2.4.

Que veut dire $(x^y)'$?

Proposition 6.2.5.

Soit $a \in \mathbb{R}$. On note $f_a : \mathbb{R}_+^* \rightarrow \mathbb{R}_+^*$.

$$x \mapsto x^a$$

1. La fonction f_a est continue, dérivable et $\forall x \in \mathbb{R}_+^*$, $f'_a(x) = ax^{a-1}$.
2. Si $a \neq 0$, f_a est bijective de $\mathbb{R}_+^*$ sur $\mathbb{R}_+^*$. Sa réciproque est $f_{1/a}$.
3. Soit $a < a'$: si $x > 1$, $x^a < x^{a'}$, si $x \in]0, 1[$, $x^a > x^{a'}$.

Démonstration. 1. Il suffit de dériver dans la définition.

2. Il suffit de vérifier que $(x^a)^{1/a} = (x^{1/a})^a = x$.

3. Il suffit de discuter suivant le signe de $\ln(x)$. $\square$

- Graphes : voir la figure II.15.

Définition 6.2.6 (Logarithme de base a).

Soit $a \in \mathbb{R}_+^* \setminus \{1\}$. La fonction « puissance en base a », $\mathbb{R} \rightarrow \mathbb{R}_+^*$, $x \mapsto a^x$, est bijective. Sa réciproque est le logarithme de base a

$$\log_a : \begin{cases} \mathbb{R}_+^* & \longrightarrow \mathbb{R}, \\ x & \longmapsto \frac{\ln(x)}{\ln(a)}. \end{cases}$$

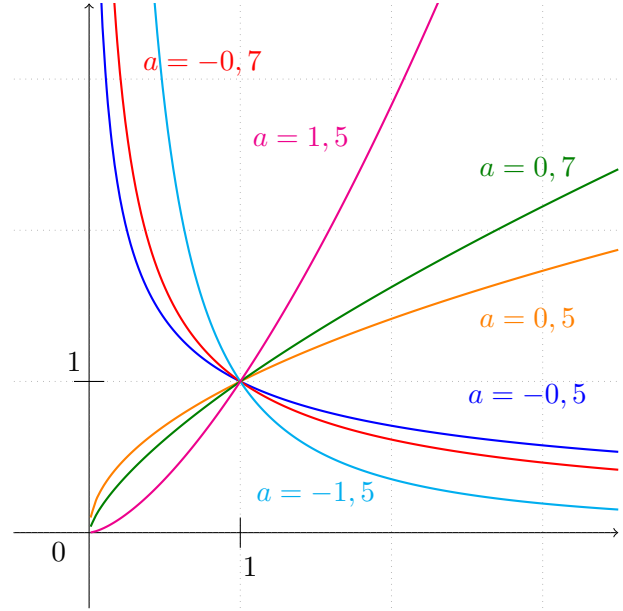


FIGURE II.15 – Quelques fonctions de la forme $x \mapsto x^a$.

- Remarque 6.2.7.** 1. Cas particuliers utiles : $\log_{10}$ et $\log_2$. Ils donnent le nombre de chiffres dans l'écriture d'un entier en base 10 ou 2 : si $10^{p-1} \leq n < 10^p$, alors n s'écrit avec p chiffres en base 10 et $\lfloor \log_{10} n \rfloor = p - 1$.
2. Propriétés fondamentales : $\log_{10}(10^x) = x$ et $10^{\log_{10} x} = x$.

6.3 Racines énièmes.

Définition 6.3.1.

Soit $n \in \mathbb{N}^*$. La fonction $x \mapsto x^n$ est continue.

- Si n est pair, $x \mapsto x^n$ est strictement croissante sur $\mathbb{R}_+$ et réalise une bijection de $\mathbb{R}_+$ sur $\mathbb{R}_+$. Sa réciproque sur $\mathbb{R}_+$ est appelée « racine n^e », notée $\sqrt[n]{\cdot}$.
- Si n est impair, $x \mapsto x^n$ est strictement croissante sur $\mathbb{R}$ et réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}$. Sa réciproque sur $\mathbb{R}$ est appelée « racine n^e », notée $\sqrt[n]{\cdot}$.

Démonstration.

Il suffit de montrer la croissance stricte. Cela peut se faire en dérivant, ou bien en factorisant $x^n - y^n$ (la formule sera vue bientôt).

Notamment, pour $n = 2$, $x^2 - y^2 = (x - y)(x + y)$ donne directement la croissance stricte de $x \mapsto x^2$ sur $\mathbb{R}_+^*$. $\square$

Exemple 6.3.2.

$(-2)^3 = -8$, donc $-2 = \sqrt[3]{-8}$, et $(\sqrt{3})^4 = (-\sqrt{3})^4 = 9$, donc $\sqrt[4]{9} = \sqrt{3}$.

Proposition 6.3.3.

Soit $n \in \mathbb{N}^*$ et $x > 0$, alors $\sqrt[n]{x} = x^{1/n}$.

Démonstration.

On a bien $x^{1/n} > 0$ et, d'après les règles de manipulation des puissances, $(x^{1/n})^n = (x^n)^{1/n} = x$. $\square$

6.4 Croissances comparées

Exercice 6.4.1.

Montrer que $\forall x \in \mathbb{R}_+$, $\exp(x) \geq 1 + x + x^2/2$. En déduire la limite de $\exp(x)/x$ lorsque $x \rightarrow +\infty$.

Proposition 6.4.2 (Croissances comparées des exponentielles, puissances et logarithmes).

Soient $a, b \in \mathbb{R}_+^*$. Alors :

1. l'exponentielle l'emporte sur les puissances :

$$|x|^a e^{bx} \xrightarrow{x \rightarrow -\infty} 0 \quad \text{et} \quad \frac{e^{bx}}{x^a} \xrightarrow{x \rightarrow +\infty} +\infty ;$$

2. les puissances l'emportent sur les logarithmes :

$$x^a \cdot |\ln x|^b \xrightarrow{x \rightarrow 0} 0 \quad \text{et} \quad \frac{x^a}{(\ln x)^b} \xrightarrow{x \rightarrow +\infty} +\infty ;$$

3. l'exponentielle l'emporte sur les logarithmes (repasser par les deux premiers points).

Démonstration. 1. On utilise le résultat de l'exercice 6.4.1, en factorisant

$$\frac{e^{bx}}{x^a} = \left(\frac{e^{bx/a}}{x} \right)^a = \left(\frac{b}{a} \right)^a \cdot \left(\frac{e^{bx/a}}{bx/a} \right)^a.$$

2. En composant la limite de l'exercice 6.4.1 par $\ln(x)$, on a directement $\frac{x}{\ln x} \xrightarrow{x \rightarrow +\infty} +\infty$. Puis, en composant par $\frac{1}{x}$, on obtient et $x \ln x \xrightarrow{x \rightarrow 0} 0$.

Ensuite, on factorise

$$\frac{x^a}{(\ln x)^b} = \left(\frac{x^{a/b}}{\ln x} \right)^b = \left(\frac{a}{b} \right)^b \left(\frac{x^{a/b}}{\ln(x^{a/b})} \right)^b.$$

On obtient l'autre limite par composition.

3. Repasser par les deux premiers points. $\square$

Exercice 6.4.3.

Déterminer la limite de la suite de terme général

$$\frac{3^n - n^2 + \ln^2(n)}{n^e + \sqrt[n]{e^n} - 2 \ln(n)}$$

7 Fonctions circulaires réciproques

7.1 Arccos et Arcsin



La fonction cosinus n'est pas bijective : pour tout $x \in [-1, 1]$, il n'existe pas un unique $t \in \mathbb{R}$ vérifiant $x = \cos(t)$.

Définition 7.1.1 (Arc cosinus).

Pour tout $x \in [-1, 1]$, il existe un unique $t \in [0, \pi]$ tel que $x = \cos(t)$. On dit que ce t est l'arc cosinus de x (noté $t = \text{Arccos}(x)$).

Plus formellement : la fonction cosinus est bijective de $[0, \pi]$ sur $[-1, 1]$. Sa fonction réciproque est appelée arc cosinus et noté Arccos.

Démonstration.

La fonction cosinus est continue, strictement décroissante sur $[0, \pi]$, $\cos(0) = 1$ et $\cos(\pi) = -1$. On conclut par le théorème de la bijection. $\square$

Proposition 7.1.2.

La fonction arc cosinus est strictement décroissante, continue sur $[-1, 1]$, dérivable sur $] -1, 1[$, de dérivée $x \mapsto -\frac{1}{\sqrt{1-x^2}}$, c'est-à-dire que pour tout $x \in] -1, 1[$,

$$\text{Arccos}'(x) = -\frac{1}{\sqrt{1-x^2}}.$$

Son graphe est représenté sur la figure II.16.

Démonstration.

Tout découle du tableau de variations du cosinus et des théorèmes généraux précédents.

Comme $\cos'(0) = 0$ et $\cos'(\pi) = 0$, Arccos n'est pas dérivable en $\cos(0) = 1$ et en $\cos(\pi) = -1$. La dérivée du

cosinus ne s'annule pas sur $]0, \pi[$, donc Arccos est dérivable sur $] -1, 1[$. Ensuite, si $-1 < x < 1$,

$$\text{Arccos}'(x) = \frac{1}{\cos'(\text{Arccos } x)} = \frac{-1}{\sin(\text{Arccos } x)}.$$

Il suffit d'utiliser le résultat du théorème 7.1.6 pour obtenir $\sin(\text{Arccos } x) = \sqrt{1 - x^2}$. $\square$

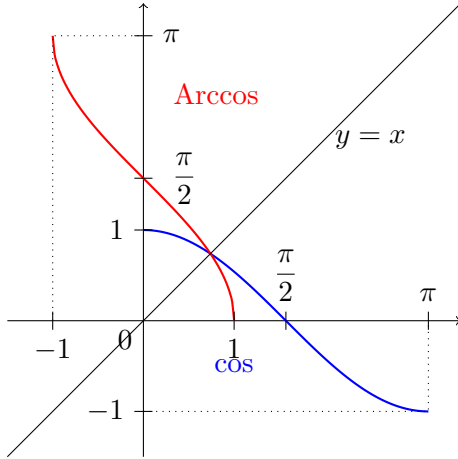


FIGURE II.16 – Fonctions cos et Arccos.



La fonction sinus n'est pas bijective : pour tout $x \in [-1, 1]$, il n'existe pas un unique $t \in \mathbb{R}$ vérifiant $x = \sin(t)$.

Définition 7.1.3 (Arc sinus).

Pour tout $x \in [-1, 1]$, il existe un unique $t \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ tel que $x = \sin(t)$. On dit que ce t est l'arc sinus de x (noté $t = \text{Arcsin}(x)$).

Plus formellement : la fonction sinus est bijective de $[-\pi/2, \pi/2]$ sur $[-1, 1]$. Sa fonction réciproque est appelée arc sinus et noté Arcsin .

Démonstration.

La fonction sinus est continue, strictement croissante sur $[-\pi/2, \pi/2]$, $\sin(-\frac{\pi}{2}) = -1$ et $\sin(\frac{\pi}{2}) = 1$. On conclut par le théorème de la bijection. $\square$

Proposition 7.1.4.

La fonction arc sinus est strictement croissante, impaire, continue sur $[-1, 1]$, dérivable sur $] -1, 1[$,

de dérivée $x \mapsto \frac{1}{\sqrt{1 - x^2}}$, c'est-à-dire que pour tout $x \in] -1, 1[$,

$$\text{Arcsin}'(x) = \frac{1}{\sqrt{1 - x^2}}.$$

Son graphe est représenté sur la figure II.17.

Démonstration.

C'est la même chose que pour l'arc cosinus.

Pour l'imparité, si $x \in [-1, 1]$, posons $t = \text{Arcsin}(x)$, donc $t \in [-\pi/2, \pi/2]$ et $\sin(t) = x$. Par imparité du sinus, $\sin(-t) = -x$, et $-t \in [-\pi/2, \pi/2]$, donc par définition $-t = \text{Arcsin}(-x)$. On vient de montrer que $\text{Arcsin}(-x) = -\text{Arcsin}(x)$. $\square$

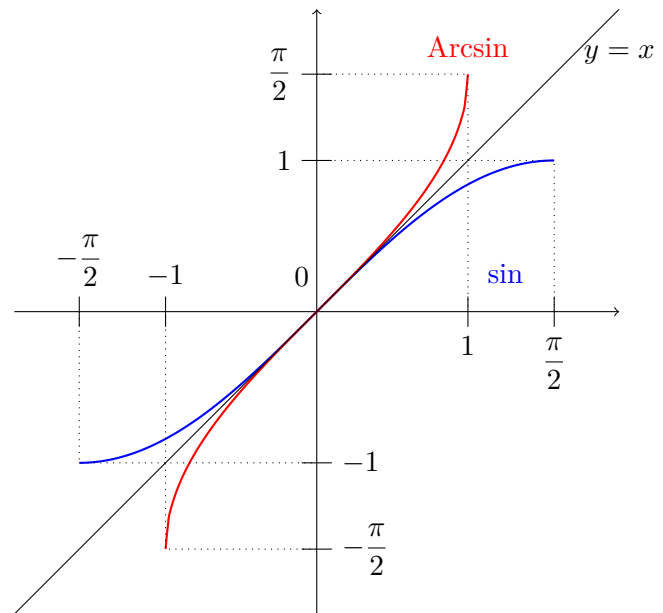


FIGURE II.17 – Fonctions sin et Arcsin.

Exercice 7.1.5.

Déterminer les arc cosinus et arc sinus des valeurs usuelles : $0, \pm \frac{1}{2}, \pm \frac{\sqrt{2}}{2}, \pm \frac{\sqrt{3}}{2}$ et ± 1 .

Théorème 7.1.6.

Pour tout $x \in [-1, 1]$,

$$\begin{aligned} \sin(\text{Arccos } x) &= \cos(\text{Arcsin } x) \\ &= \sqrt{1 - x^2}. \end{aligned}$$

Démonstration.

On a $\cos \circ \text{Arccos} = \text{Id}_{[-1,1]}$, c'est-à-dire que, par définition, pour tout $x \in [-1, 1]$, $\cos(\text{Arccos } x) = x$.

Ainsi, si $x \in [-1, 1]$, on a

$$\sin^2(\text{Arccos } x) = 1 - \cos^2(\text{Arccos } x) = 1 - x^2.$$

Pour finir, on remarque que le sinus est positif sur $[0, \pi]$, or la fonction Arccos prend ses valeurs dans $[0, \pi]$, donc $\sin(\text{Arccos } x) \geq 0$. $\square$



$\text{Arccos} \circ \cos \neq \text{Id}_{\mathbb{R}}$, on a juste que pour tout $x \in [0, \pi]$, $\text{Arccos}(\cos(x)) = x$.

Exercice 7.1.7.

Calculer $\text{Arccos}\left(\cos \frac{17\pi}{7}\right)$.

Exercice 7.1.8.

Résoudre l'équation $\text{Arcsin } x = \text{Arccos } \frac{4}{5}$, d'inconnue $x \in [-1, 1]$.



Toujours faire attention aux signes des objets, et aux ensembles auxquels ils appartiennent.

Proposition 7.1.9.

Pour tout $x \in [-1, 1]$, on a $\text{Arcsin } x + \text{Arccos } x = \pi/2$.

Démonstration.

Notons $f : [-1, 1] \rightarrow \mathbb{R}$, $x \mapsto \text{Arcsin } x + \text{Arccos } x$. Il suffit de montrer que f est constante sur $[-1, 1]$, de valeur $\pi/2$. Pour cela on peut vérifier les trois points suivants :

1. f est constante sur $] -1, 1[$. En effet, f est dérivable sur $] -1, 1[$ et d'après ce qui précède sa dérivée est nulle. Notons C sa valeur sur $] -1, 1[$.
2. f est constante sur $[-1, 1]$. En effet, on a $\forall x \in] -1, 1[$ $f(x) = C$, donc f admet une limite à droite en -1 et $f(x) \xrightarrow[x > -1]{x \rightarrow -1} C$. Or f est continue en -1 car

Arcsin et Arccos le sont. Donc $f(x) \xrightarrow[x > -1]{x \rightarrow -1} f(-1)$.

Donc $f(-1) = C$.

De même $f(1) = C$.

On a donc $\forall x \in [-1, 1]$ $f(x) = C$.

3. La valeur de f sur $[-1, 1]$ est $\pi/2$. En effet, en 0, f vaut $\text{Arcsin } 0 + \text{Arccos } 0$, qui est égal à $0 + \pi/2$. $\square$

7.2 Arctangente



La fonction tangente n'est pas bijective : pour tout $x \in \mathbb{R}$, il n'existe pas un unique $t \in \mathbb{R}$ vérifiant $x = \tan(t)$.

Définition 7.2.1 (Arc tangente).

Pour tout $x \in \mathbb{R}$, il existe un unique $t \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ tel que $x = \tan(t)$. On dit que ce t est l'arc tangente de x (noté $t = \text{Arctan}(x)$).

Plus formellement, la fonction tangente est bijective de $] -\pi/2, \pi/2[$ sur $\mathbb{R}$. Sa fonction réciproque est appelée arctangente et noté Arctan (parfois atan).

Proposition 7.2.2.

La fonction arc tangente est continue sur $\mathbb{R}$, dérivable sur $\mathbb{R}$ de dérivée $x \mapsto \frac{1}{1+x^2}$, impaire et strictement croissante. Son graphe est donné figure II.18 (noter les asymptotes).

Démonstration.

Tout découle du tableau de variations de la tangente et des théorèmes généraux précédents.

On a $\tan' = 1 + \tan^2$, donc pour tout $x \in]-\pi/2, \pi/2[$, $\tan'(x) \geq 1$. La dérivée de la tangente ne s'annule pas sur $] -\pi/2, \pi/2[$, donc Arctan est dérivable sur $\mathbb{R}$. Ensuite, si $x \in \mathbb{R}$,

$$\text{Arctan}'(x) = \frac{1}{\tan'(\text{Arctan } x)} = \frac{1}{1 + \tan^2(\text{Arctan } x)} = \frac{1}{1 + x^2}.$$

L'imparité s'obtient comme pour l'arc sinus. $\square$

Proposition 7.2.3.

À nouveau, remarquer que $\tan \circ \text{Arctan} = \text{Id}_{\mathbb{R}}$, mais pas $\text{Arctan} \circ \tan$: ce n'est l'identité que sur $] -\pi/2, \pi/2[$.

Exercice 7.2.4.

Résoudre l'équation $\text{Arctan}(2x) + \text{Arctan}(3x) = \frac{\pi}{4}$.

Exercice 7.2.5.

Étudier la fonction $f : x \mapsto \text{Arctan}(x) + \text{Arctan}\left(\frac{1}{x}\right)$.

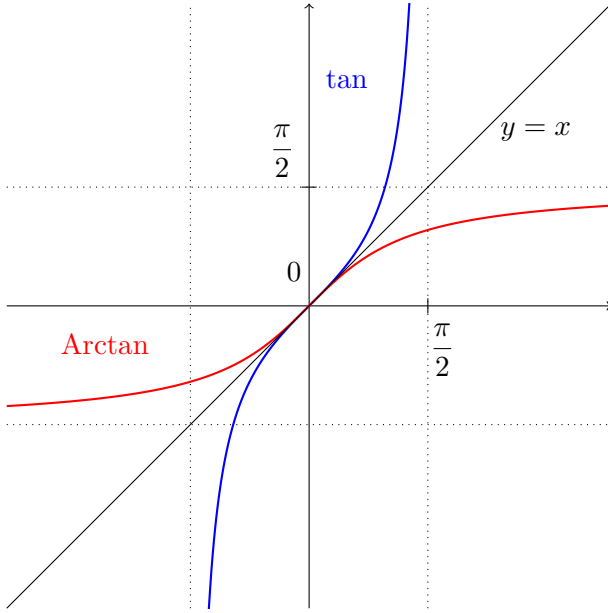


FIGURE II.18 – Fonctions tan et Arctan.

7.3 Coordonnées polaires

Soit (x, y) un couple de coordonnées cartésiennes d'un point M du plan. On veut un couple de coordonnées polaires de M . On cherche un tel couple sous la forme (r, θ) avec $r \geq 0$ et $\theta \in]-\pi, \pi]$. On a $r = \sqrt{x^2 + y^2}$. On doit avoir $x = r \cos \theta =$ et $y = r \sin \theta$, donc $\cos \theta = x/r$ et $\sin \theta = y/r$ (on écarte le cas $r = 0$, on dit par convention que toutes les $(0, \theta)$ conviennent).

On distingue deux cas :

Premier cas $y \geq 0$, donc M appartient au demi-plan supérieur, donc $\theta \in [0, \pi]$ et donc $\theta = \text{Arccos}(x/r)$.

Second cas $y < 0$, alors $\theta \in]-\pi, 0[$, donc $-\theta \in]0, \pi[$, donc $-\theta = \text{Arccos}(x/r)$, d'où $\theta = -\text{Arccos}(x/r)$.

Remarque 7.3.1.

On aurait aussi pu utiliser Arcsin en distinguant les cas $x \geq 0$ ($\theta = \text{Arcsin}(y/r)$) et $x < 0$ ($\theta = \pi - \text{Arcsin}(y/r)$).

Exemple 7.3.2.

Un couple de coordonnées polaires de $(4, -3)$ est $\left(5, -\text{Arccos} \frac{4}{5}\right)$.

Remarque 7.3.3.

Trouver le module et un argument d'un nombre complexe est le même problème que de déterminer un couple de coordonnées polaires d'un point du plan. Il se résout avec les mêmes méthodes.

8 Fonctions hyperboliques

8.1 ch, sh et th

Définition 8.1.1.

On appelle :

1. *Sinus hyperbolique* et on note sh l'application

$$\begin{aligned} \text{sh} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{e^x - e^{-x}}{2} \end{aligned}$$

2. *Cosinus hyperbolique* et on note ch l'application

$$\begin{aligned} \text{ch} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{e^x + e^{-x}}{2} \end{aligned}$$

Proposition 8.1.2. 1. La fonction ch est continue et dérivable sur $\mathbb{R}$ et sa dérivée est sh. De plus, ch est paire.

2. La fonction sh est continue et dérivable sur $\mathbb{R}$ et sa dérivée est ch. De plus, sh est impaire.

3. Les graphes de ch et sh sont donnés dans la figure II.20.

4. $\text{ch} + \text{sh} = \exp$.

5. $\text{ch}^2 - \text{sh}^2 = 1$.

Démonstration. 1. On calcule ch' , et $\text{ch}(-x)$.

2. Idem.

3. On dresse le tableau de variations de signes / variations suivant (voir figure II.19), en partant du fait que, pour tout $x \in \mathbb{R}$, $\text{ch}(x) > 0$. On rajoute : $\text{ch}(x) - \text{sh}(x) \xrightarrow{x \rightarrow +\infty} 0$, donc les graphes de ch et de sh sont asymptotiques l'un de l'autre.

4. Simple calcul.

x	$-\infty$	0	$+\infty$
$\text{ch}(x)$		$+$	
$\text{sh}(x)$	$-\infty$	0	$+\infty$
$\text{sh}(x)$	$-$	0	$+$
$\text{ch}(x)$	$+\infty$	1	$+\infty$

FIGURE II.19 – Variations de ch et de sh.

5. On factorise, en utilisant la parité de ch et l'imparité de sh et le résultat précédent : pour tout $x \in \mathbb{R}$,

$$\begin{aligned}
 \text{ch}^2(x) - \text{sh}^2(x) &= (\text{ch}(x) + \text{sh}(x))(\text{ch}(x) - \text{sh}(x)) \\
 &= (\text{ch}(x) + \text{sh}(x))(\text{ch}(-x) + \text{sh}(-x)) \\
 &= \exp(x) \exp(-x) \\
 &= 1.
 \end{aligned}$$

□

Remarque 8.1.3.

On a l'inégalité suivante : pour tout $u \in \mathbb{R}_+^*$,
 $u + \frac{1}{u} \geq 2$,

avec égalité si et seulement si $u = 1$. Cela permet de retrouver que, pour tout $x \in \mathbb{R}$, $\text{ch}(x) \geq 1$.

Exercice 8.1.4.

Démontrer l'inégalité précédente de deux manières différentes.

Définition 8.1.5.

On appelle *Tangente hyperbolique* et on note $\text{p} = \frac{\text{sh}}{\text{ch}}$, soit l'application

$$\begin{aligned}
 \text{p} : \mathbb{R} &\rightarrow \mathbb{R} \\
 x &\mapsto \frac{e^x - e^{-x}}{e^x + e^{-x}}.
 \end{aligned}$$

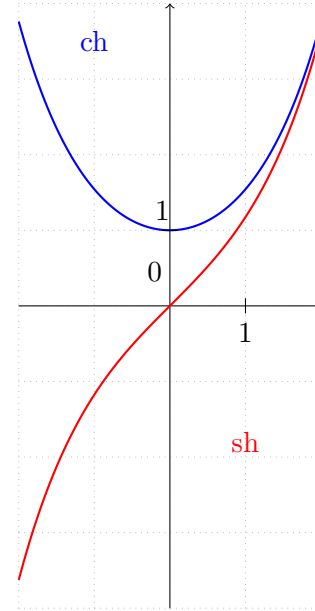


FIGURE II.20 – Fonctions ch et sh.

Proposition 8.1.6.

La fonction th est continue et dérivable sur $\mathbb{R}$ et

$$\text{p}' = 1 - \text{p}^2 = \frac{1}{\text{ch}^2}.$$

De plus, th est impaire et, pour tout $x \in \mathbb{R}$, $-1 < \text{p}(x) < 1$. Voir son graphe figure II.21.

Démonstration.

Par le calcul de $\text{ch} - \text{sh}$, on obtient que, pour tout $x \in \mathbb{R}$,

$$-\text{ch}(x) < \text{sh}(x) < \text{ch}(x)$$

et $\text{ch}(x) > 0$, donc p est bien définie et à valeurs dans $] -1, 1[$. En tant que quotient de fonctions dérivables dont le dénominateur ne s'annule pas, p est dérivable. On dérive p facilement. Les limites de p s'obtiennent aisément : on notera les deux asymptotes horizontales à son graphe.

□

Remarque 8.1.7.

Pourquoi fonctions «hyperboliques» et «circulaires» ? Car $x^2 + y^2 = 1$ est l'équation du cercle trigonométrique $\mathcal{C}$, donc $(x, y) \in \mathcal{C}$ ssi $\exists t \in \mathbb{R} \quad x = \cos t$ et $y = \sin t$.

De même, $x^2 - y^2 = 1$ est l'équation de l'hyperbole équilatère $\mathcal{H}$ d'asymptotes $x = \pm y$.

Donc $(x, y) \in \mathcal{H}$ ssi $\exists t \in \mathbb{R} \quad x = \pm \text{ch } t$ et $y =$

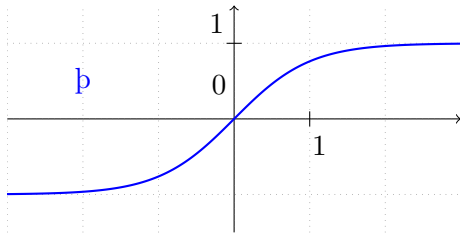


FIGURE II.21 – Fonction $\mathfrak{b}$.

$\text{sh } t$.

Remarque 8.1.8.

Toutes les formules de trigonométrie circulaire ont une analogue hyperbolique. Par exemple :

$$\text{ch}(a + b) = \text{ch } a \text{ch } b + \text{sh } a \text{sh } b,$$

$$\text{sh}(a + b) = \text{sh } a \text{ch } b + \text{ch } a \text{sh } b.$$

Ces formules ne sont pas à connaître.

Remarque 8.1.9.

Les dérivées du sinus et du cosinus hyperboliques en 0 donnent les limites suivantes, fort utiles :

$$\frac{\text{sh}(x)}{x} \xrightarrow{x \rightarrow 0} 1,$$

$$\frac{\text{ch}(x) - 1}{x} \xrightarrow{x \rightarrow 0} 0.$$

On a remarqué que ch est paire, sh est impaire et $\exp = \text{ch} + \text{sh}$. Cela se généralise comme suit.

Définition 8.1.10.

Soit $A \subset \mathbb{R}$ et $f : A \rightarrow \mathbb{R}$. Supposons que A est centré ($\forall x \in A, -x \in A$). Alors, il existe deux uniques fonctions $g : A \rightarrow \mathbb{R}$ et $h : A \rightarrow \mathbb{R}$ vérifiant :

- g est paire ;
- h est impaire ;
- $f = g + h$.

On dit que g est la *partie paire* de f et h sa *partie impaire*.

Démonstration.

On raisonne par analyse-synthèse.

Analyse : On suppose que l'on a g et h qui conviennent et l'on essaie d'obtenir des informations dessus. *Indice* : si $x \in A$, calculer $f(x) + f(-x)$.

On a en fait montré l'unicité de g et de h .

Synthèse : On vérifie que les fonctions trouvées dans la phase d'analyse conviennent.

On a alors montré l'existence de g et de h .

□

Exemple 8.1.11.

Les fonctions cosinus et sinus hyperboliques, sont les parties paires et impaires de la fonction exponentielle.

8.2 Fonctions hyperboliques inverses

Elles sont hors-programme. :'(

Mais vous pouvez très bien les retrouver, ainsi que leurs propriétés, en tant qu'exercice ! :)

Chapitre III

Un peu de calcul

Sommaire

1	Le symbole somme : Σ	52
1.1	Définition d'une somme simple et premières propriétés	52
1.2	Sommes doubles	54
1.3	Somme d'une famille finie d'objets	55
2	Le symbole produit : Π	56
3	Quelques formules à connaître	56
3.1	Sommes classiques	56
3.2	Coefficients binomiaux	57
3.3	Binôme de Newton, identités remarquables et sommation géométrique	58
4	Systèmes linéaires et pivot de Gauss	59
4.1	Définitions	59
4.2	Interprétation géométrique	60
a	Dans le plan	60
b	Dans l'espace	60
4.3	Opérations sur les lignes d'un système	60
4.4	Algorithme du pivot	61
a	Cas d'un système diagonal	61
b	Cas d'un système triangulaire inversible	61
c	Cas d'un système triangulaire non inversible	62
d	Systèmes échelonnés	62
e	Cas général	63

1 Le symbole somme : Σ

1.1 Définition d'une somme simple et premières propriétés

Définition 1.1.1.

Soit $m, n \in \mathbb{Z}$ tels que $m \leq n$. Soit $z_m, \dots, z_n$ des nombres complexes. Leur somme est notée

$$\sum_{k=m}^n z_k,$$

c'est le nombre complexe que l'on peut noter de manière abusive

$$z_m + z_{m+1} + z_{m+2} + \dots + z_n.$$

Par convention, si $m > n$, on posera $\sum_{k=m}^n z_k = 0$.

Exemple 1.1.2.

$$\sum_{k=1}^4 k^2 = 1 + 2^2 + 3^2 + 4^2 = 30.$$

Remarque 1.1.3.

Dans une expression du type $\sum_{k=m}^n f(k)$, on dit que la variable k est *muette*. En effet, on peut remplacer la lettre k par un autre nom de variable non encore utilisé, sans changer le sens de l'expression.

Ainsi $\sum_{k=m}^n f(k)$, $\sum_{i=m}^n f(i)$ et $\sum_{\text{Brandon}=m}^n f(\text{Brandon})$ sont synonymes. Par contre on ne peut pas écrire $\sum_{m=m}^n f(m)$, $\sum_{n=m}^n f(n)$ ou $\sum_{f=m}^n f(f)$, qui n'ont aucun sens.

On essaiera bien entendu de garder des notations cohérentes avec le contexte ... et raisonnables.

Les règles de manipulations vues au collège sont bien entendu valides ici.

Proposition 1.1.4 (Linéarité de la somme).

Soit $a_m, \dots, a_n, b_m, \dots, b_n$ des nombres com-

plexes, soit $\lambda, \mu \in \mathbb{C}$. Alors

$$\sum_{k=m}^n (\lambda a_k + \mu b_k) = \lambda \sum_{k=m}^n a_k + \mu \sum_{k=m}^n b_k.$$

Démonstration.

On le montre par récurrence sur n , après avoir fixé m . $\square$

Proposition 1.1.5 (Relation de Chasles).

Soit $m, n, p \in \mathbb{Z}$ tels que $m \leq n \leq p$, et $a_m, \dots, a_p$ des nombres complexes. Alors

$$\sum_{k=m}^p a_k = \sum_{k=m}^n a_k + \sum_{k=n+1}^p a_k.$$

Démonstration.

Ce résultat intuitif peut se démontrer proprement par récurrence sur p : on fixe $m \in \mathbb{Z}$ et pour tout $p \in \mathbb{Z}$ tel que $p \geq m$, on pose (H_p) : « pour tout $n \in \llbracket m, p \rrbracket$,

$$\sum_{k=m}^p a_k = \sum_{k=m}^n a_k + \sum_{k=n+1}^p a_k. \quad \square$$

Il est important de savoir manipuler des sommes écrites avec le symbole Σ . Pour cela, nous utiliserons principalement les deux outils suivants.

Le premier consiste à observer que la somme

$$z_{m+1} + z_{m+2} + z_{m+3} + \dots + z_n + z_{n+1}$$

peut s'écrire comme

$$z_{m+1} + z_{(m+1)+1} + z_{(m+2)+1} + \dots + z_{(n-1)+1} + z_{n+1}.$$

Proposition 1.1.6 (Décalage d'indice).

Soit $n, m \in \mathbb{Z}$, tels que $m \leq n$, soit $z_m, \dots, z_{n+1}$ des nombres complexes. On a

$$\sum_{k=m}^n z_{k+1} = \sum_{k=m+1}^{n+1} z_k.$$

Démonstration.

On le montre par récurrence sur n , en ayant fixé un entier m .

Si $n = m$, alors

$$\sum_{k=m}^n z_{k+1} = z_{m+1} = \sum_{k=m+1}^{n+1} z_k.$$

Soit un entier $n \geq m$, supposons que l'identité soit vraie au rang n . Alors,

$$\begin{aligned} \sum_{k=m}^{n+1} z_{k+1} &= \left(\sum_{k=m}^n z_{k+1} \right) + z_{n+1+1} \\ &= \left(\sum_{k=m+1}^{n+1} z_k \right) + z_{n+2} \\ &= \sum_{k=m+1}^{n+2} z_k. \end{aligned}$$

Ainsi, la propriété est vraie au rang $n+1$ et l'on peut conclure par récurrence. $\square$

Exercice 1.1.7.

Soit $n \in \mathbb{N}$, écrire comme une somme partant de l'indice 0 :

$$\sum_{k=2}^{n+1} k^2.$$

Le second outil consiste à remarquer que la somme

$$z_0 + z_1 + \cdots + z_{n-1} + z_n$$

peut s'écrire

$$z_{n-0} + z_{n-1} + \cdots + z_{n-(n-1)} + z_{n-n}.$$

Proposition 1.1.8 (Renversement d'indices).

Soit $n \in \mathbb{N}$, soit $z_0, \dots, z_n$ des nombres complexes. On a

$$\sum_{k=0}^n z_k = \sum_{k=0}^n z_{n-k}$$

et

$$\sum_{k=1}^n z_k = \sum_{k=0}^{n-1} z_{n-k}.$$

Démonstration.

On montre la première par récurrence sur n .

Si $n = 0$, alors

$$\sum_{k=0}^n z_k = z_0 = z_{n-0} = \sum_{k=0}^n z_{n-k}.$$

Soit un entier naturel n , supposons que l'identité soit vraie au rang n . Alors, en effectuant un décalage d'indice pour

passer de la troisième à la quatrième ligne,

$$\begin{aligned} \sum_{k=0}^{n+1} z_k &= \left(\sum_{k=0}^n z_k \right) + z_{n+1} \\ &= \left(\sum_{k=0}^n z_{n-k} \right) + z_{n+1} \\ &= \left(\sum_{k=0}^n z_{n+1-(k+1)} \right) + z_{n+1} \\ &= \left(\sum_{k=1}^{n+1} z_{n+1-k} \right) + z_{n+1-0} \\ &= \sum_{k=0}^{n+1} z_{n+1-k}. \end{aligned}$$

Ainsi, la propriété est vraie au rang $n+1$ et l'on peut conclure par récurrence.

La seconde identité se déduit immédiatement de celle-là avec un décalage d'indice. $\square$

Exemple 1.1.9.

$$\sum_{i=3}^6 i^2 = \sum_{i=2}^5 (i+1)^2 = \sum_{i=0}^3 (i+3)^2 = \sum_{i=0}^3 (6-i)^2.$$

Le résultat suivant est fondamental. Savoir repérer une somme télescopique et la simplifier (ou, réciproquement, faire apparaître une somme télescopique à la place de la différence de deux termes) est un *savoir-faire* important.

Théorème 1.1.10 (Simplification télescopique).

Soit $z_m, \dots, z_{n+1}$ des nombres complexes. Alors :

$$\sum_{k=m}^n (z_{k+1} - z_k) = z_{n+1} - z_m.$$

Remarque 1.1.11.

Ceci est l'analogue discret du résultat d'intégration $\int_a^b f'(t) dt = f(b) - f(a)$, pour les fonctions f éligibles.

Démonstration.

Commencer par écrire la somme « à la main » avec des « petits points » pour voir les simplifications apparaître.

Ensuite, par changement d'indice :

$$\begin{aligned}\sum_{k=m}^n (z_{k+1} - z_k) &= \sum_{k=m}^n z_{k+1} - \sum_{k=m}^n z_k \\ &= \sum_{k=m+1}^{n+1} z_k - \sum_{k=m}^n z_k \\ &= z_{n+1} - z_m.\end{aligned}$$

□

Remarque 1.1.12.

La dernière égalité se comprend intuitivement, on peut la montrer formellement par récurrence sur n .

Exemple 1.1.13.

Calculer la somme $\sum_{k=1}^n \frac{1}{k(k+1)}$ en utilisant $1 = k+1 - k$.

1.2 Sommes doubles

Définition 1.2.1 (Somme double).

Soit $(z_{k,\ell})_{m \leq k \leq n, p \leq \ell \leq q}$ la donnée de $(n+1-m)(q+1-p)$ nombres complexes, que l'on peut représenter dans le tableau suivant :

$$\begin{pmatrix} z_{m,p} & \cdots & z_{m,q} \\ \vdots & & \vdots \\ z_{n,p} & \cdots & z_{n,q} \end{pmatrix}.$$

Leur somme est notée

$$\sum_{m \leq k \leq n, p \leq \ell \leq q} z_{k\ell}.$$

Exemple 1.2.2.

Le nombre $\sum_{1 \leq i \leq 3, 4 \leq j \leq 5} i^2 j$ est la somme des éléments du tableau

$$\begin{pmatrix} 4 & 5 \\ 16 & 20 \\ 36 & 45 \end{pmatrix}$$

et vaut donc 126.

Remarque 1.2.3.

Par décalage d'indice, cette somme vaut $\sum_{1 \leq i \leq 3, 1 \leq j \leq 2} i^2(3+j)$.

On essaiera toujours d'écrire des sommes partant de 0 ou de 1.

La plus souvent, nous sommerons des nombres sur des tableaux carrés. Dans ce cas, nous utiliserons des notations plus légères.

Définition 1.2.4 (Somme double sur un tableau carré).

Soit $(z_{k,\ell})_{1 \leq k, \ell \leq n}$ la donnée de n^2 nombres complexes, que l'on peut représenter dans le tableau suivant :

$$\begin{pmatrix} z_{1,1} & \cdots & z_{1,n} \\ \vdots & & \vdots \\ z_{n,1} & \cdots & z_{n,n} \end{pmatrix}.$$

Leur somme est notée

$$\sum_{1 \leq k, \ell \leq n} z_{k,\ell}.$$

La somme des éléments de ce tableau situés *au dessus* de sa diagonale, diagonale comprise, est notée

$$\sum_{1 \leq k < \ell \leq n} z_{k,\ell}.$$

La somme des éléments de ce tableau situés *strictement au dessus* de sa diagonale, est notée

$$\sum_{1 \leq k < \ell \leq n} z_{k,\ell}.$$

La somme des éléments de ce tableau situés *en dessous* de sa diagonale, diagonale comprise, est notée

$$\sum_{1 \leq \ell < k \leq n} z_{k,\ell}.$$

La somme des éléments de ce tableau situés *strictement en dessous* de sa diagonale, est notée

$$\sum_{1 \leq \ell < k \leq n} z_{k,\ell}.$$

Remarque 1.2.5.

Il est important de se rappeler que les coefficients d'indice (i, j) d'un tel tableau :

- sont sur la diagonale si et seulement si $i = j$;

- sont strictement au dessus de la diagonale si et seulement si $i < j$;
- sont strictement au dessous de la diagonale si et seulement si $j < i$.

On pourra par exemple décomposer la somme des éléments d'un tel tableau sur ces trois parties :

$$\sum_{1 \leq i, j \leq n} z_{i,j} = \sum_{1 \leq i < j \leq n} z_{i,j} + \sum_{i=1}^n z_{i,i} + \sum_{1 \leq j < i \leq n} z_{i,j}.$$

Théorème 1.2.6 (Sommes doubles et permutation des Σ).

Soit $(z_{ij})_{1 \leq i, j \leq n}$ une famille de nombres complexes. Alors :

1. $\sum_{1 \leq i, j \leq n} z_{ij} = \sum_{i=1}^n \sum_{j=1}^n z_{ij} = \sum_{j=1}^n \sum_{i=1}^n z_{ij}.$
2. $\sum_{1 \leq i \leq j \leq n} z_{ij} = \sum_{i=1}^n \sum_{j=i}^n z_{ij} = \sum_{j=1}^n \sum_{i=1}^j z_{ij}.$
3. $\sum_{1 \leq i < j \leq n} z_{ij} = \sum_{i=1}^{n-1} \sum_{j=i+1}^n z_{ij} = \sum_{j=2}^n \sum_{i=1}^{j-1} z_{ij}.$

Démonstration.

Cela revient, à chaque fois, à sommer les éléments du tableau ligne par ligne ou colonne par colonne. $\square$

Remarque 1.2.7.

Par convention, une somme vide est nulle. On peut donc écrire :

$$\sum_{1 \leq i < j \leq n} z_{ij} = \sum_{i=1}^n \sum_{j=i+1}^n z_{ij} = \sum_{j=1}^n \sum_{i=1}^{j-1} z_{ij}.$$

Exercice 1.2.8.

Combien y a-t-il de cases dans un tableau de dimension $n \times n$?

Retrouver cela en calculant $\sum_{1 \leq i, j \leq n} 1.$

Faire de même pour un tableau triangulaire.

1.3 Somme d'une famille finie d'objets

Les définitions précédentes peuvent bien entendu se généraliser comme suit.

Définition 1.3.1.

Soit E, I deux ensembles, une famille $(e_i)_{i \in I}$ d'éléments de E , indexée par I , est un étiquetage d'éléments de E par les éléments de I . Formellement, c'est une application $e : I \rightarrow E$, et l'on note $e_i = e(i)$.

Exemple 1.3.2.

Un n -uplet $(x_1, \dots, x_n) \in \mathbb{R}^n$ est une famille de réels à n éléments, donc indexée par $\llbracket 1, n \rrbracket$. Cela revient à distribuer n étiquettes (portant les numéros 1 à n) parmi l'ensemble des réels. On remarquera qu'un même nombre peut porter plusieurs étiquettes différentes.

Remarque 1.3.3.

L'intérêt des familles par rapport aux n -uplets est multiple. Il permet d'étiqueter des objets par autre chose que des $\llbracket 1, n \rrbracket$, et donc de s'affranchir des contraintes d'ordre et de finitude.

Définition 1.3.4.

Soient I un ensemble **fini** et $(z_i)_{i \in I}$ une famille indexée par I d'objets que l'on peut sommer (par exemple : des nombres, des fonctions, des matrices).

La somme des z_i , pour i parcourant l'ensemble I , est notée

$$\sum_{i \in I} z_i$$

Dans le cas où $I = \emptyset$, on convient que

$$\sum_{i \in \emptyset} z_i = 0,$$

cet objet s'entendant comme le nombre zéro, la fonction nulle, la matrice nulle (en fonction du contexte).

Remarque 1.3.5.

Dans le cas où $I = \llbracket m, n \rrbracket$, où $m, n \in \mathbb{Z}$ sont tels

que $m \leq n$, on la note plus couramment $\sum_{k=m}^n z_k$

ou $\sum_{m \leq k \leq n} z_k$. Elle vaut $z_m + z_{m+1} + z_{m+2} + \dots + z_n$.

Dans le cas où $I = \llbracket m, n \rrbracket \times \llbracket p, q \rrbracket$ où m, n, p et $q \in \mathbb{Z}$ sont tels que $m \leq n$ et $p \leq q$, on la note plus couramment $\sum_{m \leq k \leq n, p \leq \ell \leq q} z_{k\ell}$.

Remarque 1.3.6.

On pourrait formellement définir ces symboles par récurrence sur le nombre d'objets sommés.

2 Le symbole produit : $\prod$

Le symbole $\prod$ est au produit ce que le symbole $\sum$ est à la somme.

Définition 2.0.1.

Soient I un ensemble **fini** et $(z_i)_{i \in I}$ une famille de nombres complexes indexée par I . Le produit des z_i , i parcourant l'ensemble I , est noté $\prod_{i \in I} z_i$.

Par convention, un produit vide vaut 1 :

$$\prod_{i \in \emptyset} z_i = 1$$

Remarque 2.0.2.

On restreindra l'écriture de ce symbole aux familles finies de nombres, ou éventuellement aux fonctions à valeurs numériques.

Nous verrons en effet que le produit matriciel n'est pas commutatif, l'écriture $\prod_{i=1}^n A_i$ n'a dès lors plus grand sens lorsqu'on l'applique à des matrices $A_1, \dots, A_n$.

Définition 2.0.3 (Factorielle).

Pour tout $n \in \mathbb{N} \setminus \{0\}$ (noté aussi $\mathbb{N}^\times$ ou $\mathbb{N}^*$), on appelle *factorielle* n , notée $n!$ le nombre

$$n! = \prod_{k=1}^n k = 1 \times 2 \times 3 \dots \times n.$$

Par convention, $0! = 1$.

Exemple 2.0.4.

Il est bon de connaître les 5 ou 6 premières factorielles : $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$ et $6! = 720$.

Les nombres factoriels vérifient la relation de récurrence suivante.

Proposition 2.0.5.

Pour tout $n \in \mathbb{N}$, $(n+1)! = (n+1) \times n!$.

Démonstration.

Immédiat. □

Théorème 2.0.6 (Simplification télescopique).

Soit $(z_k)_{m \leq k \leq n+1}$ une famille de nombres complexes non nuls. Alors : $\prod_{k=m}^n \frac{z_{k+1}}{z_k} = \frac{z_{n+1}}{z_m}$.

Il y a pour les produits l'exact analogue du théorème 1.2.6 pour les sommes, et la démonstration est elle aussi analogue.



En général on ne peut pas permuter les $\sum$ et les $\prod$. Par exemple, calculer $\sum_{i=1}^3 \prod_{j=1}^2 1$ et

$$\prod_{j=1}^2 \sum_{i=1}^3 1.$$

3 Quelques formules à connaître

3.1 Sommes classiques

Théorème 3.1.1.

Soit n un entier naturel. Alors

1. $\sum_{k=0}^n 1 = n+1$;
2. $\sum_{k=0}^n k = \frac{n(n+1)}{2}$;
3. $\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}$.

Démonstration.

Les trois se démontrent facilement par récurrence. Par curiosité et pour s'entraîner, voici deux autres démonstrations :

2. On note $S_n = \sum_{k=0}^n k$. On fait un changement d'indice :

$$S_n = \sum_{k=0}^n (n-k) \text{ et on développe : } S_n = \sum_{k=0}^n n -$$

$$\sum_{k=0}^n k = n(n+1) - S_n, \text{ d'où } 2S_n = n(n+1).$$

3. On note $S'_n = \sum_{k=0}^n k^2$. Pour tout $k \in \llbracket 0, n \rrbracket$, on a :

$(k+1)^3 - k^3 = 3k^2 + 3k + 1$. On somme tout ça de 0 à n , et on obtient, après simplification télescopique du membre de gauche : $(n+1)^3 = 3S'_n + 3\frac{n(n+1)}{2} + n+1$. Ça se simplifie pour donner le résultat voulu. $\square$

Remarque 3.1.2.

On pourrait montrer de la même manière que si $a, b \in \mathbb{Z}$ tels que $a \leq b$, alors

$$\sum_{k=a}^b k = \frac{(b-a+1)(a+b)}{2}$$

On pourra remarquer cette somme correspond bien au nombre de termes de la somme, fois la moyenne du plus petit et du plus grand élément.

On pourrait la calculer de la manière suivante :

$$\begin{aligned} \sum_{k=a}^b k &= \sum_{k=0}^{b-a} (a+k) \\ &= a(b-a+1) + \sum_{k=0}^{b-a} k \\ &= a(b-a+1) + \frac{(b-a)(b-a+1)}{2} \\ &= \frac{(b-a+2a)(b-a+1)}{2} \end{aligned}$$

Il n'est toutefois par nécessaire de retenir cette formule : vous saurez la retrouver au besoin.

3.2 Coefficients binomiaux

Définition 3.2.1 (Coefficients binomiaux).

Soit $(n, k) \in \mathbb{N}^2$ tels que $k \leq n$. On appelle *coefficient binomial*, aussi lu « k parmi n », le réel noté

$$\binom{n}{k} \text{ valant } \frac{n!}{k!(n-k)!}.$$

On étend cette définition à tout $(n, k) \in \mathbb{N} \times \mathbb{Z}$ en posant $\binom{n}{k} = 0$ pour $k > n$ ou $k < 0$.

Remarque 3.2.2.

On utilisera souvent :

$$\binom{n}{k} = \frac{\prod_{i=n-k+1}^n i}{\prod_{j=1}^k j} = \frac{n \times (n-1) \times \cdots \times (n-k+1)}{k \times (k-1) \times \cdots \times 1}.$$

Théorème 3.2.3 (Formule du triangle de Pascal).

Soit $(n, k) \in \mathbb{N}^* \times \mathbb{Z}$. Alors

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Démonstration.

Se fait par un calcul direct. $\square$

Remarque 3.2.4.

Cette formule permet de calculer par récurrence tous les coefficients binomiaux, en les représentant par exemple dans le triangle de Pascal.

Corollaire 3.2.5.

Soit $(n, k) \in \mathbb{N} \times \mathbb{Z}$, $\binom{n}{k}$ est un entier.

Démonstration.

La démonstration se fait par récurrence sur n , avec l'hypothèse : « $\forall k \in \llbracket 0, n \rrbracket$, $\binom{n}{k}$ est un entier », en utilisant la formule de Pascal pour l'hérédité. $\square$

Proposition 3.2.6.

Soit $n \in \mathbb{N}$ et $k \in \mathbb{Z}$, alors $\binom{n}{k}$ est égal au nombre de manières de choisir k éléments dans un ensemble de n éléments.

Si E est un ensemble à n éléments, alors E possède exactement $\binom{n}{k}$ parties possédant chacune exactement k éléments.

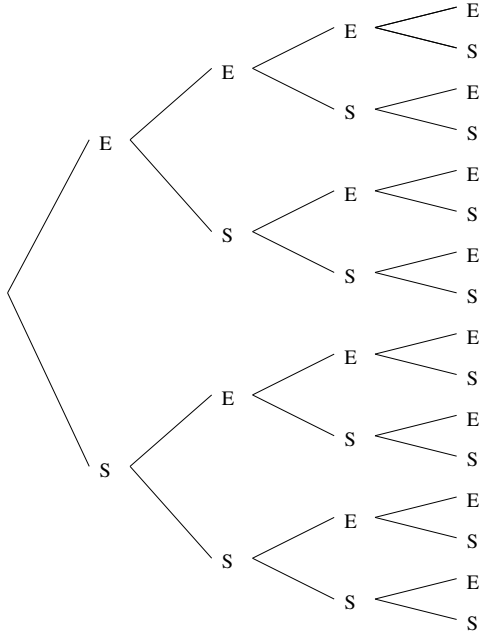


FIGURE III.1 – Chemins des succès et échecs pour 4 répétitions d’une expérience

Démonstration.

Cela sera démontré dans le cours de dénombrement, au second semestre. $\square$

Proposition 3.2.7.

Soit $n \in \mathbb{N}^*$ et $k \in \llbracket 0, n \rrbracket$. On a $\binom{n}{k} = \binom{n}{n-k}$.

Démonstration.

Remarquer que $k = n - (n - k)$! $\square$

Remarque 3.2.8.

Sur un arbre représentant les répétitions d’une même expérience aléatoire, le coefficient binomial k parmi n compte le nombre de chemins réalisant k succès pour n répétitions. En particulier, c’est un entier.

La figure 1 illustre le calcul de ces coefficients pour 4 répétitions.

La formule suivante n’est pas exigible mais est fort utile.

0 succès et 4 échecs

1 succès et 3 échecs

1 succès et 3 échecs

2 succès et 2 échecs

1 succès et 3 échecs

2 succès et 2 échecs

2 succès et 2 échecs

3 succès et 1 échec

1 succès et 3 échecs

2 succès et 2 échecs

2 succès et 2 échecs

3 succès et 1 échec

2 succès et 2 échecs

3 succès et 1 échec

3 succès et 1 échec

4 succès et 0 échec

Proposition 3.2.9.

Soit $n \in \mathbb{N}^*$ et $0 < k \leq n$, alors

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}.$$

Démonstration.

Facile et laissée en exercice. $\square$

3.3 Binôme de Newton, identités remarquables et sommation géométrique

Théorème 3.3.1 (Formule du binôme de Newton).

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. On a :

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Démonstration.

On le démontre par récurrence sur n , après avoir fixé a et b .

Pour $n = 0$, c’est évident :

$$(a + b)^0 = 1 = \sum_{k=0}^0 \binom{0}{k} a^k b^0.$$

Soit $n \in \mathbb{N}$, supposons la formule du binôme au rang n . Alors,

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= a(a + b)^n + b(a + b)^n \\ &= a \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \end{aligned}$$

On écrit alors, avec un décalage d’indice, la première somme

$$\sum_{k=0}^{n-1} \binom{n}{k+1-1} a^{k+1} b^{n+1-(k+1)} + a^{n+1} = \sum_{k=1}^n \binom{n}{k-1} a^k b^{n+1-k} + a^{n+1}$$

De même, la seconde somme s’écrit :

$$b^{n+1} + \sum_{k=1}^n \binom{n}{k} a^k b^{n+1-k}.$$

On a donc, en utilisant la formule du triangle de Pascal,

$$\begin{aligned}
 (a+b)^{n+1} &= b^{n+1} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] a^k b^{n+1-k} \\
 &\quad + a^{n+1} \\
 &= \binom{n+1}{0} b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n+1-k} \\
 &\quad + \binom{n+1}{n+1} a^{n+1} \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
 \end{aligned}$$

On peut donc conclure par récurrence. $\square$

Corollaire 3.3.2.

Soit $n > 0$. $\sum_{k=0}^n \binom{n}{k} = 2^n$ et $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.

Théorème 3.3.3.

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. Alors :

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

Démonstration.

On développe, il apparaît une simplification télescopique :

$$\begin{aligned}
 (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1} &= \sum_{k=0}^{n-1} (a-b) a^k b^{n-k-1} \\
 &= \sum_{k=0}^{n-1} a^{k+1} b^{n-(k+1)} - a^k b^{n-k} \\
 &= a^n - b^n
 \end{aligned}$$

$\square$

Corollaire 3.3.4 (HP).

Soient $n \in \mathbb{N}$ et $a, b \in \mathbb{C}$. Alors,

$$a^{2n+1} + b^{2n+1} = (a+b) \sum_{k=0}^{2n} (-1)^k a^k b^{2n-k}.$$

Démonstration.

$a^{2n+1} + b^{2n+1} = a^{2n+1} - (-b)^{2n+1}$ et on utilise le théorème précédent. $\square$

Corollaire 3.3.5 (Formule de sommation géométrique).

Soient $n \in \mathbb{N}$ et $z \in \mathbb{C}$. Alors,

$$\sum_{k=0}^{n-1} z^k = \begin{cases} \frac{z^n - 1}{z - 1} & \text{si } z \neq 1 \\ n & \text{si } z = 1 \end{cases}.$$

Démonstration.

• Si $z = 1$: on somme n fois 1.

• Sinon, $z^n - 1 = z^n - 1^n = (z-1) \sum_{k=0}^{n-1} z^k 1^{n-1-k} =$

$$(z-1) \sum_{k=0}^{n-1} z^k.$$

$\square$

Remarque 3.3.6.

Si $p \leq n$ sont deux entiers relatifs, et si $z \in \mathbb{C} \setminus \{1\}$, on a

$$\begin{aligned}
 \sum_{k=p}^n z^k &= z^p \sum_{k=p}^n z^{k-p} \\
 &= z^p \sum_{k=0}^{n-p} z^k \\
 &= z^p \times \frac{z^{n-p+1} - 1}{z - 1} \\
 &= \frac{z^{n+1} - z^p}{z - 1}.
 \end{aligned}$$



La formule de sommation géométrique revient très souvent (c'est la formule que nous utiliserons le plus cette année), mais rarement avec les mêmes indice de début et de fin. Il faut donc être extrêmement vigilant quant à ces deux indices et bien penser à factoriser par le premier terme pour revenir à une somme partant de l'indice zéro.

4 Systèmes linéaires et pivot de Gauss

4.1 Définitions

Définition 4.1.1.

On appelle *système linéaire à n équations et p inconnues* tout système de la forme :

$$\begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + \dots + a_{np}x_p = b_n \end{cases}$$

où les a_{ij} et les b_i sont dans $\mathbb{K}$, et les x_i sont les inconnues.

On dit que le système est *compatible* s'il admet une solution.

Le *système homogène associé* est le système :

$$\begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = 0 \\ \vdots \\ a_{n1}x_1 + \dots + a_{np}x_p = 0 \end{cases}$$

Dans la suite nous noterons S le premier système et S_H son système homogène associé, et nous noterons Sol et Sol_H leurs ensembles de solutions respectifs.

4.2 Interprétation géométrique

a Dans le plan

Si $p = 2$, chaque ligne du système s'interprète comme l'équation d'une droite dans le plan. Chaque droite y est en effet représentée par une équation cartésienne. On « sait » de plus que l'intersection de deux droites est

- soit l'ensemble vide (droites parallèles distinctes) ;
- soit une droite (droites confondues) ;
- soit un point (droites non parallèles).

Ainsi, l'ensemble des solutions est soit vide, soit un point, soit représente une droite.

b Dans l'espace

Si $p = 3$, chaque ligne du système s'interprète comme l'équation d'un plan dans l'espace. Chaque plan y est en effet représenté par une équation

cartésienne. On « sait » de plus que l'intersection de deux plans est

- soit l'ensemble vide (plans parallèles distincts) ;
- soit un plan (plans confondus) ;
- soit une droite (plans non parallèles).

De plus, on « sait » que l'intersection d'un plan et d'une droite est

- soit l'ensemble vide (droite parallèle au plan, non incluse dedans) ;
- soit une droite (droite incluse dans le plan) ;
- soit un point (droite non parallèle au plan).

Ainsi, l'ensemble des solutions est soit vide, soit un point, soit représente une droite, soit représente un plan.

4.3 Opérations sur les lignes d'un système

Définition 4.3.1.

On dit que deux systèmes linéaires sont *équivalents* s'ils ont le même ensemble de solutions.

Si i et j sont deux indices différents compris entre 1 et n , et λ est un scalaire, on note :

- $L_i \leftrightarrow L_j$ l'opération consistant à échanger les $i^{\text{ème}}$ et $j^{\text{ème}}$ lignes du système S ;
- $L_i \leftarrow \lambda L_i$ l'opération consistant à multiplier par λ la $i^{\text{ème}}$ ligne du système ;
- $L_i \leftarrow L_i + \lambda L_j$ l'opération consistant à ajouter la $j^{\text{ème}}$ ligne multipliée par λ à la $i^{\text{ème}}$ ligne du système.



Il faut effectuer ces opérations sur toute la ligne du système sans oublier le membre de droite.

Exemple 4.3.2.

Donner des exemples.

Théorème 4.3.3.

- Le système obtenu à partir de S après avoir effectué une opération $L_i \leftrightarrow L_j$ ou une opération $L_i \leftarrow L_i + \lambda L_j$ est encore équivalent à S .

• **Si $\lambda \neq 0$** , alors le système obtenu à partir de S après avoir effectué une opération $L_i \leftarrow \lambda L_i$ est encore équivalent à S .

Démonstration.

Si l'on a effectué $L_i \leftrightarrow L_j$, il suffit de la réeffectuer pour revenir au système de départ.

Si l'on a effectué $L_i \leftarrow L_i + \lambda L_j$, il suffit d'effectuer $L_i \leftarrow L_i - \lambda L_j$ pour revenir au système de départ.

Si $\lambda \neq 0$ et si l'on a effectué $L_i \leftarrow \lambda L_i$, il suffit d'effectuer $L_i \leftarrow \lambda^{-1} L_i$ pour revenir au système de départ. $\square$

4.4 Algorithme du pivot

L'idée du pivot de Gauss pour résoudre un système est de se ramener à un système simple à résoudre, grâce à une succession d'opérations sur les lignes. Ainsi, l'on se ramène d'abord à un système triangulaire (processus d'*élimination*), puis, si cela est possible, à un système diagonal (processus de *remontée*).

Pour étudier d'abord les cas les plus simples et finir par le cas général, étudions ces étapes à rebours.

a Cas d'un système diagonal

On dit que le système S est *diagonal* si pour tout $i, j \in \llbracket 1, n \rrbracket$, $i \neq j \Rightarrow a_{ij} = 0$. Dans ce cas le système se résout de manière immédiate.

Exemple 4.4.1.

Résoudre les systèmes $\begin{cases} x & = 2 \\ 2y & = 1 \\ z & = -2 \end{cases}$ et

$$\begin{cases} x & = 2 \\ 0 & = 1 \\ z & = -2 \end{cases}.$$

On remarque que s'il n'y a aucun zéro sur la diagonale, il y a une unique solution, sinon il n'y a aucune solution, ou une infinité de solutions.

b Cas d'un système triangulaire inversible

Un cas un peu plus compliqué est celui où le système est *triangulaire supérieur*, c'est-à-dire lorsque pour tout $i, j \in \llbracket 1, n \rrbracket$, $i > j \Rightarrow a_{ij} = 0$. Nous ne traiterons pour l'instant que le cas où le système n'a aucun zéro sur la diagonale : pour

tout $i \in \llbracket 1, n \rrbracket$, $a_{ii} \neq 0$. On dit alors que le système est *inversible*.

Le système a donc cette allure :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots + \dots = \dots \\ \dots + \dots = \dots \\ a_{n-1,n-1}x_{n-1} + a_{n-1,n}x_n = b_{n-1} \\ a_{nn}x_n = b_n \end{cases}$$

On obtient alors facilement :

$$x_n = \frac{b_n}{a_{nn}}$$

puis

$$x_{n-1} = \frac{b_{n-1} - a_{n-1,n}x_n}{a_{n-1,n-1}}$$

et, par récurrence (descendante),

$$b_k - \sum_{i=k+1}^n a_{k,i}x_i$$

pour tout $k \in \llbracket 1, n-1 \rrbracket$, $x_k = \frac{a_{k,k}}{a_{k,k}}$.

Ces relations permettent de calculer les x_k par récurrence.

Nous pouvons également appliquer une succession d'opérations sur les lignes du système pour se ramener de manière équivalente à un système diagonal.

Ce processus est parfois appelé principe de *remontée* car l'on y fait apparaître des zéros dans le haut de la matrice du système, en partant des lignes du bas.

Cette méthode peut être présentée en utilisant une suite de systèmes équivalents.

Il existe une présentation plus visuelle et plus rapide à rédiger. Par exemple, considérons le système

$$\begin{cases} x + y - z = 2 \\ -2y + z = 1 \\ -z = 3 \end{cases}.$$

Nous pouvons l'écrire

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 2 \\ 0 & -2 & 1 & 1 \\ 0 & 0 & -1 & 3 \end{array} \right).$$

Les opérations à effectuer sont alors bien visibles : dans un premier temps, nous allons faire apparaître des zéros dans toute la dernière colonne de la partie de gauche du système, sauf à la dernière ligne. Pour cela, effectuons les opérations $L_1 \leftarrow L_1 - L_3$ et $L_2 \leftarrow L_2 + L_3$, et nous obtenons (sans oublier d'effectuer également ces opérations sur la partie de droite du système !)

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & -1 \\ 0 & -2 & 0 & 4 \\ 0 & 0 & -1 & 3 \end{array} \right)$$

ce qui correspond au système

$$\begin{cases} x + y & = & -1 \\ & -2y & = & 4 \\ & & -z & = & 3 \end{cases}$$

équivalent au premier. Ensuite, nous effectuons l'opération $L_1 \leftarrow L_1 + \frac{1}{2}L_2$. Ou plutôt, pour simplifier dès à présent la deuxième ligne et obtenir la valeur de y , nous pouvons effectuer $L_2 \leftarrow -\frac{1}{2}L_2$, et ensuite $L_1 \leftarrow L_1 - L_2$, ce qui donne

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & -1 & 2 \end{array} \right)$$

ce qui correspond au système

$$\begin{cases} x & = & 1 \\ y & = & -2 \\ -z & = & 3 \end{cases}$$

qui est bien diagonal. Il vient alors directement

$$\begin{cases} x & = & 1 \\ y & = & -2 \\ z & = & -3 \end{cases}.$$

Exercice 4.4.2.

Résoudre le système

$$\begin{cases} x + 2y + 4t & = & 2 \\ & -2y + 3z & = & -1 \\ & & z - 2t & = & 3 \\ & & & -t & = & 1 \end{cases}.$$

Exercice 4.4.3.

Résoudre, en fonction de la valeur du paramètre p , le système

$$\begin{cases} x + 2y & = & 2 \\ & py & + 3z & = & -1 \\ & & p(p-1)z & = & 3 \end{cases}.$$

c Cas d'un système triangulaire non inversible

S'il y a un zéro sur la diagonale d'un système triangulaire, ce dernier est dit *non inversible*. On obtient un certain nombre de lignes de la forme $0 = c_i$, où les c_i sont des constantes. Si un de ces c_i est non nul, le système n'admet pas de solution, sinon, des lignes se simplifient.

Nous n'évoquerons ce cas que lorsque $p \leq 3$ et $n \leq 3$.

Les solutions du système s'interprètent simplement en termes géométriques.

- si $p = 2$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite du plan, soit le plan tout entier.

Exemple 4.4.4.

Résoudre les systèmes :

$$\begin{aligned} 1. & \begin{cases} y & = & 2 \\ y & = & 1 \end{cases} \\ 2. & \begin{cases} x + y & = & 2 \\ & 2y & = & 1 \end{cases} \end{aligned}$$

- si $p = 3$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite de l'espace, soit un plan de l'espace, soit l'espace tout entier.

Exemple 4.4.5.

Résoudre les systèmes :

$$\begin{aligned} 1. & \begin{cases} x + y + z & = & 1 \\ & z & = & 2 \\ & z & = & 1 \end{cases} \\ 2. & \begin{cases} x + y + z & = & 1 \\ & y + z & = & 2 \\ & z & = & 1 \end{cases} \end{aligned}$$

d Systèmes échelonnés

Nous généralisons ici le cas précédent, quand la matrice du système n'est pas carrée.

Le système S est dit échelonné de rang $r \in \{0, 1, \dots, \min(n, p)\}$ s'il est de la forme :

$$\begin{cases} a_{i_1, i_1} x_{i_1} + \dots & = & b_{i_1} \\ & a_{i_2, i_2} x_{i_2} + \dots & = & b_{i_2} \\ & & \ddots & \\ & & & a_{i_r, i_r} x_{i_r} + \dots & = & b_{i_r} \end{cases}$$

où $1 \leq i_1 < i_2 < \dots < i_r \leq p$ et les coefficients $a_{i_1, i_1}, \dots, a_{i_r, i_r}$ sont tous non nuls.

Chacune des premières lignes s'interprète comme l'équation d'un « hyperplan » de dimension $p-1$ dans $\mathbb{K}^p$. Le système possède une unique solution si et seulement si $r = p$ et une infinité de solutions si et seulement si $r < p$.

Nous n'évoquerons ce cas que lorsque $p \leq 3$ et $n \leq 3$.

Les solutions du système s'interprètent simplement en termes géométriques.

- si $p = 2$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite du plan, soit le plan tout entier.

Exemple 4.4.6.

Résoudre les systèmes :

1.
$$\begin{cases} x + y = 2 \\ 0 = 1 \end{cases}$$
2. $x + y = 1$

- si $p = 3$, l'ensemble des solutions est soit vide, soit un singleton, soit une droite de l'espace, soit un plan de l'espace, soit l'espace tout entier.

Exemple 4.4.7.

Résoudre les systèmes :

1.
$$\begin{cases} x + y + z = 1 \\ y + z = 2 \end{cases}$$
2. $x + y + z = 1$

e Cas général

Nous allons maintenant voir la méthode d'élimination qui permet de se ramener à un système échelonné.

Dans le système de départ, choisissons une ligne, et une variable. Le but est d'éliminer cette variable dans les autres lignes. Il est donc souvent intéressant de choisir une variable qui apparaît dans un minimum de lignes, comme cela une partie du travail est déjà fait.

Si la variable choisie est x et que la ligne conservée L est de la forme $ax + by + \dots$ et que l'on veuille éliminer x d'une ligne L' de la forme $cx + dy + \dots$, il suffit d'effectuer l'opération $L' \leftarrow L' - \frac{c}{a}L$. La ligne L' devient alors $(d - \frac{bc}{a})y + \dots$.

Après avoir éliminé la variable choisie dans toutes

les lignes sauf celle conservée, on ne touche plus à cette dernière ligne, et on réitère le procédé avec les lignes restantes, en choisissant une autre variable. On continue jusqu'à ce que le système soit triangulaire ou trivialement sans solution.

Exemple 4.4.8.

Considérons le système
$$\begin{cases} x + y + z = 1 \\ x - 2y + z = 2 \\ 2x \quad \quad -z = 1 \end{cases}$$

que l'on écrira sous forme matricielle
$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & -2 & 1 & 2 \\ 2 & 0 & -1 & 1 \end{array} \right).$$
 Puisque y n'apparaît

pas dans la dernière ligne, choisissons d'éliminer y dans les deux premières lignes. Afin d'éviter de manipuler des fractions, nous choisissons de conserver la première ligne, car le coefficient devant y y est 1.

Effectuons l'opération $L_2 \leftarrow L_2 + 2L_1$: le système est donc équivalent à
$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 3 & 0 & 3 & 4 \\ 2 & 0 & -1 & 1 \end{array} \right).$$

On choisit ensuite d'éliminer z de la seconde ligne en utilisant la dernière ligne, car la variable z y a un coefficient égal à -1 . Après l'opération

$L_2 \leftarrow L_2 + 3L_3$, il vient :
$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 9 & 0 & 0 & 7 \\ 2 & 0 & -1 & 1 \end{array} \right).$$

Le système obtenu n'a pas l'air très triangulaire ... en fait il l'est si on le réécrit
$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & -1 & 2 \\ 0 & 0 & 9 \end{array} \right) \begin{pmatrix} y \\ z \\ x \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 7 \end{pmatrix},$$
 ce qui revient à faire des échanges de lignes et de variables dans le dernier système obtenu.

Il vient finalement
$$\begin{cases} x = \frac{7}{9} \\ y = -\frac{1}{3} \\ z = \frac{5}{9} \end{cases}.$$

Exemple 4.4.9.

Considérons le système
$$\begin{cases} x + y + z = 1 \\ x - 2y + z = 2 \\ 2x + y - z = 1 \\ \quad \quad 2y + z = 2 \end{cases}.$$

Codons-le et exécutons l'algorithme du pivot. Il

vient successivement :

$$\begin{pmatrix} 1 & 1 & 1 & \big| & 1 \\ 1 & -2 & 1 & \big| & 2 \\ 2 & 1 & -1 & \big| & 1 \\ 0 & 2 & 1 & \big| & 2 \end{pmatrix} \begin{array}{l} L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_3 - 2L_1 \end{array} \quad (\text{III.1})$$

$$\begin{pmatrix} 1 & 1 & 1 & \big| & 1 \\ 0 & -3 & 0 & \big| & 1 \\ 0 & -1 & -3 & \big| & -1 \\ 0 & 2 & 1 & \big| & 2 \end{pmatrix} \begin{array}{l} L_3 \leftarrow L_3 + 3L_4 \end{array} \quad (\text{III.2})$$

$$\begin{pmatrix} 1 & 1 & 1 & \big| & 1 \\ 0 & -3 & 0 & \big| & 1 \\ 0 & 5 & 0 & \big| & 5 \\ 0 & 2 & 1 & \big| & 2 \end{pmatrix} \quad (\text{III.3})$$

Or les deuxième et troisième lignes sont contradictoires, donc le système n'a pas de solution.

Chapitre IV

Quelques fondamentaux

Sommaire

1 Propositions.	66	b	n valeurs sont égales	78
2 Connecteurs logiques.	66	c	Toutes les puissances valent 1	79
2.1 Négation.	66			
2.2 Conjonction « et » et disjonction « ou ».	66			
2.3 Implication.	67			
2.4 Équivalence.	68			
3 Quantificateurs universel et existentiel.	69			
3.1 Définition.	69			
3.2 Permutation de quantificateurs.	70			
3.3 Négation d'un quantificateur.	71			
3.4 Le pseudo-quantificateur $\exists!$.	71			
3.5 Quantificateurs et inégalités.	71			
4 Raisonnements par récurrence.	71			
4.1 Principe du minimum.	72			
4.2 Principe de récurrence simple.	72			
4.3 Erreurs classiques.	73			
4.4 Bonne définition d'une suite définie par récurrence.	74			
4.5 Récurrence double.	75			
a Exemple : suite définie par récurrence.	75			
b Énoncé du principe.	75			
c Rédaction par récurrence double.	75			
4.6 Récurrence triple, etc.	75			
4.7 Récurrence forte.	76			
a Exemple : suite définie par récurrence.	76			
b Énoncé du principe.	76			
c Rédaction par récurrence forte.	76			
4.8 Méthodologie : choix du type de récurrence.	77			
4.9 Récurrence à partir d'un certain rang.	77			
4.10 Récurrence sur un intervalle fini d'entiers	77			
4.11 Récurrence descendante	77			
4.12 Quelques récurrences fausses.	78			
a Suite négative minorée par un réel positif.	78			

1 Propositions.

Définition 1.0.1.

Une *proposition* est un énoncé qui peut prendre deux valeurs de vérité : « vrai » (V) ou « faux » (F).

Exemple 1.0.2.

- $2 > 7$
- Pour tout nombre réel x , il existe un entier n tel que $n \leq x < n + 1$.

2 Connecteurs logiques.

Définition 2.0.1.

Un **connecteur logique** est un outil mathématique permettant de construire une proposition à partir d'une ou plusieurs propositions.

Définition 2.0.2.

La *table de vérité* d'une proposition construite à partir de connecteurs logiques est la donnée de la valeur de vérité de cette proposition pour chaque jeu de valeur de vérité des propositions prises en argument des connecteurs.

Définition 2.0.3.

Deux propositions sont dites *équivalentes* si elles ont la même table de vérité. On utilise alors le connecteur $\equiv$.

Les paragraphes suivants présentent les connecteurs logiques les plus utilisés en mathématiques.

2.1 Négation.

Définition 2.1.1.

Soit p une proposition. La proposition « non p », notée $\neg p$, est la proposition qui est vraie quand p est fausse, et fausse quand p est vraie. Sa table de vérité est :

p	$\neg p$
V	F
F	V

Théorème 2.1.2 (Loi de la double négation).

Soit p une proposition, p et « non (non p) » sont deux propositions équivalentes, ce qui s'écrit :

$$p \equiv \neg(\neg p).$$

Démonstration.

Avec une table de vérité :

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

□

2.2 Conjonction « et » et disjonction « ou ».

Définition 2.2.1.

Soient p et q deux propositions.

- La *conjonction* de p et q est une proposition dite « p et q » et notée $p \wedge q$, qui est vraie si p et q sont vraies, et qui est fausse sinon.
- La *disjonction* de p et q est une proposition dite « p ou q » et notée $p \vee q$, qui est fausse si p et q sont fausses, et qui est vraie sinon.

Les tables de vérités de ces connecteurs sont donc :

p	q	$p \wedge q$	$p \vee q$
V	V	V	V
F	V	F	V
F	F	F	F
V	F	F	V

Remarque 2.2.2.

Il existe un autre « ou », le « ou exclusif » : si p et q sont deux propositions, la proposition « p ou exclusif q » est vraie si et seulement si p est vraie ou q est vraie, mais pas les deux. Autrement dit,

cette proposition est fausse si et seulement si p et q ont même valeur de vérité.

Dans la vie courante, on utilise intuitivement le ou exclusif. Ex : fromage ou dessert.

Très classique : une logicienne, enceinte, croise un ami.

L'ami : « c'est un garçon ou une fille ? »

La logicienne : « Oui. »

Proposition 2.2.3 (Tiers exclu).

Pour toute proposition p , $p \vee \neg p$ est vraie.

Proposition 2.2.4 (Non contradiction).

Pour toute proposition p , $p \wedge \neg p$ est fausse.

Démonstration.

Écrire les tables de vérités de $p \vee \neg p$ et $p \wedge \neg p$. $\square$

Théorème 2.2.5 (Lois de De Morgan).

Soit p et q deux propositions.

1. $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$.
2. $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$.

Démonstration. 1. Construire les tables de vérité de ces deux propositions et constater que ce sont les mêmes.

2. Par le premier point et la loi de double négation,

$$\begin{aligned} \neg(p \vee q) &\equiv \neg([\neg p] \vee [\neg q]) \\ &\equiv \neg(\neg[(\neg p) \wedge (\neg q)]) \\ &\equiv (\neg p) \wedge (\neg q). \end{aligned}$$

$\square$

Exemple 2.2.6.

- Nier « je n'aime ni le chocolat ni la vanille ».
- Dans $\mathbb{R}^2$, dessiner l'ensemble $\{(x, y) \in \mathbb{R}^2 \mid x < 2 \text{ et } y \leq 3\}$, dessiner et décrire son complémentaire.

Exercice 2.2.7.

Soit $x \in \mathbb{R}$. Nier $1 \leq x < 2$. Quel est le complémentaire dans $\mathbb{R}$ de $[1, 2[$?

Remarque 2.2.8.

Le $\wedge$ et le $\vee$ sont commutatifs et associatifs.

Exercice 2.2.9.

Soit p , q et r trois propositions. À quoi sont logiquement équivalentes $p \wedge (q \vee r)$ et $p \vee (q \wedge r)$?

2.3 Implication.

Définition 2.3.1.

Soient p et q deux propositions. On appelle $p \Rightarrow q$, qui se dit « p implique q », ou « si p alors q », la proposition $(\neg p) \vee q$. Dans l'implication $p \Rightarrow q$, p est l'antécédent, q le conséquent.

Exercice 2.3.2.

Construire la table de vérité de $p \Rightarrow q$.

Remarque 2.3.3.

En pratique, pour démontrer une implication, on commence toujours, bêtement, par « supposons p vraie ». Il faut alors montrer que sous cette hypothèse q est vraie.



- $p \Rightarrow q$ peut être vraie même si p et q n'ont rien à voir. Par exemple : si $1 \geq 0$ alors l'eau mouille.
- $p \Rightarrow q$ est toujours vraie si p est fausse (le faux implique n'importe quoi) ou q est vraie. Ainsi, si « $0 \neq 0$ » alors « $0 = 0$ » (cela peut paraître étonnant, on reviendra dessus à la fin du paragraphe « équivalence »).
- $p \Rightarrow q$ n'implique ni que p est vraie ni que q est vraie. Par exemple : Si les pommes étaient des citrouilles, Newton serait mort assommé. Ou bien : si je mesurais 2 m 20, je serais entraîneur de basket.

Proposition 2.3.4 (Modus Ponens).

Soit p et q deux propositions. Si $p \Rightarrow q$ est vraie et si p est vraie, alors q est vraie.

Autrement dit, $[p \wedge (p \Rightarrow q)] \Rightarrow q$ est toujours vraie.

Démonstration.

Consulter la table de vérité de $p \Rightarrow q$ ou de $[p \wedge (p \Rightarrow q)] \Rightarrow q$. $\square$

Théorème 2.3.5 (Négation d'une implication).

Soit p et q deux propositions, alors $\neg(p \Rightarrow q) \equiv (p \wedge (\neg q))$.

Démonstration.

C'est une conséquence simple de la loi de De Morgan. $\square$

Exemple 2.3.6.

En pratique, pour montrer $p \Rightarrow q$ est fausse on peut trouver un exemple où p est vraie mais où q est fausse.

Ainsi, avoir 18 ans n'implique pas d'avoir droit de vote (ex : si on a casier judiciaire). De même, mesurer 2 m 20 n'implique pas d'être un joueur de basket.

Exercice 2.3.7.

Soit x, y deux réels et $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction. Nier la proposition « $x \leq y \Rightarrow f(x) \geq f(y)$ ».

Théorème 2.3.8 (Contraposition).

Soit p et q deux propositions, alors $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

Démonstration.

C'est une conséquence simple de la loi de double négation. $\square$

Remarque 2.3.9.

On peut formaliser ainsi le principe de « démonstration par l'absurde » : on veut montrer que p est vraie, sachant qu'une certaine proposition q est fausse.

On suppose alors que p est fausse et si l'on arrive à montrer que q est vraie : on a obtenu une contradiction ! En fait on a montré $\neg p \Rightarrow q$, et donc $\neg q \Rightarrow p$. Comme $\neg q$ est vraie, on a p qui est vraie.

Exemple 2.3.10.

Un entier ne peut pas être pair et impair.

Démonstration.

Soit n pair et impair. Alors il existe $k, k' \in \mathbb{Z}$ tels que $n = 2k = 2k' + 1$, donc $k - k' = 1/2$ est un entier, ce qui est absurde. $\square$

Remarque 2.3.11 (Transitivité).

Pour toutes propositions P, Q, R , si $P \Rightarrow Q$ et $Q \Rightarrow R$, alors $P \Rightarrow R$.

2.4 Équivalence.

Définition 2.4.1.

Soient p et q deux propositions. La proposition $p \Leftrightarrow q$, qui se lit « p équivaut à q », est la proposition qui est vraie si et seulement si p et q ont la même valeur de vérité.

Exercice 2.4.2.

Construire la table de vérité de $p \Leftrightarrow q$.

Théorème 2.4.3 (Équivalence et double implication).

Soit p et q deux propositions, alors

$$(p \Leftrightarrow q) \equiv ([p \Rightarrow q] \wedge [q \Rightarrow p])$$

Démonstration.

Il suffit d'écrire les tables de vérités de ces propositions. $\square$

Définition 2.4.4.

$q \Rightarrow p$ est appelée la *réciproque* de $p \Rightarrow q$.

Remarque 2.4.5.

Le $\Leftrightarrow$ est commutatif (si $P \Leftrightarrow Q$, alors $Q \Leftrightarrow P$), transitif (si $P \Leftrightarrow Q$ et $Q \Leftrightarrow R$, alors $P \Leftrightarrow R$) et réflexif (on a toujours $P \Leftrightarrow P$).

Remarque 2.4.6.

En pratique, pour montrer $p \Leftrightarrow q$, il y a 2 méthodes :

1. Montrer $q \Rightarrow p$ puis $p \Rightarrow q$;
2. Montrer $p \Rightarrow q$ puis la contraposée de sa réciproque, *i.e.* $\neg p \Rightarrow \neg q$

On peut bien entendu montrer un schéma du type $p \Leftrightarrow p_1 \Leftrightarrow p_2 \dots \Leftrightarrow q$, où les p_i sont des propositions intermédiaires.

Définition 2.4.7.

Soient p et q deux propositions.

On dit que la proposition p est *nécessaire* pour avoir la proposition q si $q \Rightarrow p$ est vraie.

On dit que la proposition p est *suffisante* pour avoir la proposition q si $p \Rightarrow q$ est vraie.

On dit que la proposition p est *nécessaire et suffisante* pour avoir la proposition q si $q \Leftrightarrow p$ est vraie.

Remarque 2.4.8.

Revenons sur la table de vérité de l'implication.

Intuitivement, si p est vraie et q fausse, $p \Rightarrow q$ est fausse. De même, si p et q sont vraies, on conçoit que $p \Rightarrow q$ le soit.

Dans les deux autres cas, l'intuition se perd. Constatons que si $p \Rightarrow q$ était fausse si p était fausse et q vraie, ou si $p \Rightarrow q$ était fausse si p et q étaient fausses, la table de l'implication serait la même que celle d'une autre connecteur logique déjà connu (construire et identifier les tables de tous les connecteurs possibles de deux propositions pour s'en convaincre).

Exemple 2.4.9.

Montrons que $\sqrt{2} \notin \mathbb{Q}$.

Démonstration.

On montre d'abord que, si n est un entier, alors « n est pair » si et seulement si « n^2 est pair ».

Si n est pair, son reste dans la division euclidienne par 2 est nul : il existe $k \in \mathbb{Z}$ tel que $n = 2k$. Donc $n^2 = 2 \times 2k^2$ est pair.

Si n est impair, son reste dans la division euclidienne par 2 n'est pas nul, donc vaut 1 : il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Donc $n^2 = 2 \times (2k^2 + 2k) + 1$ est impair.

On vient bien de montrer l'équivalence annoncée.

Puis, on suppose que $\sqrt{2} \in \mathbb{Q}$ et l'on écrit $\sqrt{2}$ sous forme fractionnelle irréductible : il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ sans diviseurs communs autres que 1 ou -1 , tels que $\sqrt{2} = \frac{p}{q}$.

On élève au carré : $p^2 = 2q^2$, donc p^2 est pair, donc p aussi. Il existe donc $p' \in \mathbb{Z}$ tel que $p = 2p'$, et l'on a alors $q^2 = 2p'^2$, donc q^2 est pair et q est pair aussi.

Ainsi, p et q ont bien un diviseur non trivial, 2, c'est absurde, donc $\sqrt{2} \notin \mathbb{Q}$. $\square$

Remarque 2.4.10.

Vous remarquerez que les symboles $\Rightarrow$ et $\Leftrightarrow$ n'ont pas été utilisés dans la démonstration précédente. C'est normal : ils servent à construire des phrases formelles, pas à les démontrer. On ne les utilise donc JAMAIS dans une démonstration : à la place, on rédige EN FRANÇAIS, en utilisant par exemple la conjonction de coordination « donc ».

3 Quantificateurs universel et existentiel.

3.1 Définition.

Définition 3.1.1.

On appelle *prédicat* toute proposition dépendant d'une ou plusieurs variables, et qui, pour chaque jeu de valeurs de ces variables, prend la valeur V ou F.

Exemple 3.1.2.

$P(x, y) \equiv x + y = 2$.

Définition 3.1.3.

Si P est un prédicat qui dépend de la variable x et éventuellement d'autres variables, alors $\forall x, P(x)$ et $\exists x, P(x)$ sont deux prédicats qui ne dépendent pas de x et :

- $\forall x, P(x)$ est vrai si, pour toutes les valeurs de x , $P(x)$ est vrai ;
- $\exists x, P(x)$ est vrai s'il existe une valeur de x pour laquelle $P(x)$ est vrai.

$\forall$ est appelé *quantificateur universel* et $\exists$ est le *quantificateur existentiel*.

Remarque 3.1.4.

On spécifiera tout le temps dans les quantificateurs les ensembles sur lesquels sont considérées les variables. On écrira par exemple

$$\forall x \in \mathbb{R}, x^2 \geq 0$$

et

$$\forall a \in \mathbb{R}, \exists n \in \mathbb{Z}, a \geq n.$$

Remarque 3.1.5.

Si P est un prédicat d'une variable, $\forall x, P(x)$ est un prédicat de zéro variables, c'est-à-dire une proposition.

Exemple 3.1.6.

- Soit $P(x, y) \equiv xy = 0$. Alors $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$ est fausse, mais $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$ est vraie.
- Soit $P'(x) \equiv x.0 = 0$: alors $\forall x \in \mathbb{C}, P'(x)$ est vraie.



Les quantificateurs sont des symboles mathématiques utilisés pour construire des phrases mathématiques. Ils ne sont en aucun cas à utiliser au cours d'une démonstration. En pratique :

- Pour montrer que $\forall x \in E, P(x)$ est vraie, on commencera (presque) toujours par écrire « Soit x un élément de E » : x est maintenant fixé (et pris quelconque), on peut maintenant montrer $P(x)$.
- Pour montrer que $\exists x \in E, P(x)$ est vraie, il « suffira » d'exhiber une valeur de x dans E telle que $P(x)$ soit vraie.

Remarque 3.1.7.

Dans les propositions $\forall x, P(x)$ et $\exists x, P(x)$, la variable x est muette. On peut donc remplacer la lettre x par n'importe quelle autre lettre.

Par exemple, $\exists x \in \mathbb{R}, x^2 = -1$ est la même proposition que $\exists \xi \in \mathbb{R}, \xi^2 = -1$ et que $\exists \heartsuit \in \mathbb{R}, \heartsuit^2 = -1$



Les propositions « $\forall x \in E, (P(x) \text{ ou } Q(x))$ » et « $(\forall x \in E, P(x)) \text{ ou } (\forall x \in E, Q(x))$ » ne sont pas équivalentes.

Par exemple, « $\forall x \in \mathbb{R}, (x \geq 0 \text{ ou } x \leq 0)$ » est vraie, mais « $(\forall x \in \mathbb{R}, x \geq 0) \text{ ou } (\forall x \in \mathbb{R}, x \leq 0)$ » ne l'est pas.

Proposition 3.1.8 (Disjonction de cas).

Soit E un ensemble, $E_1, \dots, E_n$ des parties de E vérifiant $E = E_1 \cup \dots \cup E_n$.

Soit P un prédicat défini sur E . Alors

$$\forall x \in E, P(x) \equiv \bigwedge_{i=1}^n (\forall x \in E_i, P(x)).$$

Démonstration.

Admis. □

Remarque 3.1.9.

On peut aussi retrouver le raisonnement par disjonction de cas dans d'autres situations.

Exercice 3.1.10.

Montrer que pour tout $n \in \mathbb{Z}$, $n^2 - 3n + 2$ est pair.

Remarque 3.1.11 (Analyse-synthèse).

Soit E un ensemble et P un prédicat défini sur E . On demande parfois de résoudre ce problème, c'est-à-dire de déterminer $\{x \in E \mid P(x)\}$, i.e. de déterminer la partie F de E telle que

$$\forall x \in E, P(x) \Leftrightarrow x \in F.$$

Pour cela, on raisonne souvent par analyse-synthèse.

Analyse On commence par prendre un $x \in E$ quelconque, puis on suppose $P(x)$. On « travaille » ensuite pour obtenir un ensemble F' le plus petit possible pour lequel $x \in F'$.

Synthèse On prend $x \in F'$, et l'on vérifie si $P(x)$. On procède souvent ici par disjonction de cas.

La phase d'analyse est parfois appelée « raisonnement par condition nécessaire », et celle de synthèse « raisonnement par condition suffisante ».

Il arrivera souvent, mais pas toujours, que l'on obtienne $F' = F$ à la fin de la phase d'analyse.

Exercice 3.1.12.

Résoudre sur $\mathbb{R}$ l'équation

$$\sqrt{x-1} = x - |x-3|.$$

3.2 Permutation de quantificateurs.

Proposition 3.2.1.

On peut permuter les $\forall$ entre eux et les $\exists$ entre eux.

Démonstration.

Admis. □

Remarque 3.2.2.

On abrégera parfois $\forall x \in E, \forall y \in E, P(x, y)$ en $\forall x, y \in E, P(x, y)$. C'est aussi équivalent à $\forall (x, y) \in E^2, P(x, y)$.

Exemple 3.2.3.

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}, x.y \geq 0 \equiv \forall y \in \mathbb{N}, \forall x \in \mathbb{N}, x.y \geq 0$$

0

$$\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, x + y \leq 0 \equiv \exists y \in \mathbb{R}, \exists x \in \mathbb{R}, x + y \leq 0$$


On ne peut en général pas permuter un $\forall$ et un $\exists$.

Exemple 3.2.4.

Comparer les propositions : « pour toute poule il existe un oeuf d'où est sortie la poule » et « il existe un oeuf d'où sont sorties toutes les poules ».

Exercice 3.2.5.

Donner un exemple formel du dernier point.

3.3 Négation d'un quantificateur.**Proposition 3.3.1.**

Soit P un prédicat.

1. La négation de $\forall x, P(x)$ est $\exists x, \neg P(x)$.
2. La négation de $\exists x, P(x)$ est $\forall x, \neg P(x)$.

Démonstration.

Admis. □

- En pratique, il faut savoir nier une phrase avec des $\forall$ et $\exists$.

Exemple 3.3.2.

$\forall x \in \mathbb{R}, \exists y \in \mathbb{Z}$ tel que $x \leq y$ se nie en $\exists x \in \mathbb{R}$ tel que $\forall y \in \mathbb{Z}, x > y$.

Exercice 3.3.3.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$. Écrire de manière quantifiée la phrase « f est monotone » puis la nier.

3.4 Le pseudo-quantificateur $\exists!$.

Pour simplifier la rédaction, il existe le pseudo-quantificateur $\exists!$. La proposition $\exists! x, P(x)$ signifie : il existe un unique x tel que $P(x)$. Pour démontrer une telle proposition, il faut montrer d'un côté la partie existence, et d'un autre côté la partie unicité.

Exercice 3.4.1.

Écrire $\exists! x, P(x)$ en n'utilisant que les symboles $\forall$ et $\exists$.

Remarque 3.4.2.

On vous pose souvent des questions du type « montrer qu'il existe un unique objet vérifiant une propriété ». Pour cela, il convient souvent de raisonner par analyse-synthèse. La phase d'analyse montre l'unicité, la phase de synthèse l'existence.

Exercice 3.4.3.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$. Montrer qu'il existe un unique couple (g, h) tel que :

- $g : \mathbb{R} \rightarrow \mathbb{R}$ vérifie $g(42) = 1515$;
- h est une fonction linéaire (il existe $\lambda \in \mathbb{R}$ vérifiant $h : x \mapsto \lambda x$) ;
- $f = g + h$.

3.5 Quantificateurs et inégalités.

On commet souvent un abus d'écriture, notamment en analyse, en raccourcissant la phrase

$$\forall x \in \mathbb{R}, [x \geq M \Rightarrow P(x)]$$

en

$$\forall x \geq M, P(x).$$

Dans la deuxième écriture, la quantification porte implicitement sur x et non sur M (qui doit avoir été fixé ou quantifié auparavant). De plus, le domaine de P n'est plus explicitement défini.

Exemple 3.5.1.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres réels, la proposition « $u_n \xrightarrow[n \rightarrow +\infty]{} +\infty$ » (qui se lit « (u_n) tend vers $+\infty$ ») s'écrit formellement

$$\forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \geq A,$$

mais on l'écrit plutôt

$$\forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, u_n \geq A.$$

4 Raisonnements par récurrence.

L'objectif de cette partie est de montrer comment rédiger une récurrence, à partir d'exemples, en présentant en particulier quelques erreurs courantes, mais aussi de présenter une autre technique de démonstration, extrêmement puissante, appelée principe du minimum.

Il y a plusieurs façons possibles de rédiger une récurrence. Néanmoins l'expérience montre que les étudiants qui essaient de l'écrire de façon originale l'écrivent rarement correctement.

En d'autres termes : nous vous conseillons *très fortement* de suivre les modèles donnés ici, mais vous êtes absolument libres de ne pas suivre les conseils ci-dessous. Pour mémoire, dans 9 cas sur dix, ceux qui n'ont pas suivi le modèle donné ici rédigent mal leurs raisonnements par récurrence et perdent en conséquence les points correspondants dans leurs DS.

Pour fixer les idées, nous travaillerons essentiellement sur des exemples, et parfois sur des exemples très simples.

4.1 Principe du minimum.

Définition 4.1.1.

Soit E un ensemble de réels. On appelle *minimum* de E , tout réel x vérifiant $x \in E$ et $\forall y \in E \quad x \leq y$.

- Remarque 4.1.2.** 1. Certains ensembles de réels n'admettent pas de minimum. Exemples : $]0, 1]$, $\mathbb{R}$, $\mathbb{R}_+^*$, $\mathbb{R}_-$.
2. Tout ensemble de réels admet **au plus** un minimum.

Lorsqu'il existe, le minimum d'un ensemble E est noté $\min(E)$.

L'ensemble des entiers naturels possède la propriété fondamentale suivante que l'on admettra :

Proposition 4.1.3.

Tout ensemble E d'entiers naturels non vide admet un minimum.

Remarque 4.1.4.

Pour tout ensemble d'entiers naturels E , on a

$$\forall x \in \llbracket 0, \min(E) \rrbracket \quad x \notin E.$$

Corollaire 4.1.5.

Tout sous-ensemble de $\mathbb{Z}$ minoré (resp. majoré) non vide admet un minimum (resp. maximum).

Proposition 4.1.6 (Principe du minimum).

Soit P un prédicat sur les entiers naturels. Supposons qu'il existe au moins un entier rendant faux le prédicat P . Alors l'ensemble des entiers naturels sur lesquels P est faux admet un plus petit élément n_0 et on a

1. $\text{non}(P(n_0))$,
2. et $\forall n \in \llbracket 0, n_0 \rrbracket \quad P(n)$.

Exercice 4.1.7.

Soit N un entier non nul et $a_0, a_1, \dots, a_N$ des réels. On pose

$$f: \mathbb{R} \rightarrow \mathbb{R} \quad x \mapsto \sum_{k=0}^N a_k x^k.$$

On suppose $\forall x \in \mathbb{R} \quad f(x) = 0$.

Montrer que les coefficients $a_0, a_1, \dots, a_N$ sont tous nuls.

Indication : si ces coefficients ne sont pas tous nuls, on pourra s'intéresser au plus dernier coefficient a_k non nul et regarder la limite de f en $+\infty$. On pourra aussi considérer le premier coefficient a_k non nul et s'intéresser à une limite en zéro.

4.2 Principe de récurrence simple.

Définition 4.2.1.

Soit P un prédicat sur les entiers naturels. Pour $n \in \mathbb{N}$, on dit que P est *héréditaire au rang n* si on a $P(n) \Rightarrow P(n+1)$ (autrement dit, P n'est pas héréditaire au rang n si et seulement si on a $P(n)$ et $\neg P(n+1)$).

On dit que P est *héréditaire* sur $\mathbb{N}$ si P est héréditaire à tout rang, c'est-à-dire si et seulement si on a :

$$\forall n \in \mathbb{N} \quad (P(n) \Rightarrow P(n+1))$$

Exemple 4.2.2.

Le prédicat : $P(n) : \sum_{k=0}^n k = n^2$ est-il héréditaire ?

Et le prédicat $Q(n) : \sum_{k=0}^n k = \frac{n(n+1)}{2}$?

Et le prédicat $R(n) : \sum_{k=0}^n k = 2 + \frac{n(n+1)}{2}$?

Théorème 4.2.3 (Principe de récurrence simple).
Soit P un prédicat sur les entiers naturels. Supposons qu'on a $P(0)$ et que P est héréditaire. Alors P est vraie pour tout entier naturel n .

Démonstration.

Il suffit d'appliquer le principe du minimum à $\neg P$: s'il existe un entier naturel n tel que $P(n)$ est fausse, on peut alors considérer le plus petit de ces entiers, noté n_0 . Comme $P(0)$ est vraie, $n_0 > 0$ et donc $n_0 - 1 \in \mathbb{N}$. Ainsi, $P(n_0 - 1)$ est vraie et, comme P est héréditaire, $P(n_0)$ est aussi vraie, ce qui est absurde. On obtient donc bien que $\forall n \in \mathbb{N}, P(n)$. $\square$

Exemple 4.2.4.

Soit n un entier naturel. Montrons que $\sum_{k=0}^n k = \frac{n(n+1)}{2}$.

Pour tout $n \in \mathbb{N}$, notons $P(n)$ l'assertion

$$\left\langle \sum_{k=0}^n k = \frac{n(n+1)}{2} \right\rangle.$$

Montrons $\forall n \in \mathbb{N} P(n)$ par récurrence.

- Montrons $P(0)$.

On a

$$\sum_{k=0}^0 k = 0 = \frac{0(0+1)}{2},$$

donc on a $P(0)$.

- Soit $n \in \mathbb{N}$. Supposons $P(n)$ et montrons $P(n+1)$.

Alors, on a

$$\sum_{k=0}^n k = \frac{n(n+1)}{2}$$

Ainsi,

$$\begin{aligned} \sum_{k=0}^{n+1} k &= \left(\sum_{k=0}^n k \right) + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2}, \end{aligned}$$

donc on a $P(n+1)$.

On a donc

$$\forall n \in \mathbb{N} P(n).$$

4.3 Erreurs classiques.

Nous listons ici des erreurs fréquemment trouvées dans les copies.

Mauvaise définition de l'assertion Forme classique de cette erreur :

Notons $P(n)$ l'assertion

$$\left\langle \forall n \in \mathbb{N} \sum_{k=0}^n k = \frac{n(n+1)}{2} \right\rangle$$

Explications : cette définition, mathématiquement, signifie exactement la même chose que :

Notons $P(n)$ l'assertion

$$\left\langle \forall p \in \mathbb{N} \sum_{k=0}^p k = \frac{p(p+1)}{2} \right\rangle$$

Autrement dit, $P(n)$ ne dépend pas de n . Inutile alors de tenter une démonstration par récurrence...

Variante 1 :

Notons $P(n)$ l'assertion

$$\left\langle \text{pour tout } n \in \mathbb{N}, \sum_{k=0}^p k = \frac{n(n+1)}{2} \right\rangle.$$

Variante 2 :

Notons $P(n)$ l'assertion $\left\langle \sum_{k=0}^n k = \frac{n(n+1)}{2} \right\rangle$

pour tout $n \in \mathbb{N}$.

En revanche, la formulation suivante est acceptable, bien qu'à éviter :

Notons $P(n)$ l'assertion $\ll \sum_{k=0}^n k = \frac{n(n+1)}{2} \gg$ pour tout $n \in \mathbb{N}$.

Mauvaise énonciation de l'objectif Forme classique de cette erreur :

Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion

$$\ll \sum_{k=0}^n k = \frac{n(n+1)}{2} \gg.$$

Montrons $P(n)$ par récurrence.

Explications : on ne précise pas ici ce qu'est n . De plus, le principe de récurrence ne montre pas $P(n)$ pour un n donné mais pour tout n . Il convient donc d'écrire

Montrons $\forall n \in \mathbb{N}$, $P(n)$ par récurrence ou une variante, comme

Montrons par récurrence que pour tout entier naturel n on a $P(n)$.

Mauvaise démonstration de l'hérédité Forme classique de cette erreur :

Supposons $\forall n \in \mathbb{N} P(n)$.

Montrons $\forall n \in \mathbb{N} P(n+1)$.

Explications : une fois que l'on a supposé $\forall n \in \mathbb{N} P(n)$, il n'y a pas beaucoup de travail à fournir pour montrer $\forall n \in \mathbb{N} P(n) \dots$

Variante 1 :

Supposons $\forall n \in \mathbb{N} P(n)$.

Montrons $P(n+1)$.

Variante 2 :

Supposons, pour tout entier naturel n , $P(n)$ et montrons $P(n+1)$

Variante 3 :

Supposons, pour tout entier naturel n , $P(n)$ et montrons pour tout entier naturel n , $P(n+1)$.

4.4 Bonne définition d'une suite définie par récurrence.

Notons $(u_n)_{n \in \mathbb{N}}$ la suite définie par

$$\begin{cases} u_0 = 5 \\ \text{et } \forall n \in \mathbb{N} \ u_{n+1} = 2 + \sqrt{u_n - 1} \end{cases}$$

Montrer que la suite u est bien définie.

Ici, le terme «bien définie» signifie non seulement que pour tout n , on a bien donné une expression pour définir u_n mais aussi que cette expression est définie, c'est-à-dire qu'elle a mathématiquement un sens.

Pour n donné, montrer que u_n est bien définie est un préalable à la démonstration de toute propriété de u_n .

Ici, il s'agit de montrer que pour tout n l'expression $2 + \sqrt{u_n - 1}$ est bien définie, c'est-à-dire que $u_n - 1$ est positif ou nul, autrement dit $u_n \geq 1$.

Pour n donné, on voit alors que d'une part, pour montrer que u_{n+1} est bien défini, il va falloir montrer tout d'abord $u_n \geq 1$ et d'autre part, pour montrer $u_n \geq 1$, on va avoir besoin au préalable de s'assurer que u_n est bien défini.

Autrement dit : on va avoir besoin de démontrer simultanément ces deux propriétés.

Pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion

$$\ll u_n \text{ est bien défini et } u_n \geq 1 \gg$$

Montrons $\forall n \in \mathbb{N} P(n)$ par récurrence :

- On a clairement $P(0)$.
- Soit $n \in \mathbb{N}$. Supposons $P(n)$ et montrons $P(n+1)$.

u_n est bien défini et $u_n \geq 1$.

Donc $u_n - 1 \geq 0$.

Donc $\sqrt{u_n - 1}$ est bien défini.

Donc u_{n+1} est bien défini, et de plus

$$u_{n+1} \geq 2 + \sqrt{u_n - 1} \geq 2 \geq 1$$

Donc on a $P(n+1)$.

On a donc

$$\forall n \in \mathbb{N} P(n)$$

La suite u est donc bien définie (et de plus pour tout entier naturel n , $u_n \geq 1$).

Problème de définition non étudié On trouve parfois la réponse erronée suivante :

Pour tout entier naturel n , $n = 0$ ou n est de la forme $k + 1$. On a donné une définition à u_n dans chacun de ces deux cas, donc u est bien définie.

Manifestement, l'auteur du texte ci-dessus n'a pas compris que la définition $u_{n+1} = 2 + \sqrt{u_n - 1}$ pouvait poser problème.

4.5 Récurrence double.

a Exemple : suite définie par récurrence.

Notons u la suite définie par :

$$\begin{cases} u_0 = 2 \\ u_1 = 3 \\ \forall n \in \mathbb{N}, u_{n+2} = 1 + \sqrt{u_n + u_{n+1} - 2} \end{cases}$$

Montrer que u est bien définie.

On s'aperçoit vite qu'il va falloir montrer simultanément que u_n est bien défini et qu'on a $u_n \geq 1$.

On va donc, pour tout $n \in \mathbb{N}$, définir $P(n)$ comme l'assertion

$$\langle\langle u_n \text{ est bien défini et } u_n \geq 1 \rangle\rangle$$

De plus, pour montrer cette P à un rang donné, il va falloir supposer qu'elle est vérifiée au deux rangs précédents.

Il ne suffit donc pas de chercher à démontrer P par récurrence. Pour répondre à cette question on va utiliser un principe de récurrence double, dans lequel l'initialisation consiste à montrer $P(0)$ et $P(1)$ et la démonstration de l'hérédité consiste à montrer

$$\forall n \in \mathbb{N} \left((P(n) \text{ et } P(n+1)) \Rightarrow P(n+2) \right)$$

b Énoncé du principe.

Théorème 4.5.1 (Principe de récurrence double).

Soit P un prédicat portant sur $\mathbb{N}$. Si :

- $P(0)$ et $P(1)$ sont vrais,
- pour tout $n \in \mathbb{N}$, si $P(n)$ et $P(n+1)$ sont vrais alors $P(n+2)$ est vrai,

alors $\forall n \in \mathbb{N}, P(n)$.

Démonstration.

On peut montrer par récurrence simple que pour tout $n \in \mathbb{N}$, $Q(n)$: « $P(n)$ et $P(n+1)$ ».

Ou bien on peut utiliser le principe du minimum : si P n'est pas toujours vrai, on considère le plus petit entier pour lequel P est faux *etc.* $\square$

c Rédaction par récurrence double.

Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\langle\langle u_n \text{ est bien défini et } u_n \geq 1 \rangle\rangle$$

Montrons $\forall n \in \mathbb{N} P(n)$ par récurrence double.

- On a clairement $P(0)$.
- On a clairement $P(1)$.
- Soit $n \in \mathbb{N}$. Supposons $P(n)$ et $P(n+1)$ et montrons $P(n+2)$.

u_n et u_{n+1} sont bien définis et de plus $u_n \geq 1$ et $u_{n+1} \geq 1$.

Donc $u_n + u_{n+1} - 2 \geq 0$.

Donc u_{n+2} est bien défini et de plus, $u_{n+2} = 1 + \sqrt{u_n + u_{n+1} - 2} \geq 1$.

Donc on a $P(n+2)$.

On a donc

$$\forall n \in \mathbb{N} P(n)$$

En particulier la suite u est bien définie.

Exercice 4.5.2.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite vérifiant $u_0 = 2$, $u_1 = 3$ et $\forall n \in \mathbb{N}, u_{n+2} = 3u_{n+1} - 2u_n$.

Montrer que $\forall n \in \mathbb{N}, u_n = 2^n + 1$.

4.6 Récurrence triple, etc.

On peut, de la même façon, avoir besoin de principes de récurrence triple, quadruple, ...

Si cela s'avère nécessaire, on pourra les utiliser sans démonstration.

Ainsi, appliquer le principe de récurrence triple pour démontrer $\forall n \in \mathbb{N} P(n)$ consistera à démontrer d'une part $P(0)$, $P(1)$ et $P(2)$, et d'autre part à démontrer que pour tout $n \in \mathbb{N}$, si on a $P(n)$ et $P(n+1)$ et $P(n+2)$ alors on a $P(n+3)$.

Là encore, si l'on préfère, on pourra se passer d'une récurrence triple et utiliser simplement la récurrence ordinaire. Il suffira pour cela de définir, pour tout $n \in \mathbb{N}$, $Q(n)$ comme

$$\langle\langle P(n) \text{ et } P(n+1) \text{ et } P(n+2) \rangle\rangle$$

et de montrer $\forall n \in \mathbb{N} Q(n)$ par récurrence simple.

Enfin, on peut évidemment là aussi se passer de tout principe de récurrence en utilisant le principe du minimum.

4.7 Récurrence forte.

Enfin, il existe des cas où ni une récurrence simple, ni une récurrence double, ni une récurrence triple ne semblent suffire.

Dans ces cas, on pourra utiliser le principe de récurrence forte.

a Exemple : suite définie par récurrence.

Notons u la suite définie par

$$\left\{ \begin{array}{l} u_0 = \frac{\sqrt{2}}{2} - 1 \\ \text{et } \forall n \in \mathbb{N} \ u_{n+1} = -1 + \sqrt{\frac{3}{2} + n + \sum_{k=0}^n u_k} \end{array} \right.$$

Montrez que u est bien définie.

On s'aperçoit assez vite qu'on peut espérer montrer que pour tout $n \in \mathbb{N}$, on a $u_n \geq -1$. Mais pour montrer la propriété pour n donné, il va falloir supposer qu'elle est vraie pour toutes les entiers naturels strictement inférieurs.

On va donc utiliser le principe de récurrence forte.

Celui-ci peut s'énoncer comme suit :

1. Étant donné un entier naturel n , on dit qu'une propriété P est *fortement héréditaire au rang n* si

$$(\forall m \in [0, n] \ P(m)) \Rightarrow P(n+1)$$

(ou de façon équivalente, si $P(0)$ et $P(1)$ et ... et $P(n)$ implique $P(n+1)$)

2. On dit qu'une propriété P est *fortement héréditaire* si pour tout entier naturel n , P est fortement héréditaire au rang n .
3. Le principe de récurrence forte dit simplement qu'une propriété P vraie en 0 et fortement héréditaire est vraie pour tout entier naturel.

Remarque 4.7.1.

Dire que P est fortement héréditaire au rang n est équivalent à dire que $n+1$ ne peut pas être l'entier minimum pour lequel P est faux.

Exemple 4.7.2.

On peut montrer que tout prédicat héréditaire est fortement héréditaire. La réciproque est fausse comme le montre le prédicat P défini comme suit : pour $n \in \mathbb{N}$, $P(n)$ est l'assertion « $n(n-2) \neq 0$ ».

b Énoncé du principe.

Théorème 4.7.3 (Principe de récurrence forte).

Soit P un prédicat portant sur $\mathbb{N}$. Si :

- $P(0)$ est vrai,
 - pour tout $n \in \mathbb{N}$, si $P(0), P(1), \dots, P(n)$ sont vrais, alors $P(n+1)$ est vrai,
- alors $\forall n \in \mathbb{N}, P(n)$.

Démonstration.

On peut montrer par récurrence simple que pour tout $n \in \mathbb{N}$, $R(n)$: « $P(0)$ et $P(1)$ et ... et $P(n)$ ».

Ou bien on peut utiliser le principe du minimum : si P n'est pas toujours vrai, on considère le plus petit entier pour lequel P est faux *etc.* $\square$

c Rédaction par récurrence forte.

Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\text{«} u_n \text{ est bien défini et } u_n \geq -1 \text{»}$$

Montrons par récurrence forte que pour tout $n \in \mathbb{N}$, on a $P(n)$.

- On a clairement $P(0)$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $m \in \mathbb{N}$ vérifiant $m \leq n$, on a $P(m)$.

Montrons $P(n+1)$.

Pour tout $k \in \{0, \dots, n\}$, u_k est bien défini, donc la somme $\sum_{k=0}^n u_k$ est bien définie.

En outre, pour tout $k \in \{0, \dots, n\}$, $u_k \geq -1$, donc

$$\sum_{k=0}^n u_k \geq \sum_{k=0}^n -1 = -n - 1$$

Donc

$$1/2 + n + 1 + \sum_{k=0}^n u_k \geq 0$$

Donc u_{n+1} est bien défini, et de plus, on a

$$u_{n+1} = -1 + \sqrt{\frac{3}{2} + n + \sum_{k=0}^n u_k} \geq -1$$

Donc on a $P(n+1)$

Par le principe de récurrence forte, on a donc

$$\forall n \in \mathbb{N} \ P(n)$$

Donc u est bien définie.

Exercice 4.7.4.

Montrer que

$$\forall n \in \mathbb{N}^*, \exists p, q \in \mathbb{N}, n = 2^p(2q+1).$$

4.8 Méthodologie : choix du type de récurrence.

Le plus difficile dans la démonstration par récurrence d'un prédicat $(P_n)_{n \in \mathbb{N}}$ est souvent d'identifier le type de raisonnement à appliquer.

Pour cela, il convient de commencer à travailler *au brouillon* et de chercher à montrer la propriété P_n , n étant fixé. Quatre cas de figures peuvent alors survenir.

- Si vous arrivez à montrer P_n directement, c'est qu'il n'y a pas de récurrence en jeu !
- Si, pour montrer P_n , vous observez que vous devez utiliser P_{n-1} , alors vous pouvez rédiger une récurrence simple.
- Si, pour montrer P_n , vous observez que vous devez utiliser P_{n-1} et P_{n-2} , alors vous pouvez rédiger une récurrence double (*idem* pour triple, quadruple *etc.*).
- Si, pour montrer P_n , vous observez que vous devez utiliser $P_{n-1}, \dots, P_0$, alors vous pouvez rédiger une récurrence forte.

Après ce travail, vous pouvez rédiger proprement votre récurrence.

4.9 Récurrence à partir d'un certain rang.

Il s'agit maintenant de faire démarrer une récurrence (simple, multiple ou forte) à un autre rang que le rang 0.

Exemple. Soit u une suite, n_0 un entier et α un réel strictement positif.

On suppose que pour tout $n \geq n_0$, on a

$$|u_{n+1}| \leq \alpha |u_n|$$

Montrer

$$\forall n \geq n_0 \quad |u_n| \leq \alpha^{n-n_0} |u_{n_0}|$$

Modèle de rédaction proposé. Pour tout $n \geq n_0$, notons $P(n)$ la propriété $|u_n| \leq \alpha^{n-n_0}$.

Montrons par récurrence que pour tout $n \geq n_0$, $P(n)$ est vraie.

- On a $|u_{n_0}| = \alpha^{n_0-n_0} |u_{n_0}|$. Donc on a $P(n_0)$.

- Soit $n \geq n_0$. Supposons $P(n)$.

Montrons $P(n+1)$.

On a $|u_{n+1}| \leq \alpha |u_n|$ car $n \geq n_0$.

Par ailleurs $|u_n| \leq \alpha^{n-n_0} |u_{n_0}|$.

Donc $\alpha |u_n| \leq \alpha^{n+1-n_0} |u_{n_0}|$.

Donc $|u_{n+1}| \leq \alpha^{n+1-n_0} |u_{n_0}|$.

On a donc $P(n+1)$

On a donc

$$\forall n \geq n_0 \ P(n)$$

4.10 Récurrence sur un intervalle fini d'entiers

Il s'agit de démontrer un résultat valable pour un ensemble fini d'entiers seulement, de la forme $\llbracket a, b \rrbracket$, où $a, b \in \mathbb{Z}$ tels que $a < b$. Il faudra faire attention à initialiser la propriété pour $n = a$, et lors de l'hérédité, il faudra supposer que cette propriété est vraie pour un certain $n \in \llbracket a, b-1 \rrbracket$ et montrer qu'elle est vraie au rang $n+1$.

Exemple 4.10.1.

Soit $n \in \mathbb{N}^*$ et $f_n : x \mapsto x^n$. Montrer que pour tout $k \in \llbracket 0, n \rrbracket$, et pour tout $x \in \mathbb{R}$, $f_n^{(k)}(x) = \frac{n!}{(n-k)!} x^{n-k}$.

4.11 Récurrence descendante

On cherche à montrer un résultat valable sur un intervalle $\llbracket a, b \rrbracket$ comme précédemment, mais cette fois-ci on initialise pour $n = b$, et on montre que la propriété P à un rang n implique cette même propriété au rang $n-1$. Cela se démontre en posant $Q(n) = P(b-n)$. On montre alors

par récurrence que $Q(0)$ est vraie et que $Q(n)$ implique $Q(n+1)$.

Exemple 4.11.1.

Soit N un entier naturel supérieur ou égal à 2. Montrer que pour tout $k \in \llbracket 2, N \rrbracket$,

$$\sqrt{k} \sqrt{(k+1)} \sqrt{(k+2)} \sqrt{\dots} \sqrt{(N-1)} \sqrt{N} < k + 1.$$

4.12 Quelques récurrences fausses.

Exercice : chercher l'erreur dans les pseudo-démonstrations ci-dessous.

a Suite négative minorée par un réel positif...

Notons u la suite définie par

$$\begin{cases} u_0 = \frac{\pi}{4} \\ \forall n \in \mathbb{N} \ u_{n+1} = 6u_n - 4 \end{cases}$$

(il est clair que u est bien définie)

Montrons que pour tout $n \in \mathbb{N}$, $u_n \geq \frac{4}{5}$.

Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété

$$\llbracket u_n \geq \frac{4}{5} \rrbracket$$

Montrons $\forall n \in \mathbb{N} \ P(n)$ par récurrence.

- On a $P(0)$.
- Soit $n \in \mathbb{N}$. Supposons $P(n)$. Montrons $P(n+1)$.

On a :

$$\begin{aligned} & u_n \geq \frac{4}{5} \\ \text{donc} \quad & 6u_n \geq \frac{24}{5} \\ \text{donc} \quad & 6u_n - 4 \geq \frac{24 - 5 \times 4}{5} \\ \text{donc} \quad & u_{n+1} \geq \frac{4}{5}. \end{aligned}$$

Ainsi, on a $P(n+1)$.

Donc on a $\forall n \in \mathbb{N} \ P(n)$

Calculons les valeurs approchées des premiers termes de la suite avec Python :

```
def f(x) :
    """Calcule 6*x-4, précondition : x réel"""
    return 6 * x - 4
```

```
from math import pi
x = pi / 4 # u_0
u = [x] # Contient u_0
for i in range(5) :
    x = f(x) # Calcule le terme suivant de u
    u.append(x) # Ajoute le nouveau terme
print(u) # Affiche les valeurs calculées
```

On obtient les valeurs suivantes :

$$\begin{aligned} u_0 &\approx 0.7853982 \\ u_1 &\approx 0.7123890 \\ u_2 &\approx 0.2743339 \\ u_3 &\approx -2.3539967 \\ u_4 &\approx -18.12398 \\ u_5 &\approx -112.74388 \end{aligned}$$

Autrement dit, u_5 est négatif et devrait être supérieur à $\frac{4}{5}$...

b n valeurs sont égales

Montrons que pour tout entier n non nul, et tout n -uplet $(x_1, \dots, x_n)$, on a

$$x_1 = x_2 = \dots = x_n$$

Autrement dit : toutes les composantes d'un n -uplet sont égales.

Pour tout $n \geq 1$, notons $P(n)$ la propriété

$$\llbracket \text{pour tout } n\text{-uplet } (x_1, \dots, x_n), \text{ on a } x_1 = x_2 = \dots = x_n \rrbracket$$

Montrons $\forall n \geq 1 \ P(n)$ par récurrence.

- On a clairement $P(1)$.
- Soit $n \geq 1$.

Supposons $P(n)$ et montrons $P(n+1)$.

Soit $(x_1, \dots, x_{n+1})$ un $n+1$ -uplet.

$(x_1, \dots, x_n)$ est un n -uplet donc on a

$$x_1 = x_2 = \dots = x_n$$

$(x_2, \dots, x_{n+1})$ est un n -uplet donc on a

$$x_2 = \dots = x_{n+1}$$

Donc on a

$$x_1 = x_2 = \dots = x_{n+1}$$

Donc on a $P(n+1)$.

On a donc $\forall n \geq 1 \ P(n)$.

c Toutes les puissances valent 1

Soit $a \in \mathbb{R}^*$. Montrons que pour tout entier naturel non nul n , on a $a^{n-1} = 1$.

Notons $P(n)$ la propriété « $a^{n-1} = 1$ ».

Montrons $\forall n \geq 1 \ P(n)$ par récurrence forte.

- On a clairement $P(1)$.

- Soit $n \geq 1$.

Supposons $\forall m \in \llbracket 1, n \rrbracket \ P(m)$.

Montrons $P(n+1)$.

On a

$$\begin{aligned} a^{n+1-1} &= a^n \\ &= \frac{a^{n-1} \times a^{n-1}}{a^{(n-1)-1}} \end{aligned}$$

Or par hypothèse de récurrence, $P(m)$ est vraie pour tout $m \leq n$, donc $P(n)$ et $P(n-1)$ sont vraies.

Donc $a^{n-1} = 1$ et $a^{(n-1)-1} = 1$.

D'où :

$$a^{n+1-1} = \frac{1 \times 1}{1}$$

Donc on a $P(n+1)$.

On a donc

$$\forall n \geq 1 \ P(n)$$

Chapitre V

Nombres complexes

Sommaire

1	L'inégalité triangulaire	82
2	Propriétés supplémentaires de l'exponentielle complexe et des arguments . .	82
3	Groupe $\mathbb{U}$ des nombres complexes de module 1	83
4	Équations du second degré	83
4.1	Calcul des racines carrées d'un complexe sous forme algébrique	83
4.2	Résolution des équations du second degré	84
5	Racines énièmes.	85
6	Techniques de calcul	86
6.1	Formules trigonométriques	86
6.2	Technique de l'angle moitié	86
6.3	Factorisation	86
6.4	Linéarisation	86
7	L'exponentielle complexe	87
8	Nombres complexes et géométrie plane	87
8.1	Colinéarité et orthogonalité	87
a	Interprétation géométrique du rapport	87
8.2	Transformations usuelles	88
8.3	Similitudes et isométries	90

1 L'inégalité triangulaire

Commençons par démontrer l'inégalité triangulaire, déjà évoquée en début d'année :

Théorème 1.0.1 (Inégalité triangulaire).

Soit $z, z' \in \mathbb{C}$, on a

$$||z| - |z'|| \leq |z \pm z'| \leq |z| + |z'|.$$

De plus, $|z + z'| = |z| + |z'|$ si et seulement si il existe $(\lambda, \lambda') \in (\mathbb{R}^+)^2$ tel que $(\lambda, \lambda') \neq (0, 0)$ et $\lambda z = \lambda' z'$.

Démonstration.

On montre l'encadrement pour $|z + z'|$. Pour $|z - z'|$ il suffit de remplacer z' par $-z'$.

Pour montrer $|z + z'| \leq |z| + |z'|$, il suffit de montrer $|z + z'|^2 \leq (|z| + |z'|)^2$. Posons $d = (|z| + |z'|)^2 - |z + z'|^2$ et calculons d . On obtient successivement

$$\begin{aligned} d &= |z|^2 + |z'|^2 + 2|z||z'| - (z + z')(\bar{z} + \bar{z}') \\ &= 2|z||z'| - z\bar{z}' - z'\bar{z} \\ &= 2\left(|z||z'| - \frac{z\bar{z}' + z'\bar{z}}{2}\right) \\ &= 2\left(|z||z'| - \frac{zz' + \overline{zz'}}{2}\right) \\ &= 2(|zz'| - \operatorname{Re}(zz')) \\ &\geq 0 \end{aligned}$$

On a donc $|z + z'| \leq |z| + |z'|$.

Pour la seconde inégalité : $|z| = |(z + z') + (-z')| \leq |z + z'| + |-z'|$, d'où $|z| - |z'| \leq |z + z'|$. On permute les rôles de z et z' et on a $|z'| - |z| \leq |z + z'|$, ce qui permet de conclure, car

$$||z| - |z'|| = \max(|z| - |z'|, |z'| - |z|).$$

Montrons maintenant le cas d'égalité. Dans le cas où $z = z' = 0$, le résultat est immédiat.

Sinon, d'après la démonstration de l'inégalité triangulaire, l'égalité est vérifiée si et seulement si $|zz'| = \operatorname{Re}(zz')$, i.e. si et seulement si zz' est un réel positif.

Dans le cas où $z' \neq 0$, on remarque que $\frac{z}{z'} = \frac{zz'}{|z'|^2}$, donc l'égalité est vérifiée si et seulement si $\frac{z}{z'} \in \mathbb{R}_+$ si et seulement si il existe $\lambda \in \mathbb{R}_+$ tel que $z = \lambda z'$.

En inversant les rôles de z et z' dans le cas où $z' = 0$ on obtient le résultat voulu. $\square$

Remarque 1.0.2.

• Géométriquement, il y a égalité dans l'inégalité triangulaire lorsque les images de z et z' sont sur

une même demi-droite d'origine O .

• Le bloc « il existe $(\lambda, \lambda') \in (\mathbb{R}^+)^2$ tel que $(\lambda, \lambda') \neq (0, 0)$ » s'écrit aussi « $\exists(\lambda, \lambda') \in (\mathbb{R}^+)^2 \setminus \{(0, 0)\}$ » et se lit « il existe deux complexes λ et λ' non tous nuls ».

2 Propriétés supplémentaires de l'exponentielle complexe et des arguments

Théorème 2.0.1 (Formules d'Euler).

Soit $\theta \in \mathbb{R}$, alors

$$\begin{aligned} \cos \theta &= \frac{e^{i\theta} + e^{-i\theta}}{2}, \\ \sin \theta &= \frac{e^{i\theta} - e^{-i\theta}}{2i}. \end{aligned}$$

Démonstration.

Direct. $\square$

Proposition 2.0.2.

Soit $\theta \in \mathbb{R}$:

1. $e^{i\theta} \times e^{-i\theta} = e^{i0} = 1$;
2. $e^{i\theta} \neq 0$;
3. $\frac{1}{e^{i\theta}} = e^{-i\theta} = \overline{e^{i\theta}}$.

Démonstration.

Direct. $\square$

Proposition 2.0.3 (Formule de De Moivre).

Soit $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$. On a

$$\begin{aligned} e^{in\theta} &= (e^{i\theta})^n, \\ \cos(n\theta) + i \sin(n\theta) &= (\cos \theta + i \sin \theta)^n. \end{aligned}$$

Démonstration.

Se démontre par une récurrence immédiate sur n . $\square$

Proposition 2.0.4.

Soient $z, z' \in \mathbb{C}^*$. On a :

$$\begin{aligned}\arg \bar{z} &= -\arg z[2\pi] \\ \arg zz' &= \arg z + \arg z'[2\pi] \\ \text{et } \arg(1/z) &= -\arg z[2\pi].\end{aligned}$$

Démonstration.

Utiliser l'écriture trigonométrique. $\square$

Remarque 2.0.5.

L'écriture $a = b[2\pi]$ signifie que a et b sont égaux à un multiple de 2π près, *i.e.* $\exists k \in \mathbb{Z}, a = b + 2k\pi$.

Les manipulations d'arguments doivent toujours s'effectuer en indiquant à quel angle près cela s'entend ($[\pi]$, $[2\pi]$ le plus souvent).

Exercice 2.0.6.

Si $a = b[2\pi]$, a-t-on $\frac{a}{2} = \frac{b}{2}[2\pi]$? A-t-on $2a = 2b[2\pi]$?

3 Groupe $\mathbb{U}$ des nombres complexes de module 1

Définition 3.0.1.

On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1 : $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.

Remarque 3.0.2.

$\mathbb{U}$ est l'ensemble des affixes des points du cercle trigonométrique

Proposition 3.0.3.

Soit $z, z' \in \mathbb{U}$. Alors :

1. $1 \in \mathbb{U}$;
2. $zz' \in \mathbb{U}$;
3. $\frac{1}{z} \in \mathbb{U}$.

Remarque 3.0.4.

Grâce aux propriétés précédentes, on dit que $\mathbb{U}$ est un *groupe*.

Le groupe $\mathbb{U}$, qui est l'ensemble des affixes des points du cercle trigonométrique, est intimement lié à l'exponentielle complexe, comme nous l'avons déjà vu :

Théorème 3.0.5 (Paramétrisation de $\mathbb{U}$).

L'application

$$\begin{aligned}\mathbb{R} &\rightarrow \mathbb{C} \\ \theta &\mapsto e^{i\theta}\end{aligned}$$

est un *paramétrage* de $\mathbb{U}$, autrement dit, pour tout nombre complexe z on a

$$z \in \mathbb{U} \Leftrightarrow \exists \theta \in \mathbb{R} \quad z = e^{i\theta} \quad (\text{V.1})$$

De plus, pour tout complexe $z \in \mathbb{U}$ donné, le paramètre correspondant est *unique à 2π près*, autrement dit, on a

$$\forall (\theta, \theta') \in \mathbb{R}^2 \quad e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta = \theta'[2\pi] \quad (\text{V.2})$$

Remarque 3.0.6.

Ce résultat a une interprétation géométrique intuitive.

Démonstration.

Soit $z \in \mathbb{C}$. Montrons l'équivalence (V.1). L'implication de droite à gauche est évidente : s'il existe θ tel que z s'écrit $\cos \theta + i \sin \theta$, alors $|z|^2 = \sin^2 \theta + \cos^2 \theta = 1$, donc $z \in \mathbb{U}$. Réciproquement, soit $z \in \mathbb{U}$, alors $(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = 1$ donc il existe $\theta \in \mathbb{R}$ vérifiant $\operatorname{Re} z = \cos \theta$ et $\operatorname{Im} z = \sin \theta$.

Pour l'équivalence (V.2), il suffit de remarquer que pour tout couple (θ, θ') de réels, l'égalité $e^{i\theta} = e^{i\theta'}$ implique l'égalité des cosinus ainsi que des sinus de θ et θ' , donc l'égalité de θ et θ' à 2π près. L'autre sens est immédiat par 2π -périodicité des fonctions sinus et cosinus. $\square$

4 Équations du second degré

4.1 Calcul des racines carrées d'un complexe sous forme algébrique

Soit z et t deux complexes. On veut résoudre explicitement l'équation $t^2 = z$, d'inconnue z , que nous noterons (E), en n'utilisant que des complexes écrits sous forme algébrique.

On peut écrire z sous la forme $x + iy$ avec $(x, y) \in \mathbb{R}^2$ et t sous la forme $a + ib$, où $(a, b) \in \mathbb{R}^2$.

Pour résoudre (E), il y a une astuce très utile.

Astuce.

Soit t et z deux complexes. Alors

$$t^2 = z \iff \begin{cases} t^2 = z \\ |t|^2 = |z| \end{cases}$$

On en déduit successivement :

$$(E) \iff \begin{cases} a^2 - b^2 + i2ab = x + iy \\ a^2 + b^2 = \sqrt{x^2 + y^2} \end{cases}$$

$$(E) \iff \begin{cases} a^2 - b^2 = x \\ 2ab = y \\ a^2 + b^2 = \sqrt{x^2 + y^2} \end{cases}$$

$$(E) \iff \begin{cases} a^2 = \frac{x + \sqrt{x^2 + y^2}}{2} \\ b^2 = \frac{-x + \sqrt{x^2 + y^2}}{2} \\ 2ab = y \end{cases}$$

Exercice 4.1.1.

Trouver les racines carrées de $3 - 4i$.

4.2 Résolution des équations du second degré

Proposition 4.2.1.

Soit A un polynôme en z à coefficients complexes, admettant un complexe λ comme racine. Alors il existe un polynôme B en z à coefficients complexes tel que $A(z) = (z - \lambda)B(z)$.

Remarque 4.2.2.

Nous admettons pour l'instant ce résultat, il sera démontré dans le chapitre sur les polynômes.

Exercice 4.2.3.

Soit $A(z) = z^3 - iz^2 - (3 + i)z + 2 + 2i$.

1. Trouver un polynôme B tel que $A(z) = (z - 1)B(z)$.
2. Trouver un polynôme C tel que $A(z) = (z - 1)(z - 1 - i)C(z)$.

Théorème 4.2.4.

Soient $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Les solutions de l'équation $az^2 + bz + c = 0$ d'inconnue $z \in \mathbb{C}$ sont $\frac{-b \pm \delta}{2a}$, où δ est l'une quelconque des deux racines carrées du discriminant $\Delta = b^2 - 4ac$.

La somme de ces solutions vaut $-\frac{b}{a}$ et leur produit $\frac{c}{a}$.

Démonstration.

Pour tout $z \in \mathbb{C}$, on a

$$\begin{aligned} az^2 + bz + c &= a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) \\ &= a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right] \\ &= a\left[\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right] \\ &= a\left[\left(z + \frac{b}{2a}\right)^2 - \left(\frac{\delta}{2a}\right)^2\right] \\ &= a\left[z + \frac{b}{2a} - \frac{\delta}{2a}\right]\left[z + \frac{b}{2a} + \frac{\delta}{2a}\right] \\ &= a\left(z - \frac{-b - \delta}{2a}\right)\left(z - \frac{-b + \delta}{2a}\right) \end{aligned}$$

On calcule finalement :

$$\begin{aligned} \frac{-b - \delta}{2a} + \frac{-b + \delta}{2a} &= -\frac{b}{a}, \\ \frac{-b - \delta}{2a} \times \frac{-b + \delta}{2a} &= \frac{b^2 - \delta^2}{4a^2} = \frac{c}{a}. \end{aligned}$$

□

Remarque 4.2.5.

- N'importe quelle racine carrée du discriminant convient, puisqu'elles sont égales au signe près.
- Si le discriminant est nul, il n'y a qu'une racine, qui est alors dite *double*.
- Si $a, b, c \in \mathbb{R}$, alors le discriminant est réel. S'il est strictement positif, il y a deux racines réelles distinctes ; s'il est nul, il y a une racine réelle double ; s'il est strictement négatif, il y a deux racines complexes non réelles conjuguées.
- Avec $\alpha, \beta \in \mathbb{C}$, on a la relation suivante :

$$(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta.$$

- On peut donc connaître la somme et le produit des deux racines sans connaître les racines. Réciproquement, si l'on connaît la somme et le produit de deux nombres complexes, alors on connaît une

équation polynomiale du second degré dont ils sont exactement les racines.

Exercice 4.2.6.

Trouver a et b tels que $ab = 2$ et $a + b = i$.

5 Racines énièmes.

Définition 5.0.1.

Soient $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$. On appelle *racine n^e de z* tout complexe t tel que $t^n = z$.

Les racines de 1 sont appelées *racines n^es de l'unité*.

L'ensemble des racines n^es de l'unité est noté $\mathbb{U}_n$.

Remarque 5.0.2.

La notation $\sqrt[n]{\cdot}$ est **interdite** sur les complexes quelconques. En effet, elle désigne l'application réciproque de la fonction $x \mapsto x^n$ qui n'est bijective que considérée comme application de $\mathbb{R}^+$ dans $\mathbb{R}^+$ si n est pair et de $\mathbb{R}$ dans $\mathbb{R}$ si n est impair.

Théorème 5.0.3. 1. La seule racine n^e de zéro est zéro.

2. Soit $z \in \mathbb{C}$ non nul, donné sous une forme trigonométrique $z = re^{i\theta}$, avec $r > 0$. Alors z possède exactement n racines n^es , qui sont les nombres complexes

$$\sqrt[n]{r} \times e^{\left(\frac{i\theta}{n} + \frac{2ik\pi}{n}\right)}$$

pour k décrivant l'ensemble $\llbracket 0, n-1 \rrbracket$ (ou $\llbracket 1, n \rrbracket$).

3. En particulier

$$\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in \llbracket 0, n-1 \rrbracket \right\}.$$

Démonstration. 1. Soit $t \in \mathbb{C}$. Alors $t \neq 0 \Rightarrow t^n \neq 0$ donc $t^n = 0 \Rightarrow t = 0$. On vérifie enfin que $t = 0 \Rightarrow t^n = 0$, pour $n > 0$.

2. Soit $(z, t) \in \mathbb{C}^2$, $z \neq 0$.

- 1er cas : $z = 1$: on note $\rho = |t|$ et $\varphi \in \mathbb{R}$ un argument de t . On a : $t^n = 1$ si et seulement si $\rho^n \cdot e^{in\varphi} = 1 \cdot e^{i0}$ si et seulement si $\rho^n = 1$ et $n\varphi = 0[2\pi]$ si et seulement si $\rho = 1$ et $\varphi = \frac{2k\pi}{n}$.

- 2nd cas : z est quelconque non nul donc s'écrit sous la forme $re^{i\theta}$ où $r > 0$. On pose $\alpha = \sqrt[n]{r} \times e^{i\theta/n}$, donc $\alpha^n = z$. Alors, si $t = \rho \cdot e^{i\varphi}$, $t^n = z$ si et seulement si $\left(\frac{t}{\alpha}\right)^n = 1$ et on utilise le premier cas.

□

Remarque 5.0.4 (Interprétation géométrique). Soit $n \geq 3$. Posons $z_k = \frac{2ik\pi}{n}$ et notons A_k le point d'affixe z_k pour $k \in \llbracket 0, n-1 \rrbracket$. Alors $A_0 A_1 \dots A_n$ est un polygone régulier à n côtés, inscrit dans le cercle unité.

Les racines deuxièmes de 1 sont -1 et 1 (racines carrées de 1).

En posant $j = e^{2i\pi/3}$, les racines troisièmes de l'unité sont 1 , j et j^2 (et on a $j^2 = \bar{j}$). Ce sont les sommets d'un triangle équilatéral inscrits dans le cercle unité.

Les racines quatrièmes de l'unité sont 1 , i , -1 et $-i$: ce sont les sommets d'un carré inscrit dans le cercle unité.

Les racines cinquièmes de l'unité sont 1 , $e^{2i\pi/5}$, $e^{4i\pi/5}$, $e^{-4i\pi/5}$ et $e^{-2i\pi/5}$: ce sont les sommets d'un pentagone régulier inscrit dans le cercle unité.

Les racines sixièmes de l'unité sont 1 , $e^{i\pi/3}$, j , -1 , j^2 et $e^{-i\pi/3}$: ce sont les sommets d'un hexagone régulier inscrit dans le cercle unité.

Tout cela est représenté dans la figure V.1.

Proposition 5.0.5.

Soit $n \in \mathbb{N}$, $n \geq 2$. Pour tout $z \in \mathbb{C}$ on a les égalités suivantes :

$$\prod_{\omega \in \mathbb{U}_n} (z - \omega) = \prod_{k=0}^{n-1} (z - e^{\frac{2ik\pi}{n}}) = z^n - 1$$

$$\prod_{\omega \in \mathbb{U}_n \setminus \{1\}} (z - \omega) = \prod_{k=1}^{n-1} (z - e^{\frac{2ik\pi}{n}}) = \sum_{k=0}^{n-1} z^k.$$

La somme des racines n^e de l'unité est nulle, i.e. :

$$\sum_{\omega \in \mathbb{U}_n} \omega = \sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = 0.$$

En particulier $1 + j + \bar{j} = 1 + j + j^2 = 0$.

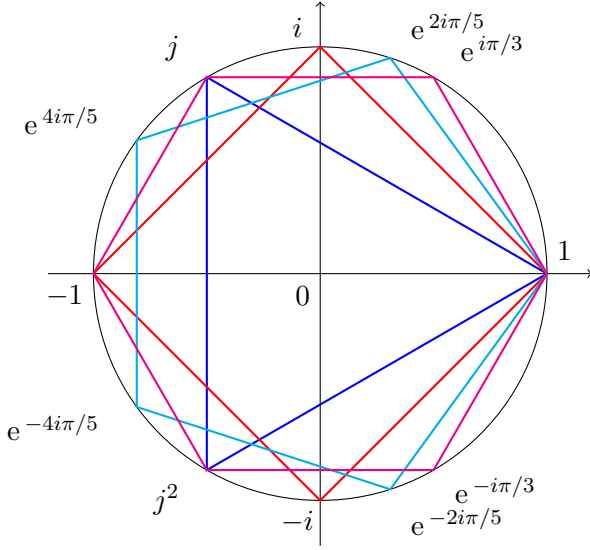


FIGURE V.1 – Racines n^{es} de l'unité pour $1 \leq n \leq 6$.

Démonstration.

Pour démontrer ce résultat, on utilisera une version généralisée de la proposition 4.2.1 : pour tout entier n et tout polynôme P un polynôme de degré n admettant n racines distinctes $z_1, \dots, z_n$, de coefficient dominant α , on a

$$\forall z \in \mathbb{C} \quad P(z) = \alpha(z - z_1) \dots (z - z_n).$$

On rappelle aussi la formule de sommation géométrique : pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}^*$,

$$z^n - 1 = (z - 1)(1 + z + \dots + z^{n-1}).$$

La première égalité est une application directe du résultat admis, en posant $P : z \mapsto z^n - 1$; P est alors un polynôme de degré n et de coefficient dominant 1.

La seconde est une application directe du même résultat en considérant $P : z \mapsto \sum_{k=0}^{n-1} z^k$. De plus $n \neq 1$ donc

$e^{\frac{2i\pi}{n}} \neq 1$ donc

$$\sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = \sum_{k=0}^{n-1} \left(e^{\frac{2i\pi}{n}} \right)^k = \frac{1 - \left(e^{\frac{2i\pi}{n}} \right)^n}{1 - e^{\frac{2i\pi}{n}}} = 0.$$

□

6 Techniques de calcul

6.1 Formules trigonométriques

Nous avons utilisé les formules de trigonométrie (cf. formulaire de trigonométrie) dans la démonstration de la forme algébrique du produit de deux nombres complexes.

Néanmoins, les propriétés de l'exponentielle « de $i\theta$ » permettent de retrouver ces formules, dans le cas inenvisageable où vous les auriez oubliées.

Par exemple : développer $e^{i(a+b)}$ de deux manières différentes, identifier les expressions obtenues et retrouver les formules donnant $\sin(a+b)$ et $\cos(a+b)$.

6.2 Technique de l'angle moitié

Déjà vu. Elles permettent aussi de retrouver les formules de factorisation du type $\cos(a) + \cos(b)$.

6.3 Factorisation

Utilise la technique de l'angle moitié, souvent après avoir identifié la somme en question comme la partie réelle ou imaginaire d'un type de somme bien connue. On utilise très souvent les formules suivantes.

Sommation géométrique : Pour tout $z \in \mathbb{C}$ et $n \in \mathbb{N}$,

$$\sum_{k=0}^n z^k = \begin{cases} n+1 & \text{si } z = 1, \\ \frac{z^{n+1} - 1}{z - 1} & \text{si } z \neq 1. \end{cases}$$

Binôme de Newton : Pour tout $(a, b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$,

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

On peut calculer les coefficients binomiaux $\binom{n}{k}$ avec le triangle de Pascal.

Exemple 6.3.1.

$$\sum_{k=0}^n \cos(4kx) = \begin{cases} \frac{\sin(2(n+1)x) \cos(2nx)}{\sin(2x)} & \text{si } x \notin \frac{\pi}{2}\mathbb{Z} \\ n+1 & \text{si } x \in \frac{\pi}{2}\mathbb{Z} \end{cases}$$

6.4 Linéarisation

Méthode pour supprimer les produits et puissances dans une expression en cosinus et sinus :

- 1- Utiliser la formule d'Euler et développer par la formule du binôme.
- 2- Regrouper les puissances pour réutiliser les formules d'Euler, mais dans l'autre sens.

Exemple 6.4.1.

$$\begin{aligned}\cos^3 x &= \frac{1}{4} \cos(3x) + \frac{3}{4} \cos x \\ \sin^3(x) \cos^2(x) &= -\frac{1}{16} \sin(5x) + \frac{1}{8} \sin(x) \\ &\quad + \frac{1}{16} \sin(3x)\end{aligned}$$

7 L'exponentielle complexe

Définition 7.0.1.

Soit $z \in \mathbb{C}$, donné sous forme algébrique $z = x + iy$. On appelle *exponentielle de z* notée e^z le nombre complexe $e^z = e^x e^{iy}$.

Remarque 7.0.2.

e^z n'est toujours pas une puissance : ce n'est qu'une notation.

Exemple 7.0.3.

$$e^{2+i\pi/2} = ie^2.$$

Théorème 7.0.4. 1. L'exponentielle complexe est $2i\pi$ -périodique.

2. Pour tout $z, z' \in \mathbb{C}$, $e^{z+z'} = e^z e^{z'}$: on dit que l'exponentielle transforme les sommes en produits.

3. L'exponentielle complexe ne s'annule pas.

4. Pour tout $z \in \mathbb{C}$ et $t \in \mathbb{C}^*$, on a

$$e^z = t \iff \exists k \in \mathbb{Z}, z = \ln|t| + i \arg t + 2ik\pi.$$

5. Pour tout $z, z' \in \mathbb{C}$, $e^z = e^{z'}$ ssi $(z - z') \in 2i\pi\mathbb{Z}$.

Démonstration. 1. Immédiat.

2. Séparer parties réelle et imaginaire.

3. L'exponentielle ne s'annule pas sur $\mathbb{R}$, et $e^{i\theta}$ non plus (déjà vu).

4. $e^z = t$ si et seulement si $e^{\operatorname{Re} z} = |t|$ et $\operatorname{Im} z = \arg t[2\pi]$.

5. $e^z = e^{z'}$ ssi $e^{z-z'} = 1$, et on utilise le point précédent. $\square$

Remarque 7.0.5.

L'exponentielle n'est ni surjective, ni injective, et il n'existe pas de « logarithme complexe ».

8 Nombres complexes et géométrie plane

Dans toute cette partie, on considère un plan, muni d'un repère orthonormé $(O, \vec{i}, \vec{j})$.

8.1 Colinéarité et orthogonalité

a Interprétation géométrique du rapport

Théorème 8.1.1.

Soit z et z' deux complexes non nuls. On note $\vec{u}$ et $\vec{u}'$ les vecteurs d'afixes respectives z et z' . Alors

$$\begin{aligned}\left| \frac{z'}{z} \right| &= \frac{\|\vec{u}'\|}{\|\vec{u}\|} \\ \arg \left(\frac{z'}{z} \right) &= (\vec{u}, \vec{u}') \quad [2\pi]\end{aligned}$$

Démonstration.

Le premier point est immédiat, le second découle de l'interprétation géométrique de l'argument. En notant $\vec{i}$ le vecteur d'afixe 1, et en posant $\theta = \arg z$, on a $z = |z|(\cos \theta + i \sin \theta)$, donc $(\vec{i}, \vec{u}) = \arg z \quad [2\pi]$. De même $(\vec{i}, \vec{u}') = \arg z'[2\pi]$. D'où

$$\begin{aligned}(\vec{u}, \vec{u}') &= (\vec{i}, \vec{u}') - (\vec{i}, \vec{u}) \quad [2\pi] \\ &= \arg z' - \arg z \quad [2\pi] \\ &= \arg \left(\frac{z'}{z} \right) \quad [2\pi]\end{aligned}$$

$\square$

Corollaire 8.1.2.

Soit A, B et M trois points deux à deux distincts d'afixes respectives a, b et z . Alors

(i) A, B et M sont alignés si et seulement si $\frac{z-a}{z-b} \in \mathbb{R}$;

(ii) $(AM) \perp (BM)$ si et seulement si $\frac{z-a}{z-b} \in i\mathbb{R}^*$.

Exemple 8.1.3.

i , 1 et $2 - i$ sont alignés, et $1 + i$, 2 et $-2i$ forment un angle droit en 2 .

Exercice 8.1.4.

Soit $A(a)$, $B(b)$ et $C(c)$ trois points du plan.

On rappelle que le centre de gravité du triangle ABC est le point d'affixe $\frac{1}{3}(a + b + c)$.

Montrer que ce centre de gravité est le point d'intersection des médianes de ABC .

Exercice 8.1.5.

Soit $A(a)$, $B(b)$ et $C(c)$ trois points du plan. On suppose que le cercle circonscrit au triangle ABC a pour centre $O(0)$.

Montrer que l'orthocentre de ABC a pour affixe $a + b + c$.

8.2 Transformations usuelles

Définition 8.2.1 (Translation).

Soit $\vec{u}$ un vecteur

La translation de vecteur $\vec{u}$ est l'application qui envoie un point M sur le point M' vérifiant $\overrightarrow{MM'} = \vec{u}$ (voir figure V.2). On la note souvent $\tau_{\vec{u}}$.

Remarque 8.2.2.

La translation de vecteur nul est l'identité. Si $\vec{u}$ n'est pas nul, la translation de vecteur $\vec{u}$ n'a pas de point fixe.

Définition 8.2.3 (Rotation).

Soit Ω un point du plan, $\theta \in \mathbb{R}$.

La rotation de centre Ω et d'angle θ est l'application qui :

- fixe Ω ;
- envoie tout point M différent de Ω sur le point M' vérifiant $\Omega M = \Omega M'$ et $(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}) = \theta[2\pi]$.

On la note souvent $\rho_{\Omega, \theta}$ (voir figure V.3).

Remarque 8.2.4.

Si θ est un multiple de 2π , toute rotation d'angle θ est l'identité.

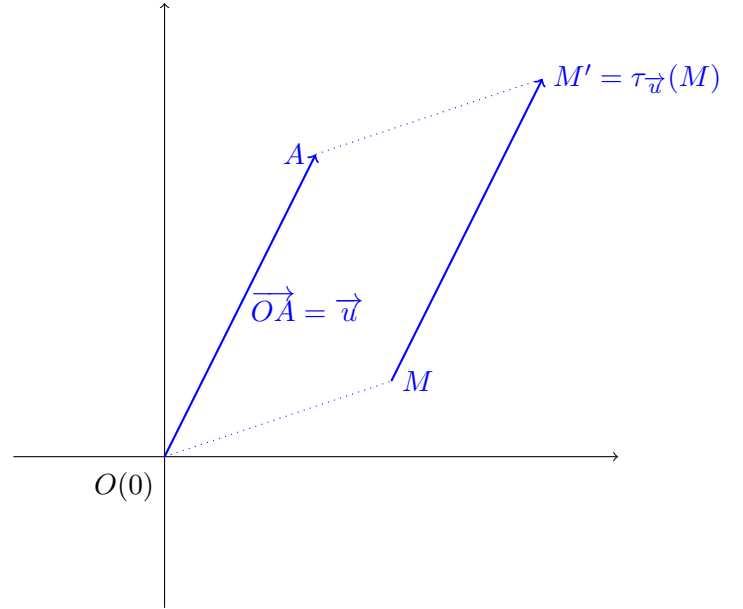


FIGURE V.2 – Translation de vecteur $\vec{u}$, $OMM'A$ est un parallélogramme.

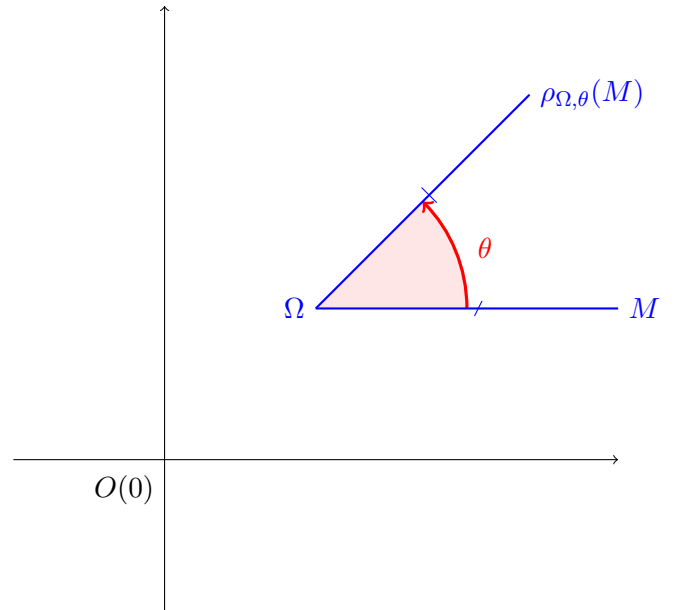


FIGURE V.3 – Rotation de centre Ω , d'angle θ .

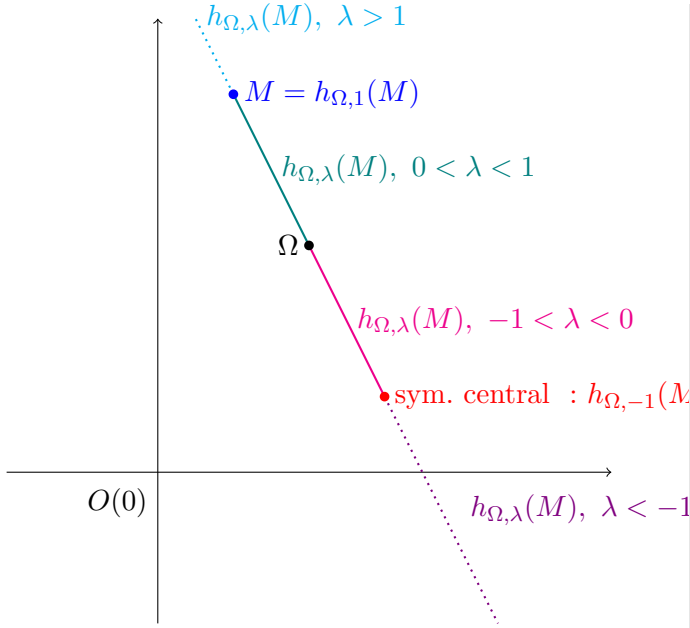


FIGURE V.4 – Quelques homothéties de centre Ω .

Sinon, une rotation d'angle θ n'a qu'un point fixe : son centre.

Enfin, si $\theta = \pi$ $[2\pi]$, la rotation d'angle θ et de centre Ω est la symétrie (centrale) par rapport à Ω .

Définition 8.2.5 (Homothétie).

Soit Ω un point du plan, $\lambda \in \mathbb{R}^*$.

L'homothétie de centre Ω et de rapport λ est l'application qui envoie tout point M sur le point M' vérifiant $\overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M}$ (voir figure V.4). On la note souvent $h_{\Omega, \lambda}$.

Remarque 8.2.6.

Si $\lambda = 1$, toute homothétie de rapport λ est l'identité.

Sinon, une homothétie de rapport λ n'a qu'un point fixe : son centre.

Si $\lambda = 0$, l'homothétie de rapport λ et de centre Ω envoie tout point sur Ω . Enfin, l'homothétie de rapport -1 et de centre Ω est la symétrie (centrale) par rapport à Ω .

Théorème 8.2.7.

Soit M un point d'affixe z , et Ω un point d'affixe ω .

1. Soit $\vec{u}$ un vecteur d'affixe u . L'image de M par la translation de vecteur $\vec{u}$ a pour affixe le nombre complexe $z + u$;
2. Soit $\lambda \in \mathbb{R}$. L'image de M par l'homothétie de centre Ω et de rapport λ a pour affixe le nombre complexe $\omega + \lambda(z - \omega)$;
3. Soit $\theta \in \mathbb{R}$. L'image de M par la rotation de centre Ω et d'angle de mesure θ a pour affixe le nombre complexe $\omega + e^{i\theta}(z - \omega)$. En particulier, iz est l'affixe de l'image de M par la rotation de centre O et d'angle de mesure $\frac{\pi}{2}$;
4. L'image de M par la symétrie centrale de centre O a pour affixe le nombre complexe $-z$;
5. L'image de M par la symétrie par rapport à l'axe des abscisses (Ox) a pour affixe le nombre complexe $\bar{z}$;
6. L'image de M par la symétrie par rapport à l'axe des ordonnées (Oy) a pour affixe le nombre complexe $-\bar{z}$.

Démonstration.

1. L'image M' de M est telle que $\overrightarrow{OM'} = \overrightarrow{OM} + \vec{u}$. On traduit cela en termes d'affixes.
2. $\overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M}$, donc $z' - \omega = \lambda(z - \omega)$.
3. $\Omega M' = \Omega M$ et $(\overrightarrow{\Omega M'}, \overrightarrow{\Omega M}) = \theta[2\pi]$, donc $|z' - \omega| = |z - \omega|$ et $\arg(z' - \omega) - \arg(z - \omega) = \theta[2\pi]$, d'où $z' - \omega = e^{i\theta}(z - \omega)$.
4. C'est une homothétie de centre O et de rapport -1 .
5. Déjà vu.
6. On compose.

□

Exemple 8.2.8.

1. L'homothétie de centre $(2 - i)$ et de rapport 3 s'écrit : $z \mapsto 3(z - 2 + i) + 2 - i = 3z - 4 + 2i$.
2. La rotation de centre 0 et d'angle $\frac{\pi}{2}$ s'écrit $z \mapsto iz$.
3. La rotation de centre $(1 + i)$ et d'angle $\frac{2\pi}{3}$ s'écrit $z \mapsto j(z - 1 - i) + 1 + i$.

Exercice 8.2.9.

Soit quatre points du plan $A(a)$, $B(b)$, $C(c)$ et $D(d)$.

1. On suppose que $ABCD$ est un carré et que a et b ont des parties imaginaires et réelles entières. Montrer qu'il en est de même pour c et d .
2. On suppose que ABC est un triangle équilatéral et que a et b ont des parties imaginaires et réelles entières. Peut-il en être de même pour c ?

8.3 Similitudes et isométries

Définition 8.3.1.

Soit $\lambda > 0$. On appelle *similitude (plane) de rapport* λ toute application f du plan dans lui-même telle que pour tous points M, N on ait :

$$f(M)f(N) = \lambda MN.$$

On appelle *isométrie (plane)* toute application f du plan dans lui-même telle que pour tous points M, N on ait :

$$f(M)f(N) = MN.$$

Remarque 8.3.2. 1. Comme le nom l'indique (racines grecques), les isométries préservent les distances.

2. Les isométries sont les similitudes de rapport 1.
3. La composée de deux isométries est une isométrie.
4. La composée de deux similitudes est une similitude de rapport le produit des rapports de celles-ci.
5. Il est clair que toute similitude est injective. On pourrait montrer que toute similitude est en fait bijective.

Exemple 8.3.3.

Les translations, les rotations, les symétries et les homothéties sont des similitudes.

Théorème 8.3.4. 1. Les applications de $\mathbb{C}$ dans $\mathbb{C}$ de la forme $z \mapsto az + b$, où $(a, b) \in \mathbb{C}^2$ avec $a \neq 0$, sont des similitudes de rapport $|a|$.

2. De plus, une telle application préserve les angles orientés : on dit que c'est une similitude *directe*.

Démonstration. 1. Soit f une application de la forme $z \mapsto az + b$, où $(a, b) \in \mathbb{C}^2$ avec a non nul.

Alors, soit $(z, z') \in \mathbb{C}^2$. On a $|f(z') - f(z)| = |a||z' - z|$. Donc f est une similitude de rapport $|a|$.

2. Soient $a, b \in \mathbb{C}$ tels que $a \neq 0$ et soit f la similitude $z \mapsto az + b$. Soient en outre u, v et w trois points distincts. Leurs images respectives par f sont notées u', v' et w' . Alors

$$\frac{u' - w'}{u' - v'} = \frac{(au + b) - (aw + b)}{(au + b) - (av + b)} = \frac{a(u - w)}{a(u - v)} = \frac{u - w}{u - v}$$

d'où égalité des arguments de ces expressions, et l'égalité des angles recherchée. $\square$

Remarque 8.3.5.

On pourrait montrer que réciproquement toutes les similitudes planes directes sont de cette forme.

Exemple 8.3.6.

Translations, rotations et homothéties vs. symétries axiales.

Théorème 8.3.7 (Caractérisation géométrique).

Soit $a, b \in \mathbb{C}$ tel que $a \neq 0$ et $f : \mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto az + b$.

1. Si $a = 1$, f est la translation de vecteur b .
2. Si $a \neq 1$, notons $\theta = \arg(a)$ et $\omega = \frac{b}{1 - a}$. Alors f est la composée de l'homothétie de rapport $|a|$ et de la rotation d'angle θ , toutes deux de centre ω . De plus cette homothétie et cette rotation commutent. On dit que f est la *similitude directe de centre ω , de rapport $|a|$ et d'angle θ* .

Démonstration. 1. Direct.

2. Supposons donc que $a \neq 1$. L'équation $f(z) = z$ n'a qu'une solution : $\omega = \frac{b}{1-a}$. On a alors :

$$\begin{aligned}
 f(z) - \omega &= f(z) - f(\omega) \\
 &= (az + b) - (a\omega + b) \\
 &= a(z - \omega) \\
 &= |a| \times \underbrace{\left(e^{i \arg a} (z - \omega) \right)}_{\substack{\text{rotation de centre } \omega \text{ et d'angle de mesure } \arg a \\ \text{homothétie de centre } \omega \text{ et de rapport } |a| > 0}} \\
 &= e^{i \arg a} \times \underbrace{\left(|a| (z - \omega) \right)}_{\substack{\text{homothétie de centre } \omega \text{ et de rapport } |a| > 0 \\ \text{rotation de centre } \omega \text{ et d'angle de mesure } \arg a}}
 \end{aligned}$$

□

Exemple 8.3.8.

L'application $f : z \mapsto (1 + i)z + 2$ est la similitude directe de centre $2i$, de rapport $\sqrt{2}$ et d'angle de mesure $\frac{\pi}{4}$.

Chapitre VI

Équations différentielles linéaires

Sommaire

1	Résultats d'analyse	94
1.1	Continuité et dérivabilité d'une fonction à valeurs complexes.	94
1.2	Primitives.	95
1.3	Intégration de fonctions complexes. . .	96
1.4	Méthodes de calcul.	97
	a Intégration par parties.	97
	b Changement de variables.	97
1.5	Primitives de fonctions de la forme $x \mapsto$ $\frac{1}{ax^2 + bx + c}$	99
	a $\Delta > 0$	99
	b $\Delta = 0$	99
	c $\Delta < 0$	99
2	Équations linéaires du premier ordre. .	100
2.1	Cadre.	100
2.2	Structure de l'ensemble des solutions. .	100
2.3	Résolution de l'équation homogène. . .	101
2.4	Résolution d'une équation avec second membre.	102
2.5	Résolution pratique.	103
	a Schéma de résolution (à connaître !).	103
3	Équations différentielles du second ordre à coefficients constants.	103
3.1	Cadre.	103
3.2	Structure de l'ensemble des solutions. .	104
3.3	Résolution d'une équation homogène. .	104
3.4	Résolution d'une équation avec second membre.	107
3.5	Seconds membres particuliers	107

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Résultats d'analyse

On utilise ici les notions d'analyse vues en terminale : continuité, dérivabilité, intégrales. Elles seront définies et travaillées ultérieurement.

1.1 Continuité et dérivabilité d'une fonction à valeurs complexes.

Si on ne le précise pas, I est toujours un intervalle de $\mathbb{R}$ et $f : I \rightarrow \mathbb{C}$.

Définition 1.1.1.

On appelle *partie réelle de f* la fonction

$$\begin{aligned} \operatorname{Re}(f) : I &\rightarrow \mathbb{R} \\ x &\mapsto \operatorname{Re}(f(x)) \end{aligned}.$$

De même on appelle *partie imaginaire de f* la fonction

$$\begin{aligned} \operatorname{Im}(f) : I &\rightarrow \mathbb{R} \\ x &\mapsto \operatorname{Im}(f(x)) \end{aligned}.$$

On peut alors décomposer : $f = \operatorname{Re}(f) + i \operatorname{Im}(f)$.

Remarque 1.1.2.

Cette définition assure que, de manière générale,

$$\operatorname{Re}(f(x)) = \operatorname{Re}(f)(x) \quad \text{et} \quad \operatorname{Im}(f(x)) = \operatorname{Im}(f)(x).$$

Exemple 1.1.3.

Avec

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{C} \\ x &\mapsto (2 + i)e^{(1+i)x}, \end{aligned}$$

on a

$$\begin{aligned} \operatorname{Re}(f) : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto e^x(2 \cos(x) - \sin(x)) \end{aligned}$$

et

$$\begin{aligned} \operatorname{Im}(f) : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto e^x(\cos(x) + 2 \sin(x)) \end{aligned}.$$

Définition 1.1.4. 1. On dit que f est *continue* (resp. *dérivable*) en a si $\operatorname{Re}(f)$ et $\operatorname{Im}(f)$ le sont. Dans le cas où f est dérivable, on appelle *dérivée de f en a* notée $f'(a)$ le complexe

$$f'(a) = (\operatorname{Re}(f))'(a) + i(\operatorname{Im}(f))'(a).$$

2. On dit que f est *continue* (resp. *dérivable*) sur un intervalle si elle l'est en tout point de cet intervalle.
3. On note (notations non officielles) $\mathcal{C}(I, \mathbb{K})$ et $\mathcal{D}(I, \mathbb{K})$ l'ensemble des fonctions respectivement continues et dérivables de I dans $\mathbb{K}$.

Remarque 1.1.5.

Le premier point de la définition précédente assure que, si $f : I \rightarrow \mathbb{C}$ est dérivable, alors

$$(\operatorname{Re} f)' = \operatorname{Re}(f') \quad \text{et} \quad (\operatorname{Im} f)' = \operatorname{Im}(f').$$

Les propriétés usuelles de la dérivée sont vraies du point de vue complexe.

Proposition 1.1.6.

Soit $A \subset \mathbb{R}$, $f, g : I \rightarrow \mathbb{C}$ dérivables.

1. Si $\lambda, \mu \in \mathbb{C}$, alors $\lambda f + \mu g$ est dérivable et

$$(\lambda f + \mu g)' = \lambda f' + \mu g'.$$

2. La fonction fg est dérivable et

$$(fg)' = f'g + fg'.$$

3. Si g ne s'annule pas, la fonction $\frac{f}{g}$ est dérivable et

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$

Démonstration.

À chaque fois, décomposer tous les objets selon leurs parties réelles et imaginaires, puis revenir aux définitions en utilisant les propriétés de la dérivation réelle. $\square$

Pour la composition, on se gardera de dériver deux fonctions à variable complexe (c'est bien plus compliqué que de dériver des fonctions à variable réelle). On dispose cependant du résultat suivant.

Théorème 1.1.7.

Soit $\varphi \in \mathcal{D}(I, \mathbb{K})$. L'application $x \mapsto e^{\varphi(x)}$ est dérivable sur I de dérivée l'application $x \mapsto \varphi'(x)e^{\varphi(x)}$.

Démonstration.

Soit $x \in I$, on a

$$e^{\varphi(x)} = e^{\operatorname{Re}(\varphi(x))} (\cos(\operatorname{Im}(\varphi(x))) + i \sin(\operatorname{Im}(\varphi(x)))).$$

On a donc

$$\operatorname{Re}(e^{\varphi(x)}) = e^{\operatorname{Re}(\varphi(x))} \cos(\operatorname{Im}(\varphi(x))),$$

$$\operatorname{Im}(e^{\varphi(x)}) = e^{\operatorname{Re}(\varphi(x))} \sin(\operatorname{Im}(\varphi(x))).$$

Ces deux expressions sont bien dérivables, par opérations sur les fonctions dérivables, donc e^{φ} est bien dérivable.

De plus,

$$\frac{d}{dx}(e^{\operatorname{Re}(\varphi(x))}) = \operatorname{Re}(\varphi'(x)) \times e^{\operatorname{Re}(\varphi(x))}.$$

Il suffit ensuite de dériver les produits :

$$\begin{aligned} \frac{d}{dx}(\operatorname{Re}(e^{\varphi(x)})) &= \operatorname{Re}(\varphi'(x))e^{\operatorname{Re}(\varphi(x))} \cos(\operatorname{Im}(\varphi(x))) \\ &\quad - \operatorname{Im}(\varphi'(x))e^{\operatorname{Re}(\varphi(x))} \sin(\operatorname{Im}(\varphi(x))). \end{aligned}$$

et

$$\begin{aligned} \frac{d}{dx}(\operatorname{Im}(e^{\varphi(x)})) &= \operatorname{Re}(\varphi'(x))e^{\operatorname{Re}(\varphi(x))} \sin(\operatorname{Im}(\varphi(x))) \\ &\quad + \operatorname{Im}(\varphi'(x))e^{\operatorname{Re}(\varphi(x))} \cos(\operatorname{Im}(\varphi(x))). \end{aligned}$$

Il suffit enfin de vérifier que

$$\frac{d}{dx}(\operatorname{Re}(e^{\varphi(x)})) + i \frac{d}{dx}(\operatorname{Im}(e^{\varphi(x)})) = \varphi'(x)e^{\varphi(x)}.$$

□

Exemple 1.1.8.

Dériver la fonction de l'exemple 1.1.3.

Définition 1.1.9 (Dérivées successives.).

On définit par récurrence les dérivées successives d'une fonction $f : I \rightarrow \mathbb{C}$.

- $f^{(0)} = f$.
- Si f est dérivable, $f^{(1)} = f'$.
- Pour tout entier naturel n , si $f^{(n)}$ est définie et est dérivable, alors on définit $f^{(n+1)} = (f^{(n)})'$.

Remarque 1.1.10.

On notera souvent f'' au lieu de $f^{(2)}$, un peu plus rarement f''' au lieu de $f^{(3)}$.

Les physiciens utilisent souvent les notations $\dot{f}$, $\ddot{f}$ et $\dddot{f}$ pour indiquer des dérivées successives par rapport à la variable temps.

Définition 1.1.11. 1. On note $\mathcal{C}^1(I, \mathbb{K})$ l'ensemble des fonctions continuellement dérivables sur I , *i.e.* l'ensemble des fonctions dérivables, dont la dérivée est continue :

$$\mathcal{C}^1(I, \mathbb{K}) = \{ f \in \mathcal{D}(I, \mathbb{K}) \mid f' \in \mathcal{C}(I, \mathbb{K}) \}.$$

2. Si $n \in \mathbb{N}$, on note $\mathcal{D}^n(I, \mathbb{K})$ l'ensemble des fonctions n fois dérivables sur I : ce sont les fonctions f telles que $f^{(n)}$ est définie.

3. Si $n \in \mathbb{N}$, on note aussi $\mathcal{C}^n(I, \mathbb{K})$ l'ensemble des fonctions n fois continuellement dérivables sur I , *i.e.* l'ensemble des fonctions n fois dérivables, dont la dérivée n^e est continue :

$$\mathcal{C}^n(I, \mathbb{K}) = \{ f \in \mathcal{D}^n(I, \mathbb{K}) \mid f^{(n)} \in \mathcal{C}(I, \mathbb{K}) \}.$$

4. On note $\mathcal{C}^\infty(I, \mathbb{K})$ l'ensemble des fonctions infiniment dérivables : c'est l'intersection

$$\bigcap_{n \in \mathbb{N}} \mathcal{C}^n(I, \mathbb{K}).$$



On ne dérive ici que des fonctions d'une variable réelle.

Remarque 1.1.12.

Si f est dans $\mathcal{C}^n(I, \mathbb{K})$, on dit que f est de *classe* $\mathcal{C}^n$ sur I .

1.2 Primitives.

Si on ne le précise pas, I est toujours un intervalle de $\mathbb{R}$ et $f : I \rightarrow \mathbb{K}$.

Définition 1.2.1.

Soit $A \subset \mathbb{R}$, soit $f : A \rightarrow \mathbb{K}$ et $F : A \rightarrow \mathbb{K}$. On dit que F est **UNE primitive** de f si F est dérivable sur A et si $F' = f$.

Théorème 1.2.2.

Soit I un intervalle de $\mathbb{R}$, soit $f : I \rightarrow \mathbb{K}$ dérivable. La fonction f est constante si et seulement si

$$\forall x \in I, f'(x) = 0.$$



L'hypothèse fondamentale est ici que I est un intervalle.

Exercice 1.2.3.

Proposer un contre-exemple au théorème précédent dans le cas où I n'est pas un intervalle.

Corollaire 1.2.4.

Toutes les primitives d'une même fonction *sur un intervalle* diffèrent d'une constante, et quand cette constante parcourt $\mathbb{K}$, on obtient toutes les primitives.

Autrement dit, I est un intervalle de $\mathbb{R}$ et si $F : I \rightarrow \mathbb{K}$ est une primitive de $f : I \rightarrow \mathbb{K}$, l'ensemble de toutes les primitives de f est

$$\{ F + \lambda \mid \lambda \in \mathbb{K} \}.$$



L'hypothèse fondamentale est ici que l'on se place sur un intervalle.

Démonstration.

Soit F et G deux primitives d'une même application sur un intervalle.

Alors, $F' = G'$, donc $(F - G)'$ est nulle sur cet intervalle, donc $F - G$ est constante sur cet intervalle. Donc toutes les primitives d'une même application diffèrent d'une constante.

Réciproquement, si F est une primitive de f , il est aisé de voir que $F + \lambda$ est une primitive de f pour tout $\lambda \in \mathbb{K}$. $\square$

Exercice 1.2.5.

Déterminer l'ensemble des primitives de la fonction inverse, définie sur $\mathbb{R}^*$.



Il convient de connaître toutes les primitives du formulaire.

1.3 Intégration de fonctions complexes.

Définition 1.3.1.

Soit I un intervalle de $\mathbb{R}$, $a, b \in I$ et $f \in \mathcal{C}(I, \mathbb{C})$. On appelle *intégrale de f sur $[a, b]$* le complexe

$$\int_a^b \operatorname{Re}(f)(t) dt + i \int_a^b \operatorname{Im}(f)(t) dt,$$

noté $\int_a^b f(t) dt$ ou $\int_a^b f$.



Pour pouvoir calculer $\int_a^b f$, f doit être définie au moins sur $[a, b]$. C'est assuré si $f : I \rightarrow \mathbb{C}$, avec I un intervalle et $a, b \in I$.

Remarque 1.3.2.

Cette définition assure que, si $f : I \rightarrow \mathbb{C}$ et si $a, b \in I$,

$$\operatorname{Re} \left(\int_a^b f \right) = \int_a^b \operatorname{Re}(f)$$

et

$$\operatorname{Im} \left(\int_a^b f \right) = \int_a^b \operatorname{Im}(f).$$

Exemple 1.3.3.

$$\int_0^{2\pi} (1 + i)e^{ix} dx = 0.$$

Proposition 1.3.4.

Soit I un intervalle de $\mathbb{R}$, $a, b \in I$, $f, g : I \rightarrow \mathbb{C}$ continues et $\lambda, \mu \in \mathbb{C}$. Alors,

$$\int_a^b (\lambda f + \mu g) = \lambda \int_a^b f + \mu \int_a^b g.$$

Démonstration.

C'est connu quand f, g, λ, μ sont réels. Il suffit de décomposer selon les parties réelles et imaginaires, puis de calculer. Pour alléger le calcul, on pourra traiter séparément le cas de la somme de celui du produit par un complexe. $\square$



L'interprétation en terme d'aire ne veut rien dire pour une fonction à valeurs complexes. Cela dit, comme pour les fonctions réelles, on peut calculer des intégrales par primitivation, ce qui est exprimé dans le théorème suivant.

Théorème 1.3.5 (Théorème fondamental du calcul intégral).

Soit I un intervalle de $\mathbb{R}$, $f \in \mathcal{C}(I, \mathbb{K})$ et $a \in I$.

1. La fonction $\begin{cases} I \rightarrow \mathbb{K} \\ x \mapsto \int_a^x f(t) dt \end{cases}$ est une primitive de f .
2. Soit $A \in \mathbb{K}$. La fonction

$$\begin{aligned} F : I &\rightarrow \mathbb{K} \\ x &\mapsto A + \int_a^x f(t) dt \end{aligned}$$

est la seule primitive de f telle que $F(a) = A$.

Corollaire 1.3.6.

Soit I un intervalle de $\mathbb{R}$, $f \in \mathcal{C}(I, \mathbb{K})$, $a, b \in I$ et F une primitive de f sur I . Alors,

$$\int_a^b f = F(b) - F(a).$$

Exemple 1.3.7.

Refaire le calcul de l'exemple 1.3.3 en primitivant directement.

Notation 1.3.8.

On note $\int_a^x f(t) dt$ une primitive « générique » de la fonction f , c'est-à-dire faisant abstraction d'une quelconque constante d'intégration.

Exemple 1.3.9.

On pourra écrire

$$\int^x \cos(t) dt = \sin(x).$$

On remarquera que le « = » n'a ici pas le rôle qu'on lui attribue habituellement : on aurait pu tout aussi bien écrire

$$\int^x \cos(t) dt = \sin(x) + 42,$$

sans pour autant signifier que $42 = 0$. Pour plus de détails, on se référera au chapitre sur les relations d'équivalences.

Exercice 1.3.10.

Soient a et b deux réels. Calculer les primitives de $x \mapsto e^{ax} \cos(bx)$ et celles de $x \mapsto e^{ax} \sin(bx)$.

1.4 Méthodes de calcul.

On donne ici les deux outils permettant de calculer l'immense majorité des intégrales que vous rencontrerez dans vos deux années de prépa. Ils sont à maîtriser parfaitement.

a Intégration par parties.

Théorème 1.4.1.

Soit I un intervalle de $\mathbb{R}$, $u, v \in \mathcal{C}^1(I, \mathbb{K})$ et $a, b \in I$. Alors,

$$\int_a^b u'v = [uv]_a^b - \int_a^b uv'.$$

Démonstration.

Puisque u, v sont de classe $\mathcal{C}^1$, $(uv)' = u'v + uv'$ est continue, donc par le théorème fondamental du calcul intégral :

$$[uv]_a^b = \int_a^b (uv)' = \int_a^b u'v + uv' = \int_a^b u'v + \int_a^b uv'.$$

□

Exemple 1.4.2 (Grands classiques).

Tous ces exemples se résolvent par intégration par parties.

- Trouver une primitive de $\ln$.
- Trouver une primitive de Arctan .
- Trouver une primitive du produit d'un polynôme et d'une exponentielle.
- Trouver une primitive du produit d'une fonction trigonométrique et d'une exponentielle.
- Trouver une primitive du produit d'un polynôme et d'une fonction trigonométrique.

Exercice 1.4.3.

Déterminer des primitives des fonctions suivantes : $x \mapsto (x^2 + 1)e^x$, $x \mapsto \cos(x)e^{2x}$, $x \mapsto x^2 \cos x$.

b Changement de variables.

Théorème 1.4.4.

Soit I, J deux intervalles de $\mathbb{R}$, $a, b \in I$, $\varphi \in \mathcal{C}^1(I, \mathbb{R})$ et $f \in \mathcal{C}^0(J, \mathbb{R})$

On suppose que $\varphi(I) \subset J$. Alors,

$$\int_{\varphi(a)}^{\varphi(b)} f(x) dx = \int_a^b \varphi'(t) \cdot (f \circ \varphi)(t) dt.$$

On dit que l'on a effectué le changement de variable « $x = \varphi(t)$ ».

Remarque 1.4.5.

Moyen mnémotechnique : on écrit « $x = \varphi(t)$ » (au brouillon seulement !). Alors $dx = \varphi'(t) dt$, donc $\int f(x) dx = \int f(\varphi(t)) \varphi'(t) dt$. Reste le problème des bornes. Quand t va de a à b , $x = \varphi(t)$ va de $\varphi(a)$ à $\varphi(b)$. Et voilà ...

Démonstration.

f est continue sur I , donc y admet une primitive F . Ainsi, F est $\mathcal{C}^1$, comme $\varphi \in \mathcal{C}^1$. On voit que $F \circ \varphi$ est $\mathcal{C}^1$, et $(F \circ \varphi)' = \varphi' \cdot f \circ \varphi$ est continue.

On déduit alors le résultat du théorème fondamental (utilisé deux fois) :

$$\begin{aligned} \int_{\varphi(a)}^{\varphi(b)} f(t) dt &= [F]_{\varphi(a)}^{\varphi(b)} \\ &= F(\varphi(b)) - F(\varphi(a)) \\ &= [F \circ \varphi]_a^b \\ &= \int_a^b f(\varphi(t)) \varphi'(t) dt. \end{aligned}$$

□

Remarque 1.4.6.

Les seuls changements de variables que l'on se permettra de ne pas justifier sont ceux affines (on les signalera quand même !).

Exemple 1.4.7.

Calculons l'aire de l'ellipse d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (voir figure VI.1).

Le quart supérieur droit de cette ellipse peut être paramétré par $\left(x, b\sqrt{1 - \frac{x^2}{a^2}}\right)$, x allant de

0 à a . On calcule donc $I = \int_0^a b\sqrt{1 - \frac{x^2}{a^2}} dx$.

On effectue le changement de variable $x = a \cos \theta$:

- la fonction $f : [0, a] \rightarrow \mathbb{R}, x \mapsto \sqrt{1 - \frac{x^2}{a^2}}$ est continue,

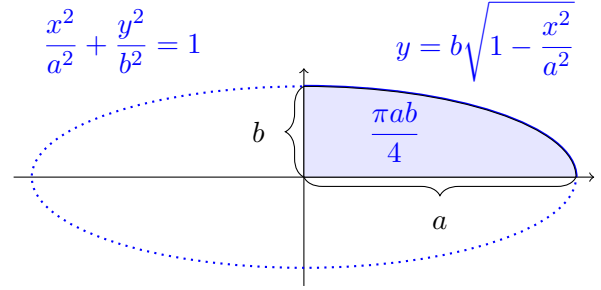


FIGURE VI.1 – Ellipse de demi-axes a et b .

- la fonction $\varphi : [0, \pi/2], \theta \mapsto a \cos \theta$ est de classe $\mathcal{C}^1$ et à valeurs dans $[0, a]$,
- on a $\varphi' : \theta \mapsto -a \sin \theta$,
- $\varphi(0) = a$ et $\varphi(\pi/2) = 0$.

Remarquons que le sinus est positif sur $[0, \pi/2]$, et si $\theta \in [0, \pi/2]$, $f(\varphi(\theta)) = |\sin \theta|$. On obtient :

$$\begin{aligned} I &= -ab \int_{\pi/2}^0 |\sin \theta| \sin \theta d\theta \\ &= -ab \int_{\pi/2}^0 \sin^2 \theta d\theta \\ &= ab \int_0^{\pi/2} \frac{1 - \cos(2\theta)}{2} d\theta \\ &= \frac{1}{4} \pi ab - \frac{ab}{2} \left[\frac{1}{2} \sin(2\theta) \right]_0^{\pi/2} \\ &= \frac{1}{4} \pi ab. \end{aligned}$$

L'aire de l'ellipse est donc πab .

Exemple 1.4.8.

En posant $x = \sqrt{t}$, on a

$$\begin{aligned} \int_1^3 \frac{dt}{\sqrt{t} + \sqrt{t^3}} &= 2 \int_1^3 \frac{1}{1 + \sqrt{t^2}} \times \frac{1}{2\sqrt{t}} dt \\ &= 2 \int_{\sqrt{1}}^{\sqrt{3}} \frac{1}{1 + x^2} dx \\ &= 2 [\text{Arctan}(x)]_{x=1}^{\sqrt{3}} \\ &= \frac{\pi}{6}. \end{aligned}$$

Proposition 1.4.9.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une application continue.

- Si f est paire et $a \in \mathbb{R}$ alors

$$\int_{-a}^a f(t) dt = 2 \int_{-a}^0 f(t) dt = 2 \int_0^a f(t) dt.$$

2. Si f est impaire et $a \in \mathbb{R}$ alors

$$\int_{-a}^a f(t) dt = 0$$

$$\text{et } \int_{-a}^0 f(t) dt = - \int_0^a f(t) dt.$$

3. Soit $a \in \mathbb{R}$ et $T > 0$, si f est T -périodique, alors

$$\int_0^T f(t) dt = \int_a^{a+T} f(t) dt.$$

Démonstration. 1. On considère $\int_0^a f(t) dt$ et on réalise le changement de variable $x = -t$. Ainsi,

$$\begin{aligned} \int_0^a f(t) dt &= \int_0^{-a} -f(-x) dx \\ &= - \int_0^{-a} f(x) dx \\ &= \int_{-a}^0 f(x) dx. \end{aligned}$$

2. Comme le point précédent avec

$$\begin{aligned} \int_0^a f(t) dt &= \int_0^{-a} -f(-x) dx \\ &= \int_0^{-a} f(x) dx \\ &= - \int_{-a}^0 f(x) dx. \end{aligned}$$

3. On peut commencer à regarder à partir d'un dessin, dans le cas où $-T < a < 0$.

On a :

$$\int_a^{a+T} f(t) dt = \int_a^0 f(t) dt + \int_0^{a+T} f(t) dt$$

Or par changement de variable $x = t + T$, on obtient

$$\int_a^0 f(t) dt = \int_{a+T}^T f(x) dx.$$

On en déduit que

$$\begin{aligned} \int_a^{a+T} f(t) dt &= \int_{a+T}^T f(t) dt + \int_0^{a+T} f(t) dt \\ &= \int_0^T f(t) dt. \end{aligned}$$

On peut remarquer que l'hypothèse $-T < a < 0$ qui a nourri notre intuition ne joue en fait aucun rôle : elle n'est utilisée nulle part dans la démonstration.

Nous avons donc le résultat attendu.

□

1.5 Primitives de fonctions de la forme

$$x \mapsto \frac{1}{ax^2 + bx + c}$$

Soit $a, b, c \in \mathbb{R}$, $a \neq 0$, et $f : x \mapsto \frac{1}{ax^2 + bx + c}$. Le programme demande de savoir calculer une primitive de f à ce stade de l'année. Mais nous reverrons cela dans le chapitre sur les fractions rationnelles.

Pour simplifier, quitte à diviser par a , on peut toujours se ramener au cas où $a = 1$. Ainsi on considère $f : x \mapsto \frac{1}{x^2 + bx + c}$. Posons $\Delta = b^2 - 4c$.

Il s'agit de distinguer trois cas :

a $\Delta > 0$

Le polynôme $X^2 + bX + c$ a donc deux racines réelles distinctes α et β , et $f(x) = \frac{1}{(x - \alpha)(x - \beta)}$. Il s'agit alors de remarquer que $f(x) = \frac{1}{\alpha - \beta} \left(\frac{1}{x - \alpha} - \frac{1}{x - \beta} \right)$. Et donc directement, une primitive de f est $x \mapsto \frac{1}{\alpha - \beta} \ln \left| \frac{x - \alpha}{x - \beta} \right|$.

b $\Delta = 0$

Le polynôme $X^2 + bX + c$ a donc une racine double réelle α et β , et $f(x) = \frac{1}{(x - \alpha)^2}$. Encore plus directement, une primitive de f est $x \mapsto -\frac{1}{x - \alpha}$.

c $\Delta < 0$

C'est le cas le plus compliqué. Ici, $b^2 - 4c < 0$. On écrit alors $f(x) = \frac{1}{x^2 + bx + c} = \frac{1}{(x + b/2)^2 + \frac{1}{4}(4c - b^2)}$. On pose alors $\delta = \sqrt{\frac{1}{4}(4c - b^2)}$, qui existe bien car $\Delta < 0$. Donc $f(x) = \frac{1}{(x + b/2)^2 + \delta^2}$, dont une primitive est $x \mapsto \frac{1}{\delta} \arctan \left(\frac{x + b/2}{\delta} \right)$.

Remarque 1.5.1.

Ces formules ne sont en aucun cas à apprendre

par cœur, mais il convient de savoir mener ces calculs sur des exemples concrets.

2 Équations linéaires du premier ordre.

2.1 Cadre.

- On s'intéressera à des équations différentielles dont les solutions sont à valeurs dans $\mathbb{K}$, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.
- On considérera I un intervalle ouvert de $\mathbb{R}$.

Définition 2.1.1.

Soit a et b des applications continues de I dans $\mathbb{K}$, alors

- On appelle *équation différentielle linéaire du premier ordre* l'équation d'inconnue y

$$y' + a(t)y = b(t). \quad (\mathcal{E})$$

- Une *solution* de cette équation est une application $f : I \rightarrow \mathbb{K}$ dérivable sur I vérifiant : pour tout $t \in I$,

$$f'(t) + a(t)f(t) = b(t).$$

- L'équation $(\mathcal{E})$ est dite *homogène* si b est la fonction nulle ($b = 0_{\mathbb{K}I}$).
- L'équation homogène associée à $(\mathcal{E})$ est

$$y' + a(t)y = 0. \quad (\mathcal{H})$$

Remarque 2.1.2.

Nous ne nous intéresserons pas dans le reste du paragraphe au cas plus général d'une équation

$$a_1(t)y' + a_0(t)y = b(t) \quad (\mathcal{E})$$

où on a également affecté y' d'un coefficient $a_1(t)$, avec a_1, a_0 des applications continues sur I .

En effet :

- Si a_1 ne s'annule pas, il suffit de diviser cette équation par $a_1(t)$ pour se ramener au cas étudié ici.

- Si a_1 s'annule, il est difficile de donner des résultats généraux. En pratique, si on rencontre une telle équation où a_1 s'annule, on cherchera en général les solutions sur les intervalles où a_1 ne s'annule pas et on regardera au cas par cas comment recoller les solutions aux points où a_1 s'annule. On rencontrera une telle situation en TD.

Définition 2.1.3 (Problème de Cauchy).

Soit

- $t_0 \in I$
- y_0 un élément de $\mathbb{K}$

La recherche des solutions f de $(\mathcal{E})$ vérifiant la *condition initiale* suivante :

$$f(t_0) = y_0$$

est appelé *problème de Cauchy linéaire d'ordre n*

Exemple 2.1.4.

Se reporter au cours de physique, pour des exemples d'équations différentielles linéaires du premier ordre, en électricité par exemple.

2.2 Structure de l'ensemble des solutions.

Théorème 2.2.1 (Structure des solutions).

Soit

- $(\mathcal{E})$ une équation différentielle linéaire du premier ordre, d'ensemble de solutions $S_{\mathcal{E}}$
- $(\mathcal{H})$ l'équation homogène associée, d'ensemble de solutions $S_{\mathcal{H}}$

Alors

1. $S_{\mathcal{E}} \subset \mathcal{C}^1(I, \mathbb{K})$
2. $0_I \in S_{\mathcal{H}}$ et $S_{\mathcal{H}}$ est stable par combinaisons linéaires.
3. Pour tout $y_0 \in S_{\mathcal{E}}$ fixé,

$$S_{\mathcal{E}} = \{ y_0 + y \mid y \in S_{\mathcal{H}} \}.$$

4. En particulier, $S_{\mathcal{E}}$ est l'ensemble vide ou un singleton ou un ensemble infini.

Démonstration.

Sous les hypothèses de l'énoncé :

1. Toute solution f est nécessairement dérivable et pour tout $t \in I$,

$$f'(t) = b(t) - a(t)f(t).$$

Or b , a et f sont des applications continues.

Donc f' est continue, donc $f \in \mathcal{C}^1(I, \mathbb{K})$.

2. L'application nulle est une solution triviale de $S_{\mathcal{H}}$, donc $S_{\mathcal{H}}$ est non vide.

Soit f et g deux applications dérivables sur I et λ et μ deux éléments de $\mathbb{K}$. Alors $\lambda f + \mu g$ est évidemment dérivable sur I . Et pour tout $t \in I$,

$$\begin{aligned} (\lambda f + \mu g)'(t) + a(t)(\lambda f + \mu g)(t) &= \lambda f'(t) + \mu g'(t) + a(t)(\lambda f + \mu g)(t) \\ &= \lambda(f'(t) + a(t)f(t)) + \mu(g'(t) + a(t)g(t)) \\ &= 0 \end{aligned}$$

puisque f et g sont dans $S_{\mathcal{H}}$. Donc $\lambda f + \mu g \in S_{\mathcal{H}}$.

3. Soit $y_0 \in S_{\mathcal{E}}$ fixé et $f : I \rightarrow \mathbb{K}$ une application dérivable. Alors

$$\begin{aligned} f \in S_{\mathcal{E}} &\iff f' + af = b \\ &\iff f' + af = y_0' + ay_0 \\ &\iff (f - y_0)' + a(f - y_0) = 0 \\ &\iff f - y_0 \in S_{\mathcal{H}} \end{aligned}$$

Donc pour tout $f \in S_{\mathcal{E}}$, f s'écrit sous la forme $y_0 + y$ où $y \in S_{\mathcal{H}}$. Donc $S_{\mathcal{E}} \subset \{y_0 + y \mid y \in S_{\mathcal{H}}\}$.

Réciproquement, pour tout $y \in S_{\mathcal{H}}$, l'application f définie par $f = y_0 + y$ est dérivable et $f - y_0 \in S_{\mathcal{H}}$, donc $f \in S_{\mathcal{E}}$. Donc $\{y_0 + y \mid y \in S_{\mathcal{H}}\} \subset S_{\mathcal{E}}$.

On a donc bien $S_{\mathcal{E}} = \{y_0 + y \mid y \in S_{\mathcal{H}}\}$.

4. On sait que $S_{\mathcal{H}}$ n'est pas vide puisqu'il contient au moins l'application nulle. Supposons qu'il contienne au moins une autre application f . Alors pour tout $\lambda \in \mathbb{K}$, λf appartient également à $S_{\mathcal{H}}$. Donc ou bien $S_{\mathcal{H}}$ est réduit à un élément, ou bien il est infini.

D'après le point précédent, si $S_{\mathcal{E}}$ possède au moins un élément y_0 , on a $S_{\mathcal{E}} = \{y_0 + y \mid y \in S_{\mathcal{H}}\}$. Donc $y \mapsto y_0 + y$ est une bijection de $S_{\mathcal{H}}$ sur $S_{\mathcal{E}}$, donc $S_{\mathcal{E}}$ est ou bien réduit à un élément (y_0) ou bien est infini.

Donc ou bien $S_{\mathcal{E}}$ est vide, ou il est réduit à un élément, ou il est infini. $\square$

Remarque 2.2.2.

Nous retrouvons ici le même type de structure de l'ensemble des solutions que dans le cas des systèmes linéaires. Ce n'est pas une coïncidence : un même type de structure algébrique se cache derrière (les espaces vectoriels et affines) !

Exemple 2.2.3.

Il a été vu en terminale (et nous redémontrons bientôt) qu'il existe une seule fonction $y : \mathbb{R} \rightarrow \mathbb{R}$ solution de $y' - y = 0$ et vérifiant $y(0) = 1$.

On en déduit que l'ensemble des solutions de l'équation $y' - y = 0$ est

$$\left\{ \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & Ce^x \end{array} \mid C \in \mathbb{R} \right\}.$$

Exercice 2.2.4.

Déterminer toutes les solutions du problème de Cauchy $y' - y = 0$ et $y(0) = 42$.

Théorème 2.2.5 (Principe de superposition).

Soit a, b_1, b_2 des applications continues de I dans $\mathbb{K}$ et $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. On considère les équations

$$y' + ay = b_1, \quad (\mathcal{E}_1)$$

$$y' + ay = b_2, \quad (\mathcal{E}_2)$$

$$y' + ay = \lambda_1 b_1 + \lambda_2 b_2. \quad (\mathcal{E})$$

Alors pour toute solution y_1 de $\mathcal{E}_1$ et toute solution y_2 de $\mathcal{E}_2$, $\lambda_1 y_1 + \lambda_2 y_2$ est une solution de $\mathcal{E}$.

Démonstration.

Soit y_1 et y_2 des solutions respectives de $\mathcal{E}_1$ et $\mathcal{E}_2$.

Donc, on a sur I , $y_1' + ay_1 = b_1$ et $y_2' + ay_2 = b_2$.

On a sur I

$$\begin{aligned} (\lambda_1 y_1 + \lambda_2 y_2)' + a(\lambda_1 y_1 + \lambda_2 y_2) &= \lambda_1 y_1' + \lambda_2 y_2' + a\lambda_1 y_1 + a\lambda_2 y_2 \\ &= \lambda_1 (y_1' + ay_1) + \lambda_2 (y_2' + ay_2) \\ &= \lambda_1 b_1 + \lambda_2 b_2 \end{aligned}$$

Ainsi, $\lambda_1 y_1 + \lambda_2 y_2$ est solution de $\mathcal{E}$. $\square$

2.3 Résolution de l'équation homogène.

Théorème 2.3.1.

Soit A une primitive de a sur I . Soit $a \in \mathcal{C}^0(I, \mathbb{K})$.

Alors, l'ensemble des solutions de l'équation homogène $y' + ay = 0$ est

$$S_{\mathcal{H}} = \left\{ \begin{array}{ccc} I & \rightarrow & \mathbb{K} \\ t & \mapsto & Ke^{-A(t)} \end{array} \mid K \in \mathbb{K} \right\}.$$

Si de plus une condition initiale est fixée, alors la solution est unique. En particulier si y s'annule en un point, elle est identiquement nulle.

Démonstration.

Toute fonction de la forme $t \mapsto Ke^{-A(t)}$ est une solution (c'est évident, il n'y a qu'à dériver).

Réciproquement, soit y une solution. On pose $z(t) = y(t)e^{A(t)}$ pour $t \in I$. z est dérivable sur I et pour tout t , $z'(t) = y'(t)e^{A(t)} + y(t)A'(t)e^{A(t)} = (y'(t) + a(t)y(t))e^{A(t)} = 0$, donc z est une constante K .

Une condition initiale $y(t_0) = y_0$ étant donnée, elle est vérifiée si et seulement si $Ke^{-A(t_0)} = y_0$, c'est-à-dire si et seulement si $K = y_0e^{A(t_0)}$. Il y a alors une et une seule solution : $t \mapsto y_0e^{A(t_0)-A(t)}$. $\square$

Remarque 2.3.2.

On dit que l'ensemble des solutions a une structure de droite vectorielle, de vecteur directeur $t \mapsto e^{-A(t)}$.

Remarque 2.3.3.

Dans le cas où a est une constante, l'ensemble des solutions est donc tout simplement $S_{\mathcal{H}} =$

$$\left\{ \begin{array}{l} I \rightarrow \mathbb{K} \\ t \mapsto Ke^{-at} \end{array} \middle| K \in \mathbb{K} \right\}.$$

Exercice 2.3.4.

Déterminer les intervalles de résolution puis résoudre les équations différentielles suivantes.

1. $y' + y = 0$
2. $y' + \frac{1}{\sqrt{1-x^2}}y = 0$ avec $y(1/2) = 1$.

Corollaire 2.3.5.

Une solution qui s'annule en un point ne peut être que la fonction nulle.

Démonstration.

En effet elle est solution d'un problème de Cauchy de la forme $y(t_0) = 0$. Or il existe une unique solution à ce problème et la fonction nulle est manifestement solution. $\square$

2.4 Résolution d'une équation avec second membre.

Remarque 2.4.1.

On a déjà vu que si l'on connaissait une solution $\tilde{y}$ de l'équation avec second membre, alors on pouvait construire toutes les solutions de l'équation avec second membre à partir de l'ensemble des solutions de l'équation homogène.

Dans le cas d'une équation d'ordre un, on dit que l'ensemble des solutions a une structure de

droite affine, car l'ensemble des solutions est l'ensemble des $\tilde{y} + y$ pour y parcourant une droite vectorielle.

Théorème 2.4.2.

Soit a et b deux applications continues de I dans $\mathbb{C}$, et A une primitive de a .

Alors le problème de Cauchy $y' + ay = b$ et $y(t_0) = y_0$ admet une unique solution.

Remarque 2.4.3.

Le théorème précédent implique que par chaque point de $I \times \mathbb{R}$, il passe une et une seule courbe solution. Les courbes solutions partitionnent donc $I \times \mathbb{R}$. Un exemple est donné dans la figure VI.2.

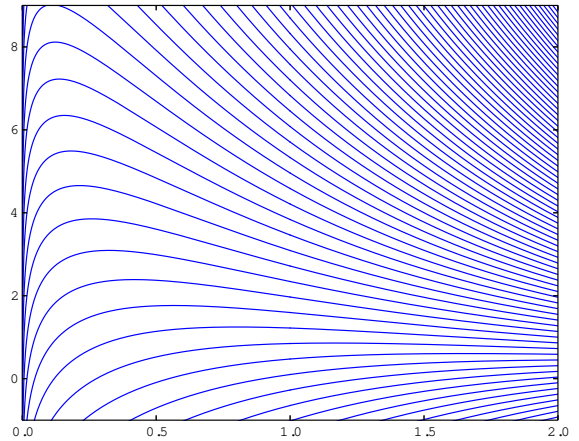


FIGURE VI.2 – Courbes solutions de l'équation $y' + y = \frac{1}{x}$, représentées sur $]0, 2] \times [-1, 9]$.

Remarque 2.4.4.

L'unicité est aisée à démontrer : si on dispose de deux solutions de ce problème, leur différence est une solution de l'équation homogène du problème s'annulant en t_0 , c'est donc l'application nulle.

On peut également assez directement montrer que l'application donnée est solution par calcul.

Nous donnons cependant ci-dessous une autre démonstration qui a l'avantage de permettre de retrouver la formule. Cette méthode est à connaître et s'appelle la *méthode de la variation de la constante*.

Lemme 2.4.5.

Soit $h : I \rightarrow \mathbb{C}$ ne s'annulant pas. Alors, pour tout $y : I \rightarrow \mathbb{C}$, il existe une unique fonction $C : I \rightarrow \mathbb{C}$ telle que $y = Ch$.

De plus, si h est dérivable, alors y est dérivable si et seulement si C l'est.

Démonstration.

C'est élémentaire : $y = Ch$ si et seulement si $C = \frac{y}{h}$.

On obtient la dérivabilité de C ou de y par opérations usuelles sur les fonctions dérivables. $\square$

Démonstration (Théorème 2.4.2).

Notons $\mathcal{E}$ l'équation $y' + ay = b$, $(\mathcal{H})$ l'équation homogène associée, $S_{\mathcal{E}}$ et $S_{\mathcal{H}}$ les ensembles de solutions respectifs de ces deux équations et S l'ensemble des solutions du problème de Cauchy $y' + ay = b$ et $y(t_0) = y_0$.

On sait que $y_{\mathcal{H}} : t \mapsto e^{-A(t)}$ est une solution de $\mathcal{H}$ qui ne s'annule jamais.

D'après le lemme 2.4.5, toute fonction $y : I \rightarrow \mathbb{K}$ dérivable est de la forme $Cy_{\mathcal{H}}$, avec $C : I \rightarrow \mathbb{K}$ dérivable..

Soit donc une fonction $C : I \rightarrow \mathbb{K}$ est une application dérivable, posons $y = Cy_{\mathcal{H}}$. La fonction y est dérivable comme produit de fonctions dérivables.

Soit alors $t \in I$. On a

$$\begin{aligned} y' + ay &= C'y_{\mathcal{H}} + Cy'_{\mathcal{H}} + aCy_{\mathcal{H}} \\ &= C'y_{\mathcal{H}} + C(y'_{\mathcal{H}} + ay_{\mathcal{H}}). \end{aligned}$$

Or $y_{\mathcal{H}}$ est solution de $(\mathcal{H})$, donc $y'_{\mathcal{H}} + ay_{\mathcal{H}} = 0$. Donc y est solution de $\mathcal{E}$ si et seulement si $C'y_{\mathcal{H}} = b$, c'est-à-dire si et seulement si C' est l'application $t \mapsto e^{A(t)}b(t)$, c'est-à-dire si et seulement si C est une primitive de $t \mapsto e^{A(t)}b(t)$, i.e. si et seulement s'il existe $\lambda \in \mathbb{K}$ tel que

$$C : t \mapsto \lambda + \int_{t_0}^t e^{A(u)}b(u) du.$$

Soit $\lambda \in \mathbb{K}$ et

$$y : t \mapsto \lambda e^{-A(t)} + e^{-A(t)} \int_{t_0}^t e^{A(u)}b(u) du.$$

Remarque : On vient donc de prendre une solution quelconque de $(\mathcal{H})$.

Alors, y est solution du problème de Cauchy ($y' + ay = b$ et $y(t_0) = y_0$) si et seulement si $y(t_0) = y_0$, donc si et seulement si $\lambda = y_0 e^{A(t_0)}$, c'est-à-dire si et seulement si y est l'application

$$t \mapsto e^{A(t_0)-A(t)}y_0 + e^{-A(t)} \int_{t_0}^t e^{A(u)}b(u) du.$$

$\square$

2.5 Résolution pratique.

a Schéma de résolution (à connaître !).

On effectuera *toujours* les actions suivantes, dans l'ordre.

1. Déterminer I .
2. Résoudre (E_H) .
3. Trouver une solution dite particulière (solution évidente, second membre d'une forme particulière ou méthode de variation de la constante).
4. S'occuper éventuellement des conditions initiales.
5. Donner la solution, ou l'ensemble des solutions.

Remarque 2.5.1.

On ne vous demande jamais que de trouver *une* solution particulière : faites le plus simplement possible ! Si vous ne voyez pas de solution évidente, la méthode de la variation de la constante est assez efficace et vous permet de retrouver la formule générale (une erreur est vite arrivée !). Il est permis de chercher une solution particulière au brouillon puis de l'exhiber sur sa copie, en justifiant qu'elle vérifie bien les conditions imposées.

Exemple 2.5.2.

On résout l'équation $y' + y = e^{2x}$ sur $\mathbb{R}$. Ses solutions sont toutes les fonctions $x \mapsto \frac{1}{3}e^{2x} + Ke^{-x}$, avec $K \in \mathbb{K}$.

Exercice 2.5.3.

Résoudre le problème de Cauchy :

$$y' - \frac{y}{x} = x \ln(x), \quad y(1) = 2.$$

3 Équations différentielles du second ordre à coefficients constants.

3.1 Cadre.

- On s'intéressera à des équations différentielles dont les solutions sont à valeurs dans $\mathbb{K}$, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.
- On considérera I un intervalle ouvert de $\mathbb{R}$.

Définition 3.1.1.

Soit a, b, c des éléments de $\mathbb{K}$ avec $a \neq 0$, et d une application continue sur I à valeurs dans $\mathbb{K}$.

- On appelle *équation différentielle linéaire du deuxième ordre à coefficients constants* l'équation d'inconnue y

$$ay'' + by' + cy = d(t). \quad (\mathcal{E})$$

- Une *solution* de cette équation est une application $f : I \rightarrow \mathbb{K}$ deux fois dérivables sur I vérifiant : pour tout $t \in I$,

$$af''(t) + bf'(t) + cf(t) = d(t).$$

- L'équation $(\mathcal{E})$ est dite *homogène* si b est la fonction nulle ($b = 0_{\mathbb{K}I}$).
- L'équation *homogène associée* à $(\mathcal{E})$ est

$$ay'' + by' + cy = 0. \quad (\mathcal{H})$$

Définition 3.1.2 (Problème de Cauchy).

Soit

- $t_0 \in I$
- y_0 et y_1 deux éléments de $\mathbb{K}$

La recherche des solutions f de $(\mathcal{E})$ vérifiant la *condition initiale* suivante :

$$f(t_0) = y_0 \text{ et } f'(t_0) = y_1$$

est appelé *problème de Cauchy linéaire du deuxième ordre*

Exemple 3.1.3.

En physique, les déplacements d'un mobile sont régis par l'équation de la dynamique reliant la dérivée seconde de la position et les forces qui s'appliquent au mobile, qui dépendent en général de sa position et ou de sa vitesse. Il s'agit donc d'une équation différentielle d'ordre 2.¹ Il est raisonnable de penser que le problème de Cauchy a alors une unique solution : une position initiale et une vitesse initiale étant données, une seule trajectoire est possible.

1. En général linéaire dans les problèmes de prépa mais dans la vraie vie c'est parfois plus compliqué.

3.2 Structure de l'ensemble des solutions.

Théorème 3.2.1 (Structure des solutions).

Soit

- $(\mathcal{E})$ une équation différentielle linéaire du deuxième ordre, d'ensemble de solutions $S_{\mathcal{E}}$
- $(\mathcal{H})$ l'équation homogène associée, d'ensemble de solutions $S_{\mathcal{H}}$

Alors

1. $S_{\mathcal{E}} \subset \mathcal{C}^2(I, \mathbb{K})$
2. $0_I \in S_{\mathcal{H}}$ et $S_{\mathcal{H}}$ est stable par combinaisons linéaires.
3. Pour tout $y_0 \in S_{\mathcal{E}}$ fixé, on a

$$S_{\mathcal{E}} = \{ y_0 + y \mid y \in S_{\mathcal{H}} \}.$$

4. En particulier, $S_{\mathcal{E}}$ est l'ensemble vide ou un singleton ou un ensemble infini.

Démonstration.

La démonstration est identique à celle du théorème sur les équations différentielles du premier ordre. $\square$

Théorème 3.2.2 (Principe de superposition).

Soit a, b, c des éléments de $\mathbb{K}$, b_1, b_2 des applications continues de I dans $\mathbb{K}$ et $(\lambda_1, \lambda_2) \in \mathbb{K}^2$. On considère les équations

$$ay'' + by' + cy = b_1, \quad (\mathcal{E}_1)$$

$$ay'' + by' + cy = b_2, \quad (\mathcal{E}_2)$$

$$ay'' + by' + cy = \lambda_1 b_1 + \lambda_2 b_2. \quad (\mathcal{E})$$

Alors pour toute solution y_1 de $\mathcal{E}_1$ et toute solution y_2 de $\mathcal{E}_2$, $\lambda_1 y_1 + \lambda_2 y_2$ est une solution de $\mathcal{E}$.

Démonstration.

La démonstration est identique à celle du théorème sur les équations différentielles du premier ordre. $\square$

3.3 Résolution d'une équation homogène.

On considère ici l'équation homogène définie sur $\mathbb{R}$

$$ay'' + by' + cy = 0. \quad (\mathcal{H})$$

Lemme 3.3.1.

Soit $r \in \mathbb{K}$, la fonction $y_r : t \mapsto e^{rt}$ est solution de $(\mathcal{H})$ si et seulement si $ar^2 + br + c = 0$.

Démonstration.

y_r est dérivable et $y'_r = ry_r$. Donc y_r est deux fois dérivable et $y''_r = r^2 y_r$. On a donc $ay''_r + by'_r + cy_r = (ar^2 + br + c)y_r$. On conclut en remarquant que y_r ne s'annule jamais. $\square$

Définition 3.3.2 (Équation et polynôme caractéristique).

L'équation caractéristique de $(\mathcal{H})$ est l'équation

$$ar^2 + br + c = 0. \quad (\text{EC})$$

Le polynôme caractéristique de $(\mathcal{H})$ est

$$aX^2 + bX + c.$$

Théorème 3.3.3 (Solutions complexes de $(\mathcal{H})$).

Soit $a, b, c \in \mathbb{C}$, avec $a \neq 0$.

1. Si (EC) a deux solutions complexes distinctes r_1, r_2 , alors les solutions complexes de $(\mathcal{H})$ sont les applications de la forme

$$\begin{cases} \mathbb{R} & \rightarrow \mathbb{C} \\ t & \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t} \end{cases}$$

pour $(\lambda, \mu) \in \mathbb{C}^2$.

2. Si (EC) a une unique solution complexe r , alors les solutions complexes de $(\mathcal{H})$ sont les applications de la forme

$$\begin{cases} \mathbb{R} & \rightarrow \mathbb{C} \\ t & \mapsto (\lambda t + \mu)e^{rt} \end{cases}$$

pour $(\lambda, \mu) \in \mathbb{C}^2$.

Démonstration.

Soit r une solution complexe de (EC), on sait d'après le lemme 3.3.1 que $y_r : t \mapsto e^{rt}$ est une solution de $(\mathcal{H})$. De plus, y_r ne s'annule jamais.

On peut donc mettre en œuvre la méthode de la variation de la constante. En effet, pour toute fonction $y : \mathbb{R} \rightarrow \mathbb{C}$ deux fois dérivable, il existe $K : \mathbb{R} \rightarrow \mathbb{C}$ deux fois dérivable telle que $y = Ky_r$ (poser $K = y/y_r$).

Soit donc $K : \mathbb{R} \rightarrow \mathbb{C}$ deux fois dérivable, posons $y = Ky_r$. La fonction y est deux fois dérivable, par produit. On a alors, comme $y'_r = ry_r$.

$$y' = K'y_r + Ky'_r = (K' + rK)y_r.$$

Le même type de calcul donne

$$y'' = (K'' + 2rK' + r^2 K)y_r.$$

On a alors

$$ay'' + by' + cy = [aK'' + (2ar + b)K' + (ar^2 + br + c)K] y_r.$$

Ainsi, comme r est solution de (EC), on a $ar^2 + br + c = 0$, donc

$$ay'' + by' + cy = (aK'' + (2ar + b)K')y_r.$$

Comme y_r ne s'annule jamais, $ay'' + by' + cy = 0$ si et seulement si

$$aK'' + (2ar + b)K' = 0.$$

Remarquons que $2ar + b = 0$ si et seulement si $r = -\frac{b}{2a}$, i.e. si et seulement si (EC) possède une unique solution complexe r .

• Si (EC) possède une unique solution complexe, alors y est solution de $(\mathcal{H})$ si et seulement si $K'' = 0$. En primitivant deux fois, on obtient directement que c'est équivalent à « K est une fonction affine », d'où le résultat dans ce cas là.

• Supposons maintenant que (EC) possède deux solutions complexes distinctes, notons r' la seconde solution. On peut tout de suite remarquer que $r + r' = -\frac{b}{a}$. Remarquons aussi que l'équation $aK'' + (2ar + b)K' = 0$ équivaut à l'équation différentielle linéaire d'ordre 1 portant sur K' :

$$(K')' + \left(2r + \frac{b}{a}\right)K' = 0.$$

Ainsi, y est solution de $(\mathcal{H})$ si et seulement s'il existe $\alpha \in \mathbb{C}$ tel que

$$K' : t \mapsto \alpha \exp \left[-\left(2r + \frac{b}{a}\right)t \right].$$

En primitivant ceci, y est solution de $(\mathcal{H})$ si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$K : t \mapsto \beta \exp \left[-\left(2r + \frac{b}{a}\right)t \right] + \gamma.$$

Ainsi, y est solution de $(\mathcal{H})$ si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$y : t \mapsto \left(\beta \exp \left[-\left(2r + \frac{b}{a}\right)t \right] + \gamma \right) \times e^{rt}.$$

Après simplification, y est solution de $(\mathcal{H})$ si et seulement s'il existe $\beta, \gamma \in \mathbb{C}$ tel que

$$y : t \mapsto \beta e^{r't} + \gamma e^{rt}.$$

$\square$

Exemple 3.3.4.

L'ensemble des solutions complexes de $y'' + y = 0$ est

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{C} \\ x \mapsto \lambda e^{ix} + \mu e^{-ix} \end{array} \middle| \lambda, \mu \in \mathbb{C} \right\}.$$

Par les formules d'Euler, c'est aussi

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{C} \\ x \mapsto \lambda \sin(x) + \mu \cos(x) \end{array} \middle| \lambda, \mu \in \mathbb{C} \right\}.$$

Théorème 3.3.5 (Solutions réelles de $(\mathcal{H})$).

Soit $a, b, c \in \mathbb{R}$, avec $a \neq 0$.

1. Si (EC) a deux solutions réelles distinctes r_1, r_2 , alors les solutions réelles de $(\mathcal{H})$ sont les applications de la forme

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t} \end{array} \right.$$

pour $(\lambda, \mu) \in \mathbb{R}^2$.

2. Si (EC) a une unique solution réelle r , alors les solutions réelles de $(\mathcal{H})$ sont les applications de la forme

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto (\lambda t + \mu) e^{rt} \end{array} \right.$$

pour $(\lambda, \mu) \in \mathbb{R}^2$.

3. Si (EC) a deux solutions complexes conjuguées distinctes, que l'on note $\alpha \pm i\omega$ avec $\alpha, \omega \in \mathbb{R}$, alors les solutions réelles de $(\mathcal{H})$ sont les applications de la forme

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto \lambda \cos(\omega t) e^{\alpha t} + \mu \sin(\omega t) e^{\alpha t} \end{array} \right.$$

pour $(\lambda, \mu) \in \mathbb{R}^2$.

Ce sont aussi exactement les applications de la forme

$$\left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto A \cos(\omega t + \varphi) e^{\alpha t} \end{array} \right.$$

pour $A \in \mathbb{R}_+$ et $\varphi \in]-\pi, \pi]$.

Lemme 3.3.6.

Soit $\alpha, \omega \in \mathbb{R}$, avec $\omega \neq 0$. Les deux ensembles de fonctions exposés au point 3. du théorème 3.3.5 sont égaux.

Démonstration.

Soit $A \in \mathbb{R}_+$ et $\varphi \in]-\pi, \pi]$, soit

$$f : \left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto A \cos(\omega t + \varphi) e^{\alpha t} \end{array} \right.$$

Par les formules d'addition, si $t \in \mathbb{R}$,

$$f(t) = A \cos(\varphi) \cos(\omega t) e^{\alpha t} - A \sin(\varphi) \sin(\omega t) e^{\alpha t},$$

donc f est bien de la première forme.

Réciproquement, soit $\lambda, \mu \in \mathbb{R}$. Si $\lambda = \mu = 0$, il suffit de prendre $A = 0$ et φ quelconque. Sinon, posons $A = \sqrt{\lambda^2 + \mu^2}$ et $\varphi \in]-\pi, \pi]$ tel que $\cos \varphi = \frac{\lambda}{\sqrt{\lambda^2 + \mu^2}}$ et $\sin \varphi = -\frac{\mu}{\sqrt{\lambda^2 + \mu^2}}$. Alors,

$$\begin{aligned} & \lambda \cos(\omega t) + \mu \sin(\omega t) \\ &= \sqrt{\lambda^2 + \mu^2} \left(\frac{\lambda}{\sqrt{\lambda^2 + \mu^2}} \cos(\omega t) + \frac{\mu}{\sqrt{\lambda^2 + \mu^2}} \sin(\omega t) \right) \\ &= A (\cos(\omega t) \cos(\varphi) - \sin(\omega t) \sin(\varphi)) \\ &= A \cos(\omega t + \varphi). \end{aligned}$$

□

Démonstration (Théorème 3.3.5).

- Les cas où (EC) admet une ou deux solutions réelles se traitent exactement comme le cas complexe.
- Supposons donc que (EC) admette deux solutions complexes conjuguées distinctes $\alpha \pm i\omega$. On raisonne par analyse-synthèse.

Analyse : Soit $y : \mathbb{R} \rightarrow \mathbb{R}$ solution de $(\mathcal{H})$. Alors y est solution complexe de $(\mathcal{H})$, donc il existe $\lambda, \mu \in \mathbb{C}$ tels que

$$y : t \mapsto \lambda e^{(\alpha+i\omega)t} + \mu e^{(\alpha-i\omega)t}$$

Or $y(0) = \lambda + \mu$ est réel donc $\lambda + \mu \in \mathbb{R}$, donc $\text{Im}(\lambda) = -\text{Im}(\mu)$.

De même $y(\pi/(2\omega)) \in \mathbb{R}$, donc

$$y\left(\frac{\pi}{2\omega}\right) = i(\lambda - \mu) \exp\left(\frac{\alpha\pi}{2\omega}\right) \in \mathbb{R},$$

donc $\text{Re}(\lambda) = \text{Re}(\mu)$.

Ainsi, $\mu = \bar{\lambda}$.

Soit $\rho \in \mathbb{R}^+$ et $\varphi \in]-\pi, \pi]$ tels que $\lambda = \rho e^{i\varphi}$. Si $t \in \mathbb{R}$, alors

$$y(t) = 2\rho \cos(\omega t + \varphi) e^{\alpha t}.$$

Ainsi, y est de la forme demandée.

Synthèse : Soit $\lambda, \mu \in \mathbb{R}$ et

$$y : \left\{ \begin{array}{l} \mathbb{R} \rightarrow \mathbb{R} \\ t \mapsto \lambda \cos(\omega t) e^{\alpha t} + \mu \sin(\omega t) e^{\alpha t} \end{array} \right.$$

D'après le théorème de structure des solutions de l'équation homogène (3.2.1 – une combinaison linéaire de solutions de l'équation homogène est solution de l'équation homogène), il suffit de montrer que

$$s_1 : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \cos(\omega t)e^{\alpha t} \end{cases}$$

et

$$s_2 : \begin{cases} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \sin(\omega t)e^{\alpha t} \end{cases}$$

sont solution de $(\mathcal{H})$. Or, si $t \in \mathbb{R}$, par les formules d'Euler,

$$s_1(t) = \frac{1}{2}e^{(\alpha+i\omega)t} + \frac{1}{2}e^{(\alpha-i\omega)t}.$$

D'après le théorème 3.3.3, $t \mapsto e^{(\alpha+i\omega)t}$ et $t \mapsto e^{(\alpha-i\omega)t}$ sont solutions de $(\mathcal{H})$, donc s_1 aussi. On effectue le même raisonnement pour s_2 . $\square$

Remarque 3.3.7.

Dans tous les cas, les solutions sont les combinaisons linéaires de deux solutions linéairement indépendantes. On dit que cet ensemble a une structure de plan vectoriel.

Exemple 3.3.8. 1. Les solutions complexes de $y'' + y' + 2y = 0$ sont les fonctions de la forme

$$\begin{aligned} t \mapsto \lambda e^{\frac{-1-i\sqrt{7}}{2}t} + \mu e^{\frac{-1+i\sqrt{7}}{2}t} \\ = e^{-\frac{1}{2}t} \left(\lambda e^{\frac{-i\sqrt{7}}{2}t} + \mu e^{\frac{i\sqrt{7}}{2}t} \right) \end{aligned}$$

avec $\lambda, \mu \in \mathbb{C}$.

2. La solution du problème de Cauchy $y'' + 2y' + y = 0$, avec $y(1) = 1$, $y'(1) = 0$ est la fonction $t \mapsto te^{1-t}$.

Théorème 3.3.9.

Le problème de Cauchy $ay'' + by' + cy = 0$ et $y(t_0) = y_0$ et $y'(t_0) = y'_0$, admet une unique solution.

Démonstration.

(hors programme) Nous traitons ici le cas où on cherche une solution à valeurs complexes et où le polynôme caractéristique a deux racines distinctes r_1 et r_2 . Alors les solutions de l'équation différentielle considérées sont les applications y de la forme $t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t}$ où λ et μ sont deux complexes. On a $y(t_0) = \lambda e^{r_1 t_0} + \mu e^{r_2 t_0}$ et $y'(t_0) = \lambda r_1 e^{r_1 t_0} + \mu r_2 e^{r_2 t_0}$.

Pour montrer que le problème de Cauchy admet une unique solution, il suffit de montrer que le système

$$\begin{cases} \lambda e^{r_1 t_0} + \mu e^{r_2 t_0} = y_0 \\ \lambda r_1 e^{r_1 t_0} + \mu r_2 e^{r_2 t_0} = y'_0 \end{cases}$$

d'inconnues λ et μ admet une unique solution.

On peut s'en assurer par le calcul, ou on peut simplement remarquer que pour que ce système admette une unique solution, il suffit que l'équation

$$\lambda \begin{pmatrix} e^{r_1 t_0} \\ r_1 e^{r_1 t_0} \end{pmatrix} + \mu \begin{pmatrix} e^{r_2 t_0} \\ r_2 e^{r_2 t_0} \end{pmatrix} = \begin{pmatrix} y_0 \\ y'_0 \end{pmatrix}$$

admette une unique solution.

Pour cela, il suffit de montrer que les vecteurs $\begin{pmatrix} e^{r_1 t_0} \\ r_1 e^{r_1 t_0} \end{pmatrix}$ et $\begin{pmatrix} e^{r_2 t_0} \\ r_2 e^{r_2 t_0} \end{pmatrix}$ forment une base de $\mathbb{R}^2$. Il suffit de vérifier qu'ils sont linéairement indépendants, ce qui est le cas puisque leur déterminant vaut $e^{r_1 t_0} r_2 e^{r_2 t_0} - r_1 e^{r_1 t_0} e^{r_2 t_0}$, qui est égal à $(r_2 - r_1)e^{(r_1+r_2)t_0}$, qui est non nul puisque $r_1 \neq r_2$. $\square$

3.4 Résolution d'une équation avec second membre.

Théorème 3.4.1.

Si l'on connaît une solution $\tilde{y}$ de l'équation avec second membre alors on en connaît toutes les solutions : l'ensemble S des solutions de l'équation avec second membre est $S = \{y_H + \tilde{y} \mid y_H \in S_H\}$.

Remarque 3.4.2.

On a déjà vu que si l'on connaissait une solution de l'équation $\tilde{y}$ avec second membre, alors on pouvait construire toutes les solutions de l'équation avec second membre à partir de l'ensemble des solutions de l'équation homogène.

Dans le cas d'une équation d'ordre deux à coefficients constants, on dit que l'ensemble des solutions a une structure de plan affine, car l'ensemble des solutions est l'ensemble des $\tilde{y} + y$ pour y parcourant un plan vectoriel.

3.5 Seconds membres particuliers

Nous avons déjà vu comment trouver une solution particulière à une équation différentielle linéaire d'ordre 1.

Cependant, quand le second membre est d'une certaine forme et que l'équation est à *coefficients constants*, il existe une autre méthode. Notons que cette seconde méthode n'est pas plus rapide ni plus efficace que la

méthode de variation de la constante. Elle a par contre le mérite de pouvoir être utilisée pour des équations d'ordre 2 présentant les mêmes caractéristiques : coefficients constants et second membre de ces mêmes formes particulières.

On considère une équation $(\mathcal{E})$ de la forme $y' + ay = c$ ou $y'' + ay' + by = c$, où $a, b \in \mathbb{K}$. Nous supposons que l'une des conditions suivantes est remplie :

1. il existe un polynôme P à coefficients dans $\mathbb{K}$ tel que $c = P$;
2. il existe $A, \alpha \in \mathbb{K}$ tels que $c(x) = Ae^{\alpha x}$;
3. il existe $A, \omega \in \mathbb{R}$ tels que $c(x) = A \cos(\omega x)$;
4. il existe $A, \omega \in \mathbb{R}$ tels que $c(x) = A \sin(\omega x)$.

Ces quatre cas sont ceux au programme, mais la méthode que nous allons développer peut également s'adapter lorsque dans les conditions précédentes la constante A est remplacée par un polynôme, et lorsque les sin et cos circulaires sont remplacés par des ch et sh hyperboliques.

Dans les quatre conditions au programme, il est possible de montrer qu'il existe à chaque fois une solution particulière d'une forme assez simple :

1. il existe un polynôme Q à coefficients dans $\mathbb{K}$ solution de $(\mathcal{E})$;
2. il existe un polynôme Q à coefficients dans $\mathbb{K}$ tel que $x \mapsto Q(x)e^{\alpha x}$ est solution de $(\mathcal{E})$;
3. il existe un polynôme Q à coefficients dans $\mathbb{C}$ tel que $x \mapsto Q(x)e^{i\omega x}$ est solution de $y' + ay = Ae^{i\omega x}$ ou $y'' + ay' + by = Ae^{i\omega x}$. On peut alors montrer, grâce au principe de superposition notamment, que $x \mapsto \operatorname{Re}(Q(x)e^{i\omega x})$ est solution de $(\mathcal{E})$. Ainsi en développant, on remarque qu'il existe deux polynômes réels R et S tels que $c(x) = R(x) \cos(\omega x) + S(x) \sin(\omega x)$;
4. suivant le même principe que dans le cas précédent, il existe un polynôme Q à coefficients dans $\mathbb{C}$ tel que $x \mapsto \operatorname{Im}(Q(x)e^{i\omega x})$ est solution de $(\mathcal{E})$, et donc en développant, on remarque qu'il existe deux polynômes réels R et S tels que $c(x) = R(x) \cos(\omega x) + S(x) \sin(\omega x)$.

Le degré du polynôme Q se devine en injectant dans $(\mathcal{E})$ une fonction de la forme voulue. On détermine ensuite les coefficients du polynôme. Voyons cela sur les exemples suivants :

Exemple 3.5.1.

Soit $(\mathcal{E}) : y' + y = 1 + 2x$, définie sur $\mathbb{R}$. Soit Q un polynôme. Alors Q est solution de $(\mathcal{E})$ si et seulement si pour tout $x \in \mathbb{R}$, $Q'(x) + Q(x) = 1 + 2x$. En particulier, pour que Q soit solution, il faut que $Q' + Q$ soit de degré 1 : cela n'est possible que si Q est de degré 1, car si Q n'est pas nul, $\deg Q' < \deg Q$. Posons alors $Q = d + ex$. Alors :

$$\begin{aligned} Q \text{ est solution de } (\mathcal{E}) &\Leftrightarrow \forall x \in \mathbb{R}, e + (d + ex) = 1 + 2x \\ &\Leftrightarrow \forall x \in \mathbb{R}, (e + d) + ex = 1 + 2x \\ &\Leftrightarrow [e + d = 1] \text{ et } [e = 2] \\ &\Leftrightarrow e = 2 \text{ et } d = -1 \end{aligned}$$

Ainsi $x \mapsto -1 + 2x$ est une solution particulière de $(\mathcal{E})$.

Exemple 3.5.2.

Soit $(\mathcal{E}) : y'' - 2y' + y = 2e^x$, définie sur $\mathbb{R}$. Soit Q un polynôme et soit $y : x \mapsto Q(x)e^x$. Ainsi $y' : x \mapsto (Q'(x) + Q(x))e^x$ et $y'' : x \mapsto (Q''(x) + 2Q'(x) + Q(x))e^x$. Alors :

$$\begin{aligned} &y \text{ est solution de } (\mathcal{E}) \\ \Leftrightarrow &\forall x \in \mathbb{R}, (Q''(x) + 2Q'(x) + Q(x))e^x \\ &\quad - 2(Q'(x) + Q(x))e^x + Q(x)e^x = 2e^x \\ \Leftrightarrow &\forall x \in \mathbb{R}, Q''(x)e^x = 2e^x \\ \Leftrightarrow &\forall x \in \mathbb{R}, Q''(x) = 2 \end{aligned}$$

Un polynôme Q vérifiant cette relation est par exemple $Q = X^2$. Ainsi, $x \mapsto x^2e^x$ est une solution particulière de $(\mathcal{E})$.

Par curiosité, démontrons le troisième point en utilisant le second, dans le cas d'une équation du premier ordre (la méthode serait la même pour le second ordre) :

Démonstration.

Soit $(\mathcal{E}) : y' + ay = B \cos(\omega x)$, où $a, B, \omega \in \mathbb{R}$. Considérons $(\mathcal{E}')$: $y' + ay = Be^{i\omega x}$. Il existe alors un polynôme complexe Q tel que $y_0 : x \mapsto Q(x)e^{i\omega x}$ est solution de $(\mathcal{E}')$. Ainsi $y'_0 + ay_0 = Be^{i\omega x}$. En passant au conjugué, on observe, puisque a, B, ω sont réels, que $\bar{y}'_0 + a\bar{y}_0 = Be^{-i\omega x}$. Par principe de superposition, $\frac{1}{2}(y_0 + \bar{y}_0)$ est solution de

$y' + ay = \frac{1}{2}B(e^{i\omega x} + e^{-i\omega x})$. Une solution de $(\mathcal{E})$ est donc bien $\operatorname{Re}(y_0)$. $\square$

Finissons par un ultime exemple :

Exemple 3.5.3.

Soit $(\mathcal{E}) : y'' + y = 2\cos(x)$. Déterminons tout d'abord une solution de l'équation $(\mathcal{E}')$: $y'' + y = 2e^{ix}$. Soit Q un polynôme et $y_0 : x \mapsto Q(x)e^{ix}$. Alors $y'_0 : x \mapsto (Q'(x) + iQ(x))e^{ix}$ et $y''_0 : x \mapsto (Q''(x) + 2iQ'(x) - Q(x))e^{ix}$. Donc y_0 est solution de $(\mathcal{E}')$ ssi pour tout $x \in \mathbb{R}$, $Q''(x) + 2iQ'(x) = 2$. On cherche donc Q de degré 1, donc de la forme $Q : x \mapsto d + ex$. Alors pour tout $x \in \mathbb{R}$, $Q''(x) + 2iQ'(x) = 2ie$, donc Q vérifie $\forall x \in \mathbb{R}, Q''(x) + 2iQ'(x) = 2$ ssi $e = -i$. Ainsi une solution particulière de $(\mathcal{E}')$ est $y_0 : x \mapsto -ixe^{ix}$. Donc pour tout $x \in \mathbb{R}$, $\operatorname{Re}(y_0)(x) = \operatorname{Re}(-ix(\cos(x) + i\sin(x))) = x\sin(x)$. Finalement, une solution particulière de $(\mathcal{E})$ est $x \mapsto x\sin(x)$.

Chapitre VII

Théorie des ensembles

Sommaire

1	Définitions.	112
1.1	Appartenance, égalité.	112
1.2	Inclusion, ensemble des parties.	112
1.3	Réunion, intersection, complémentaire.	113
1.4	Produit cartésien.	116
2	Interprétation logique	117

1 Définitions.

Nous développons ici la notion d'ensemble, en partant d'une définition intuitive et peu formelle : un ensemble est une collection d'objets mathématiques. Si un objet x est dans cette collection-ensemble E , on note alors $x \in E$ la phrase « x appartient à E ». Sa négation, « x n'appartient pas à E », s'écrit $x \notin E$.

Remarque 1.0.1.

Traditionnellement, on essaie de noter les ensembles avec des lettres majuscules et leurs éléments avec des lettres minuscules.

1.1 Appartenance, égalité.

Définition 1.1.1 (Extentionnalité).

Deux ensembles E et F sont égaux si et seulement s'ils ont les mêmes éléments :

$$E = F \iff \forall x (x \in E \iff x \in F).$$

Remarque 1.1.2.

Intuitivement, cette proposition dit que la caractéristique qui définit un ensemble, ce sont ses éléments. Autrement dit, si on voit les ensembles comme des sacs contenant des objets, le sac n'a aucune caractéristique qui puisse le distinguer d'un autre. Cette caractéristique est très particulière au monde idéalisé des ensembles mathématiques. En informatique on verra par exemple qu'on peut avoir deux tableaux contenant les mêmes éléments dans le même ordre et qui ne sont pas le même objet.

Définition 1.1.3 (Ensemble vide).

On note $\emptyset$ l'ensemble vide.

Définition 1.1.4.

Étant donnés des objets $x_1, x_2, \dots, x_n$, on note $\{x_1, \dots, x_n\}$ l'ensemble contenant exactement $x_1, \dots, x_n$.

Pour tout ensemble E et tout prédicat P , on note $\{x \in E \mid P(x)\}$ l'ensemble dont les éléments sont exactement les éléments de E vérifiant P .

Pour tout ensemble E et toute expression $e[x]$ contenant une variable x , on note $\{e[x] \mid x \in E\}$ l'ensemble des objets mathématiques qui s'écrivent sous la forme $e[x]$ pour au moins un $x \in E$.

Remarque 1.1.5. 1. Pour le premier point, l'ordre des éléments n'importe pas, ni le nombre de fois où ils apparaissent dans la liste des éléments. $\{1, 2\} = \{2, 1\} = \{1, 2, 1\}$. On parle de définition de l'ensemble en extension.

2. Pour le second point, on parle de définition en compréhension.

Exemple 1.1.6.

Un même ensemble peut parfois être défini en extension ou en compréhension :

$$\begin{aligned} E &= \{0; 1; 4; 9\} \\ &= \left\{ n \in \mathbb{N} \mid n \leq 15 \text{ et } \exists p \in \mathbb{N}, n = p^2 \right\}. \end{aligned}$$

Dans toute la suite, E et F désignent deux ensembles.

1.2 Inclusion, ensemble des parties.

Définition 1.2.1 (Inclusion).

On dit que E est *inclus* dans F , ce que l'on note $E \subset F$ si tout élément de E est aussi un élément de F , *i.e.*

$$\forall x \in E \ x \in F.$$

Si $E \subset F$, on dit que E est une *partie* ou un *sous-ensemble* de F .

Exemple 1.2.2. 1. Pour tout ensemble E , on a $\emptyset \subset E$ et $E \subset E$.

2. $\mathbb{N} \subset \mathbb{Z}$.

3. $\{1, \{1; 2\}, \mathbb{R}\} \subset \{\mathbb{Z}, \pi, 1, \{1; 2\}, \mathbb{R}\}$.

4. $\{\{1; 2\}\} \not\subset \{1; 2\}$.

Remarque 1.2.3.

Attention à ne pas confondre. $\in$ et $\subset$. Ainsi $1 \in \{1, 2\}$, $\{1\} \subset \{1, 2\}$, mais $\{1\} \notin \{1, 2\}$. En revanche on a $\{1, 2\} \in \{1, 2, \{1, 2\}\}$ ainsi que $\{1, 2\} \subset \{1, 2, \{1, 2\}\}$.

En pratique pour démontrer une inclusion, on utilise la définition et la manière usuelle de démontrer une proposition universellement quantifiée.

Exemple 1.2.4.

On note E l'ensemble des entiers relatifs pairs qui sont des multiples de 15 et F l'ensemble des entiers relatifs multiples de 6. Montrer $E \subset F$.

Proposition 1.2.5 (Transitivité).

Soit E, F, G trois ensembles, si $E \subset F$ et $F \subset G$, alors $E \subset G$.

Démonstration.

Soit x un objet. Si $x \in E$, comme $E \subset F$, on a $x \in F$. De même, comme $F \subset G$, on a $x \in G$. $\square$

Théorème 1.2.6 (Double inclusion).

Soit E, F deux ensembles, alors

$$(E = F) \Leftrightarrow (E \subset F \text{ et } F \subset E).$$

Démonstration.

Il est clair que pour tout ensemble A , on a $\forall x \in A \quad x \in A$, donc $A \subset A$. Le sens direct est donc évident.

Montrons l'implication réciproque. Supposons $E \subset F$ et $F \subset E$. Alors soit x un objet mathématique quelconque. Montrons $x \in E \Leftrightarrow x \in F$:

- Supposons $x \in E$, alors comme $E \subset F$, on a $x \in F$.
- Supposons $x \in F$, alors comme $F \subset E$, on a $x \in E$.

donc $x \in E \Leftrightarrow x \in F$.

Donc $\forall x \quad x \in E \Leftrightarrow x \in F$.

Donc $E = F$. $\square$

Remarque 1.2.7.

En pratique, on a deux méthodes pour démontrer l'égalité de deux ensembles E et F :

- ou bien on utilise ce théorème ;
- ou bien on utilise directement la propriété d'extensionnalité, en montrant que pour tout x , $x \in E \Leftrightarrow x \in F$ par équivalences successives.

Axiome 1.2.1 (Ensemble des parties de E).

Pour tout ensemble E , on admet l'existence d'un ensemble, noté $\mathcal{P}(E)$ et appelé *ensemble des parties de E* et dont les éléments sont exactement les sous-ensembles de E . Ainsi pour tout ensemble F , on a

$$F \in \mathcal{P}(E) \Leftrightarrow F \subset E.$$

Exercice 1.2.8.

Déterminer $\mathcal{P}(\{1, 2, 3\})$. Combien cet ensemble admet-il d'éléments ?

Remarque 1.2.9.

Ne pas oublier $\emptyset$ dans l'ensemble des parties.

Exercice 1.2.10.

Déterminer $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{\emptyset\})$ et $\mathcal{P}(\{\emptyset, \{\emptyset\}\})$.

Proposition 1.2.11.

Si un ensemble E possède $n \in \mathbb{N}$ éléments, alors $\mathcal{P}(E)$ possède 2^n éléments.

Démonstration.

Cela sera démontré au second semestre, dans le cours de dénombrement. $\square$

1.3 Réunion, intersection, complémentaire.

Dans cette partie A et B désignent deux ensembles.

Définition 1.3.1. 1. On appelle *réunion de A et B* notée $A \cup B$, l'ensemble dont les éléments sont exactement ceux qui sont dans A ou dans B , autrement dit, pour tout objet x ,

$$x \in A \cup B \Leftrightarrow (x \in A \text{ ou } x \in B).$$

2. On appelle *intersection de A et B* notée $A \cap B$ dont les éléments sont exactement ceux qui sont dans A et dans B à la fois, autrement dit, pour tout objet x ,

$$x \in A \cap B \Leftrightarrow (x \in A \text{ et } x \in B).$$

Exemple 1.3.2.

On pose $E = \{0, 1, 2, 4\}$ et $F = \{0, 1, 3, 4, 5, 6\}$.
Que vaut $E \cup F$? $E \cap F$?

Proposition 1.3.3.

Soit A, B, C trois ensembles.

1. $\cap$ et $\cup$ sont associatives : $A \cap (B \cap C) = (A \cap B) \cap C$ (*idem* pour $\cup$).
2. $\cap$ et $\cup$ sont commutatives : $A \cap B = B \cap A$ (*idem* pour $\cup$).
3. On a toujours $A \cap B \subset A \subset A \cup B$.
4. Si $A \subset B$, on a toujours $A \cap C \subset B \cap C$ et $A \cup C \subset B \cup C$.

Démonstration.

Élémentaire, revenir aux définitions. $\square$

Remarque 1.3.4.

La dernière propriété signifie que $A \mapsto A \cap C$ et $A \mapsto A \cup C$ sont croissantes (au sens de l'inclusion).

Définition 1.3.5.

On dit que deux ensembles sont *disjoints* si leur intersection est vide.

Définition 1.3.6.

On peut généraliser cette notion à une famille d'ensembles.

1. Si E est un ensemble d'ensembles, on note $\bigcup_{X \in E} X$ la réunion de tous les éléments de E et, dans le cas où E est non vide, $\bigcap_{X \in E} X$ l'intersection de tous les éléments de E . Pour tout x , on a les propriétés :

$$x \in \bigcup_{X \in E} X \iff \exists X \in E, x \in X;$$

$$x \in \bigcap_{X \in E} X \iff \forall X \in E, x \in X.$$

2. Plus généralement, si on considère une famille d'ensemble $(A_i)_{i \in I}$, on note $\bigcup_{i \in I} A_i$ la réunion de tous les A_i pour $i \in I$ et $\bigcap_{i \in I} A_i$

l'intersection de tous les A_i . Pour tout x , on a les propriétés :

$$x \in \bigcup_{i \in I} A_i \iff \exists i \in I, x \in A_i ;$$

$$x \in \bigcap_{i \in I} A_i \iff \forall i \in I, x \in A_i.$$

Exercice 1.3.7. 1. Que valent $\bigcup_{n \in \mathbb{N}} [n, n+1]$ et

$$\bigcap_{n \in \mathbb{N}^*} [n, n+1] ?$$

2. Quel est l'ensemble de définition de $\tan$?
3. Que vaut chacun des ensembles ci-dessous ?

$$\begin{array}{cccc} \bigcup_{\varepsilon \in]0,1]} [\varepsilon, 1] & \bigcup_{\varepsilon \in]0,1]}]\varepsilon, 1] & \bigcap_{\varepsilon \in]0,1]} [0, \varepsilon] & \bigcap_{\varepsilon \in]0,1]} [0, \varepsilon[\\ \bigcap_{\varepsilon \in]0,1]}]0, \varepsilon] & \bigcap_{\varepsilon \in]0,1]}]0, \varepsilon[& \bigcap_{\varepsilon \in]0,1] \cap \mathbb{Q}} [0, \varepsilon] & \bigcap_{\varepsilon \in]0,1] \cap \mathbb{Q}} [0, \varepsilon[\end{array}$$

Proposition 1.3.8.

Soit $(A_i)_{i \in I}$ une famille d'ensembles et B un ensemble.

1. Si, pour tout $i \in I$, $A_i \subset B$, alors $\bigcup_{i \in I} A_i \subset B$.
2. Si, pour tout $i \in I$, $B \subset A_i$, alors $B \subset \bigcap_{i \in I} A_i$.
3. Si $j \in I$, alors $\bigcap_{i \in I} A_i \subset A_j \subset \bigcup_{i \in I} A_i$.

Démonstration.

Élémentaire. $\square$

Théorème 1.3.9 (Distributivité).

La réunion et l'intersection sont distributives l'une sur l'autre. Plus précisément, soit A, B et C trois ensembles. Alors on a les deux égalités suivantes :

$$\begin{aligned} (A \cap B) \cup C &= (A \cup C) \cap (B \cup C); \\ (A \cup B) \cap C &= (A \cap C) \cup (B \cap C). \end{aligned}$$

Plus généralement, soit $(A_i)_{i \in I}$ une famille d'ensembles et B un ensemble, alors

$$\left(\bigcap_{i \in I} A_i \right) \cup B = \bigcap_{i \in I} (A_i \cup B); \quad (\text{VII.1})$$

$$\left(\bigcup_{i \in I} A_i \right) \cap B = \bigcup_{i \in I} (A_i \cap B). \quad (\text{VII.2})$$

Démonstration.

Faire un dessin pour les deux premières égalités.

Les résultats se montrent aisément par double inclusion. On donne la démonstration de l'égalité (VII.2).

Pour tout x :

$$\begin{aligned} x \in \left(\bigcup_{i \in I} A_i \right) \cap B &\Leftrightarrow x \in B \text{ et } x \in \left(\bigcup_{i \in I} A_i \right) \\ &\Leftrightarrow x \in B \text{ et } \exists i_0 \in I, x \in A_{i_0} \\ &\Leftrightarrow \exists i_0 \in I, x \in A_{i_0} \cap B \\ &\Leftrightarrow x \in \bigcup_{i \in I} (A_i \cap B). \end{aligned}$$

□

Exercice 1.3.10.

Montrer les propriétés (VII.2) et (VII.1) en raisonnant par double inclusion et en prenant soin de bien revenir aux définitions des objets manipulés.

Définition 1.3.11.

On appelle A privé de B , ou *différence de A et B* , ou A moins B , l'ensemble noté $A \setminus B$ ou $A - B$, tel que pour tout objet x , $x \in A \setminus B$ si et seulement si $x \in A$ et $x \notin B$.

Cet ensemble est bien défini d'après le schéma de compréhension.

Exercice 1.3.12.

Montrer que $A \setminus B = A \setminus (A \cap B)$.

Définition 1.3.13.

Si $A \subset E$, on appelle *complémentaire de A dans E* noté $\complement_E A$ ou A^C ou $\overline{A}$ quand il n'y a pas de confusion, l'ensemble $E \setminus A$.

Proposition 1.3.14.

Si A et B sont deux parties de E , on a $A \setminus B = A \cap B^C$.

Démonstration.

Faire un dessin.

Soit x quelconque. On a $A \subset E$ donc $x \in A \Leftrightarrow (x \in A \text{ et } x \in E)$. On a donc :

$$\begin{aligned} x \in A \setminus B &\Leftrightarrow x \in A \text{ et } x \notin B \\ &\Leftrightarrow x \in A \text{ et } (x \in E \text{ et } (x \notin B)) \\ &\Leftrightarrow x \in A \text{ et } x \in E \setminus B \\ &\Leftrightarrow x \in A \cap B^C. \end{aligned}$$

□

Proposition 1.3.15.

Soit E un ensemble et A une partie de E , alors $\overline{\overline{A}} = A$.

Démonstration.

C'est une conséquence de la propriété de double négation : soit x un élément de E , on a $x \in A \Leftrightarrow \neg(\neg(x \in A))$. □

Proposition 1.3.16.

Soit E un ensemble et A une partie de E , alors $A \cup \overline{A} = E$ et $A \cap \overline{A} = \emptyset$.

Démonstration.

Soit $x \in E$, on a $x \in A$ ou $x \notin A$ (tiers exclu), donc $x \in A \cup \overline{A}$.

De plus, on ne peut avoir simultanément $x \in A$ et $x \notin A$, donc $A \cap \overline{A} = \emptyset$. □

Théorème 1.3.17 (Relations de De Morgan).

Soit $(A_i)_{i \in I}$ une famille de parties d'un ensemble E . Alors on a

$$\begin{aligned} \left(\bigcap_{i \in I} A_i \right)^C &= \bigcup_{i \in I} (A_i^C); \\ \left(\bigcup_{i \in I} A_i \right)^C &= \bigcap_{i \in I} (A_i^C). \end{aligned}$$

Démonstration.

On montre le deuxième point. Les deux termes de l'égalité sont évidemment des sous-ensembles de E . Considérons donc un $x \in E$ quelconque et montrons que x appartient au premier ensemble si et seulement s'il appartient au deuxième. On a les équivalences :

$$\begin{aligned} x \in \left(\bigcup_{i \in I} A_i \right)^C &\iff x \notin \bigcup_{i \in I} A_i \\ &\iff \neg(\exists i \in I \ x \in A_i) \\ &\iff \forall i \in I \ x \notin A_i \\ &\iff x \in \bigcap_{i \in I} (A_i^C). \end{aligned}$$

Le premier se déduit de la seconde en passant au complémentaire pour la famille $(A_i^C)_{i \in I}$. $\square$

Définition 1.3.18.

Soit E un ensemble, soit $\mathcal{F} = (F_i)_{i \in I}$ une famille de parties de E .

Alors, $\mathcal{F}$ est un *recouvrement disjoint* de E si

- les éléments de $\mathcal{F}$ sont deux à deux disjoints :

$$\forall i, j \in I, \ i \neq j \Rightarrow F_i \cap F_j = \emptyset ;$$

- E est l'union des éléments de $\mathcal{F}$:

$$E = \bigcup_{i \in I} F_i.$$

On dit de plus que $\mathcal{F}$ est une *partition* de E si c'est un recouvrement disjoint de E sans aucune partie vide :

$$\forall i \in I, \ F_i \neq \emptyset.$$

Remarque 1.3.19.

On pourrait bien entendu parler de recouvrement, mais nous n'aurons pas l'occasion d'utiliser ce vocabulaire cette année.

Nous utiliserons davantage les partitions que les recouvrements disjoints.

Exemple 1.3.20.

On considère

$$\begin{aligned} F_0 &= \{ n \in \mathbb{Z} \mid n \equiv 0 [3] \} \\ &= \{ n \in \mathbb{Z} \mid \exists p \in \mathbb{Z}, \ n = 3p \} \\ F_1 &= \{ n \in \mathbb{Z} \mid n \equiv 1 [3] \} \\ &= \{ n \in \mathbb{Z} \mid \exists p \in \mathbb{Z}, \ n = 3p + 1 \} \\ F_2 &= \{ n \in \mathbb{Z} \mid n \equiv 2 [3] \} \\ &= \{ n \in \mathbb{Z} \mid \exists p \in \mathbb{Z}, \ n = 3p + 2 \} \end{aligned}$$

Alors, $\{F_0, F_1, F_2\}$ est une partition de $\mathbb{Z}$ (en trois parties).

1.4 Produit cartésien.

Définition 1.4.1.

On admettra qu'étant donné deux objets x et y on peut construire un objet appelé *couple* (x, y) et qu'on a la propriété suivante pour tous objets x_1, x_2, y_1, y_2 :

$$(x_1, x_2) = (y_1, y_2) \iff (x_1 = y_1 \text{ et } x_2 = y_2).$$

Remarque 1.4.2.

On peut généraliser cette notion à celle de n -uplets.

Définition 1.4.3.

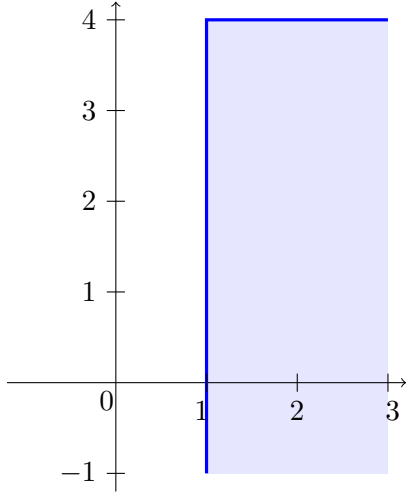
Soient E et F deux ensembles. On admet qu'on peut construire un ensemble noté $E \times F$, appelé *produit cartésien de E et F* , dont les éléments sont les couples avec $x_1 \in E$ et $x_2 \in F$. On définit de même le produit cartésien de n ensembles $E_1 \dots E_n$, noté $E_1 \times \dots \times E_n$, et formé des n -uplets $(x_1, \dots, x_n)$ avec $x_1 \in E_1, \dots, x_n \in E_n$. Si les E_i sont égaux à un ensemble E , on note ce produit E^n .

Remarque 1.4.4.

Attention à ne pas confondre l'ensemble $\{x, y\}$ avec le couple (x, y) .

Exemple 1.4.5.

L'ensemble $\mathbb{R}^2$, le rectangle $[1, 3] \times [-1, 4]$, la partie $[1, 3] \times [-1, 4]$ (voir figure VII.1), la bande $[0, 1] \times \{(x, y) \in \mathbb{R}^2 \mid y = 0\}$ (le représenter).

FIGURE VII.1 – Représentation de $[1, 3[\times]-1, 4]$.

2 Interprétation logique

Soit E un ensemble, P et Q deux prédicats. On pose

$$A = \{ x \in E \mid P(x) \};$$

$$B = \{ x \in E \mid Q(x) \}.$$

Soit $x \in E$. On a alors les équivalences logiques suivantes :

$$x \in A \cap B \iff P(x) \text{ et } Q(x);$$

$$x \in A \cup B \iff P(x) \text{ ou } Q(x);$$

$$x \notin A \iff \neg(P(x));$$

$$A = E \iff \forall x \in E, P(x);$$

$$A \neq \emptyset \iff \exists x \in E, P(x);$$

$$A \subset B \iff \forall x \in E, (P(x) \Rightarrow Q(x));$$

$$A = B \iff \forall x \in E, (P(x) \iff Q(x)).$$

Chapitre VIII

Notion d'application

Sommaire

1	Vocabulaire.	120
2	Restriction, prolongement	121
3	Composition d'applications	122
4	Injectivité, surjectivité, bijectivité . . .	122
4.1	Injectivité	122
4.2	Surjectivité	123
4.3	Bijectivité	124
4.4	Un peu de vocabulaire anglais	125
5	Image directe, tiré en arrière.	125
5.1	Image directe	125
5.2	Tiré en arrière	126

1 Vocabulaire.

- En toute rigueur, une *application* est un objet différent d'une *fonction*, mais la différence est hors programme. On emploiera donc les deux termes indifféremment.
- Une application d'un ensemble E dans un ensemble F est une relation qui, à tout élément de E associe un unique élément de F . Attention : on a forcément unicité de l'image et les ensembles de départ et d'arrivée sont une donnée de l'application.

Exemple 1.0.1.

Les applications qui à x associe x^2 , partant respectivement de $\mathbb{R}$ et de $\mathbb{R}_+$, sont différentes : la seconde permet de définir la fonction $\sqrt{\cdot}$, pas la première. Dans les deux cas, on pourra considérer comme ensemble d'arrivée $\mathbb{R}$ ou $\mathbb{R}_+$. Une formule ne définit donc pas à elle seule une application.

Définition 1.0.2.

On appelle *fonction* (ou *application*) tout triplet $f = (E, F, \Gamma)$ où E est un ensemble appelé *ensemble de départ* ou *domaine de définition*, F est un ensemble appelé *ensemble d'arrivée*, et Γ est une partie de $E \times F$ appelée *graphe de f* telle que $\forall x \in E, \exists! y \in F, (x, y) \in \Gamma$. Si $(x, y) \in \Gamma$, on note plus simplement $y = f(x)$. On dit que x est alors un antécédent de y , et y l'image de x .

Remarque 1.0.3.

Il peut y avoir plusieurs antécédents d'un élément dans l'espace d'arrivée, mais une seule image d'un élément de l'espace de départ : cela se voit sur le graphe, que l'on représente comme suit.

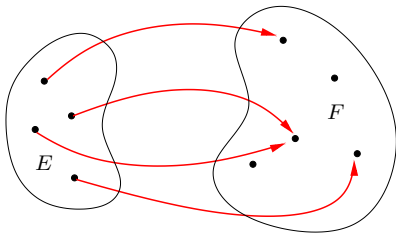


FIGURE VIII.1 – Exemple d'application – on remarque qu'une image a deux antécédents.

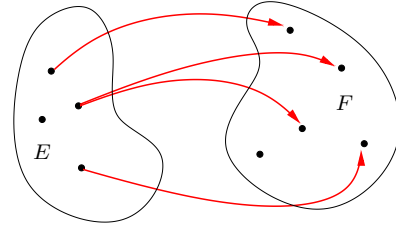


FIGURE VIII.2 – Cette relation n'est pas une application.

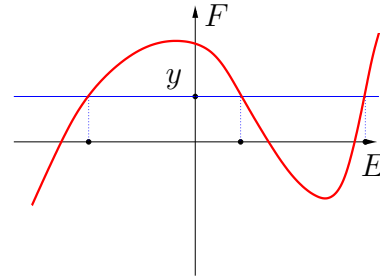


FIGURE VIII.3 – y a ici trois antécédents représentés.

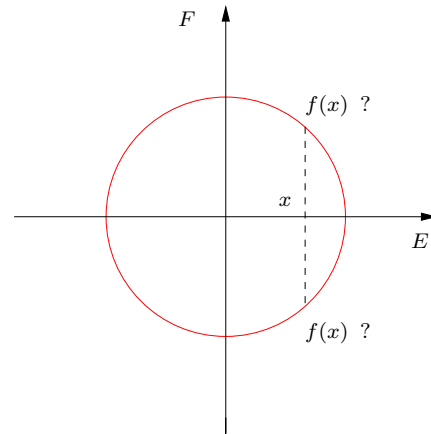


FIGURE VIII.4 – Cette courbe ne représente pas une application.

- On note une application f allant d'un ensemble E dans un ensemble F de la manière suivante : $f : E \rightarrow F$.
- Si l'application est de plus définie par une formule, on écrit alors :

$$\begin{aligned} f : E &\rightarrow F, \\ x &\mapsto \text{Formule dépendant de } x. \end{aligned}$$

Remarque 1.0.4.

La notation

$$\begin{aligned} f : E &\rightarrow F, \\ x &\mapsto f(x). \end{aligned}$$

n'est pas informative.

Remarque 1.0.5.

Si $f, g : E \rightarrow F$, alors $f = g$ équivaut à $\forall x \in E, f(x) = g(x)$.

Définition 1.0.6.

Soit E, F deux ensembles et $f : E \rightarrow F$ une application. On appelle *image* de f le sous-ensemble de F , noté $f(E)$ ou $\text{Im}(f)$, égal à $\{f(x), x \in E\}$.

Remarque 1.0.7.

La notation $f(E)$ indique bien l'ensemble de départ, contrairement à la notation $\text{Im } f$. Cet ensemble peut aussi s'écrire $\{y \in F \mid \exists x \in E, y = f(x)\}$.

Remarque 1.0.8.

Les ensembles de départ et d'arrivée peuvent être n'importe quoi, pas forcément de $\mathbb{R}$ dans $\mathbb{R}$.

Notation 1.0.9.

On note $\mathcal{F}(E, F)$, ou F^E , l'ensemble des applications de E dans F .

Remarque 1.0.10.

Comment se souvenir de cette dernière notation ? Penser que pour des ensembles finis, $\text{Card}(F^E) = \text{Card}(F)^{\text{Card}(E)}$.

En effet, il y a autant de manières de choisir une fonction $f : E \rightarrow F$ que de manières de choisir une image pour chaque élément de E . Or, il y a $\text{Card}(F)$ choix pour chaque élément de F et $\text{Card}(E)$ éléments de E . Il y a donc bien $\text{Card}(F)^{\text{Card}(E)}$ manières de choisir une application $f : E \rightarrow F$.

Exemple 1.0.11.

L'ensemble des suites réelles est noté $\mathbb{R}^{\mathbb{N}}$.

Dans $\{1\}^{\mathbb{N}}$, il y a une seule suite !

Définition 1.0.12 (Familles).

Soit I un ensemble. On appelle *famille* d'éléments de E indexée par I toute application de I dans E . Les familles sont notées $(x_i)_{i \in I}$, et rarement, voire jamais, comme des applications.

L'ensemble des familles de E indexées par I est noté E^I .

Exemple 1.0.13.

$\mathbb{R}^{\{1,2\}}$: on peut l'identifier à $\mathbb{R} \times \mathbb{R}$, que l'on note opportunément $\mathbb{R}^2$.

Définition 1.0.14.

Soit E un ensemble et A une partie de E . On appelle *fonction indicatrice* de A la fonction notée $\mathbb{1}_A$ telle que pour tout $x \in A$, $\mathbb{1}_A(x) = 1$, et pour tout $x \in E \setminus A$, $\mathbb{1}_A(x) = 0$.

Exercice 1.0.15.

Soit A et B deux ensembles. Calculer $\mathbb{1}_{A \cap B}$, $\mathbb{1}_{\bar{A}}$ et $\mathbb{1}_{A \cup B}$ en fonction de $\mathbb{1}_A$ et de $\mathbb{1}_B$.

2 Restriction, prolongement

Définition 2.0.1.

Soit E, E', F, F' quatre ensembles, $f : E \rightarrow F$ et $f' : E' \rightarrow F'$ deux applications.

- (i) Pour toute partie G de E , la restriction de f à G est l'application

$$\begin{aligned} f|_G : G &\rightarrow F, \\ x &\mapsto f(x). \end{aligned}$$

- (ii) On dit que f' est un prolongement de f si $E \subset E', F \subset F'$ et $\forall x \in E, f(x) = f'(x)$.



Il y a toujours une infinité de prolongements possibles à une application.

- Une fonction est toujours le prolongement d'une de ses restrictions.

Exemple 2.0.2.

Tout réel strictement positif a deux antécédents par la fonction $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$; mais il n'a qu'un antécédent par la restriction de f à $\mathbb{R}_+$.

3 Composition d'applications

Définition 3.0.1.

Soit E, F, G trois ensembles, $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications. On définit alors la composée de f par g comme l'application

$$\begin{aligned} g \circ f : E &\rightarrow G, \\ x &\mapsto g(f(x)). \end{aligned}$$

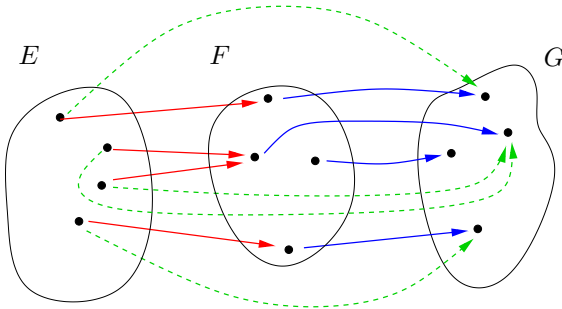


FIGURE VIII.5 – Exemple de composée.



On ne peut pas toujours composer deux applications. Par exemple : les fonctions $\mathbb{R}^* \rightarrow \mathbb{R}, x \mapsto 1/x$ et $\mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$.

• Ce n'est pas une opération commutative. Par exemple : $\exists x \in \mathbb{R}_+, \ln(x^2) \neq (\ln x)^2$.

Définition 3.0.2.

Soit E un ensemble, on définit dessus l'application identité sur E comme $\text{Id}_E : E \rightarrow E, x \mapsto x$.

4 Injectivité, surjectivité, bijectivité

On comprend vite, en considérant quelques exemples, quelles sont les propriétés qui peuvent empêcher une fonction $f : E \rightarrow E$ d'être inversible pour $\circ$.

- Si deux éléments de E ont même image par f , on ne pourra pas « revenir en arrière » et construire g vérifiant $g \circ f = \text{Id}_E$.

- Si un élément de E n'a pas d'antécédent par f , on ne pourra pas construire g vérifiant $f \circ g = \text{Id}_E$.

4.1 Injectivité

Définition 4.1.1.

Soit E, F deux ensembles non vides, $f : E \rightarrow F$ une application. On dit que f est *injective* (ou est une *injection*) si $\forall (x, y) \in E^2, f(x) = f(y) \Rightarrow x = y$.

Remarque 4.1.2.

On utilise également la contraposée de cette proposition : $\forall (x, y) \in E^2, x \neq y \Rightarrow f(x) \neq f(y)$.

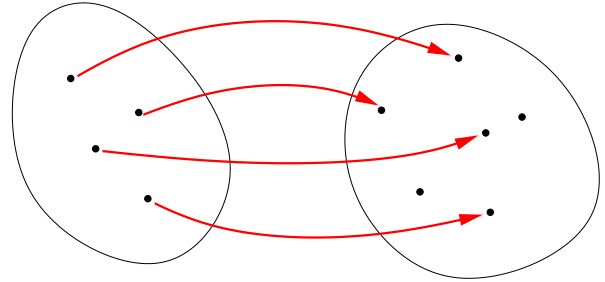


FIGURE VIII.6 – Exemple d'application injective.

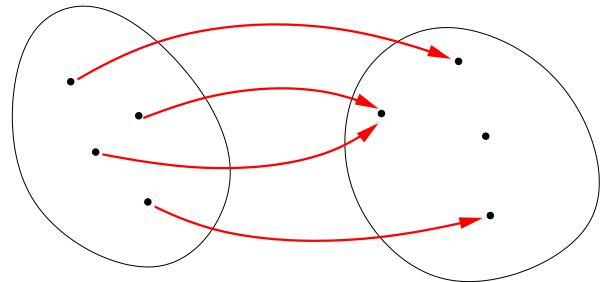


FIGURE VIII.7 – Exemple d'application non injective : une image a deux antécédents ou plus.

Remarque 4.1.3.

La donnée de l'ensemble de départ est primordiale. Exemple : l'application $[-\pi/2, \pi/2] \rightarrow \mathbb{R}, x \mapsto \sin(x)$ est injective alors que $\mathbb{R} \rightarrow \mathbb{R}, x \mapsto \sin(x)$ ne l'est pas (le montrer et tracer les courbes représentatives de ces deux applications). On peut

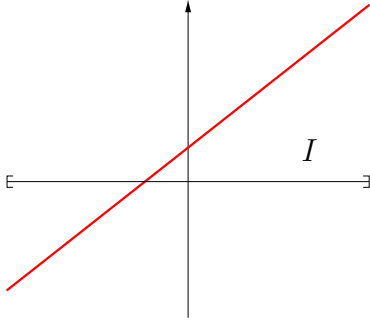
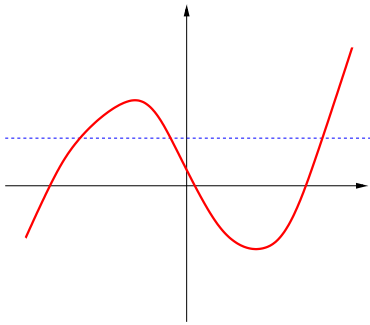

 FIGURE VIII.8 – Graphe d'application injective sur un segment I .


FIGURE VIII.9 – Graphe d'application non injective : une image a deux antécédents ou plus.

aussi se demander ce qu'il adviendrait de la figure VIII.8 si l'on ne précise pas que l'espace de départ est le segment I ici représenté.

Remarque 4.1.4.

Une application $f : E \rightarrow F$ est injective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet au plus une solution dans E .

Remarque 4.1.5.

Une restriction d'une fonction injective est toujours injective.

Remarque 4.1.6.

On a montré dans le premier chapitre que toute fonction réelle strictement monotone est injective.

Théorème 4.1.7 (Composée d'injections.).

Soit E, F et G trois ensembles, $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications injectives. Alors $g \circ f$ est injective.

Démonstration.

Soit $(x, y) \in E^2$, supposons que $g \circ f(x) = g \circ f(y)$. Alors, par injectivité de g puis de f , $f(x) = f(y)$ puis $x = y$. $\square$

Exercice 4.1.8.

Soit E, F deux ensembles, soit $f : E \rightarrow F$. Montrer que f est injective si et seulement s'il existe $g : F \rightarrow E$ vérifiant $g \circ f = \text{Id}_E$.

4.2 Surjectivité

Définition 4.2.1.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application. On dit que f est *surjective* (ou est/réalise une *surjection*) si $\forall y \in F, \exists x \in E, y = f(x)$.

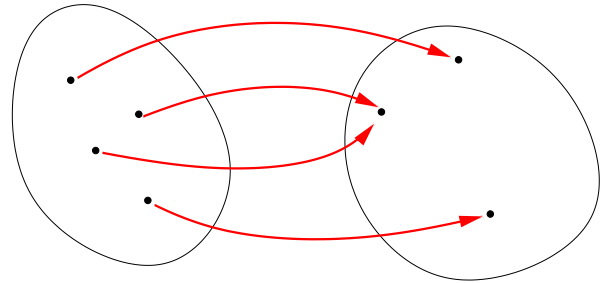


FIGURE VIII.10 – Exemple d'application surjective.

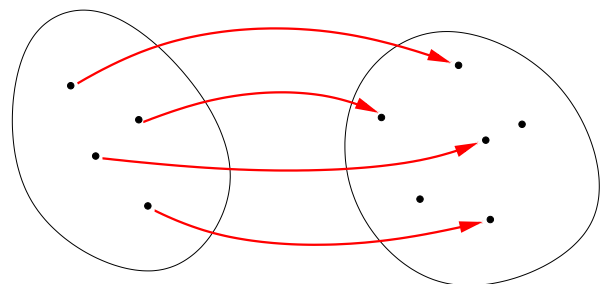


FIGURE VIII.11 – Exemple d'application non surjective.

• La donnée de l'espace de départ *et* de l'espace d'arrivée est, là encore, primordiale.

Exemple 4.2.2.

La fonction définie par $x \mapsto \sin x$ est surjective de $[0, 2\pi]$ sur $[-1, 1]$, mais pas de $[0, 2\pi]$ sur $\mathbb{R}$ ni

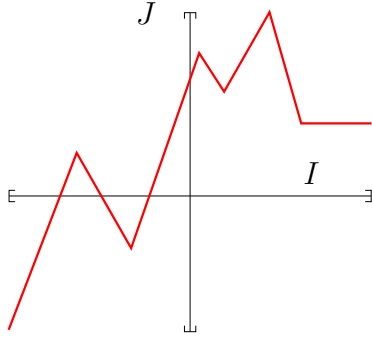


FIGURE VIII.12 – Graphe d'une application surjective d'un segment I dans un segment J .

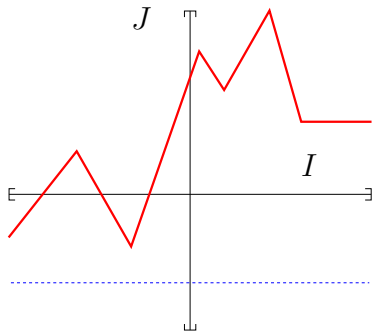


FIGURE VIII.13 – Graphe d'une application non surjective d'un segment I dans un segment J .

de $[0, \pi]$ sur $[-1, 1]$. Revenir aussi sur les figures VIII.12 et VIII.13.

Exercice 4.2.3.

Dans chaque cas, dire si cette application est surjective ou non : $(\mathbb{R}^* \text{ ou } \mathbb{R}_+^*) \rightarrow (\mathbb{R} \text{ ou } \mathbb{R}^*)$, $x \mapsto \frac{1}{x}$

Remarque 4.2.4.

Une fonction est toujours surjective sur son image (formellement : la *corestriction* d'une application à son image est toujours surjective).



Une fonction non surjective n'est pas nécessairement injective, et vice-versa.

Remarque 4.2.5.

Une application $f : E \rightarrow F$ est surjective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet au moins une solution dans E .

Exercice 4.2.6.

Étudier la surjectivité de la fonction

$$f : \mathbb{C} \setminus \{i\} \rightarrow \mathbb{C} \setminus \{1\} \\ z \mapsto \frac{z+i}{z-i}.$$

Théorème 4.2.7 (Composée de surjections.).

Soit E, F et G trois ensembles, $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications surjectives. Alors $g \circ f$ est surjective.

Démonstration.

Soit $z \in G$, g est surjective : il existe $y \in F$ vérifiant $z = g(y)$. Comme f est surjective, il existe $x \in E$ vérifiant $y = f(x)$ et on a donc $z = g \circ f(x)$. $\square$

Exercice 4.2.8.

Soit E, F deux ensembles non vides, soit $f : E \rightarrow F$. Montrer que f est surjective si et seulement s'il existe $g : F \rightarrow E$ vérifiant $f \circ g = \text{Id}_F$.

4.3 Bijectivité

Définition 4.3.1.

Une application *bijective* (ou qui réalise une *bijection*) est une application injective et surjective.

Soit E et F deux ensembles. Une application $f : E \rightarrow F$ est donc bijective si et seulement si $\forall y \in F, \exists! x \in E, y = f(x)$.

Exemple 4.3.2.

Application identité, fonctions affines de la forme $\mathbb{R} \rightarrow \mathbb{R}, x \mapsto ax + b$, avec $a \neq 0$, les similitudes ...

Théorème 4.3.3 (Fonction réciproque).

Soit $f : E \rightarrow F$ une application.

1. f est bijective si et seulement s'il existe $g : F \rightarrow E$ telle que $g \circ f = \text{Id}_E$ et $f \circ g = \text{Id}_F$.
2. Dans ce cas, g est unique et notée f^{-1} , appelée *fonction réciproque* de f , et on a, pour tout $(x, y) \in E \times F$, $f(x) = y$ si et seulement si $x = f^{-1}(y)$.
3. f^{-1} est bijective et $(f^{-1})^{-1} = f$.

Démonstration. 1. Si f bijective, on construit g . Soit $y \in F$. On note $g(y)$ l'unique antécédent de y par f : donc g est une fonction bien définie (tout point a une et une seule image). On vérifie bien que $f \circ g = \text{Id}_F$ et que $g \circ f = \text{Id}_E$.

Si g existe, on montre que f est injective et que f est surjective.

2. Unicité : on utilise l'injectivité de f .
Équivalence : facile par double implication.
3. On utilise le point (i) pour la bijectivité et le point (ii) pour l'unicité.

□



Ne JAMAIS parler de f^{-1} avant d'avoir montré qu'elle existe.



Dans le cas d'une fonction réelle, il ne faut pas confondre f^{-1} et $1/f$. Ex : $f = 1$ ($1/f$ existe, pas f^{-1}), $f : x \mapsto x$ (f^{-1} existe, pas $1/f$).

• Le graphe de la réciproque d'une fonction est le symétrique par rapport à la première bissectrice du plan du graphe de cette fonction. En effet, si on note Γ le graphe de f et Γ' celui de sa réciproque, on a par définition, pour tous x et y , $(x, y) \in \Gamma$ si et seulement si $(y, x) \in \Gamma'$.

Exemple 4.3.4.

$x \mapsto x^2$ et $x \mapsto \sqrt{x}$, $x \mapsto \ln x$ et $x \mapsto e^x$, $\tan$ et $\arctan$ (sur leurs espaces de départ et d'arrivée usuels).

Remarque 4.3.5.

Une application $f : E \rightarrow F$ est bijective si et seulement si, pour tout $y \in F$, l'équation $y = f(x)$ admet exactement une solution dans E .

• En pratique, pour montrer que f est bijective, on peut au choix :

1. montrer que f est injective et surjective ;
2. montrer que f a une réciproque en raisonnant par équivalence : $y = f(x)$ ssi $x = f^{-1}(y)$, où f^{-1} est alors à donner (on résout donc $y = f(x)$) ;
3. donner f^{-1} et vérifier que $f \circ f^{-1} = \text{Id}$ et $f^{-1} \circ f = \text{Id}$.

Exemple 4.3.6.

Reprendre l'exercice 4.2.6 et déterminer l'inverse de cette application.

Remarque 4.3.7.

Une injection réalise toujours une bijection sur son image.

Théorème 4.3.8 (Composée de bijections.).

Soit E , F et G trois ensembles, $f : E \rightarrow F$ et $g : F \rightarrow G$ deux bijections. Alors $g \circ f$ est une bijection et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration.

Utilise les résultats analogues sur injectivité et surjectivité. Ou encore : on donne l'inverse (formule à connaître !) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, et surtout ne pas inverser les membres ! □

Exercice 4.3.9.

Trouver deux applications f et g toutes les deux non bijectives, telles que $g \circ f$ est bijective.

4.4 Un peu de vocabulaire anglais ...

- Application : *mapping* ou *map* .
- Injection : *injection* ou *one-to-one mapping* .
- Surjection : *surjection* ou *onto mapping* .
- « non injection » : *many-to-one mapping* .
- Bijection : *bijection* ou *one-to-one correspondence* .

5 Image directe, tiré en arrière.

5.1 Image directe

Définition 5.1.1.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application et A une partie de E . On appelle *image directe* de A par f l'ensemble des images des éléments de A (voir figure VIII.14), i.e. la partie de F :

$$\begin{aligned} f(A) &= \{ f(x) \mid x \in A \} \\ &= \{ y \in F \mid \exists x \in A, y = f(x) \}. \end{aligned}$$

Remarque 5.1.2.

La seconde forme de $f(A)$ est la plus pratique à utiliser et est à retenir en priorité.

Remarque 5.1.3.

La notation $f(E)$ utilisée pour l'image de f est bien cohérente.

Remarque 5.1.4.

On a toujours $f(A) \subset \text{Im}(f)$.

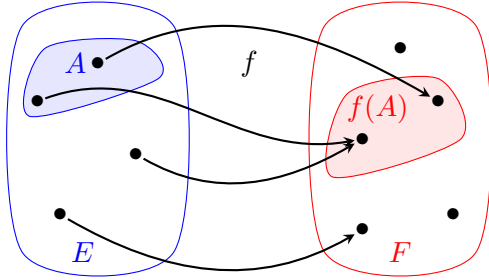


FIGURE VIII.14 – Image directe d'une partie A par une application f .

- Cela se lit aisément sur un graphe.

Exercice 5.1.5.

Soit $c : \mathbb{R} \rightarrow \mathbb{R}$, déterminer $c([2, 4])$ et $c([-1, 3])$.

Exercice 5.1.6.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application, A et B deux parties de E .

- Si $A \subset B$, est-ce que $f(A) \subset f(B)$?
- Comparer $f(A \cup B)$ et $f(A) \cup f(B)$, puis $f(A \cap B)$ et $f(A) \cap f(B)$.

Proposition 5.1.7.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application. Alors f est surjective si et seulement si $f(E) = F$.

5.2 Tiré en arrière

Définition 5.2.1.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application et B une partie de F . On appelle *tiré en arrière* de B par f l'ensemble des antécédents

des éléments de B (voir figure VIII.15), *i.e.* la partie de E :

$$f^{\leftarrow}(B) = \{x \in E \mid f(x) \in B\}.$$

Remarque 5.2.2.

Le vocabulaire officiel est plutôt « *image réciproque* de B par f » et la notation officielle est : $f^{-1}(B)$.

D'expérience, cette terminologie et cette notation sont une source de confusions désastreuses. Ne l'utilisez qu'une fois cette notion solidement acquise.

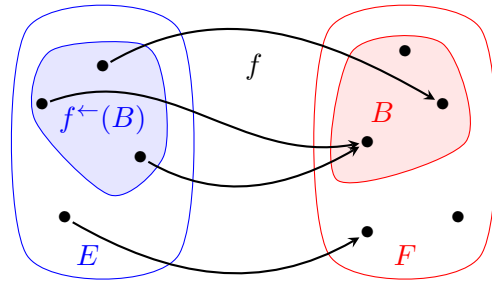


FIGURE VIII.15 – Tiré en arrière d'une partie B par une application f .

- On lit aussi le tiré en arrière d'une partie sur le graphe d'une fonction.



Ne pas confondre avec la réciproque d'une fonction, qui n'existe pas si f n'est pas bijective.

- Notamment, les notations $f^{\leftarrow}(\{x\})$ et $f^{-1}(x)$ ne font formellement pas référence au même type d'objet.

Exercice 5.2.3.

Soit $c : \mathbb{R} \rightarrow \mathbb{R}$, déterminer $c^{\leftarrow}([1, 4])$ et $c^{\leftarrow}([-3, 1])$.

Théorème 5.2.4.

Soit E et F deux ensembles. Si $f : E \rightarrow F$ est une application bijective et si $B \subset F$, alors on a $f^{\leftarrow}(B) = f^{-1}(B)$, où la deuxième écriture désigne l'image directe par f^{-1} .

Démonstration.

Soit $x \in E$, alors

$$\begin{aligned}
 x \in f^{-1}(B) &\Leftrightarrow \exists y \in B, x = f^{-1}(y) \\
 &\Leftrightarrow \exists y \in B, f(x) = y \\
 &\Leftrightarrow f(x) \in B \\
 &\Leftrightarrow x \in f^{\leftarrow}(B)
 \end{aligned}$$

□

Exercice 5.2.5.

Soit E et F deux ensembles, $f : E \rightarrow F$ une application, A et B deux parties de F .

- Si $A \subset B$, est-ce que $f^{\leftarrow}(A) \subset f^{\leftarrow}(B)$?
- Comparer $f^{\leftarrow}(A \cup B)$ et $f^{\leftarrow}(A) \cup f^{\leftarrow}(B)$, puis $f^{\leftarrow}(A \cap B)$ et $f^{\leftarrow}(A) \cap f^{\leftarrow}(B)$.

Proposition 5.2.6.

Soit E, F deux ensembles non vides, soit $f : E \rightarrow F$.

Alors, $\{ f^{\leftarrow}(\{y\}) \mid y \in F \}$ est un recouvrement disjoint de E , tandis que $\{ f^{\leftarrow}(\{y\}) \mid y \in \text{Im}(f) \}$ est une partition de E .

De même, si $(F_i)_{i \in I}$ est une partition de $\text{Im}(f)$, alors $\{ f^{\leftarrow}(F_i) \mid i \in I \}$ est une partition de E .

Chapitre IX

Calcul matriciel

Sommaire

1	Définitions élémentaires	130
1.1	Opérations sur les matrices	130
1.2	Matrices carrées	132
1.3	Matrices inversibles	133
1.4	Matrices et opérations élémentaires . .	134
1.5	Transposition et matrices symétriques	137
1.6	Inversion de matrices triangulaires. . .	138
2	Systèmes linéaires	139
2.1	Généralités	139
2.2	Systèmes et matrices inversibles	140

n, m, p, q et r désignent des entiers naturels non nuls, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Définitions élémentaires

Définition 1.0.1.

On appelle *matrice de taille* $n \times p$ (ou à n lignes et p colonnes), à valeurs (ou coefficients) dans $\mathbb{K}$, toute famille de np éléments de $\mathbb{K}$, ces éléments étant notés $(a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$, et présentés sous la forme d'un tableau de la manière suivante :

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,p} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,p} \end{pmatrix}.$$

On note $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$, les $(a_{i,j})$ étant les *coefficients* de la matrice A , $a_{i,j}$ étant le coefficient de la i^{e} ligne et de la j^{e} colonne.

La matrice $(a_{i,j})_{1 \leq j \leq p}$ est la i^{e} ligne de A , parfois notée $a_{i,*}$.

La matrice $(a_{i,j})_{1 \leq i \leq n}$ est la j^{e} colonne de A , parfois notée $a_{*,j}$.

Remarque 1.0.2.

Le premier indice indique toujours la ligne et le second indice indique toujours la colonne. En général (mais attention quand même), on les note respectivement i et j .

Exemple 1.0.3.

Donner la matrice $(i \times j)_{1 \leq i \leq 3, 1 \leq j \leq 5}$.

Définition 1.0.4 (symbole de Kronecker).

Si i, j sont deux objets, on note

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}.$$

Définition 1.0.5. • L'ensemble des matrices de taille $n \times p$ est noté $\mathcal{M}_{n,p}(\mathbb{K})$.

- On appelle *matrice carrée d'ordre* n toute matrice de taille $n \times n$. L'ensemble des matrices carrées d'ordre n est noté $\mathcal{M}_n(\mathbb{K})$.

- On appelle *matrice nulle d'ordre* n la matrice carrée d'ordre n dont tous les coefficients sont nuls. On la note simplement 0_n , ou 0 sans référence à sa taille s'il n'y a pas d'ambiguïté.
- On appelle *matrice identité d'ordre* n la matrice

$$I_n = (\delta_{i,j})_{1 \leq i,j \leq n} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

- On appelle *matrice diagonale* toute matrice carrée $(a_{ij})_{1 \leq i,j \leq n}$ telle que pour tous $i, j \in \llbracket 1, n \rrbracket$, $i \neq j \Rightarrow a_{i,j} = 0$.
- On appelle *matrice triangulaire supérieure* (resp. *inférieure*) toute matrice carrée $(a_{ij})_{1 \leq i,j \leq n}$ telle que pour tous $i, j \in \llbracket 1, n \rrbracket$ tels que $i > j$ (resp. $i < j$), $a_{i,j} = 0$.

Remarque 1.0.6. 1. On note généralement les matrices par des lettres majuscules, et la famille des coefficients par la lettre minuscule correspondante.

2. On identifie les matrices colonnes de $\mathcal{M}_{n,1}(\mathbb{K})$ avec les éléments de $\mathbb{K}^n$.
3. On se gardera d'identifier les matrices lignes avec les éléments de $\mathbb{K}^n$ car on préfère les identifier avec d'autres objets mathématiques (on verra cela plus tard).

1.1 Opérations sur les matrices

Définition 1.1.1.

Soient $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$ et $B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$ deux matrices de même taille, et $\lambda \in \mathbb{K}$ un scalaire.

Addition On appelle *somme* de A et B la matrice $(a_{ij} + b_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$, notée $A + B$.

Produit par un scalaire On note λA la matrice $(\lambda a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$.



Attention aux tailles des matrices : on ne peut additionner n'importe quoi avec n'importe quoi.

Exemple 1.1.2.

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} + 2 \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 1 & 8 \end{pmatrix}.$$

Définition 1.1.3 (Produit matriciel).

Soient $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$. On appelle *produit de A par B* noté AB la matrice de $\mathcal{M}_{n,q}(\mathbb{K})$ de coefficients $\left(\sum_{k=1}^p a_{ik} b_{kj} \right)$.



Gare aux dimensions, on ne peut pas multiplier n'importe quelles matrices.

Exemple 1.1.4. • On tâchera d'organiser les produits comme suit :

$$\begin{array}{cc} \text{Dim. OK} & \overbrace{\begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 2 \end{pmatrix}}^B \\ \underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 0 \\ 4 & 2 \end{pmatrix}}_A & \underbrace{\begin{pmatrix} 1 & 3 & 6 \\ 1 & 0 & 2 \\ 2 & 6 & 12 \end{pmatrix}}_{=AB} \end{array}$$

- Le produit impossible :

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}.$$



Ce produit comporte plein de pièges.

Remarque 1.1.5.

Le produit matriciel n'est pas commutatif, par exemple :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Et même pire, AB peut exister mais pas BA .

Remarque 1.1.6.

Le produit de deux matrices non nulles peut valoir la matrice nulle.

Par exemple, avec

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

alors $AA = 0$, $AB = 0$ et $BA \neq 0$.

Ainsi, on ne peut pas « simplifier » dans un produit. Ici : $A \times A = A \times B$ mais $A \neq B$.

Proposition 1.1.7.

Le produit matriciel est :

Associatif : si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $B \in \mathcal{M}_{p,q}(\mathbb{K})$, $C \in \mathcal{M}_{q,r}(\mathbb{K})$, alors $(AB)C$ et $A(BC)$ sont dans $\mathcal{M}_{n,r}(\mathbb{K})$ et sont égales, notées ABC .

Bilinéaire : si A, B, C, D sont des matrices de taille convenable, et si $\lambda \in \mathbb{K}$, alors $(A + \lambda B)C = AC + \lambda BC$ et $A(C + \lambda D) = AC + \lambda AD$.

Les matrices nulles et identité jouent un rôle bien particulier. Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $q \in \mathbb{N}^*$, alors

Neutre à gauche : $I_n A = A$

Neutre à droite : $A I_p = A$

Mult. par 0 à gauche : $0_{q,n} A = 0_{q,p}$

Mult. par 0 à droite : $A 0_{p,q} = 0_{n,q}$

Démonstration.

Bien qu'un peu technique, nous donnons ici la démonstration ; nous en verrons plus tard une autre.

1. $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$. Ainsi,

$$BC = \left(\sum_{k=1}^q b_{ik} c_{kj} \right)_{1 \leq i \leq p, 1 \leq j \leq r}$$

et

$$A(BC) = \left(\sum_{\ell=1}^p a_{i\ell} \times \left(\sum_{k=1}^q b_{\ell k} c_{kj} \right) \right)_{1 \leq i \leq n, 1 \leq j \leq r}.$$

Or, si $1 \leq i \leq n$ et $1 \leq j \leq r$,

$$\begin{aligned} \sum_{\ell=1}^p a_{i\ell} \times \left(\sum_{k=1}^q b_{\ell k} c_{kj} \right) &= \sum_{\ell=1}^p a_{i\ell} \times \sum_{k=1}^q b_{\ell k} c_{kj} \\ &= \sum_{\ell=1}^p \sum_{k=1}^q a_{i\ell} b_{\ell k} c_{kj} \\ &= \sum_{k=1}^q \sum_{\ell=1}^p a_{i\ell} b_{\ell k} c_{kj} \\ &= \sum_{k=1}^q \left(\sum_{\ell=1}^p a_{i\ell} b_{\ell k} \right) \times c_{kj}, \end{aligned}$$

qui est le coefficient i, j de $(AB)C$. D'où l'égalité voulue.

2. *idem*

$$3. I_n A = \left(\sum_{k=1}^n \delta_{ik} a_{kj} \right) = (\delta_{ii} a_{ij}) = (a_{ij}) = A.$$

4. Direct.

□

Remarque 1.1.8.

Par associativité, il y a 5 manières de calculer $ABCD$ qui conduisent toutes au même résultat : $((AB)C)D = (A(BC))D = A((BC)D) = A(B(CD)) = (AB)(CD)$. Mais le temps de calcul est-il le même dans les 5 cas ? C'est le problème de la *multiplication matricielle enchaînée* (Matrix chain multiplication ou Matrix Chain Ordering Problem (MCOP) en anglais). Plus généralement, le problème est de savoir dans quel ordre effectuer les produits pour calculer le plus efficacement possible un produit de matrices $M_1.M_2.\dots.M_n$. Ce problème peut se résoudre par programmation dynamique, ce qui est au programme en option informatique, mais même si ce n'est pas toujours la solution optimale, il vaut mieux commencer par les produits qui font apparaître des « petites » matrices.

Précisément, le produit d'une matrice $n \times p$ par une matrice $p \times q$ nécessite de l'ordre de $n \times p \times q$ opérations. Ainsi, si $A \in \mathcal{M}_{10,100}(\mathbb{K})$, $B \in \mathcal{M}_{100,5}$ et $C \in \mathcal{M}_{5,50}$, le calcul de $(AB)C$ demande de l'ordre de $(10 \times 100 \times 5) + 10 \times 5 \times 50 = 7\,500$ opérations, alors que celui de $A(BC)$ en demande de l'ordre de $100 \times 5 \times 50 + 10 \times 100 \times 50 = 75\,000$.

Remarque 1.1.9.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$ et

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}.$$

Alors, en notant $C_1, \dots, C_p$ les colonnes de M , on a

$$MX = \sum_{k=1}^p x_k C_k.$$

En particulier, la matrice MX est une combinaison linéaire de la famille $(C_1, \dots, C_p)$.

Remarque 1.1.10.

En reprenant les notations de la remarque précédente, si l'on note E_i la matrice colonne élémentaire de dimension p (tous ses coefficients sont nuls, sauf le i^e qui vaut 1), c'est-à-dire

$$E_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (\delta_{i,k})_{1 \leq k \leq p},$$

le 1 se trouvant en i^e position.

On a alors

$$ME_i = M \begin{pmatrix} \delta_{1i} \\ \vdots \\ \delta_{pi} \end{pmatrix} = \sum_{k=1}^p \delta_{ki} C_k = C_i.$$

1.2 Matrices carrées

Remarque 1.2.1.

Si A et B sont deux matrices carrées d'ordre n , alors AB et BA sont définies et également de taille n . On dit que le produit matriciel est une *loi de composition interne* de $\mathcal{M}_n(\mathbb{K})$.

De plus, $I_n.A = A.I_n = A$. On dit que I_n est le *neutre* de $\mathcal{M}_n(\mathbb{K})$ pour le produit matriciel.

Enfin, la propriété de bilinéarité montrée précédemment montre que $(\mathcal{M}_n(\mathbb{K}), +, \times)$ a une structure d'anneau, non commutatif.

Remarque 1.2.2.

Soit $a_1, \dots, a_n$ et $b_1, \dots, b_n$ des nombres complexes. Alors,

$$\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & & 0 \\ & \ddots & \\ 0 & & a_n b_n \end{pmatrix}$$

Définition 1.2.3 (Puissances d'une matrice carrée).

On les définit par récurrence : si $M \in \mathcal{M}_n(\mathbb{K})$, alors, $M^0 = I_n$, $M^1 = M$, et pour tout $k \in \mathbb{N}$, $M^{k+1} = M \times M^k$ (on a donc, pour tout $k \in \mathbb{N}^*$, $M^k = \underbrace{M \times M \times \dots \times M}_{k \text{ fois}}$). Ainsi pour tout $k \in \mathbb{N}$, on a $M^k \in \mathcal{M}_n(\mathbb{K})$.

Remarque 1.2.4.

On remarque que les puissances d'une même matrice commutent entre elles :

$$\begin{aligned} M^k \times M^j &= \underbrace{M \times M \times \dots \times M}_{k \text{ fois}} \times \underbrace{M \times M \times \dots \times M}_{j \text{ fois}} \\ &= \underbrace{M \times M \times \dots \times M}_{(k+j) \text{ fois}} \\ &= \underbrace{M \times M \times \dots \times M}_{j \text{ fois}} \times \underbrace{M \times M \times \dots \times M}_{k \text{ fois}} \\ &= M^j \times M^k. \end{aligned}$$

Théorème 1.2.5 (Formule du binôme de Newton).

Elle est valable pour les matrices *carrées qui commutent*.

Soit $n \in \mathbb{N}^*$ et $p \in \mathbb{N}$, soit $A, B \in \mathcal{M}_n(\mathbb{K})$ vérifiant $AB = BA$. Alors,

$$(A + B)^p = \sum_{k=0}^p \binom{p}{k} A^k B^{p-k}.$$

Lemme 1.2.6.

Soit $A, B \in \mathcal{M}_n(\mathbb{K})$ vérifiant $AB = BA$. Alors, pour tout $p, q \in \mathbb{N}$, $A^p B^q = B^q A^p$.

Démonstration.

On fixe $q = 1$ et on montre par récurrence que, pour tout $p \in \mathbb{N}$, $A^p B = B A^p$.

On fixe alors $p \in \mathbb{N}$ et on utilise ce que l'on vient de montrer avec A^p à la place de B et B à la place de A . $\square$

Démonstration (Formule du binôme de Newton).

Reprenre la démonstration du binôme de Newton pour des complexes, en repérant bien à quel endroit le fait que les deux matrices commutent intervient, on utilise alors le lemme 1.2.6. $\square$

Exemple 1.2.7.

Calculer A^2 avec

$$\begin{aligned} A &= \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \\ 0 & -2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \\ &= B + C. \end{aligned}$$

Calculer A^3 avec

$$\begin{aligned} A &= \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 4 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 3 & 4 \end{pmatrix} \\ &= B + C. \end{aligned}$$

1.3 Matrices inversibles

Définition 1.3.1.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. On dit que A est *inversible* s'il existe une matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que $AB = BA = I_n$.

Dans ce cas B est unique, est appelée *l'inverse* de A et est notée A^{-1} .

On note $GL_n(\mathbb{K})$ l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ inversibles.

Démonstration (Unicité).

Soit $B, C \in \mathcal{M}_n(\mathbb{K})$ deux « inverses » de A . Alors,

$$B = B I_n = B(AC) = (BA)C = I_n C = C.$$

$\square$

Remarque 1.3.2.

Une matrice inversible commute toujours avec son inverse.

Exercice 1.3.3.

Montrer que la matrice $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ étudiée précédemment n'est pas inversible.

Définition 1.3.4 (Puissances négatives d'une matrice inversible.).

Soit $A \in GL_n(\mathbb{K})$, soit $p \in \mathbb{Z}$. On définit :

$$A^{-p} = (A^{-1})^p$$

Proposition 1.3.5.

Soit $A \in GL_n(\mathbb{K})$. Alors, pour tout $p \in \mathbb{N}$, A^p est inversible et

$$(A^p)^{-1} = A^{-p}.$$

Démonstration.

Soit $p \in \mathbb{N}$. Comme A et A^{-1} commutent, $A^p(A^{-1})^p = (AA^{-1})^p = I_n^p = I_n$, de même de l'autre côté. $\square$

Proposition 1.3.6.

Soit $A, B \in GL_n(\mathbb{K})$. Alors AB est inversible et

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Démonstration.

$(AB)(B^{-1}A^{-1}) = AI_nA^{-1} = I_n$, de même de l'autre côté. $\square$

Enfin, le cas particulier des matrices carrées d'ordre 2 est à connaître sur le bout des doigts.

Définition 1.3.7.

Le déterminant d'une matrice *carrée d'ordre 2* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\det A = ad - bc$.

Proposition 1.3.8.

Une matrice carrée d'ordre 2, notée $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, est inversible si et seulement si son déterminant est non nul. Le cas échéant, $A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Démonstration.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a toujours (le vérifier par le calcul)

$$A^2 - (a + d)A + (ad - bc)I_2 = 0.$$

Alors, si $\det A \neq 0$, avec $B = \frac{1}{\det A}((a + d)I_2 - A)$, on a $AB = BA = I_2$ donc A est inversible, d'inverse B .

Réciproquement, si $\det A = 0$, alors $A(A - (a + d)I_2) = 0$. Si A est inversible, en multipliant par cet inverse on obtient que A est diagonale, puis que $a = 0$ ou que $d = 0$... Dans les deux cas, $A^2 = 0$ donc A ne peut être inversible (à vous de réfléchir pourquoi !). $\square$

1.4 Matrices et opérations élémentaires

Dans toute cette partie, on considère des matrices carrées de dimension n . Nous allons définir pour les matrices des opérations sur les lignes similaires à celles déjà vues pour les systèmes linéaires. En ce qui concerne les matrices, nous pourrons aussi définir des opérations analogues sur les colonnes. Nous verrons à la fin de ce chapitre en quoi ces opérations sont importantes pour la résolution des systèmes linéaires.

Définition 1.4.1 (matrice élémentaire).

Si $1 \leq i, j \leq n$, on définit la matrice

$$E_{i,j} = \begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ & & 1 & \\ \vdots & & & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} = (\delta_{i,k}\delta_{j,\ell})_{1 \leq k, \ell \leq n},$$

le 1 se trouvant sur la i^e ligne et la j^e colonne de M .

Remarque 1.4.2.

Si $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{K})$, alors

$$M = \sum_{1 \leq i, j \leq n} m_{i,j} E_{i,j}.$$

Remarque 1.4.3.

On pourrait très bien considérer des matrices élémentaires qui ne soient pas carrées. Les résultats suivants sont alors valides, sous réserve de compatibilité des dimensions lors des produits, mais les notations deviennent alors plus lourdes.

Commençons par voir qu'une telle matrice élémentaire peut simplement s'écrire comme le produit d'une colonne élémentaire par une ligne élémentaire.

Lemme 1.4.4.

Si $1 \leq i, j \leq n$, notons Γ_i la matrice colonne de dimension n dont tous les coefficients sont nuls, sauf le i^{e} qui vaut 1, et Λ_j la matrice ligne de dimension n dont tous les coefficients sont nuls, sauf le j^{e} qui vaut 1 :

$$\Gamma_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (\delta_{i,k})_{1 \leq k \leq n},$$

le 1 se trouvant en i^{e} position, et

$$\Lambda_j = (0 \quad \cdots \quad 0 \quad 1 \quad 0 \quad \cdots \quad 0) = (\delta_{j,\ell})_{1 \leq \ell \leq n},$$

le 1 se trouvant en j^{e} position.

Alors, $E_{i,j} = \Gamma_i \Lambda_j$.

Remarque 1.4.5.

Cela signifie que la i^{e} ligne de $E_{i,j}$ est Λ_j , la j^{e} colonne de $E_{i,j}$ est Γ_i , les autres lignes et colonnes étant nulles.

Démonstration.

Cela peut s'observer en dessinant le produit $\Gamma_i \Lambda_j$.

On peut aussi l'observer sur la formule définissant $E_{i,j}$. Comme $\Gamma_i = (\delta_{i,k})_{1 \leq k \leq n}$ et comme $\Lambda_j = (\delta_{j,\ell})_{1 \leq \ell \leq n}$, alors par la formule du produit matriciel on a $\Gamma_i \Lambda_j = (\delta_{i,k} \delta_{j,\ell})_{1 \leq k, \ell \leq n} = E_{i,j}$. $\square$

Donnons maintenant deux résultats techniques, dont la maîtrise se révèlera être importante : vous devrez savoir les retrouver efficacement.

Proposition 1.4.6 (produit de deux matrices élémentaires).

On a

$$E_{i,j} E_{k,\ell} = \delta_{j,k} E_{i,\ell} = \begin{cases} E_{i,\ell} & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases}.$$

Nous pouvons donner trois démonstrations (ou plutôt, trois versions d'une même démonstration) de ce résultat. Le plus important est toutefois de savoir tracer le dessin du produit de ces deux matrices : le produit s'y lit immédiatement.

Tout d'abord, utilisons la remarque 1.1.10.

Démonstration.

Soit $\alpha \in \llbracket 1, n \rrbracket$. La α^{e} colonne de $E_{i,j} \times E_{k,\ell}$ est $E_{i,j} C_\alpha$ où C_α est la α^{e} colonne de $E_{k,\ell}$ (c'est une colonne élémentaire).

Si $\alpha \neq \ell$, $C_\alpha = 0_{n,1}$, donc toutes les colonnes de $E_{i,j} \times E_{k,\ell}$ sont nulles sauf peut-être la ℓ^{e} .

Cette ℓ^{e} colonne de $E_{k,\ell}$ est égale à Γ_k (colonne élémentaire introduite dans le lemme 1.4.4). Par la remarque 1.1.10, $E_{i,j} \Gamma_k$ est la k^{e} colonne de $E_{i,j}$. Celle-ci est nulle si $j \neq k$. Sinon, il s'agit de la colonne élémentaire Γ_i .

On en déduit le résultat. $\square$

On peut également adopter une démonstration purement calculatoire.

Démonstration.

Notons $(m_{ab})_{(a,b) \in \llbracket 1, n \rrbracket \times \llbracket 1, q \rrbracket}$ les coefficients du produit $E_{i,j} E_{k,h}$. Alors, soit $(a, b) \in \llbracket 1, n \rrbracket \times \llbracket 1, q \rrbracket$. On a

$$\begin{aligned} m_{ab} &= \sum_{c=1}^p (\delta_{ai} \delta_{cj}) (\delta_{ck} \delta_{bh}) \\ &= (\delta_{ai} \delta_{jj}) (\delta_{jk} \delta_{bh}) \\ &= \delta_{jk} (\delta_{ai} \delta_{bh}) \end{aligned}$$

m_{ab} est donc le coefficient de la ligne a , colonne b de $\delta_{jk} E_{ih}$. $\square$

Utilisons maintenant le résultat du lemme 1.4.4 pour obtenir une forme différente de cette démonstration.

Démonstration.

Reprenons les notations du lemme 1.4.4. On a

$$E_{i,j} E_{k,\ell} = C_i \underbrace{L_j C_k}_{\in \mathbb{K}} L_\ell = (L_j C_k) C_i L_\ell = (L_j C_k) E_{i,\ell}.$$

Il suffit alors de considérer le produit

$$L_j C_k = \sum_{a=1}^n \delta_{j,a} \delta_{a,k}.$$

Remarquons que si $a \neq j$ ou si $a \neq k$, on a $\delta_{j,a} \delta_{a,k} = 0$.

Si $j \neq k$, on ne peut jamais avoir simultanément $a = j$ et $a = k$, donc on a toujours $\delta_{j,a} \delta_{a,k} = 0$, donc $L_j C_k = 0$.

Si $j = k$, on a $L_j C_k = \delta_{j,j} \delta_{j,k} = 1$.

En résumé, on a $L_j C_k = \delta_{j,k}$, donc $E_{i,j} E_{k,\ell} = \delta_{j,k} E_{i,\ell}$. $\square$

Lemme 1.4.7 (produit matrice - matrice élémentaire).

Soit $M \in \mathcal{M}_n(\mathbb{K})$, dont on note les colonnes $C_1, \dots, C_n$ et dont on note les lignes $L_1, \dots, L_n$.

Soit $1 \leq i, j \leq n$.

1. $ME_{i,j}$ est la matrice dont toutes les colonnes sont nulles, sauf la j^{e} qui vaut C_i .
2. $E_{i,j}M$ est la matrice dont toutes les lignes sont nulles, sauf la i^{e} qui vaut L_j .

Démonstration.

Le plus efficace est de réaliser le dessin du produit matriciel. On peut aussi voir cela comme une traduction de la remarque (fondamentale) 1.1.10.

On peut aussi effectuer un calcul :

$$\begin{aligned} ME_{i,j} &= \sum_{1 \leq k, \ell \leq n} m_{k,\ell} E_{k,\ell} E_{i,j} \\ &= \sum_{1 \leq k, \ell \leq n} m_{k,\ell} \delta_{\ell,i} E_{k,j} \\ &= \sum_{k=1}^n m_{k,i} E_{k,j}, \end{aligned}$$

ce qui est exactement le résultat annoncé.

On procède de même pour l'autre produit. $\square$

Définition 1.4.8.

Il existe trois types d'opérations élémentaires sur les lignes et colonnes d'une matrice :

1. l'échange de deux lignes ou deux colonnes ;
2. la multiplication d'une ligne/colonne par un scalaire **non nul** ;
3. l'addition à une ligne/colonne d'une **autre** ligne/colonne multipliée par un scalaire.

Ces opérations sont notées respectivement :

1. $L_i \leftrightarrow L_j$ et $C_i \leftrightarrow C_j$;

2. $L_i \leftarrow \lambda L_i$ avec $\lambda \neq 0$ (*idem* avec des colonnes) ;

3. $L_i \leftarrow L_i + \lambda L_j$, avec $i \neq j$ (*idem* avec des colonnes).

Définition 1.4.9 (matrices d'opérations élémentaires).

Soit $1 \leq i \neq j \leq n$, soit $\lambda \in \mathbb{K}$.

1. On appelle matrice d'échange de coefficients i, j la matrice $\varepsilon_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$ (la dessiner).
2. On appelle matrice de dilatation de coefficient i et de rapport λ la matrice $D_i(\lambda) = I_n + (\lambda - 1)E_{ii}$ (la dessiner).
3. On appelle matrice de transvection de coefficients i, j et de rapport λ la matrice $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ (la dessiner).

Théorème 1.4.10.

Soit $A \in \mathcal{M}_n(\mathbb{K})$, et $i, j \in \llbracket 1, n \rrbracket$.

1. L'opération $L_i \leftrightarrow L_j$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice ε_{ij} .
2. L'opération $L_i \leftarrow \lambda L_i$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice $D_i(\lambda)$.
3. L'opération $L_i \leftarrow L_i + \lambda L_j$ est équivalente à la multiplication de la matrice A à sa gauche par la matrice $T_{ij}(\lambda)$.
4. L'opération $C_i \leftrightarrow C_j$ est équivalente à la multiplication de la matrice A à sa droite par la matrice ε_{ij} .
5. L'opération $C_i \leftarrow \lambda C_i$ est équivalente à la multiplication de la matrice A à sa droite par la matrice $D_i(\lambda)$.
6. L'opération $C_j \leftarrow C_j + \lambda C_i$ est équivalente à la multiplication de la matrice A à sa droite par la matrice $T_{ij}(\lambda)$ (attention aux coefficients !).

Démonstration.

On appelle $L_1, \dots, L_n$ les lignes de A et $C_1, \dots, C_p$ ses colonnes.

Tout est fondé sur le lemme 1.4.7.

$E_{i,j}A$ est la matrice nulle, sauf pour sa i^e ligne qui vaut L_j . On a alors immédiatement les effets demandés. $\square$

Exemple 1.4.11.

Calculer

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On trouve $\begin{pmatrix} 7 & 3 & 2 \\ 32 & 12 & 10 \\ 25 & 9 & 8 \end{pmatrix}$.

Théorème 1.4.12 (inversion des matrices d'opérations élémentaires).

Soit $1 \leq i \neq j \leq n$, soit $\lambda \in \mathbb{K}$. Alors, les trois matrices d'opérations élémentaires introduites ci-dessus sont inversibles et

$$\begin{aligned} \varepsilon_{ij}^{-1} &= \varepsilon_{ij}, \\ D_i(\lambda)^{-1} &= D_i(\lambda^{-1}), \\ T_{ij}(\lambda)^{-1} &= T_{ij}(-\lambda). \end{aligned}$$

Démonstration.

Il suffit d'utiliser le résultat précédent. Par exemple, effectuer le calcul

$$\varepsilon_{ij}^2 = \varepsilon_{ij} \varepsilon_{ij} = I_n$$

revient à échanger deux fois les lignes i et j de I_n . On revient donc à la configuration de départ, et donc $\varepsilon_{ij}^2 = I_n$.

On procède de même pour les deux autres.

On peut aussi calculer directement, par exemple, comme I_n et λE_{ij} commutent :

$$\begin{aligned} T_{ij}(\lambda)T_{ij}(-\lambda) &= (I_n + \lambda E_{ij})(I_n - \lambda E_{ij}) \\ &= I_n^2 - \lambda^2 E_{ij}^2 \\ &= I_n. \end{aligned}$$

En effet, comme $i \neq j$, alors $E_{ij}^2 = \delta_{ij} E_{ij} = 0$. $\square$

Remarque 1.4.13.

Si par opérations élémentaires sur les lignes ou les colonnes d'une matrice on arrive à I_n , on obtient donc rapidement l'inverse de cette matrice.

Exercice 1.4.14.

Avec $A = \begin{pmatrix} 1 & 3 \\ -2 & 2 \end{pmatrix}$, montrer que A est inversible et calculer A^{-1} en procédant par opérations

élémentaires sur les lignes et/ou les colonnes de A .

1.5 Transposition et matrices symétriques

Définition 1.5.1.

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $A = (a_{ij})$. On appelle *transposée de A* la matrice de dimension $p \times n$ notée $A^\top$ et définie par

$$\forall i \in \llbracket 1, p \rrbracket, \forall j \in \llbracket 1, n \rrbracket, (A^\top)_{i,j} = a_{j,i}.$$

Remarque 1.5.2.

On trouvera parfois aussi la notation ${}^t A$.

Exemple 1.5.3.

$$\begin{pmatrix} 4 & 2 \end{pmatrix}^\top = \begin{pmatrix} 4 \\ 2 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}^\top = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

On a aussi $I_n^\top = I_n$.

Proposition 1.5.4.

Soient $A, B \in \mathcal{M}_{n,p}(\mathbb{K})$, $\lambda \in \mathbb{K}$.

1. $(A + \lambda B)^\top = A^\top + \lambda B^\top$, i.e. $A \mapsto A^\top$ est linéaire.
2. Si $C \in \mathcal{M}_{p,q}(\mathbb{K})$, $(AC)^\top = C^\top A^\top$.
3. $(A^\top)^\top = A$.
4. Si A est inversible, alors $A^\top$ est inversible et $(A^{-1})^\top = (A^\top)^{-1}$.

Démonstration. 1. Élémentaire.

2. $A = (a_{ij})$, $C = (c_{ij})$, $A^\top = (\alpha_{ij})$, $C^\top = (\gamma_{ij})$, avec $\alpha_{ij} = a_{ji}$, $\gamma_{ij} = c_{ji}$, et on conclut par calcul direct.
3. Élémentaire.
4. On a $AA^{-1} = I_n$, donc en transposant $(A^{-1})^\top \times A^\top = I_n^\top = I_n$. $\square$

Remarque 1.5.5.

La transposition permet de transformer des résultats sur les colonnes en résultats sur les lignes, et inversement. Par exemple, une matrice est inversible si et seulement si ses lignes sont linéairement indépendantes.

Définition 1.5.6.

$A \in \mathcal{M}_n(\mathbb{K})$ est dite *symétrique* (resp. *antisymétrique*) si $A = A^\top$ (resp. $A = -A^\top$).

On note souvent $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques de dimension n à coefficients dans $\mathbb{K}$, et $\mathcal{A}_n(\mathbb{K})$ celui des matrices antisymétriques.

Remarque 1.5.7.

Une matrice symétrique ou antisymétrique est toujours carrée.

Exemple 1.5.8.

$\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$ est symétrique, pas $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

Exemple 1.5.9.

$\begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$ est anti-symétrique, pas $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Proposition 1.5.10.

Les coefficients diagonaux d'une matrice antisymétrique sont nuls.

Démonstration.

Soit $i \in \llbracket 1, n \rrbracket$, on a $a_{ii} = -a_{ii}$ donc $a_{ii} = 0$. $\square$

Exercice 1.5.11.

Soit $M \in \mathcal{M}_n(\mathbb{R})$. Montrer qu'il existe un unique couple (A, S) tel que

- $M = A + S$;
- $A \in \mathcal{A}_n(\mathbb{R})$;
- $S \in \mathcal{S}_n(\mathbb{R})$.

1.6 Inversion de matrices triangulaires.

Lemme 1.6.1.

Le produit de deux matrices triangulaires de même type est aussi une matrice triangulaire, de même type.

Démonstration.

On réalisera bien entendu un dessin.

On le démontre pour deux matrices triangulaires supérieures, on obtient par transposition le résultat désiré sur les matrices triangulaires inférieures.

Soit $A, B \in \mathcal{M}_n(\mathbb{R})$ deux matrices triangulaires supérieures, soit $1 \leq j < i \leq n$. Le coefficient d'indice (i, j) de AB est

$$\sum_{k=1}^n a_{i,k} b_{k,j}$$

Considérons $k \in \llbracket 1, n \rrbracket$. Si $k > j$, on a $b_{k,j} = 0$, car B est triangulaire supérieure. Sinon, on a $k \leq j$, donc $k < i$, donc on a $a_{i,k} = 0$, car A est triangulaire supérieure.

Ainsi, $\sum_{k=1}^n a_{i,k} b_{k,j} = 0$, donc AB est triangulaire supérieure. $\square$

Théorème 1.6.2.

Une matrice triangulaire est inversible si et seulement si aucun de ses coefficients diagonaux n'est nul.

Le cas échéant, l'inverse d'une matrice triangulaire est triangulaire, de même type.

On donne ici une preuve élémentaire de ce résultat, nous en donnerons une plus abstraite (et plus efficace) au second semestre.

Démonstration.

Quitte à transposer, il suffit de considérer une matrice $T = (t_{i,j})$ triangulaire supérieure.

Supposons que pour tout $1 \leq j \leq n$, $t_{j,j} \neq 0$. On effectue pour tout j allant de n à 1 et pour chaque $1 \leq i \leq j-1$ l'opération

$$L_i \leftarrow L_i - \frac{t_{i,j}}{t_{j,j}} L_j,$$

puis l'opération

$$L_j \leftarrow \frac{1}{t_{j,j}} L_j,$$

on obtient la matrice identité. Or, toutes les matrices d'opérations élémentaires utilisées sont triangulaires supérieures. Il existe donc des matrices triangulaires supérieures $T_1 \dots T_p$ telles que

$$T_1 \dots T_p T = I_n.$$

Ainsi, avec $T' = T_1 \dots T_p$, on a

$$T' T = I_n.$$

Il suffit d'observer qu'avec les mêmes opérations sur les colonnes, dans l'ordre inverse, on obtient

$$T T' = I_n.$$

Comme produit de matrices triangulaires supérieures, T' est triangulaire supérieure. Ainsi, T est inversible et $T' = T^{-1}$ est triangulaire supérieure.

Réciproquement, supposons qu'il existe $1 \leq i \leq n$ tel que $t_{i,i} = 0$. Notons k le plus grand tel indice i . Alors,

en effectuant les mêmes opérations que précédemment, il existe une matrice T' inversible telle que

$$T'T = \begin{pmatrix} * & \dots & * & * & & \\ \vdots & & \vdots & \vdots & & \\ * & \dots & * & * & & \\ & & & 0 & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix},$$

les coefficients non inscrits étant nuls. Or, une matrice possédant une ligne nulle ou une colonne nulle n'est pas inversible : si une matrice A a sa i^{e} ligne nulle, alors pour toute matrice B la i^{e} ligne de AB sera nulle, donc $AB \neq I_n$.

Ainsi, $T'T$ n'est pas inversible, donc T' étant inversible, T ne l'est pas. $\square$

2 Systèmes linéaires

2.1 Généralités

Rappel 2.1.1.

On appelle *système linéaire à n équations et p inconnues* tout système de la forme :

$$\begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + \dots + a_{np}x_p = b_n \end{cases}$$

où les a_{ij} et les b_i sont dans $\mathbb{K}$, et les x_i sont les inconnues.

On dit que le système est *compatible* s'il admet une solution.

Le *système homogène associé* est le système :

$$\begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = 0 \\ \vdots \\ a_{n1}x_1 + \dots + a_{np}x_p = 0 \end{cases}$$

Dans la suite nous noterons S le premier système et S_H son système homogène associé, et nous noterons Sol et Sol_H leurs ensembles de solutions respectifs.

Remarque 2.1.2.

Le système S peut aussi s'écrire sous forme matricielle $AX = B$, avec $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$,

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \text{ et } B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

S_H s'écrit alors $AX = 0$.

Définition 2.1.3.

Cette matrice A est appelée *matrice du système* S .

Théorème 2.1.4. 1. Sol_H contient toujours l'élément $(0, \dots, 0)$ et est stable par combinaison linéaire.

2. L'ensemble Sol est :

- soit vide ;
 - soit non vide, et dans ce cas, si $X_0 = (x_1, \dots, x_p)$ est un élément de Sol , alors $\text{Sol} = \{X_0 + X_H, X_H \in \text{Sol}_H\}$, ce que l'on note $\text{Sol}_H + (x_1, \dots, x_p)$.
- Par conséquent, Sol contient 0, 1 ou une infinité d'éléments.

Démonstration.

On utilise les notations matricielles, le système S s'écrivant $S : AX = B$, avec $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$. Le système homogène associé à S est $S_H : AX = 0$. Soit $X, Y \in \mathcal{M}_{p,1}(\mathbb{K})$ et $\lambda, \mu \in \mathbb{K}$. On a bien

$$A \times \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

donc le vecteur nul est solution du système homogène. De plus, si X et Y sont solutions de S_H , alors

$$A(\lambda X + \mu Y) = \lambda AX + \mu AY = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Notamment, si X est une solution de S_H , tous les vecteurs colinéaires à X seront aussi solution de S_H , donc S_H est infini.

Ensuite, soit $X_0 \in \mathcal{M}_{n,1}(\mathbb{K})$ solution de S . On a

$$\begin{aligned} X \in \text{Sol} &\Leftrightarrow AX = B \\ &\Leftrightarrow AX = AX_0 \\ &\Leftrightarrow A(X - X_0) = 0 \\ &\Leftrightarrow X - X_0 \in \text{Sol}_H, \end{aligned}$$

ce qui montre bien que $\text{Sol} = \{X_0 + X_H \mid X_H \in \text{Sol}_H\}$. $\square$

Remarque 2.1.5.

Si $\text{Sol}_H \neq \{(0, \dots, 0)\}$, alors Sol_H est infini.

Exemple 2.1.6.

On considère le système

$$\begin{cases} x + 3y &= 2 \\ 2y + z &= 1 \end{cases}$$

Le système homogène associé est

$$\begin{cases} x + 3y &= 0 \\ 2y + z &= 0 \end{cases}$$

Si $(x, y, z) \in \mathbb{R}^3$, on a

$$\begin{cases} x + 3y &= 0 \\ 2y + z &= 0 \end{cases} \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = y \begin{pmatrix} -3 \\ 1 \\ -2 \end{pmatrix}.$$

Ainsi, l'ensemble des solutions homogènes est une droite vectorielle dirigée par le vecteur de coordonnées $(-3, 1, -2)$.

De même, si $(x, y, z) \in \mathbb{R}^3$, on a

$$\begin{cases} x + 3y &= 2 \\ 2y + z &= 1 \end{cases} \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} -3 \\ 1 \\ -2 \end{pmatrix}.$$

Ainsi, l'ensemble des solutions du système est une droite passant par le point de coordonnées $(2, 0, 1)$ et dirigée par le vecteur de coordonnées $(-3, 1, -2)$.

2.2 Systèmes et matrices inversibles

L'inversibilité des matrices d'opérations élémentaires est la raison pour laquelle le pivot de Gauss est bien une méthode de résolution des systèmes linéaires.

On a en effet le résultat élémentaire suivant.

Lemme 2.2.1.

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$, soit $X \in \mathcal{M}_{p,1}(\mathbb{K})$, soit $B \in \mathcal{M}_{n,1}(\mathbb{K})$. Considérons une matrice $M \in \text{GL}_n(\mathbb{K})$.

Alors,

$$AX = B \Leftrightarrow (MA)X = MB.$$

Démonstration.

Il suffit de multiplier par M ou par M^{-1} , dans un sens ou dans l'autre. $\square$

Proposition 2.2.2.

Effectuer une opération élémentaire sur les lignes d'un système linéaire donne un système équivalent.

Démonstration.

Effectuer une opération élémentaire sur les lignes d'un système linéaire revient à multiplier à gauche la matrice de ce système ainsi que le membre de droite par une matrice d'opération élémentaire, qui est inversible. Par le lemme 2.2.1, les deux systèmes sont équivalents. $\square$

Le cas particulier où la matrice du système est carrée et inversible (on parle de *système de Cramer*) est simple.

Proposition 2.2.3.

Soit $A \in \text{GL}_n(\mathbb{K})$, soit $X, B \in \mathcal{M}_{n,1}(\mathbb{K})$. Alors,

$$AX = B \Leftrightarrow X = A^{-1}B.$$

Démonstration.

Il suffit de multiplier par A ou par A^{-1} , dans un sens ou dans l'autre. On peut aussi voir cela comme une conséquence du lemme 2.2.1. $\square$

Ce point est toutefois le départ de la méthode efficace d'inversion de matrices. Anticipons un peu un résultat que nous étudierons ultérieurement.

Théorème 2.2.4.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. La matrice A est inversible si et seulement si pour tout $B \in \mathcal{M}_{n,1}(\mathbb{K})$, le système $AX = B$ admet une unique solution.

Démonstration.

Cela sera démontré au second semestre. $\square$

Remarque 2.2.5.

Le cas échéant, on utilise la proposition 2.2.3 pour lire l'expression de A^{-1} .

Exemple 2.2.6.

Considérons la matrice $A = \begin{pmatrix} 1 & 2 \\ -2 & -3 \end{pmatrix}$. Soit

$x, y, a, b \in \mathbb{R}$, notons $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $B = \begin{pmatrix} a \\ b \end{pmatrix}$.

On résout le système suivant.

$$\begin{aligned}
 AX = B &\Leftrightarrow \begin{cases} x + 2y = a \\ -2x - 3y = b \end{cases} \\
 &\xrightarrow{L_2 \leftarrow L_2 + 2L_1} \begin{cases} x + 2y = a \\ y = 2a + b \end{cases} \\
 &\xrightarrow{L_1 \leftarrow L_1 - 2L_2} \begin{cases} x = -3a - 2b \\ y = 2a + b \end{cases} \\
 &\Leftrightarrow X = \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix} B
 \end{aligned}$$

Ainsi, A est inversible, et on lit

$$A^{-1} = \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix}.$$

Exercice 2.2.7.

Pour chacune des matrices suivantes, déterminer si elle est inversible et, le cas échéant, donner son inverse.

1. $A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}$
2. $B = \begin{pmatrix} 4 & -2 \\ -2 & 1 \end{pmatrix}$
3. $C = \begin{pmatrix} 4 & 2 & 3 \\ 2 & 2 & 1 \\ -1 & -1 & 0 \end{pmatrix}$
4. $D = \begin{pmatrix} -4 & -3 & -5 \\ 4 & 2 & -2 \\ 4 & 3 & 5 \end{pmatrix}$

Chapitre X

Relations d'ordre et d'équivalence

Sommaire

1	Relations binaires.	144
2	Relations d'équivalence.	144
3	Relations d'ordre.	145
4	Majorants, minorants et compagnie.	146
4.1	Majorants, minorants.	146
4.2	Plus grand et plus petit éléments.	146
4.3	Bornes supérieure et inférieure.	147
4.4	Application aux fonctions réelles.	148
5	Relation d'ordre naturelle sur $\mathbb{N}$.	149
6	Relation d'ordre naturelle sur $\mathbb{R}$.	149
6.1	Opérations usuelles.	149
6.2	Propriété de la borne supérieure.	150
6.3	Caractère archimédien de $\mathbb{R}$ et partie entière.	151
a	Propriété d'Archimède.	151
b	Partie entière.	151
c	Densité de $\mathbb{Q}$ dans $\mathbb{R}$.	152
d	Approximations décimales.	152
6.4	Intervalles de $\mathbb{R}$.	152

Dans tout ce chapitre, E est un ensemble.

1 Relations binaires.

Définition 1.0.1.

On appelle *relation binaire* tout triplet $\mathcal{R} = (E, F, \Gamma)$ où E et F sont des ensembles et où Γ est une partie de $E \times F$. Au lieu de noter $(x, y) \in \Gamma$, on note $x\mathcal{R}y$ ce qui se lit : x est en relation avec y .

Remarque 1.0.2.

On considérera uniquement des relations binaires sur un seul ensemble E , *i.e.* avec $E = F$.

Exemple 1.0.3. • « Aimer » est une relation binaire : Brandon aime Sue Ellen mais Sue Ellen n'aime pas Brandon. On voit sur cet exemple qu'en général $x\mathcal{R}y$ n'implique pas $y\mathcal{R}x$.

- L'égalité est l'exemple le plus courant de relation binaire.
- Soit $f : \mathbb{R} \rightarrow \mathbb{R}$. On peut définir pour tous $x, y \in \mathbb{R}$, $x\mathcal{R}y$ ssi $y = f(x)$ (on a en fait défini ainsi une application via son graphe).
- Sur $\mathbb{R}$, $\leq$ et $<$ (autre exemple où $x\mathcal{R}y$ est vrai mais $y\mathcal{R}x$ est faux).
- $\subset$ est une relation binaire sur $\mathcal{P}(E)$.
- les divisibilités sur $\mathbb{N}$ et $\mathbb{Z}$.

Définition 1.0.4.

Soit $\mathcal{R}$ une relation binaire sur E . On dit que $\mathcal{R}$ est :

- (i) *réflexive* si $\forall x \in E, x\mathcal{R}x$.
- (ii) *transitive* si $\forall x, y, z \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.
- (iii) *symétrique* si $\forall x, y \in E, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- (iv) *antisymétrique* si $\forall x, y \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y$.

Exemple 1.0.5. • « Aimer » ne vérifie aucune de ces propriétés.

- L'égalité est réflexive, symétrique, antisymétrique et transitive.

- Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ et $x\mathcal{R}y$ ssi $y = f(x)$: les propriétés de cette relation dépendent du choix de f mais ne vérifie aucune de ces propriétés en général (considérer par exemple $f : x \mapsto x + 1$ et $f : x \mapsto x$).
- $\leq$ est réflexive, transitive et antisymétrique sur $\mathbb{R}$.
- $<$ est transitive et antisymétrique sur $\mathbb{R}$.
- $\subset$ est réflexive, transitive et antisymétrique sur $\mathcal{P}(E)$.
- la divisibilité sur $\mathbb{N}$ est réflexive, transitive et antisymétrique.
- la divisibilité sur $\mathbb{Z}$ est réflexive et transitive mais pas antisymétrique.

Démonstration. • Montrons le résultat pour $\subset$: Soient $A, B, C \in \mathcal{P}(E)$.

- On a bien entendu $A \subset A$, donc $\subset$ est réflexive.
 - On suppose $A \subset B$ et $B \subset C$. Alors $A \subset C$ et donc $\subset$ est transitive.
 - On suppose $A \subset B$ et $B \subset A$. Alors $A = B$, et $\subset$ est antisymétrique.
 - Montrons le résultat pour la divisibilité sur $\mathbb{N}$: soient $n, p, q \in \mathbb{N}$.
 - On a $n = 1 \times n$ donc $n|n$.
 - Si $n|p$ et $p|q$, alors il existe $k, \ell \in \mathbb{N}$ tels que $p = kn$ et $q = \ell p$, donc $q = (\ell k)n$ et ainsi $n|q$.
 - Si $n|p$ et $p|n$, alors il existe $k, \ell \in \mathbb{N}$ tels que $p = kn$ et $n = \ell p$, donc $n = (\ell k)n$. Si $n = 0$, alors $p = kn = 0$ donc $p = n$. Sinon, $\ell k = 1$. Mais ℓ et k sont deux entiers naturels et sont donc égaux à 1, donc $n = p$.
- Dans le cas de la divisibilité dans $\mathbb{Z}$, on aurait pour ce point $k, \ell \in \mathbb{Z}$, et donc $\ell k = 1$ serait aussi vérifié si $k = \ell = -1$, et en effet si $n = -p$ on a bien $n|p$ et $p|n$, mais $n \neq p$! □

2 Relations d'équivalence.

Définition 2.0.1.

On appelle *relation d'équivalence* toute relation binaire réflexive, transitive et symétrique.

Exemple 2.0.2.

- L'égalité sur E est l'exemple le plus classique de relation d'équivalence.
- La relation de congruence modulo n sur $\mathbb{Z}$ en est aussi une : on fixe $n \in \mathbb{Z}$ non nul, et on dit que deux entiers p et q sont *congrus modulo n* s'il existe $k \in \mathbb{Z}$ tel que $p = q + kn$, ce qui se note

$p = q[n]$ ou $p \equiv q[n]$.

- Si $x \in \mathbb{R}$, on définit sur $\mathbb{R}$ la relation d'équivalence modulo x par $a \equiv b [x]$ s'il existe $k \in \mathbb{Z}$ tel que $a - b = kx$.

Attention, cette relation n'est pas compatible avec la multiplication.

- Sur $\mathbb{R}^n$, on a la relation d'équivalence : $M \mathcal{R} N$ si $\overrightarrow{OM}$ et $\overrightarrow{ON}$ sont colinéaires. C'est le point de départ de la *géométrie projective*.

- Sur $\mathcal{M}_n(\mathbb{K})$, deux matrices M et N sont dites semblables si $\exists P \in GL_n(\mathbb{K}), M = P^{-1}NP$. Cela définit une relation d'équivalence.

- Sur $\mathcal{M}_n(\mathbb{K})$, deux matrices M et N sont dites équivalentes si $\exists (P, Q) \in GL_n(\mathbb{K})^2, M = Q^{-1}NP$. Cela définit une relation d'équivalence.

- Sur un intervalle I , et parmi les fonctions de classe $\mathcal{C}^1$ sur I , on peut considérer la relation « f et g sont deux primitives d'une même fonction », i.e. $f' = g'$. C'est une relation d'équivalence, qui donne son sens à la manipulation du symbole de primitivation générique $\int^x$.

Définition 2.0.3.

Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E . Alors, pour tout élément x de E , on appelle *classe d'équivalence* de x l'ensemble $\{y \in E \mid x \mathcal{R} y\}$, que l'on note parfois $\bar{x}$.

Proposition 2.0.4.

Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E . Soit $(x, y) \in E^2$. Alors,

1. $x \in \bar{x}$.
2. $x \mathcal{R} y \iff x \in \bar{y}$.
3. $x \mathcal{R} y \iff \bar{x} = \bar{y}$.

Démonstration.

Le premier point découle de la réflexivité. Le second découle de la définition de $\bar{y}$. Pour le troisième, il s'agit de montrer l'équivalence. Le sens direct se fait en montrant une double inclusion, qui découle de la transitivité. Le sens indirect découle du premier point et du second. $\square$

Définition 2.0.5.

Soit E un ensemble, $(A_i)_{i \in I}$ une famille de parties de E indexée par un ensemble I . On dit que $(A_i)_{i \in I}$ est une *partition* de E si les éléments de cette famille sont tous non vides, sont disjoints et si leur réunion vaut E .

Proposition 2.0.6.

1. Si $\mathcal{R}$ est une relation d'équivalence sur E , alors l'ensemble des classes d'équivalences de $\mathcal{R}$ forme une partition de E .
2. Réciproquement, si $(A_i)_{i \in I}$ est une partition de E , alors la relation binaire définie sur E par $x \mathcal{R} y$ si $\exists i \in I, (x \in A_i) \wedge (y \in A_i)$ est une relation d'équivalence.

Nous introduisons maintenant dans un but culturel l'ensemble quotient (hors programme).

Définition 2.0.7.

Si $\mathcal{R}$ est une relation d'équivalence sur E , on appelle ensemble quotient de E par $\mathcal{R}$ l'ensemble des classes d'équivalences, noté $E/\mathcal{R}$.

Exemple 2.0.8.

Si $f : E \rightarrow F$ est une application, la relation binaire sur E définie par $x \mathcal{R} y$ si $f(x) = f(y)$ est une relation d'équivalence. Quelle est alors la partition qui lui est naturellement associée ? On pourra alors se poser la question suivante : y a-t-il un moyen naturel de construire une injection $\tilde{f} : E/\mathcal{R} \rightarrow F$?

Exemple 2.0.9.

On manipule naturellement certains ensembles quotients : les vecteurs de $\mathbb{R}^n$ et les fractions, par exemple.

3 Relations d'ordre.

Définition 3.0.1.

On appelle *relation d'ordre* toute relation binaire réflexive, transitive et antisymétrique.

Remarque 3.0.2.

L'usage est de noter $\preccurlyeq$, parfois $\leq$, les relations d'ordre.

Exemple 3.0.3.

Reprendre tous les exemples précédents et repérer les relations d'ordre.

Définition 3.0.4.

Soit $\preccurlyeq$ une relation d'ordre sur E .

1. On dit que $x, y \in E$ sont des *éléments comparables* si $x \preccurlyeq y$ ou $y \preccurlyeq x$.
2. On dit que $\preccurlyeq$ est une *relation d'ordre totale* (ou que cet ordre est total) si tous les éléments de E sont comparables deux à deux. Sinon la relation est dite *partielle* (ou l'ordre est dit partiel).

Exemple 3.0.5. • On définit la relation d'ordre usuelle sur $\mathbb{N}$, notée $\leq$ par : $a \leq b$ si $\exists k \in \mathbb{N}, b = a + k$. C'est une relation d'ordre totale.

- La relation d'ordre usuelle $\leq$ sur $\mathbb{R}$ est totale : quand on choisit deux réels, il y en a toujours un des deux qui est inférieur ou égal à l'autre.
- La relation d'ordre $\subset$ sur $\mathcal{P}(E)$ est partielle (si $\text{Card } E \geq 2$) : en effet, quand on choisit deux parties de E , il n'y a aucune raison pour que l'une soit incluse dans l'autre.
- La relation de divisibilité sur $\mathbb{N}$ est une relation d'ordre partielle : quand on choisit deux entiers positifs, l'un n'est pas forcément multiple ou diviseur de l'autre.

4 Majorants, minorants et compagnie.

Dans toute cette section, $\preccurlyeq$ est une relation d'ordre sur E et A est une partie de E .

4.1 Majorants, minorants.

Définition 4.1.1. (i) On dit que A est *majorée* (resp. *minorée*) pour $\preccurlyeq$ s'il existe un élément $M \in E$ tel que pour tout $a \in A$, $a \preccurlyeq M$ (resp. $M \preccurlyeq a$) ; on dit alors que M est UN *majorant* (resp. *minorant*) de A ou que M majore (resp. minore) A .

(ii) on dit que A est *bornée* si elle est à la fois majorée et minorée.



En général, une partie majorée a plusieurs majorants, et peut même en avoir une infinité !

Exemple 4.1.2.

- $[1, 2]$ dans $\mathbb{R}$ est majoré par tout réel x tel que $2 \leq x$, et minoré par tout réel y tel que $y \leq 1$.
- $] - \infty, 2[$ est majoré mais non minoré.
- Pour la relation $\subset$, $\mathcal{P}(E)$ est minorée par $\emptyset$ et majorée par E .

Exercice 4.1.3.

On considère dans $\mathcal{P}(\mathbb{Z})$ muni de $\subset$ la partie $A = \{ [0, n] \mid n \in \mathbb{N} \}$.

Déterminer l'ensemble des minorants et celui des majorants de A .

4.2 Plus grand et plus petit éléments.

Définition 4.2.1.

On dit que $x \in E$ est un *plus grand élément* ou *maximum* (resp. *plus petit élément* ou *minimum*) de A si x est un majorant (resp. minorant de A) ET $x \in A$.

Exemple 4.2.2.

- $I = [-1, 2[$ a un plus petit élément, mais pas de plus grand élément. En effet, -1 est un minorant de I et $-1 \in I$. Mais supposons par l'absurde que I ait un plus grand élément M . Alors $M \in I$, donc $M < 2$. Ainsi il existe $a \in]M, 2[$, donc $a \in I$ et $M < a$, ce qui est en contradiction avec le fait que M majore I .
- $\mathbb{R}$ n'est ni majoré ni minoré, donc n'a ni plus grand ni plus petit élément.

Théorème 4.2.3.

Si A a un plus grand élément, ce dernier est unique. Il en est de même pour un petit élément, s'il existe. Dans le cas d'existence, le plus grand élément de A est alors noté $\max A$, et le plus petit élément de A est noté $\min A$.

Démonstration.

On suppose que A a deux maxima : ils sont alors réciproquement plus grand l'un que l'autre, et par antisymétrie ils sont égaux. $\square$

Exemple 4.2.4.

Dans $\mathbb{N}$ muni de la relation d'ordre $|$: 0 est le plus grand élément et 1 est le plus petit. En effet tout entier divise 0, et 1 divise tout entier.

Exercice 4.2.5.

En reprenant les notations de l'exercice 4.1.3, déterminer si A possède un maximum, ainsi qu'un minimum.

4.3 Bornes supérieure et inférieure.

Définition 4.3.1. (i) S'il existe, le plus petit élément de l'ensemble des majorants de A est appelé la borne supérieure de A et noté $\sup A$.

(ii) S'il existe, le plus grand élément de l'ensemble des minorants de A est appelé la borne inférieure de A et noté $\inf A$.



Il y a une grosse différence entre $\max$ et $\sup$: le premier doit appartenir à A , pas le deuxième.

Exemple 4.3.2.

$I = [-1, 2[$ a une borne inférieure et une borne supérieure : l'ensemble des minorants de I est $] -\infty, -1]$, qui admet -1 comme maximum, et donc -1 est la borne inférieure de I . De même $[2, +\infty[$ est l'ensemble des majorants de I , et il admet 2 comme minimum, donc 2 est la borne supérieure de I .

Exercice 4.3.3.

En reprenant les notations de l'exercice 4.1.3, déterminer si A possède une borne supérieure, ainsi qu'une borne inférieure.

Exercice 4.3.4.

On considère la relation d'ordre $|$ sur $\mathbb{N}$. Déterminer les ensembles des minorants et majorants des parties suivantes, puis dire si ces parties sont majorées, minorées, admettent un maximum, un minimum, une borne supérieure ou inférieure (que l'on déterminera le cas échéant).

1. $A = \{1\}$
2. $B = \{2, 3\}$
3. $C = \{2p + 1 \mid p \in \mathbb{N}\}$
4. $D = \{2p \mid p \in \mathbb{N}\}$

Proposition 4.3.5. 1. Si A admet une borne supérieure, alors $\sup A \preccurlyeq M \Leftrightarrow \forall x \in A \quad x \preccurlyeq M$.

2. Si E est totalement ordonné, alors $(M = \sup A)$ si et seulement si M vérifie deux points :

- (i) M majore A
- (ii) si $x \in E$ et $x \prec M$, alors il existe $a \in A$ tel que $x \prec a \preccurlyeq M$.

Remarque 4.3.6.

L'idée est la suivante : si on peut « caser » un élément de E entre M et A , ce qui revient en fait à trouver un majorant de A plus petit que M , alors M n'est pas la borne supérieure de A : la borne supérieure « colle » à A .

Démonstration. 1. $\Rightarrow$: car $\sup A$ est un majorant de A .

$\Leftarrow$: car $\sup A$ est le plus petit majorant de A .

2. Remarquons qu'ici, $x \prec y$ signifie $x \preccurlyeq y$ et $x \neq y$.

Par définition d'une borne supérieure, il suffit pour montrer cette équivalence de démontrer que le point (ii) équivaut à : M est le plus petit majorant de A . Supposons que nous avons (ii). Soit alors N un majorant de A , tel que $N \prec M$. Alors avec (ii), il existe $a \in A$ tel que $N \prec a$. Ceci est absurde car N majore A , donc $M \preccurlyeq N$: M est bien inférieur à tout majorant de A .

Supposons réciproquement que M est le plus petit majorant de A . Soit $x \in E$ tel que $x \prec M$. Alors, x étant plus petit que M , x n'est pas un majorant de A . En prenant la négation de la phrase « x majore

A », nous obtenons : il existe $a \in A$ tel que $x \prec a$.
Mais si de plus M majore A , alors $a \preccurlyeq M$ et nous
avons fini.
Ce dernier raisonnement sera très souvent utilisé dans
les exercices. $\square$

Théorème 4.3.7.

Si A possède un maximum (resp. minimum), alors
 A a une borne supérieure (resp. inférieure) et
cette borne est justement le maximum (resp. le
minimum) de A : $\sup A = \max A$ (resp. $\inf A = \min A$).

Démonstration.

On ne donne la démonstration que pour la borne supérieure
(c'est la même pour la borne inférieure) : soit $\mathcal{E}$ l'ensemble
des majorants de A . Il faut montrer que $\mathcal{E}$ a un plus petit
élément. Par définition $\max A$ est un majorant de A , donc
 $\max A \in \mathcal{E}$. Soit $M \in \mathcal{E}$. M est plus grand que tout
élément de A , or $\max A$ appartient à A donc $\max A \preccurlyeq M$,
et ce pour tout M de $\mathcal{E}$: $\max A$ est donc un minorant
de $\mathcal{E}$. De ces deux points on tire $\max A = \min \mathcal{E}$, et donc
 $\max A = \sup A$. $\square$

4.4 Application aux fonctions réelles.

Définition 4.4.1.

Soient A une partie de $\mathbb{R}$ et $f : A \rightarrow \mathbb{R}$.

- (i) On dit que f est *majorée* (resp. *minorée*)
sur A si $f(A)$ l'est pour la relation naturelle
sur $\mathbb{R}$, i.e. : $\exists M \in \mathbb{R} \quad \forall x \in A \quad f(x) \leq M$
(resp. $M \leq f(x)$). Dans ce cas on dit que M
est un *majorant* (resp. *minorant*) de f , ou
que M *majore* (resp. *minore*) f .
- (ii) On dit que f est *bornée* si elle est majorée
et minorée. Ceci est équivalent à : $|f|$ est
majorée.



Un majorant ou minorant ne doit pas
dépendre de la variable de la fonction ! Ainsi sur
 $\mathbb{R}_+$, $x \mapsto x$ n'est pas un majorant de $\sin$, bien
que $\forall x \in \mathbb{R}_+, \sin x \leq x$. Un majorant est une
CONSTANTE.

Définition 4.4.2.

Si l'ensemble $f(A)$ a un maximum (resp. un
minimum), alors ce dernier est appelé le *maxi-*
mum (resp. *minimum*) de f sur A , et noté $\max_A f$
ou $\max_{x \in A} f(x)$ (resp. $\min_A f$ ou $\min_{x \in A} f(x)$). Ainsi
 $\max_A f(A) = \max_A f$. Un maximum ou minimum
d'une fonction est donc un majorant ou minorant
ATTEINT.
On appelle *extremum* de f tout minimum ou
maximum de f .



Les extrema sont uniques mais peuvent
être atteints plusieurs fois. Considérer pas
exemple les fonctions continues périodiques
comme $\sin$ ou $\cos$.

Exemple 4.4.3.

- $x \mapsto x^2$ admet un minimum mais pas de majo-
rant sur $\mathbb{R}$.
- Arctan est majorée et minorée sur $\mathbb{R}$, mais n'ad-
met ni minimum ni maximum.

Définition 4.4.4.

Si l'ensemble $f(A)$ admet une borne supérieure
(resp. une borne inférieure), alors cette dernière est
appelée la *borne supérieure* (resp. *inférieure*) de
 f sur A . On la note $\sup_A f$ ou $\sup_{x \in A} f(x)$ (resp. $\inf_A f$
ou $\inf_{x \in A} f(x)$). Ainsi $\sup_A f(A) = \sup_A f$.

Théorème 4.4.5.

Si f admet un maximum (resp. un minimum) sur
 A , alors f admet également une borne supérieure
(resp. une borne inférieure) sur A , et $\sup_A f =$
 $\max_A f$ (resp. $\inf_A f = \min_A f$).

Exercice 4.4.6.

Soit

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \max(0, \text{Arctan}(x)) \end{aligned}$$

Déterminer les ensembles de majorants et de minorants de f , puis si f admet un maximum, un minimum, une borne supérieure ou inférieure (que l'on déterminera le cas échéant). Tracer l'allure de la fonction

5 Relation d'ordre naturelle sur $\mathbb{N}$.

La relation naturelle est la relation usuelle $\leq$.

Théorème 5.0.1.

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

On donne ici deux démonstrations de cette propriété. On remarquera que l'on utilise ici des récurrences et que l'on a montré le principe de récurrence en utilisant cette propriété : cette dernière est donc équivalente au principe de récurrence.

Démonstration.

Soit $A \subset \mathbb{N}$, tel que $A \neq \emptyset$, et soit $a_0 \in A$. On suppose que A n'a pas de plus petit élément. Puisque $a_0 \in A$, a_0 ne peut pas être un minorant de A , sinon ce serait un minimum. Donc il existe $a_1 < a_0$ dans A . Mais de même, a_1 ne peut pas être un minorant, donc il existe $a_2 < a_1$ dans A . Par récurrence, on construit une suite d'éléments de A (a_n) telle que pour tout n , $a_{n+1} < a_n$, ou encore $a_{n+1} \leq a_n - 1$, donc à nouveau par récurrence on a :

$$\forall n \in \mathbb{N} \quad a_n \leq a_0 - n$$

Cette proposition est en particulier vraie pour l'entier $a_0 + 1$, c'est-à-dire : $a_{a_0+1} \leq a_0 - a_0 - 1$. Mais ceci est absurde car $a_{a_0+1} \in \mathbb{N}$. $\square$

Démonstration.

Notons, pour $n \in \mathbb{N}$, $P(n)$ l'assertion «toute partie de $\mathbb{N}$ contenant l'entier n possède un plus petit élément». Montrons $\forall n \in \mathbb{N} \quad P(n)$ par récurrence forte.

- Toute partie de $\mathbb{N}$ contenant l'entier 0 possède 0 pour plus petit élément. Donc on a clairement $P(0)$.
- Soit $n \in \mathbb{N}$. Supposons que pour tout $k \leq n$, on a $P(k)$ et montrons $P(n+1)$.

Soit A une partie de $\mathbb{N}$ contenant l'entier $n+1$. Alors ou bien A contient un entier k strictement inférieur à $n+1$, ou bien elle n'en contient pas.

- Dans le premier cas, on sait qu'on a $P(k)$, donc A admet un plus petit élément.
- Dans le second, cela signifie que $n+1$ est le plus petit élément de A . A admet donc un plus petit élément.

On a donc $P(n+1)$.

Donc P est héréditaire.

On a donc

$$\forall n \in \mathbb{N} \quad P(n)$$

On en déduit le résultat :

Soit A une partie non vide de $\mathbb{N}$. Alors A possède un élément n , or on a $P(n)$, donc A possède un plus petit élément n . $\square$

Corollaire 5.0.2.

Toute partie non vide minorée (resp majorée) de $\mathbb{Z}$ possède un plus petit (resp. grand) élément.

Démonstration.

Soit $A \subset \mathbb{Z}$ avec $A \neq \emptyset$ et m un minorant de A (resp. M un majorant de A). On pose $B = \{n - m \mid n \in A\}$ (resp. $B = \{M - n \mid n \in A\}$).

Alors B est une partie non vide de $\mathbb{N}$.

Donc B possède un plus petit (resp. plus grand) élément. On en déduit le résultat. $\square$

Exercice 5.0.3.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice nilpotente (*i.e.* il existe $p \in \mathbb{N}$ vérifiant $A^p = 0$).

Montrer qu'il existe $n_0 \in \mathbb{N}^*$ tel que $A^{n_0-1} \neq 0$ et $A^{n_0} = 0$.

Cet entier n_0 s'appelle *l'indice de nilpotence* de A .

6 Relation d'ordre naturelle sur $\mathbb{R}$.

On admettra l'existence de $\mathbb{R}$ et les propriétés usuelles sur $\mathbb{R}$.

6.1 Opérations usuelles.

Théorème 6.1.1 (Compatibilité de la relation d'ordre avec l'addition et la multiplication).

On a, $\forall x, y, z \in \mathbb{R}$,

$$x \leq y \Rightarrow x + z \leq y + z$$

et

$$(x \leq y \text{ et } 0 \leq z) \Rightarrow xz \leq yz.$$

On en déduit les règles usuelles de manipulation des inégalités, pour tous $x, y, x', y' \in \mathbb{R}$:

$$(x \leq y \text{ et } x' \leq y') \Rightarrow x + x' \leq y + y'$$

$$(0 \leq x \leq y \text{ et } 0 \leq x' \leq y') \Rightarrow xx' \leq yy'$$

$$x \leq y \Rightarrow -y \leq -x$$

$$0 < x \leq y \Rightarrow 0 < \frac{1}{y} \leq \frac{1}{x}.$$

Tout cela reste vrai avec des inégalités strictes.

Remarque 6.1.2.

Les résolutions d'inéquations sur $\mathbb{R}$ se résolvent la plupart du temps par factorisation, puis par l'établissement d'un tableau de signe. Lors d'une multiplication ou d'une division, on fera particulièrement attention à mener une disjonction de cas sur le signe de la quantité manipulée.

Exercice 6.1.3.

Résoudre les inéquations suivantes.

1. $\frac{x-1}{x+3} > 2$
2. $\frac{\sqrt{x-1}}{\sqrt{10-x}} < 1$
3. $\ln(x) \geq \frac{1}{2}$
4. $-1 < \frac{1-x}{1+x} < 1$

Définition 6.1.4.

On appelle droite achevée l'ensemble $\bar{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, où $-\infty$ et $+\infty$ sont deux éléments distincts n'appartenant pas à $\mathbb{R}$. De plus, on prolonge l'ordre sur $\mathbb{R}$, l'addition et la multiplication de façon à avoir les propriétés suivantes :

- (i) Prolongement de l'ordre : $\forall x \in \mathbb{R} \quad -\infty < x < +\infty$.
- (ii) Prolongement de l'addition : pour tout $x \in \mathbb{R}$, on a $x + +\infty = +\infty$, $x + (-\infty) = -\infty$, $+\infty + +\infty = +\infty$, $-\infty + (-\infty) = -\infty$.
- (iii) Prolongement de l'opposé : $-(+\infty) = -\infty$, $-(-\infty) = +\infty$.
- (iv) Prolongement de la multiplication : pour tout $x \in \bar{\mathbb{R}} \setminus \{0\}$, $+\infty \times x = +\infty$ si $x > 0$, $+\infty \times x = -\infty$ si $x < 0$ et $(-\infty) \times x = -(+\infty \times x)$.
- (v) Prolongement de l'inverse : $\frac{1}{+\infty} = 0$ et $\frac{1}{-\infty} = 0$.



Il y a des formes indéterminées : $+$ et $\times$ ne sont pas des lois de composition interne sur $\bar{\mathbb{R}}$.

6.2 Propriété de la borne supérieure.

Cette propriété fait partie des propriétés inhérentes à $\mathbb{R}$ de par sa construction.

Théorème 6.2.1.

Toute partie non vide majorée (resp. minorée) de $\mathbb{R}$ admet une borne supérieure (resp. inférieure) dans $\mathbb{R}$.

Remarque 6.2.2.

C'est un résultat d'existence : il assure l'existence d'un objet sans donner sa valeur. Ce théorème est tout à fait inutile pour calculer une borne sup. Au mieux, il permet de montrer que la borne sup d'un ensemble existe, et donc on peut en parler (ce qui est interdit sinon).

Il est cependant fondamental dans un grand nombre de résultats théoriques qui servent tous les jours : TVI, théorèmes de la limite monotone, de Rolle, TAF, construction de l'intégrale ...

Corollaire 6.2.3.

Toute partie de $\bar{\mathbb{R}}$ admet une borne supérieure (resp. inférieure) dans $\bar{\mathbb{R}}$.

Démonstration.

Soit A une partie de $\bar{\mathbb{R}}$. Et posons $A' = A \cap \mathbb{R}$.

- Si $+\infty \in A$, alors A admet $+\infty$ pour maximum.
- Dans le cas contraire, on a les possibilités suivantes :
 - Si A' est vide, alors A admet $-\infty$ pour borne supérieure.
 - Si A' est non vide alors on a deux possibilités :
 - Si A' est non majorée dans $\mathbb{R}$, alors A admet $+\infty$ comme borne supérieure.
 - Si A' est majorée dans $\mathbb{R}$, alors d'après la propriété de la borne supérieure, elle admet une borne supérieure M dans $\mathbb{R}$. Cette borne supérieure est aussi une borne supérieure de A dans $\bar{\mathbb{R}}$.

□

Remarque 6.2.4.

Dans le cas d'une fonction réelle (définie sur un ensemble non vide), l'image de cette fonction est forcément non vide.

Ainsi, une fonction réelle majorée admet une borne supérieure et une fonction réelle minorée admet une borne inférieure.

On a aussi une caractérisation fort utile des bornes supérieures et inférieures.

Proposition 6.2.5. 1. Soit A une partie non vide, majorée de $\mathbb{R}$. Alors, $a \in \mathbb{R}$ est la borne supérieure de A si et seulement si $\forall x \in A, x \leq a$ et $\forall \varepsilon > 0, \exists x \in A \cap]a - \varepsilon, a]$.

2. Soit A une partie non vide, minorée de $\mathbb{R}$. Alors, $a \in \mathbb{R}$ est la borne inférieure de A si et seulement si $\forall x \in A, x \geq a$ et $\forall \varepsilon > 0, \exists x \in A \cap [a, a + \varepsilon[$.

Démonstration.

On ne démontre que la partie concernant les bornes supérieures, l'autre en découle immédiatement.

Supposons d'abord que a est la borne supérieure de A . Alors, a majore A et donc $\forall x \in A, x \leq a$. Soit $\varepsilon > 0$, $a - \varepsilon < a$ et $a - \varepsilon$ n'est donc pas un majorant de A . Il existe donc $x \in A$ vérifiant $a - \varepsilon < x$ et, comme a majore A , on a $x \leq a$, ce qui permet de conclure pour cette implication.

Réciproquement, si a vérifie : $\forall x \in A, x \leq a$ et $\forall \varepsilon > 0, \exists x \in A \cap]a - \varepsilon, a]$. Ainsi, a est bien un majorant de A . Montrons que c'en est le plus petit. Sinon, il existerait $b \in \mathbb{R}$ majorant A , avec $b < a$. Alors, $]b, a] \cap A = \emptyset$, ce qui contredit l'hypothèse. a est donc la borne supérieure de A . $\square$

Exercice 6.2.6.

Soit (u_n) une suite réelle croissante et majorée. Montrer que $\ell = \sup \{ u_n \mid n \in \mathbb{N} \}$ existe.

En utilisant la définition de limite vue en terminale, montrer que $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$.

Est-ce toujours le cas si (u_n) n'est pas bornée ?

Remarque 6.2.7 (passage à la borne supérieure). Soit A une partie non vide de $\mathbb{R}$, soit $M \in \mathbb{R}$ vérifiant

$$\forall a \in A, a \leq M.$$

Alors, M est un majorant de A , donc $\sup(A) \leq M$.

Cet enchaînement est souvent couvert par la locution « par passage à la borne supérieure ».

6.3 Caractère archimédien de $\mathbb{R}$ et partie entière.

a Propriété d'Archimède.

Proposition 6.3.1.

Soient deux réels x et y tels que $x > 0$. Alors il existe un entier N tel que $Nx \geq y$.

• Slogan : « quelle que soit la taille de nos enjambées, on peut aller au bout du monde si on fait assez de pas ».

Démonstration.

Soit $A = \{nx \mid n \in \mathbb{N}\}$. On souhaite montrer que A n'est pas majoré et l'on raisonne par l'absurde. Si A est majoré, comme $0 = 0x \in A$, A est aussi non vide et par la propriété de la borne supérieure, A admet une borne supérieure, que nous noterons α . Remarquons que $\alpha - x < \alpha$, donc $\alpha - x$ ne majore pas A , donc il existe $n \in \mathbb{N}$ tel que $\alpha - x < nx$. On a alors $\alpha < (n+1)x$, ce qui contredit le fait que α majore A . Ainsi, A n'est pas majoré. $\square$

Exercice 6.3.2.

En revenant aux définitions vues en terminale, montrer que $\frac{1}{n} \xrightarrow[n \rightarrow +\infty]{} 0$.

b Partie entière.

Définition 6.3.3.

Soit $x \in \mathbb{R}$, il existe un unique entier, noté $\lfloor x \rfloor$ (parfois $E(x)$ ou $\mathbb{E}(x)$) et que l'on appelle *partie entière* de x , vérifiant : $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Démonstration.

Soit $A = \{k \in \mathbb{Z} \mid k \leq x\}$.

La propriété d'Archimède implique qu'il existe $k \in \mathbb{N}$ tel que $k \times 1 \geq -x$, donc $-k \leq x$, donc $-k \in A$. Ainsi, A est non vide.

Une seconde fois, la propriété d'Archimède implique qu'il existe $\ell \in \mathbb{N}$ tel que $\ell \times 1 \geq x$. Ainsi, si $k \in A$, alors $k \leq x \leq \ell$, donc A est majorée par ℓ .

Ainsi, A est une partie non vide et majorée de $\mathbb{Z}$, donc A possède un plus grand élément, noté n . On a alors $n \leq x$ et comme $n+1 > n$, $n+1 \notin A$ donc $n+1 > x$, d'où l'existence.

Soit N un entier vérifiant $N \leq x < N+1$. Alors $N \in A$. De plus, si $k \in A$, alors $k \leq x < N+1$ donc $k < N+1$ donc $k \leq N$. N est donc bien le plus grand élément de A , d'où l'unicité. $\square$

Remarque 6.3.4.

On vient de montrer que $\lfloor x \rfloor$ est le plus grand entier relatif inférieur ou égal à x . On peut très bien définir $\lfloor x \rfloor$ de cette manière, et voir la définition 6.3.3 comme une caractérisation de $\lfloor x \rfloor$.

Remarque 6.3.5.

Ce résultat permet de montrer que si deux réels x et y vérifient $y - x > 1$, il existe un entier n tel que $x < n < y$: il suffit de prendre $n = \lfloor x \rfloor + 1$. On a alors $x < n$ et aussi $n \leq x + 1 < x + (y - x) = y$.



Ne pas confondre la partie entière avec la troncature. Ainsi $\lfloor -3, 2 \rfloor = -4$ et non -3 !

c Densité de $\mathbb{Q}$ dans $\mathbb{R}$.**Définition 6.3.6.**

Une partie A de $\mathbb{R}$ est *dense* dans $\mathbb{R}$ si pour tout $x, y \in \mathbb{R}$ vérifiant $x < y$, il existe $a \in A$ vérifiant $x < a < y$.

Théorème 6.3.7.

$\mathbb{Q}$ est dense dans $\mathbb{R}$.

Démonstration.

Soit x et y deux réels. D'après la propriété d'Archimède, on peut trouver un entier naturel non nul r tel que $r(y - x) > 1$. D'après la remarque précédente, il existe un entier $p \in \mathbb{Z}$ tel que $rx < p < ry$. En posant $q = p/r$ on a le résultat. $\square$

Corollaire 6.3.8.

$\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$.

Démonstration.

Soit x et y deux réels. En vertu du théorème précédent, il existe un rationnel r **non nul** entre $x\sqrt{2}$ et $y\sqrt{2}$. En effet, si $0 \leq x < y$, on a $r > x\sqrt{2}$ donc $r \neq 0$, si $x < y \leq 0$, même raisonnement, et si $x < 0 < y$, on applique le théorème précédent à 0 et y par exemple pour obtenir r . Il suffit alors de prendre $q = \frac{r}{\sqrt{2}}$. q est forcément irrationnel, sinon $\sqrt{2}$ serait rationnel. $\square$

d Approximations décimales.**Définition 6.3.9.**

Soit x un réel et ε un réel strictement positif. On appelle *valeur approchée de x à la précision ε* tout réel y tel que $|x - y| \leq \varepsilon$. Si $y \leq x$ on dit que y est une valeur approchée *par défaut*, si $y \geq x$, on dit que y est une valeur approchée *par excès*.

- Souvent on cherche des valeurs approchées qui soient des décimaux.

Théorème 6.3.10.

Soit $a \in \mathbb{R}$. Pour tout entier n on note $a_n = \frac{\lfloor 10^n a \rfloor}{10^n}$ et $a'_n = \frac{\lfloor 10^n a \rfloor + 1}{10^n}$. Alors a_n et a'_n sont respectivement des valeurs approchées par défaut et excès de a à 10^{-n} près, qui de plus sont des décimaux.

Démonstration.

Évident par propriété de la partie entière. $\square$

Exercice 6.3.11.

Calculer une approximation décimale de $1/7$ à 10^{-5} près.

Ce dernier résultat a pour corollaire le résultat fondamental suivant :

Corollaire 6.3.12.

Tout réel est limite d'une suite de rationnels.

Exercice 6.3.13.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction continue vérifiant $\forall q \in \mathbb{Q}, f(q) = q$.

Quelle est cette fonction f ?

6.4 Intervalles de $\mathbb{R}$.

Il existe neuf types d'intervalles dans $\mathbb{R}$ (avec $a, b \in \mathbb{R}$) :

1. $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$;
2. $[a, b[= \{x \in \mathbb{R} \mid a \leq x < b\}$;
3. $]a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$;
4. $]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$;

5. $[a, +\infty[= \{x \in \mathbb{R} \mid a \leq x\}$;
6. $]a, +\infty[= \{x \in \mathbb{R} \mid a < x\}$;
7. $] - \infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$;
8. $] - \infty, b[= \{x \in \mathbb{R} \mid x < b\}$;
9. $] - \infty, +\infty[= \mathbb{R}$.

Les intervalles de types 1 à 4 sont dits *bornés*. Ceux de types 1, 5, 7 et 9 sont dits *fermés*. Ceux de types 4, 6 et 8 et 9 sont dits *ouverts*. Ceux de type 2 et 3 sont dits *semi-ouverts* ou *semi-fermés*. Seuls les intervalles de type 1 sont à la fois fermés et bornés : on dit que ce sont des *segments*.

Un intervalle peut être *vide* ou *réduit à un point* (dans le cas 1 si $a = b$). Un intervalle qui n'est ni vide ni réduit à un point est dit *non trivial*.

Énoncer tous ces intervalles est fastidieux : on préfère une définition unifiée d'intervalle qui les définit tous d'un coup :

- Si I n'est pas minoré mais majoré : idem avec $] - \infty, b[$.
- Si I n'est ni majoré ni minoré, alors $I = \mathbb{R}$.

□

Théorème 6.4.1.

Soit I une partie de $\mathbb{R}$. Alors les deux propositions suivantes sont équivalentes :

- (i) I est un intervalle de $\mathbb{R}$;
- (ii) Pour tous $u, v \in I$ et pour tout $t \in \mathbb{R}$, on a :
 $u \leq t \leq v \Rightarrow t \in I$.

Démonstration.

C'est trivial si $I = \emptyset$ (on a alors (ii) et (i) car $I = [0, -1]$).

(i) $\Rightarrow$ (ii) Facile et connu.

(ii) $\Rightarrow$ (i) On distingue plusieurs cas :

- Supposons d'abord que I majoré et minoré. On pose $a = \inf I$ et $b = \sup I$. Alors pour tout $x \in I$, on a $x \leq b$ et $x \geq a$, donc $x \in [a, b]$, et donc $I \subset [a, b]$ (1).
- Si $a = b$, alors $I = \{a\} = [a, a]$ (car I non vide).
- Si $a < b$, alors soit $x \in]a, b[$. Par définition de la borne inf il existe $u \in I$ tel que $a \leq u < x$. De même il existe $v \in I$ tel que $x < v \leq b$. Alors $x \in [u, v]$ et donc $x \in I$. Donc $]a, b[\subset I$ (2).
Ainsi on a la chaîne d'inégalité : $]a, b[\subset I \subset [a, b]$, donc I est de de l'un des types précédents. On détermine précisément lequel en regardant juste si a et b appartiennent ou pas à I .
- Si I n'est pas majoré mais est minoré, alors I n'a pas de sup, donc $I \subset [a, +\infty[$, et comme toute à l'heure, $]a, +\infty[\subset I$. On finit comme précédemment.

Chapitre XI

Entiers relatifs et arithmétique de $\mathbb{Z}$

Sommaire

1	Divisibilité.	156
1.1	Définition.	156
1.2	Division euclidienne.	156
2	PGCD, PPCM.	157
2.1	PGCD de deux entiers.	157
2.2	PGCD d'une famille finie d'entiers. . .	160
2.3	Nombres premiers entre eux.	161
2.4	PPCM.	162
3	Nombres premiers.	163

Dans tout ce chapitre, a, b, c, d, m, n, p, q et r sont des entiers relatifs, sauf mention contraire.

1 Divisibilité.

1.1 Définition.

Définition 1.1.1.

On dit que n *divise* m , que n *est un diviseur de* m ou que m *est un multiple de* n et on note $n|m$ si et seulement s'il existe $k \in \mathbb{Z}$ vérifiant $m = kn$.

Proposition 1.1.2. 1. La relation $|$ est réflexive, transitive, mais pas symétrique (sur $\mathbb{Z}$ comme sur $\mathbb{N}$). Elle n'est pas antisymétrique sur $\mathbb{Z}$ mais l'est sur $\mathbb{N}$: plus précisément on a sur $\mathbb{Z}$:

$$a|b \text{ et } b|a \iff |a| = |b| \iff a = \pm b$$

2. Si a divise b et c , il divise toute combinaison linéaire à coefficients entiers de b et c :

$$a|b \text{ et } a|c \Rightarrow a|bn + cm$$

3. La relation $|$ est compatible avec le produit :

$$a|b \text{ et } c|d \Rightarrow ac|bd$$

En particulier, pour tout $k \in \mathbb{N}$, $a|b$ implique $a^k|b^k$;

4. Si $c \neq 0$, $a|b \Leftrightarrow ac|bc$.

Démonstration. 1. on ne montre que la dernière partie (le reste a déjà été fait dans le chapitre VIII). Soient $a, b \in \mathbb{Z}$ tels que $a|b$ et $b|a$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $b = a\ell$, donc $b = bkl$. Si $b = 0$, alors $a = 0$ également, car $b|a$. Si $b \neq 0$, alors $k\ell = 1$, et donc $k \neq 0$, $\ell \neq 0$, et $|k| \leq 1$, ainsi que $|\ell| \leq 1$. Par conséquent $k = \ell = 1$ ou $k = \ell = -1$, et donc $a = b$ ou $a = -b$.

2. Élémentaire.
3. Élémentaire.
4. Élémentaire.

□

Remarque 1.1.3.

Pour tout $n \in \mathbb{Z}$, on a $n | 0$, $1 | n$ et, si $0 | n$, alors $n = 0$.

Remarque 1.1.4.

Pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, si $a | b$, alors $|a| \leq |b|$.

Exercice 1.1.5.

Montrer que si $a \in \mathbb{Z}$ vérifie $a|1$, alors $a = \pm 1$.

Définition 1.1.6.

On dit que a *est congru à* b *modulo* n et on note $a \equiv b \pmod{n}$ (voire $a \equiv b \pmod{n}$) si et seulement si n divise $a - b$:

$$a \equiv b \pmod{n} \iff n|a - b.$$

Remarque 1.1.7.

Pour tout entier n , la relation de congruence modulo n est une relation d'équivalence.

Proposition 1.1.8.

La relation de congruence modulo n est compatible avec l'addition et la multiplication : si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv b + d \pmod{n}$ et $ac \equiv bd \pmod{n}$.

Démonstration.

On sait qu'il existe $(k, \ell) \in \mathbb{Z}^2$ vérifiant $a = b + nk$ et $c = d + n\ell$. On a alors $a + c = b + d + n(k + \ell)$, donc $a + c \equiv b + d \pmod{n}$, et $ac = bd + n(b\ell + dk + nk\ell)$, donc $ac \equiv bd \pmod{n}$. □

Remarque 1.1.9.

Attention, ce n'est pas le cas de la relation usuelle de congruence modulo 2π . Ainsi, $2\pi \equiv 0 \pmod{2\pi}$ mais $4\pi^2 \not\equiv 0 \pmod{2\pi}$.

Remarque 1.1.10.

On a $n|a$ si et seulement si $a \equiv 0 \pmod{n}$.

Exercice 1.1.11.

Retrouver les critères de divisibilité énoncés au collège.

Exercice 1.1.12.

Soit $a \in \mathbb{Z}$. Montrer que a est pair si et seulement si a^2 est pair.

1.2 Division euclidienne.

Théorème 1.2.1.

Soient $a \in \mathbb{Z}$, et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leq r < b$. q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b . b est appelé le diviseur et a le dividende de cette division.

Démonstration.

On montre l'existence puis l'unicité.

Existence : On note $A = \{k \in \mathbb{Z} \mid kb \leq a\}$. Alors :

- A est non vide car si $a \geq 0$, $0 \in A$, et si $a < 0$ on a $a \in A$ car $b \geq 1$.
- De plus A est majoré, par 0 si $a \leq 0$ et par a si $a > 0$.

A a donc un plus grand élément noté q . Alors par construction $qb \leq a < (q+1)b$, d'où le résultat en posant $r = a - qb$.

Unicité : Soit (q, r) et (q', r') deux couples vérifiant les conditions considérées.

Alors $a = qb + r = q'b + r'$, donc $b(q - q') = r' - r$ et ainsi $b|q - q'| = |r - r'|$. Or on a $0 \leq r < b$ et $-b < -r' \leq 0$, donc $|r - r'| < b$, donc $|q - q'| < 1$, or $q - q'$ est un entier donc $q = q'$, donc $r = r'$. $\square$

Remarque 1.2.2.

On a donc $r \equiv a[b]$.

Exemple 1.2.3.

$$2356 = 18 \times 125 + 106.$$

Exercice 1.2.4.

Poser $360 \div 7$.

Proposition 1.2.5.

Soit $n \in \mathbb{N}^*$, alors $a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n .

Démonstration.

Si a et b ont le même reste dans la division euclidienne par n , on écrit $a = nq_1 + r$ et $b = nq_2 + r$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $0 \leq r < n$. On a donc bien $a - b = n(q_1 - q_2)$, donc $n|(a - b)$.

Réciproquement, si $a \equiv b[n]$, on écrit les divisions euclidiennes de a et b par n : $a = nq_1 + r_1$ et $b = nq_2 + r_2$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $(r_1, r_2) \in \mathbb{N}^2$ vérifiant, pour tout $i \in \{1, 2\}$, $0 \leq r_i < n$. On a alors $a - b - n(q_1 - q_2) = r_1 - r_2$, donc $n|(r_1 - r_2)$. Or, $-n < r_1 - r_2 < n$ et il existe un seul entier dans $[-n + 1, n - 1]$ divisible par n (le montrer !) : c'est 0. Ainsi, $r_1 = r_2$. $\square$

Exemple 1.2.6.

Exercice classique : calculer à la main le reste de la division euclidienne de $11^{42424244}$ par 7.

2 PGCD, PPCM.

Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est noté $a\mathbb{Z}$. C'est donc $\{ak \mid k \in \mathbb{Z}\}$. Remarquons que, si $a \neq 0$, $|a|$ est le plus petit entier strictement positif de $a\mathbb{Z}$.

On notera aussi $\mathcal{D}(a)$ l'ensemble des diviseurs de a : c'est donc $\{k \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z}, a = k\ell\}$. On remarquera que, si $a \neq 0$, $\mathcal{D}(a)$ est borné par $|a|$.

2.1 PGCD de deux entiers.

Dans cette partie, pour tout couple $(a, b) \in \mathbb{Z}^2$, on note $\mathcal{D}(a, b)$ l'ensemble des diviseurs communs à a et b . Ainsi, $\mathcal{D}(a, b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

Remarque 2.1.1.

Si $b = 0$, alors $\mathcal{D}(a, b) = \mathcal{D}(a)$.

Définition 2.1.2.

Soit a et b deux entiers avec $(a, b) \neq (0, 0)$, alors on appelle plus grand diviseur commun de a et b (pgcd de a et b) et on note $\text{PGCD}(a, b)$ ou $a \wedge b$ le plus grand élément de $\mathcal{D}(a, b)$.

Remarque 2.1.3.

L'un des deux entiers est non nul, donc $\mathcal{D}(a, b)$ est majoré par la valeur absolue de cet entier. Par ailleurs, $1 \in \mathcal{D}(a, b)$. Donc $\mathcal{D}(a, b)$ est un ensemble d'entiers non vide majoré, donc il admet un plus grand élément, ce qui justifie la définition.

Lemme 2.1.4 (Lemme d'Euclide).

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, r le reste de la division euclidienne de a par b . Alors $\mathcal{D}(a, b) = \mathcal{D}(b, r)$.

Démonstration.

Soit $d \in \mathcal{D}(a, b)$. Alors a s'écrit sous la forme $bq + r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise toute combinaison linéaire de a et b , donc divise r . Donc $\mathcal{D}(a, b) \subset \mathcal{D}(b, r)$.

Réciproquement, soit $d \in \mathcal{D}(b, r)$, alors a s'écrit sous la forme $bq + r$ or $d|b$ et $d|r$ donc $d|a$, donc $\mathcal{D}(b, r) \subset \mathcal{D}(a, b)$. $\square$

Théorème 2.1.5.

Soit $(a, b) \in \mathbb{Z}^2$ avec $(a, b) \neq (0, 0)$. Alors il existe un unique entier $d > 0$ tel que $\mathcal{D}(a, b)$ soit l'ensemble des diviseurs de d . Cet entier est $a \wedge b$.

Démonstration.

Montrons tout d'abord l'unicité sous réserve d'existence. Soit d et d' deux entiers strictement positifs tels que $\mathcal{D}(a, b)$ soit l'ensemble des diviseurs de d et soit également l'ensemble des diviseurs de d' . Alors on a $d \in \mathcal{D}(a, b)$. Or $\mathcal{D}(a, b)$ est l'ensemble des diviseurs de d' , donc $d|d'$. De même $d'|d$. Or $d > 0$ et $d' > 0$ donc $d = d'$.

L'existence repose sur un algorithme, appelé algorithme d'Euclide. En pseudo-code, il s'écrit :

```

Fonction euclide( $a, b$ ) :
# Précondition :  $a > 0$  et  $b > 0$ 
 $(R_0, R_1) \leftarrow (a, b)$ 
TantQue  $R_1 > 0$  Faire
     $R_2 \leftarrow \text{reste de } R_0 \div R_1$ 
     $(R_0, R_1) \leftarrow (R_1, R_2)$ 
FinTantQue
Renvoyer  $R_0$ 
    
```

Soit a et b deux entiers relatifs non tous les deux nuls. Il est clair que l'appel `euclide( $a, b$ )` termine. La valeur d retournée vérifie $\mathcal{D}(a, b) = \mathcal{D}(d, 0)$, $d \geq 0$ et $(d, 0) \neq (0, 0)$. Or $\mathcal{D}(d, 0)$ est l'ensemble des diviseurs de d donc $\mathcal{D}(a, b)$ est bien l'ensemble des diviseurs d'un entier $d > 0$.

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante : $r_0 = |a|$, $r_1 = |b|$ et pour tout $n \in \mathbb{N}$, si $r_{n+1} \neq 0$, alors r_{n+2} est le reste de $r_n \div r_{n+1}$ (on peut poser $r_{n+2} = 0$ sinon, ou considérer que l'on arrête la suite).

Il est clair que cette suite est à valeurs positives ou nulles. À partir d'un certain rang, cette suite est nulle, sinon r serait strictement décroissante et infini (du moins à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0, 0)$, on a $\mathcal{D}(r_n, r_{n+1}) = \mathcal{D}(a, b)$. En particulier, pour la dernière valeur non nulle r_n , on a $\mathcal{D}(r_n, 0) = \mathcal{D}(a, b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au n^{e} tour de boucle, R_0 contient la valeur de r_n , et R_1 celle de r_{n+1} . $\square$

Remarque 2.1.6. • Sur $(\mathbb{N}^*)^2$, le pgcd de deux nombres a et b est donc la borne inférieure de $\{a, b\}$ pour l'ordre $|$. C'est donc aussi le maximum de $\mathcal{D}(a, b) \cap \mathbb{N}^*$ pour l'ordre $|$ et pour l'ordre $\leq$.

- Sur $\mathbb{Z}^*$, la relation $|$ n'est pas un ordre car elle n'est pas antisymétrique : on a à la fois $1| -1$ et $-1|1$ (on dit qu'on a affaire à un préordre). L'ensemble des diviseurs de a et b a alors deux «plus grands» éléments pour la relation de divisibilité : $a \wedge b$ et $-(a \wedge b)$. On peut donc en fait considérer que a et b ont deux pgcd : $a \wedge b$ et $-(a \wedge b)$; lorsqu'on parle du pgcd, on considère alors qu'il s'agit du pgcd positif.

On peut donner la caractérisation suivante : le PGCD de deux nombres est bien le plus grand diviseur commun, au sens de la relation de divisibilité (sur $\mathbb{N}$).

Proposition 2.1.7.

Soient $a, b, d \in \mathbb{Z}$, avec $(a, b) \neq (0, 0)$. On a l'équivalence :

$$\begin{aligned}
 & (d \text{ est le PGCD de } a \text{ et } b) \\
 \Leftrightarrow & (d|a, d|b, d \geq 0 \\
 & \text{et } \forall n \in \mathbb{Z}, (n|a \text{ et } n|b) \Rightarrow n|d).
 \end{aligned}$$

Démonstration.

Le sens $\Rightarrow$ découle du théorème précédent.

Réciproquement, si $d \in \mathbb{N}$ vérifie $d|a$, $d|b$ et $\forall n \in \mathbb{N}$, $n|a$ et $n|b \Rightarrow n|d$. Alors d'après les deux premiers points $d|a \wedge b$ et d'après le dernier, $a \wedge b|d$. On conclut avec $d \geq 0$ et $a \wedge b \geq 0$. $\square$

Théorème 2.1.8 (Théorème de Bézout, première partie).

Soient $a, b \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Il existe deux entiers u, v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b .

Démonstration.

L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires de a et b . À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b .

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0a + V_0b$ et $R_1 = U_1a + V_1b$.

```

Fonction euclide_etendu( $a, b$ ) :
    # Précondition :  $a > 0$  et  $b > 0$ 
    ( $R_0, R_1$ )  $\leftarrow$  ( $a, b$ )
    ( $u_0, u_1$ )  $\leftarrow$  ( $1, 0$ )
    ( $v_0, v_1$ )  $\leftarrow$  ( $0, 1$ )
    # Invariant :  $R_0 = u_0a + v_0b$  et  $R_1 = u_1a + v_1b$ 
    TantQue  $R_1 > 0$  Faire
         $R_2 \leftarrow$  reste de  $R_0 \div R_1$ 
         $q \leftarrow$  quotient de  $R_0 \div R_1$ 
        ( $u_2, v_2$ )  $\leftarrow$  ( $u_0 - qu_1, v_0 - qv_1$ )
        ( $R_0, u_0, v_0$ )  $\leftarrow$  ( $R_1, u_1, v_1$ )
        ( $R_1, u_1, v_1$ )  $\leftarrow$  ( $R_2, u_2, v_2$ )
    FinTantQue
    Renvoyer ( $R_0, u_0, v_0$ )
    
```

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r, u et v , où r est la suite considérée précédemment, et où u et v sont construites par récurrence double comme suit.

On a $a = 1 \times a + 0 \times v$, on pose donc $u_0 = 1$ et $v_0 = 0$ et $r_0 = au_0 + bv_0$.

On a $b = 0 \times a + 1 \times v$, on pose donc $u_1 = 0$ et $v_1 = 1$ et $r_1 = au_1 + bv_1$.

En supposant (par récurrence double) qu'il existe $u_n, v_n, u_{n+1}, v_{n+1} \in \mathbb{Z}$ tels que

$$\begin{aligned} r_n &= au_n + bv_n \\ r_{n+1} &= au_{n+1} + bv_{n+1}, \end{aligned}$$

alors en notant q le quotient de $r_n \div r_{n+1}$, on a

$$\begin{aligned} r_{n+2} &= r_n - qr_{n+1} \\ &= a(u_n - qu_{n+1}) + b(v_n - qv_{n+1}). \end{aligned}$$

Avec $u_{n+2} = u_n - qu_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$, on a bien $r_{n+2} = au_{n+2} + bv_{n+2}$, et l'on peut conclure par récurrence double. $\square$



Le couple des coefficients de Bézout n'est pas unique. Par exemple on a $-1 \times 2 + 1 \times 3 = 1$ et $2 \times 2 + (-1) \times 3 = 1$.

Exercice 2.1.9.

Calculer un couple de Bézout pour 1750 et 644.

On peut alors faire la remarque suivante :

Corollaire 2.1.10.

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Alors

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid (u, v) \in \mathbb{Z}^2\} = (a \wedge b)\mathbb{Z}$$

Démonstration.

L'inclusion gauche-droite découle du fait que, a et b étant des multiples de $a \wedge b$, toute combinaison linéaire de a et b est également un multiple de $a \wedge b$.

L'inclusion droite-gauche découle du fait que $a \wedge b$ s'écrit comme combinaison linéaire à coefficients entiers de a et b (d'après le théorème de Bézout) et que tout multiple d'une combinaison linéaire de a et b à coefficients entiers est encore une combinaison linéaire à coefficients entiers. $\square$

Remarque 2.1.11.

C'est en fait une caractérisation du PGCD : pour tout $d \in \mathbb{N}$,

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \Leftrightarrow d = a \wedge b.$$

Corollaire 2.1.12.

Soient $a, b, c \in \mathbb{Z}$ avec $c \neq 0$. Alors $(ac) \wedge (bc) = |c|(a \wedge b)$.

Démonstration.

Posons $p = (ac) \wedge (bc)$ et $q = |c|(a \wedge b)$. On a $p > 0$ et $q > 0$ donc p et q sont respectivement les plus petits éléments strictement positifs de $p\mathbb{Z}$ et $q\mathbb{Z}$.

Il suffit donc de montrer $p\mathbb{Z} = q\mathbb{Z}$.

Or d'après ce qui précède, on a successivement :

$$\begin{aligned}(a \wedge b)\mathbb{Z} &= \{ au + bv \mid (u, v) \in \mathbb{Z}^2 \} \\ q\mathbb{Z} &= \{ |c|(au + bv) \mid (u, v) \in \mathbb{Z}^2 \} \\ &= \{ cau + cbv \mid (u, v) \in \mathbb{Z}^2 \} \\ &= p\mathbb{Z}\end{aligned}$$

□

Exercice 2.1.13.

Calculer le plus simplement possible $1230 \wedge 555$.

2.2 PGCD d'une famille finie d'entiers.

Les définitions et résultats de la section précédente se généralisent à une famille finie d'entiers.

Ainsi, si $a_1, \dots, a_p$ sont p entiers non tous nuls, on note $\mathcal{D}(a_1, \dots, a_p)$ l'ensemble des diviseurs communs à tous les entiers $a_1, \dots, a_p$. Cet ensemble étant non vide (il contient 1) et fini, il admet un plus grand élément, appelé *plus grand commun diviseur* des entiers $a_1, \dots, a_p$ et noté

$$\bigwedge_{i=1}^p a_i, \text{ ou } a_1 \wedge \dots \wedge a_p.$$

De plus, on remarque que $\mathcal{D}(0) = \mathbb{Z}$, donc si l'un des entiers de la famille $(a_1, \dots, a_p)$ est nul, on peut l'enlever de cette famille sans changer l'ensemble des diviseurs de ces entiers. Par exemple, $\mathcal{D}(a_1, a_2, 0, a_3) = \mathcal{D}(a_1, a_2, a_3)$. Dans la suite nous pourrions donc ne considérer que des familles d'entiers tous non nuls.

Proposition 2.2.1.

Soient $(a_1, \dots, a_p) \in (\mathbb{Z}^*)^p$ une famille d'entiers tous non nuls, avec $p \in \mathbb{N}^*$.

- (i) Soit $k \in \mathcal{D}(a_1, \dots, a_p)$, alors $k \mid a_1 \wedge \dots \wedge a_p$.
- (ii) $a_1 \wedge \dots \wedge a_p = (a_1 \wedge \dots \wedge a_{p-1}) \wedge a_p$.

Démonstration.

Démontrons les deux résultats en une récurrence, en posant pour chaque $p \in \mathbb{N}^*$:

(H_p) : pour tout $(a_1, \dots, a_p) \in (\mathbb{Z}^*)^p$, on a (i) et (ii).

Le résultat est connu pour $p = 1$ et $p = 2$.

Soit $p \in \mathbb{N}^*$ tel que (H_p) soit vraie.

Soient $a_1, \dots, a_{p+1} \in \mathbb{Z}^*$.

Notons $d = a_1 \wedge \dots \wedge a_p$, $D = a_1 \wedge \dots \wedge a_p \wedge a_{p+1}$ et $D' = d \wedge a_{p+1}$.

Par définition, D divise $a_1, \dots, a_p$: par hypothèse de

récurrence (i), D divise donc d . De plus, D divise a_{p+1} , donc $D \mid D'$.

Par définition, D' divise d et a_{p+1} , et d divise $a_1, \dots, a_p$. Par transitivité de la relation de divisibilité, D' est donc un diviseur de $a_1, \dots, a_{p+1}$. Par définition de D , on a donc $D' \leq D$: il vient donc $D = D'$.

Soit k un autre diviseur de $a_1, \dots, a_{p+1}$. En particulier, k est un diviseur de $a_1, \dots, a_p$, donc $k \mid d$. Et comme $k \mid a_{p+1}$, alors $k \mid D'$, et donc $k \mid D$: (H_{p+1}) est bien démontrée. □

Remarque 2.2.2.

La proposition précédente assure que l'on peut calculer le PGCD d'une famille $a_1, \dots, a_p$ d'entiers en plusieurs étapes : on calcule d'abord $a_1 \wedge a_2$ puis $(a_1 \wedge a_2) \wedge a_3$, et ainsi de suite. Par commutativité du PGCD, on peut aussi choisir les entiers dans un autre ordre, et tout ceci prouve l'associativité du PGCD et assure que la notation $a_1 \wedge \dots \wedge a_p$ est sans ambiguïté.

Le théorème de Bézout peut alors se généraliser par récurrence :

Théorème 2.2.3.

Soient $a_1, \dots, a_p$ des entiers tous non nuls. Alors il existe des entiers $u_1, \dots, u_p$ tels que

$$u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p.$$

Démonstration.

Montrons-le par récurrence sur p .

On sait déjà que la propriété est vraie pour $p = 2$.

Soit $p \geq 2$ tel que la propriété soit vraie, et soient $a_1, \dots, a_p, a_{p+1}$ des entiers.

Par hypothèse de récurrence, il existe des entiers $u_1, \dots, u_p$ tels que $u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p$. Mais $a_1 \wedge \dots \wedge a_p \wedge a_{p+1} = (a_1 \wedge \dots \wedge a_p) \wedge a_{p+1}$ et d'après le théorème de Bézout pour deux entiers, il existe $b, c \in \mathbb{Z}$ tels que $b(a_1 \wedge \dots \wedge a_p) + c a_{p+1} = a_1 \wedge \dots \wedge a_{p+1}$. D'où $a_1 \wedge \dots \wedge a_{p+1} = b u_1 a_1 + \dots + b u_p a_p + c a_{p+1}$, et l'hérédité est démontrée. □

Exemple 2.2.4.

Trouver trois entiers a, b, c tels que $72a + 180b + 120c = 12$.

Remarque 2.2.5.

Le corollaire 2.1.12 se généralise : soient $a_1, \dots, a_n$ une famille finie d'entiers et $c \in \mathbb{Z}^*$.

Alors $\bigwedge_{i=1}^n (c a_i) = |c| \bigwedge_{i=1}^n a_i$.

2.3 Nombres premiers entre eux.

Définition 2.3.1.

Deux entiers relatifs a et b sont dit premiers entre eux si et seulement si $(a, b) \neq (0, 0)$ et $a \wedge b = 1$.

Remarque 2.3.2.

Deux entiers a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1 , en d'autres termes si et seulement si $\mathcal{D}(a, b) \subset \{-1, 1\}$ (ce qui est équivalent à $\mathcal{D}(a, b) = \{-1, 1\}$).

Théorème 2.3.3 (Théorème de Bézout, seconde partie).

Soient $a, b \in \mathbb{Z}$. Alors, a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

Démonstration.

Le cas $(a, b) = (0, 0)$ est direct : les deux propositions sont fausses, donc équivalentes. Considérons donc $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout (première partie), on a le résultat.

Réciproquement, supposons qu'il existe deux entiers u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathcal{D}(a, b)$. On a $d|a$ et $d|b$, donc $d|(au + bv)$, donc $d|1$, donc $d = \pm 1$. Donc $\mathcal{D}(a, b) \subset \{-1, +1\}$. $\square$

Corollaire 2.3.4.

On a donc $a \wedge b = 1$ si et seulement si a est inversible modulo b , *i.e.* si et seulement s'il existe $k \in \mathbb{Z}$ vérifiant $ak = 1[b]$.

Exercice 2.3.5.

Résoudre sur $\mathbb{Z}$ l'équation

$$5x \equiv 8 [17].$$



$au + bv = 1$ implique $a \wedge b = 1$, mais $au + bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b) | d$.

Corollaire 2.3.6.

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Alors en posant $d = a \wedge b$, $a' = a/d$ et $b' = b/d$, on a

$$a' \wedge b' = 1$$

Démonstration.

On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a'u + b'v$, d'où a' et b' sont premiers entre eux. $\square$

Remarque 2.3.7.

Ce corollaire est très fréquemment utilisé.

Corollaire 2.3.8. (i) Soient a premier avec k entiers relatifs $b_1, b_2, \dots, b_k$. Alors a est premier avec $b_1 \times b_2 \times \dots \times b_k$.

(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}$, a^m et b^n sont également premiers entre eux.

Démonstration. (i) On traite le cas $k = 2$, le cas général s'en déduit immédiatement par récurrence. Il existe u_i et v_i vérifiant $au_i + b_i v_i = 1$ pour $i = 1, 2$. En multipliant ces deux relations, il vient successivement

$$1 = (au_1 + b_1 v_1)(au_2 + b_2 v_2)$$

$$1 = a^2 u_1 u_2 + au_1 b_2 v_2 + b_1 v_1 au_2 + b_1 v_1 b_2 v_2$$

$$1 = a(au_1 u_2 + u_1 b_2 v_2 + b_1 v_1 u_2) + b_1 b_2 (v_1 v_2)$$

D'où le résultat.

(ii) On applique (i) à a et $b \times b \times b \times \dots \times b$, puis (i) à b^n et $a \times a \times a \times \dots \times a$. $\square$

Remarque 2.3.9.

La réciproque de ces deux points est vraie.

Théorème 2.3.10 (Lemme de Gauss).

Soient $a, b, c \in \mathbb{Z}$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.

Ce résultat est une généralisation d'un lemme d'Euclide. On a $a \wedge b = 1$ donc 1 s'écrit comme combinaison linéaire $au + bv$ de a et b . Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire de a et bc . Or bc est un multiple de a donc c est un multiple de a .

On peut aussi le voir d'un point de vue plus algébrique : le théorème de Bézout (2^e partie) nous indique que $a \wedge b = 1$

si et seulement si b est inversible modulo a (i.e, il existe $k \in \mathbb{Z}$ tel que $kb = 1[a]$). On a alors $bc = 0[a]$, donc $kbc = c = 0[a]$. $\square$

Corollaire 2.3.11 (Forme irréductible d'un rationnel).

Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ et $p \wedge q = 1$. Ce couple est appelé la forme irréductible de r .

Démonstration.Existence C'est une conséquence directe du corollaire 4.2.4.

Unicité Soit (p, q) et (p', q') deux formes irréductibles d'un même rationnel r . Alors $p/q = p'/q'$ donc $pq' = p'q$. Donc $q|pq'$ et $p \wedge q = 1$. Donc d'après le théorème de Gauss, on a $q|q'$. De même $q'|q$. Donc $q = q'$ ou $q = -q'$. Or q et q' sont tous deux positifs, donc $q = q'$, donc $p = p'$. $\square$

Définition 2.3.12.

On dit que des entiers $a_1, \dots, a_p$ sont *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Remarque 2.3.13.

Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».

Remarque 2.3.14.

La deuxième partie du théorème de Bézout se généralise sans problème à une famille finie d'entiers : soient $a_1, \dots, a_p$ des entiers. Ces entiers sont premiers entre eux dans leur ensemble si et seulement si il existe des entiers $u_1, \dots, u_p$ tels que $u_1 a_1 + \dots + u_p a_p = 1$.

2.4 PPCM.

Définition 2.4.1.

Soit a et b deux entiers relatifs. L'ensemble de leurs multiples communs est $a\mathbb{Z} \cap b\mathbb{Z}$. Si a et b sont tous deux non nuls, alors cet ensemble possède un plus petit élément strictement positif. Celui-ci est appelé ppcm de a et b et est noté $\text{PPCM}(a, b)$ ou $a \vee b$.

Remarque 2.4.2.

$|ab|$ est un multiple commun à a et b . De plus, comme a et b sont non nuls, c'est un nombre strictement positif. L'ensemble des multiples communs de a et de b strictement positifs est donc non vide. Il est évidemment minoré (par 0), donc il admet un plus petit élément.

Théorème 2.4.3.

Soit a et b deux entiers relatifs. Alors il existe un unique $m \geq 0$ vérifiant $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Dans le cas où a et b sont non (tous) nuls, cet entier m est le ppcm de a et b et vaut $\frac{|ab|}{a \wedge b}$.

Démonstration.

Le cas où a ou b est nul est trivial : on a alors $a\mathbb{Z} \cap b\mathbb{Z} = \{0\} = 0\mathbb{Z}$. On suppose donc dans la suite de cette démonstration que a et b sont non nuls. Posons $d = a \wedge b$, $a' = a/d$ et $b' = b/d$. a' et b' sont premiers entre eux.

Posons $m = |ab/d| = |a'b'd|$. m est un multiple de a et de b , donc tout multiple de m est un multiple commun de a et b : $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

Soit alors p un multiple de a et de b . Alors p s'écrit à la fois sous la forme au et sous la forme bv . On a donc $p = au = bv$, donc $a'du = b'dv$, donc $a'u = b'v$. Donc $a'|b'v$, or $a' \wedge b' = 1$ donc $a'|v$. Donc il existe k vérifiant $v = ka'$. On a alors $p = bv = bka' = ka'b'd$, donc p est un multiple de m . Donc $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$.

On a donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. De plus, m est le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ et pour tout $m' \geq 0$ vérifiant $m'\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, m' est également le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$, donc $m' = m$. $\square$

Remarque 2.4.4. • Sur $(\mathbb{N}^*)^2$, le ppcm de deux nombres a et b est donc la borne supérieure de $\{a, b\}$ pour l'ordre $|$. C'est donc aussi le minimum de $a\mathbb{N} \cap b\mathbb{N}$ pour l'ordre $|$ et le minimum de $a\mathbb{N}^* \cap b\mathbb{N}^*$ pour l'ordre $\leq$.
• De même que pour le pgcd, sur $\mathbb{Z}^*$, l'ensemble des diviseurs de a et b a deux «plus petits» éléments pour la relation de divisibilité : $a \vee b$ et $-(a \vee b)$. On peut donc en fait considérer que a et b ont deux ppcm : $a \vee b$ et $-(a \vee b)$; lorsqu'on parle du ppcm, on considère alors qu'il s'agit du ppcm positif.

On peut donner la caractérisation suivante : le PPCM de deux nombres est bien le plus petit multiple commun à ces deux nombres, au sens de la relation de divisibilité (sur $\mathbb{N}$).

Proposition 2.4.5.

Soient $a, b \in \mathbb{Z}$ (non nuls) et $m \in \mathbb{Z}$. On a l'équivalence :

$$\begin{aligned} & (m \text{ est le PPCM de } a \text{ et } b) \\ \Leftrightarrow & (a|m, b|m, m \geq 0 \text{ et } \forall n \in \mathbb{Z}, (a|n \text{ et } b|n) \Rightarrow m|n) \end{aligned}$$

Et également (le point (ii) a d'ailleurs été démontré au cours de la démonstration du théorème 2.4.3) :

Proposition 2.4.6.

Soient $a, b, c \in \mathbb{Z}$ (non nuls). Alors :

- (i) $(ac) \vee (bc) = |c|(a \vee b)$.
- (ii) si $(a, b) \neq (0, 0)$, alors $|ab| = (a \wedge b).(a \vee b)$.

Remarque 2.4.7.

Avant de calculer un PPCM, on factorisera au maximum les nombres manipulés.

Exercice 2.4.8.

Calculer $1750 \vee 644$.

Corollaire 2.4.9.

Si $a \wedge b = 1$, alors $a \vee b = |ab|$.

Notamment, dans le cas où $a \wedge b = 1$, si $a | c$ et $b | c$, alors $ab | c$.

Remarque 2.4.10.

Là encore, si $a_1, \dots, a_n$ est une famille finie d'entiers, on peut définir le PPCM de cette famille, et démontrer des résultats similaires à ceux concernant les PGCD des familles d'entiers. En particulier, si $c \in \mathbb{Z}^*$, alors $\bigvee_{i=1}^n (ca_i) = |c| \bigvee_{i=1}^n a_i$.

3 Nombres premiers.

Définition 3.0.1.

Soit $p \in \mathbb{N}^*$. On dit que p est *premier* si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p . On dit que p est *composé* si $p \neq 1$ et p est non premier.

Exemple 3.0.2.

Le *crible d'Eratosthène* est un procédé permettant de trouver tous les nombres entiers inférieurs à un entier naturel N en se basant sur la remarque suivante : tout entier composé $n \in \mathbb{N}^*$ possède un diviseur premier inférieur ou égal à $\sqrt{n}$.

Par conséquent, les nombres premiers inférieurs ou égaux à 100 sont les entiers naturels inférieurs à 100 n'ayant aucun diviseur inférieur ou égal à 10.

Les premiers nombres premiers : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...

2 est le seul nombre premier pair.

Remarque 3.0.3.

On appelle *diviseur strict* de n tout entier naturel diviseur de n différent de n . Un nombre premier est donc un entier autre que 1 sans diviseur strict autre que 1.

Proposition 3.0.4.

Soit p et q sont deux nombres premiers distincts. Alors p et q sont premiers entre eux.

Démonstration.

Par l'absurde, supposons $p \wedge q \neq 1$. Alors $p \wedge q$ est un diviseur de p et de q autre que 1. p et q étant premiers, ce ne peut être un diviseur strict, donc $p = p \wedge q = q$. Or $p \neq q$, donc c'est absurde. $\square$

Proposition 3.0.5.

Soit $a \in \mathbb{Z}$ et p un nombre premier, si p ne divise pas a , alors a et p sont premiers entre eux.

Démonstration.

L'ensemble des diviseurs positifs de p est $\{1, p\}$, si p ne divise pas a , l'ensemble des diviseurs positifs communs à a et p est donc $\{1\}$. $\square$

Corollaire 3.0.6.

Soit p un nombre premier et $a, b \in \mathbb{Z}$. Si $p | ab$, alors $p | a$ ou $p | b$.

Démonstration.

C'est une simple application du lemme de Gauss et de la proposition précédente. $\square$

Le résultat suivant, fondamental, ainsi que la démonstration donnée, sont connus depuis Euclide.

Théorème 3.0.7.

L'ensemble des nombres premiers est infini.

Démonstration.

En effet, soient $p_1, \dots, p_n$ n nombres premiers, avec $n \geq 1$. Montrons qu'il en existe nécessairement un autre.

On considère la quantité $p_1 p_2 \dots p_n + 1$. Cette quantité est un entier strictement supérieur à 1. L'ensemble de ses diviseurs (positifs) différents de 1 est donc non vide et possède donc un plus petit élément q , strictement supérieur à 1. Or, q ne peut posséder aucun diviseur strict autre que 1 : q est donc premier.

Alors q est nécessairement différent de tous les p_i . Car si $q = p_i$ pour un certain $i \in \llbracket 1, n \rrbracket$, q divise $p_1 p_2 \dots p_n$ d'une part, et divise $p_1 p_2 \dots p_n + 1$ d'autre part, donc divise la différence qui vaut 1, ce qui est impossible.

q est donc un $(n+1)^{\text{e}}$ nombre premier. $\square$

Théorème 3.0.8.

Tout entier naturel supérieur ou égal à 1 se décompose de manière unique (à l'ordre des facteurs près) en un produit de nombres premiers (ce produit est éventuellement réduit à zéro ou un terme, et peut avoir plusieurs facteurs égaux). Plus précisément, pour tout $n \in \mathbb{N} \setminus \{0, 1\}$, il existe $k \in \mathbb{N}^*$, des entiers premiers $p_1, \dots, p_k$ distincts et $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^k p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}.$$

Démonstration. **Existence** on en donne trois démonstrations

Principe de la descente infinie de Fermat

Si n est un nombre ne se décomposant pas en facteurs premiers, alors n n'est lui-même pas premier (sinon, $n = n$ est une décomposition). Donc, n s'écrit $n = ab$, avec $1 < a < n$ et $1 < b < n$. n ne se décomposant pas en facteurs premiers, nécessairement, a ou b ne se décompose pas en facteurs premiers. On trouve donc, pour tout entier ne se décomposant pas en facteurs premiers, un entier strictement plus petit ne se décomposant pas en facteurs premiers. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers.

Principe du bon ordre Soit A l'ensemble des entiers n'admettant pas de décomposition. Nous voulons montrer que A est vide. S'il était non vide, il y aurait un plus petit élément a . Si a n'admet pour diviseur que 1 et lui-même, a est premier. $a = a$ est une décomposition de a en facteurs premiers, ce qui est contraire à l'hypothèse. Donc a s'écrit $b \times c$ où b et c sont des entiers différents de a et de 1. a étant le minimum de A , b et c ne sont pas éléments de A et se décomposent donc en produit de facteurs premiers. Il en est donc de même de a .

Principe de récurrence On suppose que tout entier inférieur ou égal à n se décompose en produits de facteurs premiers (ce qui est vrai pour $n \leq 2$). Considérons $n+1$:

- Si $n+1$ est premier, alors $n+1 = n+1$ est une décomposition.
- Sinon, $n+1 = ab$, avec $1 < a < n+1$, et $1 < b < n+1$. L'hypothèse de récurrence s'applique sur a et b , qui se décomposent donc en produits de facteurs premiers. Il en est donc de même de $n+1$.

Unicité Commençons par remarquer que pour tout entier non nul p , $p^0 = 1$. Ainsi si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ et si p_{k+1} est un nombre premier distinct des k précédents, on peut écrire $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} \cdot p_{k+1}^{\alpha_{k+1}}$, avec $\alpha_{k+1} = 0$.

On suppose que n a deux décompositions en facteurs premiers, que l'on peut donc écrire $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$, les deux membres étant éventuellement complétés par p^0 pour avoir les mêmes facteurs premiers dans les deux membres. Le théorème de Gauss permet de dire que $p_1^{\alpha_1}$ divise le membre de droite, mais puisqu'il est premier avec $p_2, \dots, p_k$ car tous ces nombres premiers sont distincts, il divise $p_1^{\beta_1}$, et donc $\alpha_1 \leq \beta_1$. Symétriquement, $\alpha_1 \geq \beta_1$, et ainsi $\alpha_1 = \beta_1$. Il en est de même pour les autres puissances. $\square$

Définition 3.0.9.

Pour un nombre premier p on définit l'application

$$\nu_p : \mathbb{Z} \rightarrow \mathbb{N} \cup \{+\infty\}$$

$$n \mapsto \begin{cases} +\infty & \text{si } n = 0 \\ \max \left\{ k \in \mathbb{N} \mid p^k \mid n \right\} & \text{sinon} \end{cases}$$

qui à un entier n associe l'exposant de p dans la décomposition de n en facteurs premiers, avec la convention $\nu_p(0) = +\infty$. Cette fonction est appelée *valuation p -adique* sur $\mathbb{Z}$.

Démonstration.

Il faut démontrer que $\max \{ k \in \mathbb{N} \mid p^k \mid n \}$ existe bien.

L'ensemble $\{k \in \mathbb{N} \mid p^k \mid n\}$ est non vide car il contient 0 ; de plus $p^k \xrightarrow[k \rightarrow +\infty]{} +\infty$, donc il existe $K \in \mathbb{N}$ tel que $p^K > n$, donc cet ensemble est majoré. Comme c'est une partie de $\mathbb{N}$, il admet bien un maximum. $\square$

Exemple 3.0.10.

$$\nu_5(50) = 2, \nu_3(50) = 0.$$

Exercice 3.0.11.

Décomposer 240 en produit de facteurs premiers et déterminer $\nu_2(240)$, $\nu_3(240)$, $\nu_5(240)$ et $\nu_7(240)$.

Proposition 3.0.12.

Soient $a, b \in \mathbb{Z}$. On note $\mathcal{P}$ l'ensemble des nombres premiers.

- (i) Pour tout entier p premier, p divise a si et seulement si $\nu_p(a) > 0$.
- (ii) Si $a \neq 0$, $|a| = \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$.
- (iii) Si $a, b \in \mathbb{Z}$ et $p \in \mathcal{P}$, alors $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
- (iv) On a $a \mid b$ si et seulement si, pour tout $p \in \mathcal{P}$, $\nu_p(a) \leq \nu_p(b)$.
- (v) Si $(a, b) \neq (0, 0)$, $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p(a), \nu_p(b))}$.
- (vi) si $a \neq 0$ et $b \neq 0$, $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p(a), \nu_p(b))}$.
- (vii) Les entiers a et b sont premiers entre eux si et seulement si ils n'ont aucun facteur premier en commun (*i.e.* pour tout p , $\nu_p(a) = 0$ ou $\nu_p(b) = 0$).

Démonstration. (i) Évident.

- (ii) C'est une simple réécriture de la décomposition de a en facteurs premiers.
- (iii) Il suffit de multiplier les écritures précédentes pour a et b .
- (iv) Si $a \mid b$, soit $p \in \mathcal{P}$. Alors, $p^{\nu_p(a)}$ divise a donc b , donc $\nu_p(b) \geq \nu_p(a)$.
Réciproquement, supposons que pour tout $p \in \mathcal{P}$, $\nu_p(a) \leq \nu_p(b)$. On voit alors dans la décomposition en facteurs premiers de b que l'on peut factoriser a dans b , donc $a \mid b$.
- (v) Commençons par remarquer que le produit considéré est bien défini : c'est un produit faisant intervenir une infinité de termes car $\mathcal{P}$ est infini, mais en fait seul un nombre fini de ces termes sont différents de 1. En effet, les diviseurs premiers de a sont en nombre fini, donc la valuation de a n'est non nulle que pour

un nombre fini d'entiers premiers. Il en est de même pour b , et donc $\min(\nu_p(a), \nu_p(b))$ n'est non nulle que pour un nombre fini d'entiers premiers p .

On note $d = \prod_{p \in \mathcal{P}} p^{\min(\nu_p(a), \nu_p(b))}$. Alors :

$$d \times \prod_{p \in \mathcal{P}} p^{\nu_p(a) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} = a$$

$$\text{et } d \times \prod_{p \in \mathcal{P}} p^{\nu_p(b) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathcal{P}} p^{\nu_p(b)} = b$$

donc d est un diviseur commun à a et b .

Soit d' un autre diviseur commun à a et b . Alors d' s'écrit nécessairement : $d' = \prod_{p \in \mathcal{P}} p^{\delta(p)}$, avec pour

tout p , $\delta(p) \in \mathbb{N}$, et il n'y a qu'un nombre fini d'entiers premiers p tels que $\delta(p) > 0$. Mais si $d' \mid a$, on doit avoir pour tout $p \in \mathcal{P}$, $\delta(p) \leq \nu_p(a)$. De même, $d' \mid b$ donc pour tout $p \in \mathcal{P}$, $\delta(p) \leq \nu_p(b)$. On a donc pour tout $p \in \mathcal{P}$, $\delta(p) \leq \min(\nu_p(a), \nu_p(b))$, et par conséquent $d' \mid d$, et d est bien le pgcd de a et b .

(vi) S'inspirer de la démonstration du point précédent.

- (vii) a et b sont premiers entre eux
 - $\Leftrightarrow a \wedge b = 1$
 - $\Leftrightarrow$ pour tout entier premier p , $\nu_p(a \wedge b) = 0$
 - $\Leftrightarrow$ pour tout entier premier p , $\min(\nu_p(a), \nu_p(b)) = 0$
 - $\Leftrightarrow$ pour tout entier premier p , $\nu_p(a) = 0$ ou $\nu_p(b) = 0$
 - $\Leftrightarrow$ pour tout entier premier p , p ne divise pas a ou p ne divise pas b
 - $\Leftrightarrow$ ils n'ont aucun facteur premier en commun.

$\square$

Exercice 3.0.13.

Calculer simplement $240 \wedge 42$ et $240 \vee 42$.

Finissons par un dernier résultat classique, le petit théorème de Fermat (Pierre de, Beaumont-de-Lomagne, première décennie du XVII^e siècle - Castres, 1665) (le grand n'est malheureusement pas à notre portée), qui a deux formulations équivalentes :

Théorème 3.0.14 (Petit théorème de Fermat, 1640).

Soit p un nombre premier. Alors on a :

- (i) pour tout $a \in \mathbb{Z}$, p divise $a^p - a$.
- (ii) pour tout $a \in \mathbb{Z}$ qui n'est pas un multiple de p , p divise $a^{p-1} - 1$.

Démonstration.

Ce théorème admet plus de 100 démonstrations. Fermat disait en connaître une mais ne l'a jamais publiée et elle n'est pas parvenue jusqu'à nous. La première démonstration est due à Leibniz en 1683, dans un manuscrit qui lui non plus n'a pas été publié. Il faut attendre 1736 pour qu'Euler donne la première démonstration publique, qui est essentiellement la même que celle de Leibniz.

Un petit nombre de ces démonstrations ainsi qu'une introduction historique peuvent être lus à l'adresse suivante :

<https://irem.univ-lille.fr/2021/08/13/fermat-revisite/>

Donnons-en encore une autre :

Commençons par montrer l'équivalence des deux énoncés¹ :

Si (i) est vrai et que a n'est pas un multiple de p , alors puisque p est premier, a et p sont premiers entre eux. Par conséquent, grâce au théorème de Gauss, $p|a(a^{p-1} - 1)$ donc $p|a^{p-1} - 1$.

Si (ii) est vrai, soit $a \in \mathbb{Z}$. Si a est un multiple de p , $p|a$ donc $p|a(a^{p-1} - 1)$. Et si a n'est pas un multiple de p , alors avec (ii) $p|a^{p-1} - 1$ donc $p|a(a^{p-1} - 1)$. Dans tous les cas, (i) est vrai.

Montrons maintenant le point (ii).

Soit a un entier non multiple de p . Posons $N = a(2a)(3a)\dots((p-1)a)$. Nous allons calculer N modulo p de deux manières.

Tout d'abord, réécrivons $N = a^{p-1} \times (p-1)!$.

Ensuite, pour tout $i \in \llbracket 1, p-1 \rrbracket$, appelons r_i le reste de la division euclidienne de ia par p . Alors $N \equiv r_1 r_2 \dots r_{p-1} [p]$. Supposons qu'il existe $i, j \in \llbracket 1, p-1 \rrbracket$ tels que $r_i = r_j$. Alors $ia \equiv ja [p]$ donc $p|(i-j)a$. Or $a \wedge p = 1$ donc avec le théorème de Gauss, $p|(i-j)$. Mais $|i-j| < p$ donc nécessairement $i-j = 0$, donc $i = j$. Ainsi les $r_1, \dots, r_{p-1}$ sont deux à deux distincts. Mais comme ils sont tous dans l'intervalle $\llbracket 1, p-1 \rrbracket$, qui contient exactement $p-1$ éléments, $\{r_1, \dots, r_{p-1}\} = \llbracket 1, p-1 \rrbracket$, et donc $r_1 r_2 \dots r_{p-1} = (p-1)!$.

Finalement, $N = a^{p-1} \times (p-1)! \equiv (p-1)! [p]$, donc $p|(p-1)!(a^{p-1} - 1)$. Or p est premier avec tous les entiers de 1 à $p-1$, donc il est premier avec $(p-1)!$, et à nouveau avec le théorème de Gauss, il vient bien $p|a^{p-1} - 1$. $\square$

Exercice 3.0.15.

Calculer le reste de la division euclidienne de $42^{835} 720$ par 37.

Le Petit théorème de Fermat donne donc une condition nécessaire pour qu'un nombre entier soit premier. Il est d'ailleurs très largement utilisé dans les tests de primalité, comme celui de Rabin-Miller. Mais, sa réciproque étant fausse, il n'est pas possible de savoir de manière certaine

qu'un nombre est premier en n'utilisant que ce théorème. Ainsi, on appelle *nombre de Carmichael* ou *menteurs de Fermat* les nombres entiers qui ne sont pas premiers mais vérifient tout de même le Petit théorème de Fermat. Le plus petit nombre de Carmichael est 561, et a été découvert par Carmichael en 1910, bien que les propriétés de tels nombres aient déjà été énoncées en 1899 par Korselt. Les nombres de Carmichael étant relativement rares par rapport aux nombres premiers, un test de primalité basé sur le petit théorème de Fermat aura peu de chances de donner un résultat erroné, mais il n'est cependant pas considéré comme un test suffisamment fiable. C'est pourquoi on le combine avec d'autres tests pour obtenir des tests de primalité probabilistes plus fiables.

1. Ici, nous n'avons besoin que de montrer que (ii) implique (i) puisque nous allons montrer (ii) par la suite.

Chapitre XII

Suites réelles et complexes

Sommaire

1	Vocabulaire.	168
2	Limite d'une suite réelle.	169
2.1	Définition et premières propriétés.	169
2.2	Opérations sur les limites.	171
a	Étude de $(u_n + v_n)_{n \in \mathbb{N}}$.	171
b	Étude de $(u_n v_n)_{n \in \mathbb{N}}$.	171
c	Étude de $\left(\frac{1}{u_n}\right)_{n \in \mathbb{N}}$.	171
d	Étude de $(u_n)_{n \in \mathbb{N}}$.	172
e	Étude de $(\max(u_n, v_n))_{n \in \mathbb{N}}$.	172
f	Exemples de formes indéterminées.	172
2.3	Limites et suites extraites.	172
2.4	Limites et inégalités.	173
3	Résultats de convergence.	173
3.1	Composition.	173
3.2	Utilisation d'inégalités.	174
a	Techniques d'encadrement.	174
b	Suites monotones.	174
c	Suites adjacentes.	175
3.3	Théorème de Bolzano-Weierstrass.	176
4	Traduction séquentielle de certaines propriétés.	176
5	Suites particulières.	177
5.1	Suites arithmétiques.	177
5.2	Suites géométriques.	177
5.3	Suites arithmético-géométriques.	178
5.4	Suites récurrentes linéaires doubles.	179
6	Suites définies par une relation de récurrence d'ordre 1.	181
6.1	Définition de la suite.	181
6.2	Recherche d'une limite éventuelle.	181
6.3	Cas où f est croissante sur A .	182
6.4	Cas où f est décroissante sur A .	182
7	Suites à valeurs complexes.	182
8	Premiers exemples de séries numériques.	184
8.1	Séries télescopiques.	184
8.2	Séries géométriques.	184

1 Vocabulaire.

Définition 1.0.1 (Suite réelle).

- Une *suite à valeurs réelles* ou *suite réelle* u est une application de $\mathbb{N}$ dans $\mathbb{R}$, u . On note en général u_n au lieu de $u(n)$ l'image de n par u .
- Étant donnée une expression e contenant la variable n , on note $(e)_{n \in \mathbb{N}}$ la suite $\mathbb{N} \rightarrow \mathbb{R}$:

$$n \mapsto e$$

Ainsi, la suite u est souvent notée $(u_n)_{n \in \mathbb{N}}$.

- La suite $(u_n)_{n \in \mathbb{N}}$ est aussi appelée *la suite de terme général* u_n .
- On note $\mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles.

Remarque 1.0.2 (Représentation graphique des termes d'une suite).

Cela peut se faire en plaçant les termes sur la droite des réels (représentation unidimensionnelle) ou en traçant le "graphe" de la suite (représentation bidimensionnelle). Chacune présente des avantages et des inconvénients.

Remarque 1.0.3 (Modes de définition).

Il existe plusieurs manières de définir une suite.

Définition explicite : on donne le terme général. On peut par exemple étudier la suite de terme général $u_n = \left(1 + \frac{1}{n}\right)^n$.

Définition par récurrence : on définit le premier terme, ainsi qu'une relation de récurrence vérifiée par la suite. On peut par exemple étudier la suite définie par $u_0 = 1$ et $\forall n \in \mathbb{N}, u_{n+1} = \sin(u_n)$. Ces suites feront l'objet d'une première étude dans la partie 6.

Définition implicite : on étudie souvent des suites dont le terme général est solution d'une équation. On peut par exemple étudier la suite dont le terme général est l'unique réel solution sur $\mathbb{R}_+$ de l'équation $x^2 + x = n$.

Définition 1.0.4 (Opérations sur les suites).

- Étant donné deux suites u et v on peut former leur somme $u + v$, définie comme $(u_n + v_n)_{n \in \mathbb{N}}$.
- Étant donné une suite u et un scalaire λ , on

peut former la suite λu définie comme $(\lambda u_n)_{n \in \mathbb{N}}$.

- On dit que $\mathbb{R}^{\mathbb{N}}$ muni de ces deux opérations est un *espace vectoriel*.

• Étant donné deux suites u et v on peut former leur produit uv , définie comme $(u_n v_n)_{n \in \mathbb{N}}$.

- Étant donné deux suites u et v telles que v ne s'annule pas, on peut former leur quotient $\frac{u}{v}$,

définie comme $\left(\frac{u_n}{v_n}\right)_{n \in \mathbb{N}}$.

- Étant donné une suite u , on peut former la suite $|u|$ définie comme $(|u_n|)_{n \in \mathbb{N}}$.

• Étant donné deux suites u et v , on peut former les suites $\min(u, v)$ et $\max(u, v)$, définie comme $(\min(u_n, v_n))_{n \in \mathbb{N}}$ et $(\max(u_n, v_n))_{n \in \mathbb{N}}$.

Définition 1.0.5.

- Étant donné une propriété P sur les suites réelles et un entier n_0 et une suite réelle u , on dit que P est *vraie à partir du rang* n_0 si la propriété P est vraie pour la suite des termes $u_{n_0}, u_{n_0+1}, u_{n_0+2}, \dots$ autrement dit pour la suite v où v est définie par $\forall n \in \mathbb{N} v_n = u_{n_0+n}$.

- On dit que P est *vraie à partir d'un certain rang* s'il existe un entier n_0 tel que la propriété P est vraie à partir du rang n_0 .

Remarque 1.0.6.

En général, seul le comportement des suites quand n tend vers l'infini nous intéresse, et non les premiers termes de la suite, d'où l'intérêt de la notion de propriété vraie à partir d'un certain rang.

Exemple 1.0.7.

- La suite $(n(n-5))_{n \in \mathbb{N}}$ n'est pas à valeurs positives ou nulles mais elle est à valeurs positives ou nulles à partir du rang 5 (ainsi d'ailleurs qu'à partir du rang 10, du rang 2389, ...).
- La suite u définie par

$$\forall n \in \mathbb{N} u_n = \begin{cases} n & \text{si } n < 735 \\ 735 & \text{sinon} \end{cases}$$

n'est pas constante mais est constante à partir du rang 735.

Exemple 1.0.8.

Dire qu'une suite est positive ou nulle à partir d'un certain rang est équivalent à

$$\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, u_{n+n_0} \geq 0,$$

autrement dit :

$$\exists n_0 \in \mathbb{N}, \forall k \in \mathbb{N}, k \geq n_0 \Rightarrow u_k \geq 0.$$

Définition 1.0.9.

Une suite réelle u est dite :

- (i) *constante* si $\forall n \in \mathbb{N}, u_n = u_0$;
- (ii) *stationnaire* si elle est constante à partir d'un certain rang, c'est-à-dire si

$$\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n = u_{n_0}.$$

Remarque 1.0.10.

Jusque là, toutes les définitions données sur les suites à valeurs réelles s'étendent directement aux suites à valeurs complexes. Ce n'est plus le cas pour ce qui suit.

Définition 1.0.11.

Une suite réelle u est dite :

- (i) *croissante* (resp. *stric. croissante*) si pour tout $n \in \mathbb{N}, u_n \leq u_{n+1}$ (resp. $u_n < u_{n+1}$) ;
- (ii) *décroissante* (resp. *stric. décroissante*) si pour tout $n \in \mathbb{N}, u_n \geq u_{n+1}$ (resp. $u_n > u_{n+1}$) ;
- (iii) *monotone* si la suite est croissante ou décroissante ;
- (iv) *strictement monotone* si la suite est strictement croissante ou strictement décroissante ;
- (v) *majorée* (resp. *minorée*) s'il existe $M \in \mathbb{R}$ tel que pour tout $n \in \mathbb{N}, u_n \leq M$ (resp. $u_n \geq M$) ;
- (vi) *bornée* si elle est majorée et minorée.

Remarque 1.0.12.

- Toutes ces propriétés peuvent s'énoncer « à partir d'un certain rang ».

Cependant, une suite est majorée à partir d'un certain rang si et seulement si cette suite est majorée (*idem* pour minorée et bornée).

- « (u_n) est bornée » s'écrit aussi : $\exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |u_n| \leq M$.

Cela permet d'ailleurs de définir la notion de suite complexe bornée, alors même qu'une suite complexe ne peut être ni minorée ni majorée.

- Pour montrer qu'une suite est croissante, on peut utiliser plusieurs méthodes : la plus classique consiste à étudier le signe de $u_{n+1} - u_n$. On peut aussi comparer $\frac{u_{n+1}}{u_n}$ à 1, à condition de connaître le signe de u_n .
- Une suite u est croissante si et seulement si pour tout $p \in \mathbb{N}$ et tout $n \geq p, u_n \geq u_p$.

2 Limite d'une suite réelle.

2.1 Définition et premières propriétés.

Définition 2.1.1.

Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$, soit $\ell \in \mathbb{R}$. On dit que (u_n) tend (ou converge) vers ℓ si

$$\forall \varepsilon \in \mathbb{R}_+^*, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n - \ell| < \varepsilon.$$

On note ceci $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$, ou plus simplement $u \rightarrow \ell$.

Remarque 2.1.2.

Ceci est équivalent à

$$\forall \varepsilon \in \mathbb{R}_+^*, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n - \ell| < \varepsilon.$$

En pratique, on préférera souvent (mais pas toujours) utiliser des inégalités larges.

Remarque 2.1.3.

On utilise souvent les abus de notation suivants :

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, |u_n - \ell| \leq \varepsilon.$$

Exemple 2.1.4.

Montrer que la suite de terme général $u_n = \frac{n-1}{n+1}$ converge vers 1.

Définition 2.1.5.

Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) est convergente s'il existe $\ell \in \mathbb{R}$ tel que $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$. Si (u_n) n'est pas convergente, on dit qu'elle est divergente (ou diverge).

Théorème 2.1.6.

Toute suite convergente est bornée.

Démonstration.

Soit (u_n) convergeant vers $\ell \in \mathbb{R}$. Alors d'après la proposition précédente, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $|u_n - \ell| \leq 1$, et donc $\ell - 1 \leq u_n \leq \ell + 1$. Par conséquent, (u_n) est bornée à partir du rang n_0 . Mais les n_0 premiers termes de la suite étant en nombre fini, ils forment un ensemble borné. L'ensemble des termes de la suite (u_n) étant la réunion de deux ensembles bornés, il est borné également, et donc la suite (u_n) est bornée. $\square$

Remarque 2.1.7.

La réciproque est évidemment fausse, comme le prouve la suite $((-1)^n)_{n \in \mathbb{N}}$.

Définition 2.1.8.

Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) tend vers $+\infty$ si

$$\forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \geq A.$$

On note ceci $u_n \xrightarrow[n \rightarrow +\infty]{} +\infty$, ou plus simplement $u \rightarrow +\infty$.

Définition 2.1.9.

Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$. On dit que (u_n) tend vers $-\infty$ si

$$\forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \leq A.$$

On note ceci $u_n \xrightarrow[n \rightarrow +\infty]{} -\infty$, ou plus simplement $u \rightarrow -\infty$.

Remarque 2.1.10.

Une suite qui tend vers $+\infty$ (ou vers $-\infty$) diverge.

On peut cependant introduire l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$, que l'on appelle *droite numérique achevée*. Dans $\overline{\mathbb{R}}$, une suite tendant vers $+\infty$ (ou moins $-\infty$) converge. Le théorème 2.1.6 est toujours valable : toute suite à valeurs dans $\overline{\mathbb{R}}$ est bornée (par $-\infty$ et $+\infty$) !

Par défaut, la notion de convergence s'entendra dans $\mathbb{R}$.

Théorème 2.1.11 (Unicité de la limite).

Soit (u_n) une suite réelle, soit $\ell_1, \ell_2 \in \overline{\mathbb{R}}$ tels que $u_n \xrightarrow[n \rightarrow +\infty]{} \ell_1$ et $u_n \xrightarrow[n \rightarrow +\infty]{} \ell_2$. Alors, $\ell_1 = \ell_2$.

Démonstration.

Il convient *a priori* de distinguer 9 cas. Par symétrie, et en supposant $\ell_1 \neq \ell_2$, il suffit de considérer les cas :

- $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$;
- $\ell_1 = -\infty$ et $\ell_2 = +\infty$.

Nous ne détaillerons ici que les deux premiers, les deux derniers sont laissés au lecteur.

Si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$, posons $\varepsilon = \frac{1}{3}|\ell_1 - \ell_2| > 0$. Alors, il existe $n_1, n_2 \in \mathbb{N}$ tels que, pour tout $n \in \mathbb{N}$:

- si $n \geq n_1$, $|u_n - \ell_1| \leq \varepsilon$;
- si $n \geq n_2$, $|u_n - \ell_2| \leq \varepsilon$.

Alors, pour $n \geq \max(n_1, n_2)$, on a par l'inégalité triangulaire

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - u_n - (\ell_2 - u_n)| \\ &\leq |\ell_1 - u_n| + |\ell_2 - u_n| \\ &\leq \frac{2}{3}|\ell_1 - \ell_2|. \end{aligned}$$

C'est impossible !

Si $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$, posons $A = \ell_1 - 1$ et $\varepsilon = \frac{1}{2}$. Alors, il existe $n_1, n_2 \in \mathbb{N}$ tels que, pour tout $n \in \mathbb{N}$:

- si $n \geq n_1$, $|u_n - \ell_1| \leq \varepsilon$;
- si $n \geq n_2$, $u_n \leq A$.

Alors, pour $n \geq \max(n_1, n_2)$, on a $u_n \leq A < \ell_1 - \frac{1}{2} \leq u_n$. C'est impossible ! $\square$

Définition 2.1.12 (Limite).

Soit $u \in \mathbb{R}^{\mathbb{N}}$. Lorsqu'il existe un élément $\ell \in \overline{\mathbb{R}}$ vérifiant $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$, on l'appelle **la limite** de u , et on le note $\lim u$ ou $\lim_{n \rightarrow +\infty} u_n$.



Le symbole $\lim_{n \rightarrow +\infty}$ ne peut s'utiliser qu'après avoir montré l'existence de ladite limite. L'utiliser avant est une erreur grave. On préférera *systématiquement* utiliser l'écriture $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$.

Proposition 2.1.13.

Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$. On a les propriétés suivantes :

$$\begin{aligned} u_n \xrightarrow{n \rightarrow +\infty} \ell &\iff u_n - \ell \xrightarrow{n \rightarrow +\infty} 0 \\ u_n \xrightarrow{n \rightarrow +\infty} 0 &\iff |u_n| \xrightarrow{n \rightarrow +\infty} 0 \end{aligned}$$

Corollaire 2.1.14.

Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$.

$$u_n \xrightarrow{n \rightarrow +\infty} \ell \iff |u_n - \ell| \xrightarrow{n \rightarrow +\infty} 0$$

Corollaire 2.1.15.

Soit $u \in \mathbb{R}^{\mathbb{N}}$, $\ell \in \mathbb{R}$. Alors u tend vers ℓ si et seulement s'il existe $v \in \mathbb{R}^{\mathbb{N}}$ tendant vers 0 telle que $u = \ell + v$.

Proposition 2.1.16.

Soit u une suite convergeant vers 0 et v une suite bornée. Alors uv converge vers 0.

Démonstration.

Soit $M > 0$ un majorant de $|v|$. Soit $\varepsilon > 0$, il existe donc un rang $N \in \mathbb{N}$ tel que pour, tout entier naturel $n \geq N$, $|u_n| \leq \frac{\varepsilon}{M}$. Ainsi, si $n \geq N$, $|u_n v_n| \leq \varepsilon$, d'où le résultat. $\square$

Exemple 2.1.17.

Étudier la convergence de la suite $\left(\frac{\cos n}{n}\right)_{n \in \mathbb{N}^*}$

Proposition 2.1.18.

L'ensemble des suites convergeant vers 0 est stable par addition et par multiplication par un scalaire. On dit que l'ensemble des suites convergeant vers 0 est un *sous-espace vectoriel de l'espace vectoriel des suites à valeurs réelles*.

Démonstration.

Comme un scalaire peut-être vu comme une suite constante, donc bornée, il suffit de montrer que la somme de deux suites convergeant vers 0 converge vers 0.

Soit u et v tendant vers 0, soit $\varepsilon > 0$. Il existe deux rangs $N \in \mathbb{N}$ et $N' \in \mathbb{N}$ tels que, pour tout entier n ,

- si $n \geq N$, $|u_n| \leq \frac{\varepsilon}{2}$;
- si $n \geq N'$, $|v_n| \leq \frac{\varepsilon}{2}$.

Ainsi, si $n \geq \max(N, N')$, alors $|u_n + v_n| \leq |u_n| + |v_n| \leq \varepsilon$, d'où le résultat. $\square$

2.2 Opérations sur les limites.

Soit u et v deux suites qui admettent chacune pour limite $\ell, \ell' \in \overline{\mathbb{R}}$.

a Étude de $(u_n + v_n)_{n \in \mathbb{N}}$.

v_n	$\ell' \in \mathbb{R}$	$+\infty$	$-\infty$
u_n			
$\ell \in \mathbb{R}$			
$+\infty$			
$-\infty$			

b Étude de $(u_n v_n)_{n \in \mathbb{N}}$.

v_n	$\ell' \in \mathbb{R}_+^*$	$\ell' \in \mathbb{R}_-^*$	0	$+\infty$	$-\infty$
u_n					
$\ell \in \mathbb{R}_+^*$					
$\ell \in \mathbb{R}_-^*$					
0					
$+\infty$					
$-\infty$					

c Étude de $\left(\frac{1}{u_n}\right)_{n \in \mathbb{N}}$.

Si la suite u ne s'annule pas.

Remarque 2.2.1.

Si v tend vers 0, alors $\frac{1}{1+v}$ tend vers 1.

$u_n \rightarrow$	$\ell \in \mathbb{R} \setminus \{0\}$	0	$+\infty$	$-\infty$
$1/u_n \rightarrow$				

On obtient alors le comportement de $\left(\frac{u_n}{v_n}\right)_{n \in \mathbb{N}}$ en utilisant les deux tableaux précédents.

d Étude de $(|u_n|)_{n \in \mathbb{N}}$.

$u_n \rightarrow$	$\ell \in \mathbb{R}$	$+\infty$	$-\infty$
$ u_n \rightarrow$			

e Étude de $(\max(u_n, v_n))_{n \in \mathbb{N}}$.

Proposition 2.2.2.

Si $u_n \xrightarrow[n \rightarrow +\infty]{} \ell \in \overline{\mathbb{R}}$ et $v_n \xrightarrow[n \rightarrow +\infty]{} \ell' \in \overline{\mathbb{R}}$, alors $\max(u_n, v_n) \xrightarrow[n \rightarrow +\infty]{} \max(\ell, \ell')$.

Démonstration.

Il suffit d'écrire $\max(u_n, v_n) = \frac{|u_n - v_n| + u_n + v_n}{2}$. $\square$

Remarque 2.2.3.

On a bien sûr le même résultat avec le minimum.

f Exemples de formes indéterminées.

Exemple 2.2.4.

Déterminer les limites (si elles existent) des suites de termes généraux suivants :

- $u_n = \frac{3n^2 + n + 15}{n^2 + \sin n}$
- $u_n = \frac{e^n - 3^n}{n^2 - 2^n}$
- $u_n = \left(1 + \frac{1}{n}\right)^n$.

2.3 Limites et suites extraites.

Définition 2.3.1.

On appelle *suite extraite* ou *sous-suite* de la suite u toute suite $(u_{\varphi(n)})_{n \in \mathbb{N}}$ où φ est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$. La fonction φ est une *extraction*, ou *extractrice*.

Remarque 2.3.2.

On ne conserve que les termes de rang $\varphi(n)$ pour $n \in \mathbb{N}$, d'où la dénomination suite extraite.

Exemple 2.3.3.

$(u_{n+1})_{n \in \mathbb{N}}$, $(u_{2n})_{n \in \mathbb{N}}$ et $(u_{2n+1})_{n \in \mathbb{N}}$ sont des suites extraites de $(u_n)_{n \in \mathbb{N}}$.

Exercice 2.3.4.

Soit u une suite, φ et ψ deux extractrices. Quelle est la suite extraite de $(u_{\varphi(n)})_{n \in \mathbb{N}}$ par ψ ?

Lemme 2.3.5.

Soit φ une fonction strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$. Alors pour tout $n \in \mathbb{N}$, $\varphi(n) \geq n$.

Théorème 2.3.6.

Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \overline{\mathbb{R}}$. Si $u \xrightarrow[n \rightarrow +\infty]{} \ell$ alors toute suite extraite de u tend aussi vers ℓ .

Démonstration.

On traite le cas $\ell \in \mathbb{R}$, les deux autres cas sont laissés au lecteur.

Soit $\varepsilon > 0$. Il existe donc un rang $n_0 \in \mathbb{N}$ tel que, pour tout $n \geq n_0$, $|u_n - \ell| \leq \varepsilon$. Soit $n \geq n_0$, on a alors $\varphi(n) \geq n \geq n_0$ et donc $|u_{\varphi(n)} - \ell| \leq \varepsilon$. $\square$

Corollaire 2.3.7.

Si une suite admet deux suites extraites ne convergeant pas vers la même limite alors cette suite n'a pas de limite.

Si une suite admet une suite extraite n'ayant pas de limite, alors cette suite n'a pas de limite.

Exemple 2.3.8.

Montrer que les suites $((-1)^n)_{n \in \mathbb{N}}$ et $(\cos \frac{n\pi}{3})_{n \in \mathbb{N}}$ ne convergent pas.

Théorème 2.3.9.

Soit u une suite à valeurs réelles et $\ell \in \overline{\mathbb{R}}$. Si on a $u_{2n} \xrightarrow[n \rightarrow +\infty]{} \ell$ et $u_{2n+1} \xrightarrow[n \rightarrow +\infty]{} \ell$, alors $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$.

Démonstration.

On traite le cas $\ell \in \mathbb{R}$, les deux autres cas sont laissés au lecteur.

Soit $\varepsilon > 0$. Il existe donc deux rangs N et N' tels que, pour tout entier naturel n ,

- si $n \geq N$, $|u_{2n} - \ell| \leq \varepsilon$;
- si $n \geq N'$, $|u_{2n+1} - \ell| \leq \varepsilon$.

Ainsi, si $n \geq \max(2N, 2N' + 1)$, on a $|u_n - \ell| \leq \varepsilon$ (il suffit de distinguer selon la parité de n), d'où le résultat. $\square$

2.4 Limites et inégalités.

Proposition 2.4.1.

Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $(a, b, \ell) \in \mathbb{R}^3$. Supposons $u \xrightarrow{+\infty} \ell$ et $a < \ell < b$. Alors à partir d'un certain rang, les valeurs de u sont comprises strictement entre a et b . Autrement dit :

$$\exists n_0 \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad n \geq n_0 \Rightarrow a < u_n < b$$

Démonstration.

On pose $\varepsilon = \frac{1}{2} \min(\ell - a; b - \ell) > 0$. Soit $n_0 \in \mathbb{N}$ tel que, pour tout $n \geq n_0$, $|u_n - \ell| \leq \varepsilon$. On a $a < \ell - \varepsilon < \ell + \varepsilon < b$. Alors, si $n \geq n_0$, on a $\ell - \varepsilon \leq u_n \leq \ell + \varepsilon$, donc $a < u_n < b$. $\square$

Corollaire 2.4.2.

En particulier toute suite convergeant vers une limite strictement positive (resp. strictement négative) est strictement positive (resp. strictement négative) à partir d'un certain rang.

Corollaire 2.4.3.

Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $(a, \ell) \in \mathbb{R}^2$. Supposons $u \xrightarrow{n \rightarrow +\infty} \ell$.

1. Si à partir d'un certain rang $u_n \leq a$, alors $\ell \leq a$.
2. Si à partir d'un certain rang $a \leq u_n$, alors $a \leq \ell$.



Ne pas croire que si à partir d'un certain rang $u_n < a$, alors $\ell < a$. En passant à la limite dans une inégalité, les inégalités strictes deviennent des inégalités larges. (Par exemple : la suite $(\frac{1}{n})_{n \in \mathbb{N}^*}$ converge vers 0, et pourtant tous les termes sont strictement positifs).

Corollaire 2.4.4.

Soient u et v deux suites réelles telles que, à partir d'un certain rang, $u_n \leq v_n$. Si les suites u et v convergent respectivement vers ℓ et ℓ' , alors $\ell \leq \ell'$.



Là encore, même si à partir d'un certain rang, $u_n < v_n$, il se peut que $\ell = \ell'$.

Exemple 2.4.5.

$\forall n \in \mathbb{N}^*$, $1 - \frac{1}{n} < 1 + \frac{1}{n}$, pourtant $1 - \frac{1}{n} \xrightarrow{n \rightarrow +\infty} 1$ et $1 + \frac{1}{n} \xrightarrow{n \rightarrow +\infty} 1$.

Exercice 2.4.6.

Montrer que la suite $(H_n) = \left(\sum_{k=1}^n \frac{1}{k} \right)_{n \in \mathbb{N}^*}$ ne converge pas. On pourra commencer par montrer que pour tout $n \geq 1$, $H_{2n} - H_n \geq \frac{1}{2}$.

Proposition 2.4.7.

Si une suite $(u_n)_{n \in \mathbb{N}}$ est croissante (resp. décroissante) et converge vers un réel ℓ , alors $\forall n \in \mathbb{N}$, $u_n \leq \ell$ (resp. $\forall n \in \mathbb{N}$, $u_n \geq \ell$).

Si une suite $(u_n)_{n \in \mathbb{N}}$ est strict. croissante (resp. strict. décroissante) et converge vers un réel ℓ alors $\forall n \in \mathbb{N}$, $u_n < \ell$ (resp. $\forall n \in \mathbb{N}$, $u_n > \ell$).

Démonstration.

On ne traite que le premier cas. S'il existe $N \in \mathbb{N}$ tel que $u_N > \ell$ alors, si $n \geq N$, $u_n - \ell \geq u_N - \ell > 0$, ce qui est impossible. $\square$

Remarque 2.4.8.

Ces propriétés ne permettent pas de montrer la convergence d'une suite. Elles se contentent de donner des renseignements sur la suite ou sa limite, *en cas de convergence*.

3 Résultats de convergence.

3.1 Composition.

Théorème 3.1.1.

Soient $a \in \bar{D}$ et $b \in \bar{\mathbb{R}}$ et f une fonction à valeurs réelles définie sur une partie D de $\mathbb{R}$ vérifiant

$$f(x) \xrightarrow{x \rightarrow a} b$$

et u une suite réelle telle que la suite $(f(u_n))_{n \in \mathbb{N}}$ soit bien définie (c'est-à-dire vérifiant $\forall n \in \mathbb{N} \quad u_n \in D$) et vérifiant

$$u_n \xrightarrow{n \rightarrow +\infty} a.$$

Alors,

$$f(u_n) \xrightarrow{n \rightarrow +\infty} b.$$

Remarque 3.1.2.

Ce théorème est temporairement admis, la définition de convergence pour les fonctions n'ayant pas encore été donnée.

Exemple 3.1.3.

Si u est une suite qui converge vers 0, alors la suite $(e^{u_n})_{n \in \mathbb{N}}$ est une suite convergeant vers 1.

3.2 Utilisation d'inégalités.

a Techniques d'encadrement.

Théorème 3.2.1.

Soient u , v et w trois suites à valeurs réelles et $\ell \in \mathbb{R}$.

- (i) **Th. de minoration** : Si $u_n \xrightarrow{n \rightarrow +\infty} +\infty$ et $u_n \leq v_n$ à partir d'un certain rang, alors $v_n \xrightarrow{n \rightarrow +\infty} +\infty$.
- (ii) **Th. de majoration** : Si $u_n \xrightarrow{n \rightarrow +\infty} -\infty$ et $v_n \leq u_n$ à partir d'un certain rang, alors $v_n \xrightarrow{n \rightarrow +\infty} -\infty$.
- (iii) **Th. d'encadrement** : Si $u_n \xrightarrow{n \rightarrow +\infty} \ell$ et $w_n \xrightarrow{n \rightarrow +\infty} \ell$ et $u_n \leq v_n \leq w_n$ à partir d'un certain rang, alors $v_n \xrightarrow{n \rightarrow +\infty} \ell$.

Remarque 3.2.2.

Le troisième résultat est souvent appelé « Théorème des gendarmes » dans le secondaire. Vous pouvez utiliser cette dénomination, ou tout simplement dire « par encadrement » quand vous l'utilisez.

Démonstration.

Ces trois résultats se démontrent aisément. $\square$

Corollaire 3.2.3.

Soient u et v deux suites à valeurs réelles.

Si $v_n \xrightarrow{n \rightarrow +\infty} 0$ et $|u_n| \leq v_n$ à partir d'un certain rang, alors $u_n \xrightarrow{n \rightarrow +\infty} 0$.

b Suites monotones.

Théorème 3.2.4 (de la limite monotone).

Soit u une suite réelle.

1. Si u est croissante, elle admet une limite (dans $\overline{\mathbb{R}}$) et

$$u_n \xrightarrow{n \rightarrow +\infty} \sup_{n \in \mathbb{N}} u_n.$$

- (a) Dans le cas où u est majorée par un réel, cette limite est réelle et est le plus petit majorant de u .
- (b) Dans le cas où u n'est pas majorée, cette limite vaut $+\infty$.

2. Même résultat, dans le cas d'une suite u décroissante *mutatis mutandis* (sup en inf, «majorée» en «minorée», $+\infty$ en $-\infty$).

Démonstration. 1. (a) Notons $\ell = \sup_{n \in \mathbb{N}} u_n$. Soit $\varepsilon > 0$, il existe donc un entier naturel n_0 tel que $\ell - \varepsilon < u_{n_0} \leq \ell$. Par croissance de u et majoration de u par ℓ , on a, pour tout $n \geq n_0$, $\ell - \varepsilon \leq u_n \leq \ell$. Cela montre donc bien la convergence de u vers ℓ .

- (b) Soit $A \in \mathbb{R}$, A ne majore pas u : il existe donc $n_0 \in \mathbb{N}$ tel que $u_{n_0} \geq A$. Ainsi, par croissance de u , on a, pour tout $n \geq n_0$, $u_n \geq A$. Ainsi, u tend vers $+\infty$.

2. Idem

$\square$

Exemple 3.2.5.

On exprime souvent le premier point du théorème en disant que «toute suite croissante majorée converge». Soit u et v les suites définies par

$$\forall n \in \mathbb{N} \quad u_n = n \text{ et } v_n = n + n^2$$

La suite u est croissante, majorée par la suite v : c'est donc une suite croissante majorée. Donc u converge ?



Une suite croissante majorée converge vers le plus petit de tous ses majorants. Le plus

petit de ses majorants n'est **pas** nécessairement le plus petit de ceux que vous avez déjà trouvés ! Retenir :

Corollaire 3.2.6.

Si u est croissante et majorée par $M \in \mathbb{R}$, alors u converge et sa limite est inférieure ou égale à M .

c Suites adjacentes.

Définition 3.2.7.

Deux suites u et v sont dites *adjacentes* si l'une est croissante, l'autre est décroissante et leur différence tend vers 0.

Théorème 3.2.8.

Soit u et v deux suites adjacentes. Alors u et v convergent, et ont la même limite.

Démonstration.

Si u et v convergent, $u - v$ converge vers la différence de leurs limites, soit 0 : u et v ont donc même limite.

On peut supposer, sans perte de généralité, que u est croissante et que v est décroissante. Montrons maintenant que u converge (il suffit ensuite d'écrire $v = v - u + u$ pour conclure à la convergence de v). Il suffit de montrer que u est majorée par un réel, par exemple v_0 . Sinon, il existe $n_0 \in \mathbb{N}$ vérifiant $u_{n_0} > v_0$ et l'on aurait, par croissance de u et décroissance de v ainsi que pour tout entier $n \geq n_0$, $u_n - v_n > u_{n_0} - v_0$, ce qui contredit la convergence de $u - v$ vers 0. Ainsi, u converge. $\square$



La définition et le théorème des suites adjacentes sont fondamentaux. Le fait qu'ils s'écrivent de façon très concise n'en réduit pas l'importance mais rend en revanche inexcusable les confusions entre ce qui relève de la définition et ce qui relève du théorème.

Remarque 3.2.9.

Soient $(u_n)_{n \in \mathbb{N}}$ et $(v_n)_{n \in \mathbb{N}}$ deux suites réelles adjacentes, avec $(u_n)_{n \in \mathbb{N}}$ croissante.

Notons ℓ leur limite commune. Alors, $\forall n \in \mathbb{N}$, $u_n \leq \ell \leq v_n$ et $\forall (p, q) \in \mathbb{N}^2$, $u_p \leq \ell \leq v_q$.

Exemple 3.2.10.

Les suites $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$ définies par $u_n = \sum_{k=0}^n \frac{1}{k!}$ et $v_n = u_n + \frac{1}{n \cdot n!}$ sont adjacentes.

Exemple 3.2.11 (Moyenne arithmetico - géométrique).

Soient $u_0, v_0 \in \mathbb{R}_+^*$. On définit deux suites en posant, pour tout $n \in \mathbb{N}$, $u_{n+1} = \frac{u_n + v_n}{2}$ et $v_{n+1} = \sqrt{u_n \cdot v_n}$. Alors ces deux suites sont adjacentes et leur limite commune est appelée *moyenne arithmetico - géométrique* de u_0 et v_0 .

Exercice 3.2.12 (Algorithme des Babyloniens).

On pose $v_0 = 2$. On définit deux suites en posant, pour tout $n \in \mathbb{N}$, $u_n = \frac{2}{v_n}$ et $v_{n+1} = \frac{u_n + v_n}{2}$. Montrer que ces deux suites sont adjacentes. Quelle est leur limite ?

Définition 3.2.13.

Étant donné I un intervalle de $\mathbb{R}$, on appelle diamètre de I et on note $\delta(I)$ la valeur de $b - a$ où a et b sont les extrémités gauche et droite de I si celles-ci sont réelles et $+\infty$ si l'une au moins n'est pas réelle.

Théorème 3.2.14 (Des segments emboîtés).

Soit $(I_n)_{n \in \mathbb{N}}$ une suite décroissante de segments non vides emboîtés, c'est-à-dire vérifiant $I_0 \supset I_1 \supset I_2 \supset \dots$ (autrement dit, pour tout $n \in \mathbb{N}$, $I_{n+1} \subset I_n$) et vérifiant $\delta(I_n) \xrightarrow{n \rightarrow +\infty} 0$. Alors l'ensemble

$$\bigcap_{n \in \mathbb{N}} I_n$$

est un singleton. Autrement dit, il existe un unique réel appartenant à I_n pour tout $n \in \mathbb{N}$.

De plus, tout suite u à valeur réelle telle que pour tout $n \in \mathbb{N}$, $u_n \in I_n$ converge vers ce réel.

Démonstration.

Il suffit de noter, pour tout $n \in \mathbb{N}$, a_n et b_n respectivement les extrémités gauche et droite de I_n . Les conditions sur les segments entraînent que a et b sont deux suites adjacentes. Elles ont donc une limite commune ℓ . De plus pour tout n , $a_n \leq \ell \leq b_n$. Donc $\{\ell\} \subset \bigcap_{n \in \mathbb{N}} I_n$. Réciproquement, si $x \in \bigcap_{n \in \mathbb{N}} I_n$, alors pour tout $n \in \mathbb{N}$, $a_n \leq x \leq b_n$ donc, par encadrement, $x = \ell$.

Tout suite u vérifiant les conditions données est alors encadrée par a et b donc converge vers ℓ . $\square$

Corollaire 3.2.15 (Méthode de la dichotomie). Soit $(I_n)_{n \in \mathbb{N}}$ une suite de segments telle que pour tout $n \in \mathbb{N}$, I_{n+1} est soit la moitié gauche du segment I_n , soit la moitié droite du segment I_n .

Alors la suite $(I_n)_{n \in \mathbb{N}}$ est une suite décroissante de segments emboîtés, dont le diamètre tend vers 0.

Les extrémités gauche et droite de ces segments constituent donc des suites adjacentes.

3.3 Théorème de Bolzano-Weierstrass.

Nous avons déjà vu que toute suite convergente est bornée. La réciproque est évidemment fausse, par exemple la suite $((-1)^n)_{n \in \mathbb{N}}$ est bornée et divergente. Mais une version plus faible est vraie : c'est l'objet du théorème suivant.

Théorème 3.3.1 (Bolzano-Weierstrass).

On peut extraire de toute suite réelle bornée une suite convergente.

Remarque 3.3.2.

On peut remplacer « bornée » par « à valeurs dans un segment ».

Démonstration (Principe de la dichotomie à connaître, formalisation non exigible).

Le cas où le segment est réduit à un point est trivial. Considérons donc un segment $[a, b]$ de $\mathbb{R}$ avec $a < b$ et une suite u à valeurs dans $[a, b]$ et montrons que u admet une suite extraite qui converge.

Définissons tout d'abord par dichotomie une suite $(I_n)_{n \in \mathbb{N}}$ de segments comme suit :

1. $I_0 = [a, b]$
2. Pour tout n , on définit I_{n+1} comme étant la moitié gauche de I_n si u prend une infinité de fois ses valeurs dans cette moitié gauche. Sinon, on définit I_{n+1} comme étant la moitié droite de I_n .

Il est clair que la suite $(I_n)_{n \in \mathbb{N}}$ est une suite de segments emboîtés de diamètre tendant vers 0, d'intersection réduite à un singleton l .

On peut démontrer par récurrence que pour tout $n \in \mathbb{N}$, u prend une infinité de fois ses valeurs dans I_n .

On va maintenant extraire une suite $(u_{\varphi(n)})_{n \in \mathbb{N}}$ de u telle que pour tout $n \in \mathbb{N}$, $u_n \in I_n$.

Le principe est relativement simple : on prend u_0 pour premier terme de cette suite extraite. On a $u_0 \in I_0$. On prend alors pour terme suivant le premier terme suivant de u appartenant à I_1 . Un tel terme existe puisque u prend une infinité de fois ses valeurs dans I_1 . On prend alors pour terme suivant le premier terme suivant de u appartenant à I_2 . Etc.

Plus formellement, on définit par récurrence l'application φ comme suit :

- (a) $\varphi(0) = 0$.
- (b) pour tout $n \in \mathbb{N}$, $\varphi(n+1)$ est le plus petit entier k strictement supérieur à $\varphi(n)$ vérifiant $u_k \in I_{n+1}$. La suite u prenant une infinité de fois ses valeurs dans $I(n+1)$, un tel k existe.

Posons alors, pour $n \in \mathbb{N}$, $v_n = u_{\varphi(n)}$.

On a pour tout $n \in \mathbb{N}$, $v_n \in I_n$. Donc v converge.

La suite u admet donc bien une suite extraite convergente. $\square$

4 Traduction séquentielle de certaines propriétés.

Définition 4.0.1.

On dit qu'une partie de $\mathbb{R}$ est dense dans $\mathbb{R}$ si elle rencontre tout intervalle ouvert non vide de $\mathbb{R}$.

Remarque 4.0.2.

On a déjà vu que l'ensemble des décimaux, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ étaient denses dans $\mathbb{R}$.

Proposition 4.0.3.

Soit $X \subset \mathbb{R}$. X est dense dans $\mathbb{R}$ si et seulement si pour tout $\ell \in \mathbb{R}$ il existe une suite u à valeurs dans X convergeant vers ℓ .

Démonstration.

Supposons que X est dense dans $\mathbb{R}$, soit $\ell \in \mathbb{R}$. Alors, pour tout entier naturel n , $X \cap]\ell - \frac{1}{n+1}, \ell + \frac{1}{n+1}[$ est non vide et l'on peut donc construire une suite u d'éléments de X telle que, pour tout entier naturel n , $\ell - \frac{1}{n+1} \leq u_n \leq \ell + \frac{1}{n+1}$. Par encadrement, u converge vers ℓ .

Réciproquement, soit une telle partie X , montrons que X est dense dans $\mathbb{R}$. Soit I un intervalle ouvert non vide de $\mathbb{R}$. Si $I \cap X = \emptyset$, il suffit de prendre ℓ comme étant le milieu de I : aucune suite à valeurs dans X ne peut converger vers ℓ . En effet, en considérant ε le quart du diamètre de I , on a, pour tout $x \in X$, $|x - \ell| > \varepsilon$. Ainsi, X rencontre I . $\square$

Proposition 4.0.4.

Soit X une partie non vide de $\mathbb{R}$. Alors il existe une suite u à valeurs dans X de limite $\sup X$.

1. Si X est majorée, $\sup X \in \mathbb{R}$ et u converge.
2. Si X n'est pas majorée, alors $\sup X = +\infty$ et u tend vers $+\infty$.

Démonstration.

Si X n'est pas majorée, c'est facile : pour tout $n \in \mathbb{N}$, il existe $x \in X$ vérifiant $x \geq n$. On construit donc une suite u à valeurs dans X vérifiant $\forall n \in \mathbb{N}, u_n \geq n$.

Si X est majorée, revenir à la caractérisation de la borne supérieure dans le cas réel donnée dans le chapitre VIII. $\square$

Remarque 4.0.5.

Un résultat analogue existe concernant la borne inférieure.

Exercice 4.0.6.

Soit X une partie non vide de $\mathbb{R}$ majorée par un réel a tel qu'il existe une suite u à valeurs dans X de limite a . Montrer que $a = \sup X$.

5 Suites particulières.

5.1 Suites arithmétiques.

Définition 5.1.1.

Soit α et r deux complexes. On appelle *suite arithmétique* de premier terme α et de *raison* r la suite u définie par

$$\begin{cases} u_0 = \alpha, \\ \forall n \in \mathbb{N}, u_{n+1} = r + u_n. \end{cases}$$

Remarque 5.1.2.

Une suite arithmétique est à valeurs réelles si et seulement si son premier terme et sa raison sont réels.

Remarque 5.1.3.

u est arithmétique de raison r si et seulement si

$$(u_{n+1} - u_n)_{n \in \mathbb{N}} = (r)_{n \in \mathbb{N}}.$$

On peut voir cela comme une équation portant sur une transformation linéaire de u .

Ce que l'on pourrait appeler « l'équation homogène associée » a pour solution toutes les suites constantes.

Le résultat suivant montre d'ailleurs que l'ensemble des suites arithmétiques de raison r est de la forme « solution particulière + solutions homogènes ».

Proposition 5.1.4.

Soit $r \in \mathbb{C}$ et u une suite arithmétique de raison r . Alors $\forall n \in \mathbb{N}, u_n = nr + u_0$. De plus

$$\forall n \in \mathbb{N} \quad \sum_{k=0}^n u_k = (n+1) \frac{u_0 + u_n}{2}.$$

Démonstration.

Revenir à la formule donnant $\sum_{k=0}^n k$. $\square$

Remarque 5.1.5.

Cette dernière formule est assez peu utile, il vaut souvent mieux revenir à la formule donnant $\sum_{k=0}^n k$.

Proposition 5.1.6.

Soit $r \in \mathbb{R}$ et u une suite arithmétique à valeurs réelles de raison r . Alors,

- si $r > 0$, $u_n \xrightarrow{n \rightarrow +\infty} +\infty$;
- si $r = 0$, u est la suite constante de valeur u_0 donc $u_n \xrightarrow{n \rightarrow +\infty} u_0$;
- si $r < 0$, $u_n \xrightarrow{n \rightarrow +\infty} -\infty$.

5.2 Suites géométriques.

Définition 5.2.1.

Soit α et r deux complexes. On appelle *suite géométrique* de premier terme α et de *raison* r la suite u définie par

$$\begin{cases} u_0 = \alpha, \\ \forall n \in \mathbb{N}, u_{n+1} = r \cdot u_n. \end{cases}$$

Remarque 5.2.2.

Une suite géométrique est à valeurs réelles si et seulement si son premier terme est nul ou son premier terme et sa raison sont réels.

Remarque 5.2.3.

u est géométrique de raison r si et seulement si

$$(u_{n+1} - ru_n)_{n \in \mathbb{N}} = (0)_{n \in \mathbb{N}}.$$

On peut voir cela comme une équation homogène portant sur une transformation linéaire de u .

Le résultat suivant montre d'ailleurs que l'ensemble des suites géométriques de raison q a la structure habituelle d'un ensemble de solutions homogènes.

Proposition 5.2.4.

Soit $r \in \mathbb{C}$ et u une suite géométrique de raison r . Alors $\forall n \in \mathbb{N}$, $u_n = r^n u_0$. De plus

- si $r \neq 1$, alors

$$\forall n \in \mathbb{N}, \sum_{k=0}^n u_k = u_0 \sum_{k=0}^n r^k = u_0 \frac{1 - r^{n+1}}{1 - r};$$

- si $r = 1$, alors

$$\forall n \in \mathbb{N} \quad \sum_{k=0}^n u_k = (n+1)u_0.$$

Démonstration.

Revenir à la formule donnant $\sum_{k=0}^n r^k$. □

Proposition 5.2.5.

Soit $r \in \mathbb{R}$ et u une suite réelle géométrique de raison r , avec $u_0 \neq 0$.

- Si $r \in]-\infty, -1]$, alors u n'a pas de limite (ni finie, ni infinie).
- Si $r \in]-1, 1[$ (i.e. $|r| < 1$), alors u converge vers 0.
- Si $r = 1$, alors u est la suite constante, de valeur u_0 (elle converge donc vers u_0).
- Si $r \in]1, +\infty[$, alors u diverge vers $+\infty$ si $u_0 > 0$ et vers $-\infty$ sinon.
- La suite u converge si et seulement si $r \in]-1, 1]$ (c'est-à-dire $|r| < 1$ ou $r = 1$).

Démonstration.

Direct d'après la proposition précédente. □

On peut aussi énoncer les résultats de convergence dans $\mathbb{C}$ (voir la partie 7 pour une définition précise de la notion de limite de suite de complexes).

Proposition 5.2.6.

Soit $r \in \mathbb{C}$ et u une suite complexe géométrique de raison r , avec $u_0 \neq 0$.

- La suite u converge si et seulement si $|r| < 1$ ou $r = 1$.
- Si $|r| < 1$, alors u tend vers 0.

Démonstration.

Il suffit de voir que $|u|$ est géométrique de raison $|r|$. Le cas où $r \in \mathbb{U} \setminus \{-1, 1\}$ sera traité en TD. □

5.3 Suites arithmético-géométriques.

Définition 5.3.1.

Une suite u est dite suite *arithmético-géométrique* s'il existe deux nombres complexes a et b vérifiant :

$$\forall n \in \mathbb{N}, u_{n+1} = au_n + b.$$

Remarque 5.3.2.

Il s'agit d'une généralisation des notions de suites arithmétiques et géométriques :

- Si $a = 1$, alors u est une suite arithmétique.
- Si $b = 0$, alors u est une suite géométrique.

Remarque 5.3.3.

Ces suites interviennent fréquemment dans des problèmes concrets :

- évolution du capital restant à rembourser en fonction du temps dans le cas d'un emprunt à mensualités constantes ;
- modélisation de l'évolution d'une population.

Soit a et b deux complexes. On s'intéresse maintenant à l'ensemble des suites u solutions de l'équation

$$\forall n \in \mathbb{N}, u_{n+1} = au_n + b. \quad (\text{AG})$$

Remarque 5.3.4.

On peut écrire cela

$$(u_{n+1} - au_n)_{n \in \mathbb{N}} = (b)_{n \in \mathbb{N}}.$$

Ce que l'on pourrait appeler « l'équation homogène associée » a pour solution toutes les suites géométriques de raison a .

Le résultat suivant montre d'ailleurs que l'ensemble des suites solutions de **AG** est de la forme « solution particulière + solutions homogènes ».

Proposition 5.3.5.

Soit v une solution de (**AG**) et u une suite. Alors u est solution de **AG** si et seulement si $u - v$ (*i.e.* la suite de terme général $u_n - v_n$ pour $n \in \mathbb{N}$) est géométrique de raison a .

Démonstration.

Très facile. □

Proposition 5.3.6.

Si $a \neq 1$, alors il existe une unique suite constante solution de (**AG**).

Démonstration.

Très facile. □

Remarque 5.3.7.

Si $a = 1$, on étudie une suite arithmétique ...

Méthode de résolution de (AG**)**

1. Si $a = 1$, les solutions de (**AG**) sont les suites arithmétiques de raison b (*i.e.* pour tout $u \in \mathbb{C}^{\mathbb{N}}$, u est solution de E si et seulement si $\forall n \in \mathbb{N}, u_n = u_0 + nb$).
2. Si $a \neq 1$, on cherche une solution constante. Pour cela, on détermine l'unique α vérifiant

$$\alpha = a\alpha + b.$$

3. Les solutions de (**AG**) sont alors les suites $u \in \mathbb{C}^{\mathbb{N}}$ telles que la suite $u - \alpha$ (*c'est-à-dire* $(u_n - \alpha)_{n \in \mathbb{N}}$) soit une suite géométrique de raison a . Autrement dit, les solutions de (**AG**) sont les suites $u \in \mathbb{C}^{\mathbb{N}}$ vérifiant :

$$\forall n \in \mathbb{N} \quad u_n = \alpha + a^n(u_0 - \alpha).$$

Remarque 5.3.8.

L'ensemble des solutions de (**AG**) a ici la même structure que dans les cas des systèmes linéaires et des équations différentielles linéaires (espace affine). Ce n'est pas une coïncidence ! Cela vient du fait que l'on résout $(u_{n+1} - au_n)_{n \in \mathbb{N}} = (b)_{n \in \mathbb{N}}$ et que $(u_{n+1} - u_n)_{n \in \mathbb{N}}$ dépend *linéairement* de u .

Exemple 5.3.9.

Donner le terme général de la suite u définie par :

$$\begin{cases} u_0 = 0, \\ \forall n \in \mathbb{N} \quad u_{n+1} = 2u_n + 1. \end{cases}$$

Exemple 5.3.10.

Votre banquier vous propose un prêt à la consommation de 10 000 € «à un taux de 18% annuel» sur 5 ans, à mensualités fixes (soit 60 mensualités). Après avoir signé le contrat, vous constatez que le taux est de 1,5% par mois. Quel est le montant des mensualités ? Quel est le coût total du crédit ? Que pensez-vous de la manière dont le prêt est présenté ?

5.4 Suites récurrentes linéaires doubles.**Définition 5.4.1.**

On appelle *équation de récurrence linéaire double* ou *équation de récurrence linéaire d'ordre deux* toute équation de la forme

$$\forall n \in \mathbb{N} \quad u_{n+2} + au_{n+1} + bu_n = 0.$$

où a et b sont des complexes fixés et où la suite u (réelle ou complexe) est l'inconnue.

Toute solution de cette équation est appelée suite *récurrente linéaire double* (ou *d'ordre deux*).

On appelle *équation caractéristique* de cette équation de récurrence linéaire double, l'équation

$$r^2 + ar + b = 0.$$

On appelle *polynôme caractéristique* de cette équation de récurrence linéaire double, le polynôme

$$X^2 + aX + b.$$

Remarque 5.4.2.

Si $r \in \mathbb{C}$, alors r est solution de l'équation caractéristique si et seulement si $(r^n)_{n \in \mathbb{N}}$ est solution de l'équation de récurrence linéaire double.

Soit $(a, b) \in \mathbb{C}^2$, avec $b \neq 0$. On s'intéresse maintenant à l'ensemble des suites u solution de

$$\forall n \in \mathbb{N} \quad u_{n+2} + au_{n+1} + bu_n = 0. \quad (\mathbf{E})$$

On note alors l'équation caractéristique de $(\mathbf{E})$:

$$r^2 + ar + b = 0. \quad (\mathbf{C})$$

Théorème 5.4.3 (Solutions complexes de $(\mathbf{E})$).
On considère l'équation $(\mathbf{E})$.

- (i) Si $(\mathbf{C})$ admet deux solutions distinctes r_1 et r_2 , les solutions de $(\mathbf{E})$ sont les suites de la forme $(\lambda r_1^n + \mu r_2^n)_{n \in \mathbb{N}}$, où λ et μ sont des complexes.
- (ii) Si $(\mathbf{C})$ admet une unique solution, r_0 , alors les solutions de $(\mathbf{E})$ sont les suites de la forme $(\lambda r_0^n + \mu n r_0^n)_{n \in \mathbb{N}}$, où λ et μ sont des complexes.

Dans les deux cas, il existe une unique solution à $(\mathbf{E})$ pour u_0 et u_1 fixés.

Démonstration.

La preuve n'est pas exigible, en voici un schéma.

1. Montrer que s'il existe une solution, elle est entièrement déterminée par la donnée de u_0 et u_1 .
2. Montrer selon les cas que les suites données dans l'énoncé du théorème sont effectivement *des* solutions.
3. Montrer, selon les cas, que pour tout choix de u_0 et u_1 , une de ces suites est solution.
4. En déduire selon les cas que les suites données dans l'énoncé du théorème sont effectivement *les* solutions.

□

Dans tout ce qui suit, on ne s'intéressera qu'au cas où les coefficients a et b sont réels.

Théorème 5.4.4 (Solutions réelles de $(\mathbf{E})$).
On considère l'équation $(\mathbf{E})$, avec $(a, b) \in \mathbb{R} \times \mathbb{R}^*$.

- (i) Si $(\mathbf{C})$ admet deux solutions (réelles) distinctes r_1 et r_2 , alors les solutions réelles de $(\mathbf{E})$ sont les suites de la forme $(\lambda r_1^n + \mu r_2^n)_{n \in \mathbb{N}}$, où λ et μ sont des réels.

(ii) Si $(\mathbf{C})$ admet une unique solution (réelle) r_0 , alors les solutions réelles de $(\mathbf{E})$ sont les suites de la forme $(\lambda r_0^n + \mu n r_0^n)_{n \in \mathbb{N}}$, où λ et μ sont des réels.

(iii) Si $(\mathbf{C})$ admet deux solutions complexes conjuguées, $re^{i\theta}$ et $re^{-i\theta}$, alors les solutions réelles de $(\mathbf{E})$ sont les suites de la forme $(r^n(\lambda \cos(n\theta) + \mu \sin(n\theta)))_{n \in \mathbb{N}}$ où λ et μ sont des réels.

Dans tous les cas, il existe une unique solution à $(\mathbf{E})$ pour u_0 et u_1 fixés.

Remarque 5.4.5.

En pratique, on rencontrera des suites définies par la valeur de u_0 et u_1 et une équation linéaire de récurrence d'ordre deux. On détermine alors les solutions générales de l'équation en utilisant le théorème ci-dessus, puis on détermine les constantes λ et μ avec les valeurs de u_0 et u_1 .

Démonstration.

La preuve n'est pas exigible, en voici un schéma.

1. Montrer, en étudiant les différents cas que les suites données ci-dessus sont effectivement des solutions.
2. Montrer en étudiant les différents cas, que toute solution est une suite donnée ci-dessus (astuce bien pratique : si u est une solution à valeurs réelles de $(\mathbf{E})$, alors, pour tout $n \in \mathbb{N}$, $u_n = \operatorname{Re}(u_n)$ et u est aussi une solution complexe de $(\mathbf{E})$).
3. En déduire que les suites données dans l'énoncé du théorème sont effectivement *les* solutions.

□

Exemple 5.4.6 (Application pratique).

On considère la suite $(u_n)_{n \in \mathbb{N}}$ définie par

$$\begin{cases} u_0 = 0 \text{ et } u_1 = 1 \\ \forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n \end{cases}$$

Déterminer une expression de u_n en fonction de n .

Remarque 5.4.7.

La méthode vue ici est très proche de celle utilisée pour résoudre les équations différentielles linéaires de degré deux à coefficients constants. Ce n'est d'ailleurs pas une coïncidence ...

6 Suites définies par une relation de récurrence d'ordre 1.

On étudie dans cette partie *les suites (réelles) récurrentes d'ordre 1*, c'est-à-dire les suites réelles u vérifiant une relation du type : $\forall n \in \mathbb{N}, u_{n+1} = f(u_n)$, où f est une fonction définie sur une partie D de $\mathbb{R}$ et à valeur dans $\mathbb{R}$.

6.1 Définition de la suite.

On se donne donc une partie D de $\mathbb{R}$, $f : D \rightarrow \mathbb{R}$, et $a \in \mathbb{R}$. On veut définir la suite u par récurrence de la façon suivante

$$\begin{cases} u_0 = a \\ \text{et } \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

Une telle définition n'est pas nécessairement légitime : par exemple, si $a \notin D$, alors u_1 est mal défini donc la suite est mal définie. Autre exemple : on prend pour f l'application $x \mapsto \sqrt{x} - 1$ et pour a la valeur 4. On a bien $a \in \mathbb{R}^+$ mais $u_1 = 1$, $u_2 = 0$, $u_3 = -1 < 0$ et u_4 est mal défini.

Une condition suffisante¹ pour que la suite soit bien définie est de trouver une partie A de D (i.e. une partie A de $\mathbb{R}$ sur laquelle f est bien définie) *stable par f* (i.e. $\forall x \in A, f(x) \in A$) et contenant le premier terme de la suite ($a \in A$).

En notant, pour $n \in \mathbb{N}$, $P(n)$ la propriété « u_n est bien définie et $u_n \in A$ », on peut alors montrer par récurrence que pour tout $n \in \mathbb{N}$, on a $P(n)$; on en déduit que pour tout $n \in \mathbb{N}$, u_n est bien définie, donc que u est bien définie.

Exemple 6.1.1. 1. Soit $a \in [-1, +\infty[$, et notons u la suite définie par

$$\begin{cases} u_0 = a \\ \text{et } \forall n \in \mathbb{N} \ u_{n+1} = \sqrt{1 + u_n} \end{cases}$$

Notons f la fonction $x \mapsto \sqrt{1 + x}$. Alors l'ensemble de définition $[-1, +\infty[$ est stable par f . Donc la suite $(u_n)_{n \in \mathbb{N}}$ est bien définie.

1. Cette condition est aussi nécessaire (pourquoi ?) mais en pratique, c'est le fait qu'elle soit suffisante qui nous intéressera.

2. Notons v la suite définie par

$$\begin{cases} v_0 = 5 \\ \text{et } \forall n \in \mathbb{N} \ v_{n+1} = v_n^{\frac{3}{2}} - 1 \end{cases}$$

Posons

$$\begin{aligned} f : \mathbb{R}^+ &\rightarrow \mathbb{R} \\ x &\mapsto x^{\frac{3}{2}} - 1 \end{aligned}$$

L'ensemble de définition de f est $\mathbb{R}^+$, qui n'est pas stable par f puisque $f(0) \notin \mathbb{R}^+$. En revanche, en posant $A = [4, +\infty[$, on peut remarquer que A est une partie de l'ensemble de définition de f stable par f : en effet, f est croissante sur $\mathbb{R}^+$ et $f(4) = 7 \geq 4$ donc pour tout $x \in A$, on a $f(x) \geq f(4) \geq 4$ donc $f(x) \in A$. Or 5 appartient à A donc on peut montrer que v est bien définie.

Dans toute la suite, A désigne une partie de $\mathbb{R}$, et f une application définie (au moins) sur A et telle que $f(A) \subset A$ et a un élément de A .

6.2 Recherche d'une limite éventuelle.

Proposition 6.2.1.

Si la suite $(u_n)_{n \in \mathbb{N}}$ converge vers un réel ℓ et f est continue en ℓ , alors $f(\ell) = \ell$. On dit que ℓ est un *point fixe* de f .

Remarque 6.2.2.

Cette proposition sert à déterminer les limites *éventuelles* de la suite $(u_n)_{n \in \mathbb{N}}$ ou à montrer qu'elle n'admet pas de limite.



En aucun cas, elle ne permet de montrer que u a une limite.

Exemple 6.2.3. • Étudier la convergence de la suite $(u_n)_{n \in \mathbb{N}}$ définie par

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = u_n^2 + 1 \end{cases}$$

• Étudier la convergence de la suite $(u_n)_{n \in \mathbb{N}}$ définie par

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = u_n^2 + \frac{1}{4} \end{cases}$$

6.3 Cas où f est croissante sur A .

Proposition 6.3.1.

Si f est une fonction *croissante* sur A : alors la suite u est *monotone*. Plus précisément :

- si $u_0 \leq u_1$, alors u est croissante ;
- si $u_0 \geq u_1$, alors u est décroissante.

Démonstration.

Montrons le premier point (le second est similaire). Supposons f croissante sur A et $u_0 \leq u_1$. Alors, pour $n \in \mathbb{N}$, notons $P(n)$ l'assertion « $u_n \leq u_{n+1}$ ».

- On a $u_0 \leq u_1$ donc on a $P(0)$.
- Soit $n \in \mathbb{N}$, supposons $P(n)$. Alors on a $u_n \leq u_{n+1}$. Or f est croissante sur A , donc $f(u_n) \leq f(u_{n+1})$, donc $u_{n+1} \leq u_{n+2}$, donc on a $P(n+1)$.

On a donc, d'après le principe de récurrence, $\forall n \in \mathbb{N} \ u_n \leq u_{n+1}$. $\square$

Remarque 6.3.2.

Vous n'avez pas besoin de retenir cette proposition. En revanche, vous devez retenir la technique de démonstration pour être en mesure de l'adapter à un cas concret.

Exemple 6.3.3.

Étudier, pour $a = 0$ et pour $a = 2$, la suite u définie par

$$\begin{cases} u_0 = a, \\ \forall n \in \mathbb{N}, u_{n+1} = \sqrt{1 + u_n}. \end{cases}$$

Exemple 6.3.4.

Étudier la suite u définie par

$$\begin{cases} u_0 = 0, \\ \forall n \in \mathbb{N}, u_{n+1} = u_n^2 + 2u_n + 1. \end{cases}$$

La suite u admet-elle une limite ? laquelle ?

Exercice 6.3.5.

Montrer qu'une fonction croissante et continue $f : I \rightarrow I$, où I est un segment, possède un point fixe.

6.4 Cas où f est décroissante sur A .

Proposition 6.4.1.

Si f est une fonction *décroissante* sur A , alors les suites $(u_{2n})_{n \in \mathbb{N}}$ et $(u_{2n+1})_{n \in \mathbb{N}}$ sont monotones et de sens contraire. Plus précisément :

- si $u_0 \leq u_2$, alors $(u_{2n})_{n \in \mathbb{N}}$ est croissante et $(u_{2n+1})_{n \in \mathbb{N}}$ est décroissante ;
- si $u_0 \geq u_2$, alors $(u_{2n})_{n \in \mathbb{N}}$ est décroissante et $(u_{2n+1})_{n \in \mathbb{N}}$ est croissante.

Démonstration.

Montrons le premier point (le second se montre de la même façon).

Supposons f décroissante. Alors $f \circ f$ est croissante.

Supposons de plus $u_0 \leq u_2$.

Montrons alors que $(u_{2n})_{n \in \mathbb{N}}$ est croissante et $(u_{2n+1})_{n \in \mathbb{N}}$ est décroissante.

En posant $v = (u_{2n})_{n \in \mathbb{N}}$, on a $\forall n \in \mathbb{N}, v_{n+1} = (f \circ f)(v_n)$ et $v_0 \leq v_1$.

Donc v est croissante, d'après la proposition 6.3.1.

On a donc $\forall n \in \mathbb{N}, u_{2n} \leq u_{2n+2}$.

f étant décroissante, on en déduit $\forall n \in \mathbb{N}, f(u_{2n}) \geq f(u_{2n+2})$.

Donc $\forall n \in \mathbb{N}, u_{2n+1} \geq u_{2n+3}$. $\square$

Remarque 6.4.2.

Même remarque que pour la proposition 6.4.1.

Exemple 6.4.3.

Étudier la suite u définie par

$$\begin{cases} u_0 = 2, \\ \forall n \in \mathbb{N}, u_{n+1} = 2 - \sqrt{u_n}. \end{cases}$$

Remarque 6.4.4.

On remarquera que, quelle que soit la situation, la plupart des informations pertinentes pour l'étude d'une suite définie par $u_{n+1} = f(u_n)$ sont données par le signe de $f - \text{Id}$. Dans tout exercice sur les suites définies par récurrence, il est fondamental de déterminer le tableau des signes de $f - \text{Id}$.

7 Suites à valeurs complexes.

Nous allons définir la notion de convergence de suites à valeurs complexes en s'appuyant sur les convergences des suites (réelles) des parties réelles et imaginaires associées.

On pourrait définir de manière intrinsèque cette convergence, le lecteur intéressé se rapportera à la partie ??.

Soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite à valeurs complexes. Notons $\text{Re}(u)$ la suite $\text{Re}(u_n)_{n \in \mathbb{N}}$, $\text{Im}(u)$ la suite $\text{Im}(u_n)_{n \in \mathbb{N}}$ et $|u|$ la suite $|u_n|_{n \in \mathbb{N}}$.

Soit alors ℓ un complexe.

Remarque 7.0.1. 1. On rappelle que pour tout complexe z , on a

$$\begin{aligned} |z| &\leq |\operatorname{Re}(z)| + |\operatorname{Im}(z)| \\ |\operatorname{Re}(z)| &\leq |z| \\ |\operatorname{Im}(z)| &\leq |z| \end{aligned}$$

2. En particulier, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} |u_n - \ell| &\leq |\operatorname{Re}(u_n) - \operatorname{Re}(\ell)| \\ &\quad + |\operatorname{Im}(u_n) - \operatorname{Im}(\ell)| \\ |\operatorname{Re}(u_n) - \operatorname{Re}(\ell)| &\leq |u_n - \ell| \\ |\operatorname{Im}(u_n) - \operatorname{Im}(\ell)| &\leq |u_n - \ell| \end{aligned}$$

Proposition 7.0.2.

On a

$$|u_n - \ell| \xrightarrow{n \rightarrow +\infty} 0$$

si et seulement si

$$\operatorname{Re}(u_n) \xrightarrow{n \rightarrow +\infty} \operatorname{Re}(\ell) \text{ et } \operatorname{Im}(u_n) \xrightarrow{n \rightarrow +\infty} \operatorname{Im}(\ell).$$

Définition 7.0.3.

On dit que u converge vers ℓ si

$$|u_n - \ell| \xrightarrow{n \rightarrow +\infty} 0.$$

Démonstration.

C'est une conséquence directe de la remarque précédente. $\square$

Remarque 7.0.4. 1. Cette définition étend la définition de la convergence pour les suites à valeurs réelles.

2. Il n'y a pas de notion similaire à $+\infty$ et $-\infty$ sur $\mathbb{C}$, donc pas de notion de limite infinie pour les suites à valeurs complexes (mais on peut regarder si $|u|$ tend vers $+\infty$).
3. Les résultats usuels sur les suites à valeurs réelles s'étendent naturellement aux suites à valeurs complexes... sauf ceux qui font appel à l'ordre sur $\mathbb{R}$ vu qu'il n'y a pas d'ordre «raisonnable» sur $\mathbb{C}$.

La proposition suivante peut être utile.

Proposition 7.0.5.

$$u \xrightarrow{+\infty} \ell \Rightarrow |u_n| \xrightarrow{n \rightarrow +\infty} |\ell|$$

Démonstration.

De la définition 7.0.3 et de l'inégalité triangulaire :

$$\forall n \in \mathbb{N} \quad ||u_n| - |\ell|| \leq |u_n - \ell|$$

on déduit immédiatement $|u_n| \xrightarrow{n \rightarrow +\infty} |\ell|$, d'où le résultat. $\square$

Remarque 7.0.6. 1. La réciproque est évidemment fautive

2. Cette proposition permet notamment d'assurer que si u a une limite ℓ non nulle alors, à partir d'un certain rang, $|u|$ est compris entre $\frac{1}{2}|\ell|$ et $\frac{3}{2}|\ell|$.

Proposition 7.0.7.

Soit u, v deux suites complexes convergeant respectivement vers ℓ et ℓ' , soit $\lambda, \mu \in \mathbb{C}$. Alors $\lambda u + \mu v$ converge, vers $\lambda\ell + \mu\ell'$.

Définition 7.0.8.

On dit que u est bornée si son module l'est.

Remarque 7.0.9.

C'est équivalent au fait que $\operatorname{Re}(u)$ et $\operatorname{Im}(u)$ soient bornées.

Proposition 7.0.10.

Toute suite complexe convergente est bornée.

Théorème 7.0.11 (Bolzano-Weierstrass).

De toute suite à valeurs complexes bornée, on peut extraire une sous-suite convergente.

Démonstration (non exigible).

Considérons une suite u à valeurs complexes bornées. Notons r et j respectivement les suites $\operatorname{Re}(u)$ et $\operatorname{Im}(u)$.

r et j sont bornées et à valeurs réelles. D'après le théorème de Bolzano-Weierstrass sur les suites à valeurs réelles, on peut donc extraire de chacune une sous-suite convergente. Pourtant cela ne suffit pas à montrer le résultat. Pourquoi ?

Considérons φ une extraction de r telle que $r \circ \varphi$ converge.

Alors $j \circ \varphi$ est bornée. On peut donc en trouver une extraction ψ telle que $j \circ \varphi \circ \psi$ converge.

$r \circ \varphi$ converge donc $r \circ \varphi \circ \psi$ converge vers la même valeur.

Or $r \circ \varphi \circ \psi = \operatorname{Re}(u \circ \varphi \circ \psi)$ et $j \circ \varphi \circ \psi = \operatorname{Im}(u \circ \varphi \circ \psi)$.

Donc $u \circ \varphi \circ \psi$ converge. $\square$

8 Premiers exemples de séries numériques.

Les séries numériques sont des cas particuliers de suites, que nous étudierons en fin d'année. Nous pouvons cependant commencer à étudier quelques exemples significatifs.

8.1 Séries télescopiques.

Soit $(u_n)_{n \in \mathbb{N}}$ une suite à valeurs complexes.

Proposition 8.1.1.

Les suites $(u_n)_{n \in \mathbb{N}}$ et $\left(\sum_{k=0}^N (u_{k+1} - u_k)\right)_{N \in \mathbb{N}}$ ont même nature.

Dans le cas de convergence, si $u_n \xrightarrow{n \rightarrow +\infty} \ell$, alors

$$\sum_{k=0}^N u_{k+1} - u_k \xrightarrow{N \rightarrow +\infty} \ell - u_0.$$

Démonstration.

Nous savons déjà que les suites $(u_n)_{n \in \mathbb{N}}$ et $(u_{n+1})_{n \in \mathbb{N}}$ ont même nature.

De plus la somme $\sum_{k=0}^N (u_{k+1} - u_k)$ vaut $u_{N+1} - u_0$ par sommation télescopique. Elle est donc égale au terme u_{N+1} ,

à une constante près, et la suite $\left(\sum_{k=0}^N (u_{k+1} - u_k)\right)_{N \in \mathbb{N}}$ a donc la même nature que la suite $(u_{n+1})_{n \in \mathbb{N}}$.

Dans le cas de convergence, il reste à passer à la limite dans la relation $\sum_{k=0}^N (u_{k+1} - u_k) = u_{N+1} - u_0$. $\square$

8.2 Séries géométriques.

Soit z un nombre complexe, p un entier naturel.

Proposition 8.2.1.

La suite $\left(\sum_{n=p}^N z^n\right)_{N \in \mathbb{N}}$ converge si et seulement si $|z| < 1$. Le cas échéant,

$$\sum_{n=p}^N z^n \xrightarrow{N \rightarrow +\infty} \frac{z^p}{1-z}.$$

Démonstration.

C'est une conséquence directe de la formule de sommation géométrique :

$$\sum_{n=p}^N z^n = \frac{z^p}{1-z} - \frac{z^{N+1}}{1-z} \text{ si } z \neq 1 \text{ et } N+1-p \text{ sinon.}$$

Il suffit donc de voir que si $z \neq 1$, (z^{N+1}) converge si et seulement si $|z| < 1$ et, dans le cas de convergence, converge vers 0.

Le cas $|z| \neq 1$ s'obtient aisément en considérant le module. Le cas $|z| = 1$ est un exercice classique et sera traité en TD. $\square$

Chapitre XIII

Groupes, anneaux, corps

Sommaire

1	Lois de composition internes.	186
1.1	Définition.	186
1.2	Propriétés usuelles des loi.	186
2	Structure de groupe.	188
2.1	Définition et exemples.	188
2.2	Sous-groupes.	188
2.3	Morphismes de groupes.	189
3	Anneaux	193
3.1	Structure d'anneau.	193
3.2	Sous-anneaux	195
3.3	Morphismes d'anneaux	195
4	Structure de corps.	196

On remarque que dans des domaines a priori distincts, des similitudes apparaissent, notamment concernant les structures. Pour avoir une théorie générale, on définit des structures algébriques abstraites, on en démontre les propriétés, puis on les applique dans les exemples mathématiques qui vérifient ces structures.

Dans ce chapitre on s'intéresse aux structures algébriques de base : groupes, anneaux et corps. Plus tard, nous étudierons une structure fondamentale : celle d'espace vectoriel.

1 Lois de composition internes.

Dans tout ce chapitre, E est un ensemble.

1.1 Définition.

Définition 1.1.1.

On appelle *loi de composition interne sur E* (lci) toute application de $E \times E$ dans E .

- Cette définition a déjà été vue, ainsi que des exemples, dans le chapitre IV sur les complexes.

Remarque 1.1.2.

On appelle *magma* tout couple constitué d'un ensemble et d'une lci.

Exemple 1.1.3.

$(\mathbb{Z}, -)$ est un magma, mais pas $(\mathbb{N}, -)$, car $-4 \notin \mathbb{N}$.

Dans toute la suite, $*$ est une lci sur E .

1.2 Propriétés usuelles des lci.

Définition 1.2.1.

Soit $(E, *)$ un magma.

1. On dit que E est *associatif* si pour tout $x, y, z \in E$, on a : $x * (y * z) = (x * y) * z$. L'élément $x * (y * z) = (x * y) * z$ est alors noté $x * y * z$.
2. On dit que E est *commutatif* si pour tout $x, y \in E$, on a : $x * y = y * x$.

3. Soit $\top$ une seconde lci sur E . On dit que dans E $*$ est *distributive* par rapport à $\top$ si pour tout $x, y, z \in E$, on a :

- $x * (y \top z) = (x * y) \top (x * z)$;
- $(y \top z) * x = (y * x) \top (z * x)$.

Remarque 1.2.2.

On dit que dans E $*$ est *distributive à gauche* par rapport à $\top$ si pour tout $x, y, z \in E$, on a : $x * (y \top z) = (x * y) \top (x * z)$.

De même, on a la notion de *distributivité à droite*.

Exemple 1.2.3.

- $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ avec $+$ ou $\times$ sont associatifs, mais pas $(\mathbb{Z}, -)$ car $1 - (2 - 3) \neq (1 - 2) - 3$, ni $(\mathbb{R}^3, \wedge)$.
- $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ avec $+$ ou $\times$ sont commutatifs, mais pas $(\mathbb{Z}, -)$ ni $(\mathbb{R}^3, \wedge)$, ni $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$.
- Sur $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ $\times$ est distributive par rapport à $+$, et sur $\mathcal{P}(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.

Définition 1.2.4. 1. Soit $e \in E$. on dit que e est un *élément neutre à gauche* (resp. à droite) pour $*$ si pour tout $x \in E$ on a $e * x = x$ (resp. $x * e = x$). On dit que e est un *élément neutre* pour $*$ si c'est un élément neutre à gauche et à droite, i.e. pour tout $x \in E$, $e * x = x * e = x$.

2. Soit e un neutre pour $*$ et soit $x \in E$. On dit que x est *inversible à gauche* (resp. à droite) s'il existe un élément $y \in E$ tel que $y * x = e$ (resp. $x * y = e$). Un tel élément y s'appelle *UN inverse à gauche* (resp. à droite) de x . On dit que x est *inversible* s'il est inversible à gauche et à droite, i.e. il existe $y \in E$ tel que $y * x = x * y = e$. Dans ce cas y est *UN inverse* de x .

Exemple 1.2.5.

- 0 est un élément neutre pour $+$ dans $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$.
- 1 est un élément neutre pour $\times$ dans $\mathbb{R}, \mathbb{C}, \mathbb{Q}$.
- Id est un élément neutre pour $\circ$ dans $\mathcal{F}(E, E)$, et les bijections sont tous les éléments inversibles de cet ensemble.

• Par contre $(\mathbb{R}^3, \wedge)$ n'a pas de neutre. S'il y avait un neutre u , on devrait avoir $u \wedge u = u$, mais $u \wedge u = 0$, donc $u = 0$. Mais pour tout $v \neq 0$, on a $u \wedge v = 0$, et non $u \wedge v = v$.



Être inversible d'un seul côté ne suffit pas pour être inversible tout court : un exemple a été vu dans le TD du chapitre sur les applications (ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$ muni de $\circ$).

Remarque 1.2.6.

Un neutre est toujours inversible et est son propre inverse.

Proposition 1.2.7.

Si $*$ admet un neutre, alors ce neutre est unique.

Démonstration.

Soient e et e' deux neutres.¹ Alors $e * e' = e$ et $e * e' = e'$, donc $e = e'$. $\square$

Proposition 1.2.8.

On suppose la loi $*$ associative, et admettant un neutre e . Si un élément est inversible, alors il a un seul inverse.

Démonstration.

Soient y et y' deux inverses² de $x \in E$. Alors $y * x = e$ et $x * y' = e$. Donc $y * (x * y') = y * e = y$ et $(y * x) * y' = e * y' = y'$, d'où $y = y'$. $\square$

1. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que e est neutre à gauche et e' neutre à droite. Donc en fait tout neutre à gauche est égal à tout neutre à droite, d'où l'on déduit d'une part que l'existence d'un neutre à gauche et d'un neutre à droite suffit à assurer l'existence d'un neutre et d'autre part que ce neutre est alors le seul neutre à gauche et le seul neutre à droite. Pour qu'un élément ait plusieurs neutres à gauche, il est donc nécessaire (mais pas suffisant) qu'il n'ait aucun neutre à droite et *vice-versa*.

2. On pourra remarquer que dans cette démonstration on utilise uniquement le fait que y est inverse à gauche et y' inverse à droite. Donc en fait tout inverse à gauche est égal à tout inverse à droite, d'où l'on déduit d'une part que l'existence d'un inverse à gauche et d'un inverse à droite pour x suffit à assurer l'existence d'un inverse et d'autre part que cet inverse est alors le seul inverse à gauche et le seul inverse à droite de x . Pour qu'un élément ait plusieurs inverses à gauche, il est donc nécessaire qu'il n'ait aucun inverse à droite et *vice-versa*.

Remarque 1.2.9.

On utilise souvent les notations additives et multiplicatives.

- En notation additive, $+$ est en général notée $+$, $\underbrace{x + x + \dots + x}_{n \text{ fois}}$ se note nx , et si x est inversible, son inverse se note $-x$. On l'appelle alors plutôt *l'opposé de x* . De même, on notera le neutre d'une telle structure 0 , ou 0_E .
- En notation multiplicative, $*$ est en général remplacée par $\times$ (et ce symbole est même souvent omis), $\underbrace{x \times x \times \dots \times x}_{n \text{ fois}}$ se note x^n et si x est inversible, son inverse se note x^{-1} . De même, on notera le neutre d'une telle structure 1 , ou 1_E .

Pour éviter toute erreur, on essaiera au maximum de n'utiliser la notation additive que pour des lois qui ont les mêmes propriétés que la loi $+$ sur $\mathbb{R}$. Par exemple, noter $+$ une loi non commutative peut-être déroutant, ainsi que pour une loi pour laquelle tous les éléments ne sont pas inversibles. La notation $+$ est en général réservée à des lois commutatives et pour lesquelles les éléments sont tous inversibles..

Ce n'est pas le cas pour la notation multiplicative, qui est la plus couramment utilisée pour des lois associatives, mais sans plus. Par exemple il est fréquent d'utiliser $\times$ même pour une loi non commutative et pour laquelle les éléments ne sont pas tous inversibles. Donc faites attention, par défaut on aura $xy \neq yx$, et x^{-1} n'existera pas forcément !

Dans toute la suite, on adoptera la notation multiplicative, et on suppose que E a un neutre noté 1 .

Proposition 1.2.10.

On suppose la loi $*$ associative. Soient $x, y, z \in E$.

- Simplification par un inversible : si x est inversible, alors $x * y = x * z \Leftrightarrow y = z$.
- Inverse d'un produit : si x et y sont inversibles alors $x * y$ l'est aussi et $(x * y)^{-1} = y^{-1} * x^{-1}$. **Attention** : l'inverse de $x * y$ n'a aucune raison d'être $x^{-1} * y^{-1}$.

(iii) Puissances négatives : si x est inversible, on pose pour $n \in \mathbb{N}^*$, $x^{-n} = (x^{-1})^n$. Alors $x^{-n} = (x^n)^{-1}$.

(iv) Inverse d'un inverse : si x est inversible, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.

Démonstration. (iii) Par récurrence. Vrai si $n = 0$ ou 1 . Si vrai pour n , alors $x^{n+1} * x^{-n-1} = x^n * x * x^{-1} * x^{-n} = x^n * e * x^{-n} = x^n * x^{-n} = e$.

(iv) Vrai par unicité de l'inverse. $\square$

Définition 1.2.11.

Soit $(E, *)$ un magma et F une partie de E . On dit que F est une *partie stable* (de E par $*$) si pour tous $x, y \in F$, $x * y \in F$.

Exemple 1.2.12.

$\{-1, 1\}$ est une partie stable de $(\mathbb{R}, \times)$, mais pas $\{-2, 2\}$.

2 Structure de groupe.

2.1 Définition et exemples.

Définition 2.1.1.

On appelle *groupe* tout ensemble muni d'une loi de composition interne associative, ayant un élément neutre, et dont tout élément est inversible.

Si un groupe est *commutatif* (ce qui signifie en fait que sa loi est commutative), il est dit *abélien*.

Par défaut on utilise la notation multiplicative pour un groupe, sauf pour les groupes abéliens pour lesquels on utilise la notation additive.

Exemple 2.1.2.

- $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sont des groupes avec la loi $+$, mais pas avec la loi $\times$.
- Pour $n \in \mathbb{N}^*$, $\mathbb{C}^n, \mathbb{R}^n, \mathbb{Q}^n, \mathbb{Z}^n$ sont des groupes avec la loi $+$.
- $\mathbb{C} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{Q} \setminus \{0\}$, sont des groupes avec la loi $\times$.
- $\mathbb{N}$ n'est un groupe ni avec la loi $+$ ni avec la loi $\times$.

Exemple 2.1.3.

En spé, vous manipulerez le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, que l'on peut voir comme « l'ensemble des congruences modulo n », avec $n \in \mathbb{N}^*$.

Définition 2.1.4.

Soit X un ensemble non vide. On appelle *groupe des permutations de X* l'ensemble des bijections de X dans X . Comme son nom l'indique, c'est un groupe, si on le munit de la loi de composition $\circ$. On le note S_X (on trouvera parfois la notation $\mathfrak{S}(X)$).

Démonstration.

L'application identité, $\text{Id} : X \rightarrow X, x \mapsto x$, est évidemment une bijection de X , donc S_X est non vide.

On sait déjà que la composée de deux bijections est une bijection, donc $\circ$ est une loi sur S_X . Il est évident que Id en est le neutre. On sait également que cette loi est associative, et que la réciproque d'une bijection est encore une bijection. Cela assure que $(S_X, \circ)$ est un groupe. $\square$

2.2 Sous-groupes.

Dans toute la suite, $(G, *)$ est un groupe de neutre e . On adopte la notation *multiplicative*.

Définition 2.2.1.

On appelle *sous-groupe* de G tout ensemble H vérifiant les propriétés suivantes :

- (i) $H \subset G$;
- (ii) $e \in H$;
- (iii) Stabilité par produit : $\forall x, y \in H, x * y \in H$;
- (iv) Stabilité par passage à l'inverse : $\forall x \in H$, on a $x^{-1} \in H$.

Remarque 2.2.2 (peu utile, mais traditionnelle).

En vertu des points (iii) et (iv), le point (ii) peut être remplacé par $H \neq \emptyset$.

Exemple 2.2.3.

Sont des sous-groupes :

- $\{e\}$ et G dans $(G, *)$.
- $\mathbb{U}$ dans $(\mathbb{C}^*, \times)$.
- $n\mathbb{Z}$ dans $(\mathbb{Z}, +)$.
- $H = \{f \in S_{\mathbb{R}} \mid f(0) = 0\}$ dans $(S_{\mathbb{R}}, \circ)$.

Proposition 2.2.4.

Un ensemble H est un sous groupe de G si et seulement si H est un sous-ensemble non vide de G et pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$.

Démonstration.

Montrons l'implication et sa réciproque :

- Supposons que H est un sous-groupe de G . Alors H contient e et n'est donc pas vide. De plus, soit $(x, y) \in H$. H étant stable par passage à l'inverse, on a alors $x^{-1} \in H$ et par stabilité par produit, on a donc $x^{-1} * y \in H$.
- Réciproquement, supposons que H est non vide et que pour tout $(x, y) \in H^2$, on a $x^{-1} * y \in H$. Montrons que H possède les trois propriétés énumérées dans sa définition :
 - (i) H étant non vide, il possède au moins un élément x_0 . On a alors $e = x_0^{-1} x_0 \in H$.
 - (iii) Soit $x \in H$. On a alors $(x, e) \in H^2$, donc $x^{-1} * e \in H$.
 - (ii) Soit $(x, y) \in H$. D'après ce qui précède, on a alors $x^{-1} \in H$, donc $(x^{-1}, y) \in H^2$, donc $x * y = (x^{-1})^{-1} * y \in H$.

□

Remarque 2.2.5.

On obtient une proposition vraie également en remplaçant ci-dessus la condition $x^{-1}y \in H$ par $xy^{-1} \in H$.

Théorème 2.2.6.

Un sous-groupe muni de la loi induite du groupe est lui-même un groupe.

Démonstration.

Soit $(G, *)$ un groupe de neutre e et H un sous-groupe de G .

1. Montrons qu'on peut restreindre $*$: $G \times G \rightarrow G$ au départ à $H \times H$ et à l'arrivée à H . On appellera alors loi induite par $*$ sur H cette restriction de $*$. On a $H \times H \subset G \times G$, donc la restriction au départ est légitime, pour effectuer la restriction à l'arrivée, il suffit de montrer que pour tout $(x, y) \in H^2$, on a $x * y \in H$, c'est-à-dire que H est stable par $*$. Or H est un sous-groupe de G donc c'est évident.
2. H muni de la loi induite par $*$ est un magma associatif. En effet $(G, *)$ est un magma associatif, on a donc

$$\forall (x, y, z) \in G^3 \quad (x * y) * z = x * (y * z)$$

Or $H \subset G$ donc

$$\forall (x, y, z) \in H^3 \quad (x * y) * z = x * (y * z)$$

Donc la restriction de $*$ à H est associative, d'où le résultat.

3. e est neutre pour la loi induite par $*$ sur H . En effet, e est le neutre de $*$, donc

$$\forall x \in G \quad e * x = x * e = x$$

Or $H \subset G$ donc

$$\forall x \in H \quad e * x = x * e = x$$

D'où le résultat.

4. Tout élément de H admet un inverse pour la loi induite par $*$. En effet tout élément x de H admet un inverse x^{-1} dans G pour la loi $*$ et par stabilité de l'inverse sur le sous-groupe H , on a $x^{-1} \in H$. Donc tout élément de H admet un inverse dans H pour la loi induite par $*$.
5. On déduit des points précédents que H muni de la loi induite par $*$ est un groupe. □

Remarque 2.2.7.

Il est plus facile de montrer qu'un ensemble est un sous-groupe que de montrer que c'est un groupe (pas besoin de redémontrer l'associativité, etc.). Par exemple $(\mathbb{U}, \times)$ est un groupe, vu comme sous-groupe de $(\mathbb{C}^*, \times)$.

À chaque fois que l'on essaiera de montrer qu'un ensemble est muni d'une structure de groupe, on tentera de le voir comme un sous-groupe d'un groupe bien connu.

Remarque 2.2.8.

La réciproque de ce théorème est également vraie (bien que moins utilisée) : si H est un sous-ensemble de G tel que, muni de la loi induite par celle de G , H soit un groupe, alors H est un sous-groupe de G .

Exemple 2.2.9.

Si $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{U}, \times)$, donc $(\mathbb{U}_n, \times)$ est un groupe.

2.3 Morphismes de groupes.

Définition 2.3.1.

Soient $(G, *)$ et $(G', \top)$ deux groupes et $\varphi : G \rightarrow G'$.

1. On dit que φ est un *morphisme du groupe* $(G, *)$ *dans le groupe* $(G', \top)$ ou, par abus de langage, un *morphisme du groupe* G *dans le groupe* G' , si pour tous $x, y \in G$, $\varphi(x * y) = \varphi(x) \top \varphi(y)$.

2. Tout morphisme d'un groupe dans lui-même est appelé *endomorphisme*.
3. Tout morphisme de G dans G' qui est une bijection est appelé *isomorphisme de G sur G'* . Dans ce cas on dit que G et G' sont *isomorphes*. Un morphisme qui est à la fois un isomorphisme et un endomorphisme est appelé *automorphisme*.

Remarque 2.3.2.

- « Morphisme » signifie « forme » en grec.

Exemple 2.3.3.

- $(\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, est un morphisme, mais

$$x \mapsto 2x$$
 pas un isomorphisme.
- $(\mathbb{C}^*, \times) \rightarrow (\mathbb{R}^*, \times)$, est un morphisme, mais

$$z \mapsto |z|$$
 pas un isomorphisme.
- $(\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \times)$, est un morphisme, mais

$$x \mapsto e^{ix}$$
 pas un isomorphisme.
- $(\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un isomorphisme de

$$x \mapsto e^x$$
 réciproque $\ln$, qui est aussi un isomorphisme.

Exemple 2.3.4.

On a déjà manipulé les morphismes suivants, lors des chapitres précédents.

- Si $n \in \mathbb{N}^*$, $(\mathbb{C}^*, \times) \rightarrow (\mathbb{C}^*, \times)$.

$$z \mapsto z^n$$
- Si $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{K}^n$, l'application

$$(\mathbb{K}^n, +) \rightarrow (\mathbb{K}, +)$$

$$(x_1, \dots, x_n) \mapsto a_1 x_1 + \dots + a_n x_n$$
- Si I est un intervalle de $\mathbb{R}$, si $a : I \rightarrow \mathbb{K}$ est continue, l'application

$$(\mathcal{C}^1(I, \mathbb{K}), +) \rightarrow (\mathcal{C}(I, \mathbb{K}), +)$$

$$f \mapsto f' + af$$
- Si $a, b \in \mathbb{Z}$, l'application

$$(\mathbb{Z}^2, +) \rightarrow (\mathbb{Z}, +)$$

$$(x, y) \mapsto ax + by$$
- Si $a \in \mathbb{K}$, l'application

$$(\mathbb{K}^{\mathbb{N}}, +) \rightarrow (\mathbb{K}^{\mathbb{N}}, +)$$

$$u \mapsto (u_{n+1} - au_n)_{n \in \mathbb{N}}$$

Dans toute la suite, $(G, *)$ et $(G', \top)$ sont deux groupes de neutres e et e' , on adopte une notation multiplicative, et $\varphi : G \rightarrow G'$ est un morphisme.

Théorème 2.3.5.

Soit φ un morphisme de G sur G' , on a, e et e' désignant les neutres de G et G' :

1. $\varphi(e) = e'$;
2. $\forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}$.

Démonstration. 1. En effet, $\varphi(e) \top \varphi(e) = \varphi(e * e) = \varphi(e) = \varphi(e) \top e'$, donc en simplifiant par $\varphi(e)$, on en déduit $\varphi(e) = e'$.

2. Soit $x \in G$. Alors $\varphi(x^{-1}) \top \varphi(x) = \varphi(x^{-1} * x) = \varphi(e) = e'$. □

Corollaire 2.3.6.

Sous les mêmes hypothèses, on a

$$\forall x \in G \quad \forall k \in \mathbb{Z} \quad \varphi(x^k) = (\varphi(x))^k.$$

Démonstration.

Soit $x \in G$. D'après le théorème ci-dessus, on a

$$\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0$$

On peut alors démontrer par récurrence que pour tout $n \in \mathbb{N}$, on a $\varphi(x^n) = (\varphi(x))^n$ (l'hérédité résulte directement de la définition de morphisme).

D'après le théorème ci-dessus, pour tout $n \in \mathbb{N}$, $\varphi(x^{-n}) = (\varphi(x^n))^{-1}$, d'où $\varphi(x^{-n}) = (\varphi(x))^{-n}$.

On en déduit le résultat. □

Exemple 2.3.7. 1. $\mathbb{C}^* \rightarrow \mathbb{R}^*$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$, donc pour tout $z \in \mathbb{C}^*$, on a

$$\left| \frac{1}{z} \right| = \frac{1}{|z|}$$

2. $\exp$ est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$, donc pour tout $z \in \mathbb{C}$, $e^{-z} = \frac{1}{e^z}$
3. $\ln$ est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, donc pour tout $x \in \mathbb{R}_+^*$, on a $\ln(1/x) = -\ln x$.

Remarque 2.3.8.

On peut adapter le théorème 2.3.5 dans le cas où on sait seulement que $(G, *)$ est un groupe, G' est un ensemble muni d'une loi de composition interne $\top$ et où φ est une application $G \rightarrow G'$ vérifiant $\forall (x, y) \in G^2 \varphi(x * y) = \varphi(x) \top \varphi(y)$. Dans ce cas, on ne peut pas déduire que $(G', \top)$ est un groupe mais seulement que $(\varphi(G), \top)$ est un groupe. Voir aussi le théorème disant que «l'image d'un sous-groupe par un morphisme est un sous-groupe».

Théorème 2.3.9. (i) La composée de deux morphismes de groupes est un morphisme de groupe. Plus précisément, soit $(G_1, *_1)$, $(G_2, *_2)$ et $(G_3, *_3)$ trois groupes, φ un morphisme de G_1 dans G_2 et ψ un morphisme de G_2 dans G_3 . Alors $\psi \circ \varphi$ est un morphisme de G_1 dans G_3 .

(ii) La fonction réciproque d'un isomorphisme (en tant qu'application bijective) est un isomorphisme. Plus précisément, soit $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et φ un isomorphisme de G_1 sur G_2 . Alors φ^{-1} est un isomorphisme de G_2 sur G_1 .

Démonstration.

Les démonstrations pour montrer qu'une application est un morphisme ont TOUJOURS la même structure.

1. $\psi \circ \varphi$ est clairement une application de G_1 dans G_3 . Soit $(x, y) \in G_1^2$, montrons qu'on a $\psi \circ \varphi(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
 φ est un morphisme de groupes donc on a $\varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$. Or ψ est un morphisme de groupes donc on a $\psi(\varphi(x) *_2 \varphi(y)) = (\psi(\varphi(x)) *_3 \psi(\varphi(y)))$.
 D'où $(\psi \circ \varphi)(x *_1 y) = (\psi \circ \varphi)(x) *_3 (\psi \circ \varphi)(y)$.
2. φ^{-1} est évidemment une bijection de G_2 sur G_1 . Il suffit donc de montrer que φ^{-1} est un morphisme de G_2 dans G_1 .
 Soit $(x, y) \in G_2^2$. Montrons $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
 On a d'une part $\varphi(\varphi^{-1}(x *_2 y)) = x *_2 y$ et d'autre part, comme φ est un morphisme, $\varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) *_2 \varphi(\varphi^{-1}(y)) = x *_2 y$, d'où $\varphi(\varphi^{-1}(x *_2 y)) = \varphi(\varphi^{-1}(x) *_1 \varphi^{-1}(y))$.
 Or φ est injective donc $\varphi^{-1}(x *_2 y) = \varphi^{-1}(x) *_1 \varphi^{-1}(y)$.
 Donc φ^{-1} est un morphisme, donc un isomorphisme. $\square$

Remarque 2.3.10.

L'ensemble des automorphismes d'un groupe G est donc un sous-groupe de $(S_G, \circ)$.

Exemple 2.3.11.

On a vu que $\exp$ et $\ln$ sont des isomorphismes réciproques.

Théorème 2.3.12. (i) L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe (du groupe d'arrivée).

(ii) Le tiré en arrière d'un sous-groupe par un morphisme est un sous-groupe (du groupe de départ).

Démonstration.

Les démonstrations pour montrer qu'un ensemble est un sous-groupe ont TOUJOURS la même structure.

- (i) Soient $(G, *)$ et $(G', \top)$ deux groupes de neutres respectifs e et e' , et $\varphi : G \rightarrow G'$ un morphisme de groupes. Soit H un sous-groupe de G . Montrons que $\varphi(H)$ est un sous-groupe de G' .
1. On a évidemment $\varphi(H) \subset G'$ et de plus $e \in H$ et $e' = \varphi(e) \in \varphi(H)$.
2. Soit $x, y \in \varphi(H)$. Alors x possède un antécédent $x' \in H$ et y un antécédent $y' \in H$ par φ . On a alors successivement

$$\begin{aligned} x \top y^{-1} &= \varphi(x') \top \varphi(y')^{-1} && \text{par définition de } x' \text{ et } y' \\ &= \varphi(x') \top \varphi(y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \\ &= \varphi(x' * y'^{-1}) && \text{car } \varphi \text{ est un morphisme} \end{aligned}$$

$$\text{Donc } x \top y^{-1} \in \varphi(H).$$

$\varphi(H)$ est donc un sous-groupe de G' .

- (ii) Gardons les mêmes notations que dans le premier point, et notons H' un sous-groupe de G' .
1. On a évidemment $\varphi^{\leftarrow}(H') \subset G$ et de plus $e' \in H'$ et $e' = \varphi(e) \in H'$ donc $e \in \varphi^{\leftarrow}(H')$.
2. Soit $x, y \in \varphi^{\leftarrow}(H')$. Alors $\varphi(x), \varphi(y) \in H'$ et donc $\varphi(x * y^{-1}) = \varphi(x) \top (\varphi(y))^{-1} \in H'$ donc $x * y^{-1} \in \varphi^{\leftarrow}(H')$.
 $\varphi^{\leftarrow}(H')$ est donc un sous-groupe de G . $\square$

Remarque 2.3.13.

On complète la remarque 2.2.7 comme suit :

lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme image réciproque (ou directe) d'un sous-groupe d'un groupe bien connu par un morphisme.

Définition 2.3.14. (i) On appelle *noyau* de φ , noté $\text{Ker } \varphi$, l'image réciproque de $\{e'\}$ par φ , autrement dit l'ensemble des antécédents de e' par φ : $\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e'\}$.
(ii) On appelle *image* de φ notée $\text{Im } \varphi$, l'image directe de G par φ . Autrement dit $\text{Im } \varphi = \{\varphi(x) \mid x \in G\}$.

Exemple 2.3.15.

Déterminer les images et noyaux des exemples de 2.3.3.

Théorème 2.3.16.

Les noyaux et les images sont des sous-groupes respectivement de G et G' .

Démonstration.

Ceci découle directement du théorème 2.3.12. Néanmoins, redémontrons-le dans le cas particulier du noyau :

Montrons que $\text{Ker } \varphi$ est un sous-groupe de G :

1. On a évidemment $\text{Ker } \varphi \subset G$ et de plus $\varphi(e) = e'$ donc $\text{Ker } \varphi$ est un sous-ensemble non vide de G .
2. Soit $x, y \in \text{Ker } \varphi$. Alors on a successivement

$$\begin{aligned} \varphi(x * y^{-1}) &= \varphi(x) \top \varphi(y)^{-1} \\ &= e' \top e'^{-1} \\ &= e' \end{aligned}$$

Donc $x * y^{-1} \in \text{Ker } \varphi$.

Donc $\text{Ker } \varphi$ est un sous-groupe de G . □

Exemple 2.3.17.

Constataion avec les Im et Ker tirés des exemples de 2.3.3.

Remarque 2.3.18.

On complète la remarque 2.3.13 comme suit : lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme noyau ou image d'un morphisme.

Exemple 2.3.19.

$\mathbb{U}$ est le noyau du morphisme « module », de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}^*, \times)$.

La proposition suivante est primordiale.

Proposition 2.3.20.

Soit $\varphi : G \rightarrow G'$ un morphisme de groupes, soit $x, y \in G$. Alors $\varphi(x) = \varphi(y)$ si et seulement si $x * y^{-1} \in \text{Ker } \varphi$.

Démonstration.

$\varphi(x) = \varphi(y)$ si et seulement si $\varphi(x) \top \varphi(y)^{-1} = e'$ si et seulement si $\varphi(x * y^{-1}) = e'$. □

Remarque 2.3.21.

Avec les mêmes notations, si on a $a \in G$ et $y \in G'$ vérifiant $y = \varphi(a)$, l'ensemble des solutions sur G de l'équation $y = \varphi(x)$ est $\{ax \mid x \in \text{Ker}(\varphi)\}$.

Exemple 2.3.22.

Reprendre les exemples exposés en 2.3.4.

On retrouve ainsi la structure des racines n^{es} d'un nombre complexe, la structure des solutions d'un système linéaire, la structure des solutions d'une équation différentielle linéaire, les solutions d'une relation de Bézout et la structure des suites vérifiant une relation de récurrence arithmético-géométrique.

Théorème 2.3.23. (i) φ injectif si et seulement si $\text{Ker } \varphi = \{e\}$.

(ii) φ surjectif si et seulement si $\text{Im } \varphi = G'$.

Démonstration. (ii) Rien de nouveau.

(i) On montre l'implication et sa réciproque :

- Supposons φ injectif. Alors e' a au plus un antécédent par φ . Or $\varphi(e) = e'$ donc il en a au moins un : e . Donc $\text{Ker } \varphi = \{e\}$.
- Réciproquement, supposons $\text{Ker } \varphi = \{e\}$ et montrons que φ est injectif.

Soit $(x, y) \in G^2$ vérifiant $\varphi(x) = \varphi(y)$. Alors on a successivement

$$\begin{aligned} \varphi(x * y^{-1}) &= \varphi(x) \top \varphi(y)^{-1} \quad \text{car } \varphi \text{ est un} \\ &\hspace{15em} \text{morphisme} \\ &= \varphi(x) \top \varphi(x)^{-1} \\ &= e' \end{aligned}$$

Donc $x * y^{-1} \in \text{Ker } \varphi$, donc $x * y^{-1} = e$, donc $x = y$.

□

Remarque 2.3.24.

Pour montrer qu'un morphisme est injectif, on utilisera **TOUJOURS** le noyau et **JAMAIS** (ou presque) la méthode classique pour des fonctions quelconques : c'est beaucoup plus rapide !

Exemple 2.3.25.

Reprendre les exemples de $\exp$ et $\ln$, ainsi que les morphismes vus en 2.3.4.

3 Anneaux

3.1 Structure d'anneau.

Définition 3.1.1.

On appelle *anneau* tout triplet $(A, +, \times)$ constitué d'un ensemble A et de deux lois internes sur A , une loi $+$ appelée *addition* et une loi $\times$ appelée *multiplication*, vérifiant :

1. $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0 (ou 0_A si ambiguïté) ;
2. $(A, \times)$ est un magma associatif possédant un neutre noté 1 (ou 1_A si ambiguïté) ;
3. La multiplication est distributive par rapport à l'addition.

Si la loi $\times$ est commutative, on dit que l'anneau A est commutatif.

Exemple 3.1.2.

- $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ et $\mathcal{F}(\mathbb{R}, \mathbb{R})$ avec $+$ et $\times$ sont des anneaux.
- $(\mathbb{R}^3, +, \wedge)$ et $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n'en sont pas.
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ en est un.
- $(\mathcal{M}_n(\mathbb{R}), +, \times)$ est un anneau.
- On note $\mathcal{L}(\mathbb{R}^2)$ l'ensemble des endomorphismes de $\mathbb{R}^2$. Alors $(\mathcal{L}(\mathbb{R}^2), +, \circ)$ est un anneau.
- Si X est un ensemble, $(\mathbb{R}^X, +, \times)$ est un anneau.

Remarque 3.1.3.

Quand il n'y a pas d'ambiguïté, on dit juste que A est un anneau sans préciser les lois. Pour la multiplication, on utilise les mêmes raccourcis de notation que dans $\mathbb{R}$ (omission du $\times$, etc).



Tous les éléments de A ne sont pas inver-

sibles pour $\times$. Les éléments inversibles sont parfois appelés *éléments unités* de A et leur ensemble est noté $U(A)$, $A^\times$, A^* , voire $E(A)$ (*Einheit*).



Avec cette notation, A^* n'est pas nécessairement $A \setminus \{0\}$.

Théorème 3.1.4 (Règles de calcul dans un anneau).

Soit A un anneau, $a, b \in A$ et $n \in \mathbb{Z}$.

1. $a \times 0 = 0 \times a = 0$.
2. $-(a \times b) = (-a) \times b = a \times (-b)$. Cas particuliers : $(-a)(-b) = ab$, $(-a)^2 = a^2$, $(-1)^2 = 1$.
3. $n(ab) = (na)b = a(nb)$.

Démonstration. 1. Il suffit de remarquer $a \times 0 + a \times 0 = a \times (0 + 0) = a \times 0$ et de simplifier par $a \times 0$ (ce qui est légitime car il est inversible pour la loi $+$).

2. On a successivement :

$$\begin{aligned} a \times b + (-a) \times b &= (a - a) \times b \quad \text{par distributivité} \\ &= 0 \times b \\ &= 0 \end{aligned} \quad \text{d'après (1)}$$

Donc $(-a) \times b$ est l'opposé de $a \times b$, donc $(-a) \times b = -(a \times b)$.

On montre de même $a \times (-b) = -(a \times b)$.

3. **Cas où $n \in \mathbb{N}$** : On peut s'en convaincre par récurrence. Le cas $n = 0$ se déduit du (1), l'hérédité se montre par application de la distributivité.

Cas où $n < 0$: alors $-n \in \mathbb{N}$, et on a

$$\begin{aligned} n(a \times b) &= (-n)(-(a \times b)) \quad \text{par définition de} \\ &\quad \text{la multiplication par un entier} \\ &= (-n)((-a)b) \quad \text{d'après 2} \\ &= ((-n)(-a))b \\ &\quad \text{d'après le cas précédent} \end{aligned}$$

L'autre égalité se démontre de la même façon. □

Remarque 3.1.5.

On voit ainsi que si l'anneau A possède au moins deux éléments, alors $1_A \neq 0_A$ et 0_A n'est pas inversible.

Exercice 3.1.6.

Étant donné un anneau $(A, +, \times)$, la notation $n \times a$ peut désigner d'une part le produit dans A de n par a si n et a sont deux éléments de A , d'autre

part si $a \in A$ et $n \in \mathbb{Z}$, la valeur $a + \dots + a$ où a est répété n fois dans le cas où $n \geq 0$ et l'opposé de $a + \dots + a$ où a est répété $-n$ fois si $n < 0$.

Dans le cas où A et $\mathbb{Z}$ sont disjoints, cette ambiguïté n'est évidemment pas gênante si on sait auquel des deux ensembles A et n appartient.

Dans le cas contraire, cette ambiguïté n'est pas gênante non plus. Pourquoi ?

Théorème 3.1.7.

Soient $n \in \mathbb{N}$, $(A, +, \times)$ un anneau et $a, b \in A$ tels que a et b commutent (i.e. $a \times b = b \times a$). Alors :

(i) Formule du binôme de Newton :

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

(ii) $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-k-1}.$

Démonstration.

On remarque d'abord que si a, b commutent, alors toutes les puissances de a et de b commutent (le faire par récurrence).

Recopier la démonstration concernant des complexes ou des matrices carrées, à nouveau en étant conscient de l'importance de l'hypothèse " a et b commutent". $\square$

Proposition 3.1.8 (Groupe des inversibles).

Soit $(A, +, \times)$ un anneau. Alors $(A^*, \times)$ est un groupe, autrement dit l'ensemble des éléments inversibles de A , muni de (la loi induite par) la multiplication de A est un groupe.

Démonstration.

- Remarquons tout d'abord que $\times$ induit une loi sur A^* . Soit x et y deux éléments de A^* . x et y sont donc deux éléments inversibles du magma $(A, \times)$ donc, d'après la proposition 1.2.10, $x \times y$ est inversible.
 - $\times$ étant une loi associative sur A , elle l'est aussi sur A^* .
 - 1_A est inversible car $1_A \times 1_A = 1_A$. Donc $1_A \in A^*$. De plus 1_A est élément neutre pour la multiplication sur A , donc est élément neutre pour la multiplication sur A^* .
 - Pour tout $x \in A^*$, x possède un inverse y dans A . On remarque immédiatement que y est lui-même inversible (d'inverse x), donc $y \in A^*$. Tout élément du magma $(A^*, \times)$ est donc inversible dans A^* .
- $(A^*, \times)$ est donc un groupe, de neutre 1_A . $\square$

Exemple 3.1.9.

Quel est le groupe des inversibles des anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$?

Définition 3.1.10.

1. On appelle *anneau nul* tout anneau $(\{0\}, +, \times)$ (0 est alors le neutre pour les deux lois !).
2. Dans un anneau A , on appelle *diviseur de 0* tout élément a *non nul*, tel qu'il existe b *non nul* vérifiant $a \times b = 0_A$ ou $b \times a = 0_A$.
3. On appelle *anneau intègre* tout anneau commutatif non nul *ne possédant aucun diviseur de 0*, c'est-à-dire vérifiant

$$\forall (a, b) \in A^2 \quad ab = 0 \Rightarrow (a = 0 \text{ ou } b = 0).$$

Remarque 3.1.11.

Pour tout anneau A , on a $0_A = 1_A$ si et seulement si A est un anneau nul. En effet, supposons $0_A = 1_A$, alors pour tout $x \in A$, on a $x = 1_A \times x = 0_A \times x = 0_A$, donc tout élément de A est nul, donc A est l'anneau nul. Réciproquement si A est un anneau nul, tous les éléments de A sont égaux (puisqu'il n'y en a qu'un !) donc $0_A = 1_A$.

Remarque 3.1.12.

Un élément inversible a n'est jamais un diviseur de 0. En effet, pour tout b vérifiant $ab = 0$, on a nécessairement $a^{-1}ab = 0$, donc $b = 0$.

Exemple 3.1.13.

- Les anneaux usuels $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ sont intègres.
- $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ n'est pas intègre : ex : considérer $f, g : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 0$ si $x \geq 0$ et $g(x) = 0$ si $x \leq 1$.
- $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre : $\bar{2} \times \bar{3} = \bar{0}$. De manière générale, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre quand n est composé.
- $(\mathcal{L}(\mathbb{R}^2), +, \circ)$ n'est pas intègre. Par exemple avec $f(x, y) = (x, 0)$ et $g(x, y) = (0, y)$ nous avons $f \circ g = 0$.
- $\mathcal{M}_n(\mathbb{K})$ n'est pas intègre non plus, comme nous l'avons déjà vu en début d'année. En effet, $\mathcal{M}_n(\mathbb{K})$ n'est pas un anneau commutatif, et de plus cet anneau possède des diviseurs de zéro non nuls.

Remarque 3.1.14.

Attention donc aux simplifications de produits

dans les anneaux : si l'anneau est intègre, tout fonctionne comme dans $\mathbb{R}$: $ab = ac \Rightarrow a(b - c) = 0 \Rightarrow (a = 0 \text{ ou } b = c)$.

Sinon, on sait qu'on peut simplifier par des éléments inversibles mais on a du mal à en dire plus (quand un élément est non inversible, il se peut qu'il soit simplifiable ou non³).

3.2 Sous-anneaux

Un sous-anneau est à un anneau ce qu'un sous-groupe est à un groupe, à un détail près.

Définition 3.2.1.

Soit $(A, +, \times)$ un anneau, soit B un ensemble. Alors, B est un sous-anneau de $(A, +, \times)$ si

- $B \subset A$;
- B est un sous-groupe de $(A, +)$;
- B est stable par $\times$: pour tout $x, y \in B$, $xy \in B$;
- $1_A \in B$.

Remarque 3.2.2.

Le caractère de sous-groupe d'un sous-anneau B implique que $B \neq \emptyset$, la condition $1_A \in B$ est toutefois primordiale.

Par exemple, $2\mathbb{Z}$ vérifie les trois premiers points, mais n'est pas un sous-anneau de $(\mathbb{Z}, +, \times)$.

Exemple 3.2.3.

Si $(A, +, \times)$ est un anneau, alors A est un sous-anneau de $(A, +, \times)$.

$\mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 3.2.4 (anneau des entiers de Gauss).

On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

Exercice 3.2.5.

Quel est le plus petit sous-anneau d'un anneau $(A, +, \times)$?

Proposition 3.2.6.

Soit $(A, +, \times)$ un anneau, soit B une partie de A .

Alors, B est un sous-anneau de $(A, +, \times)$ si et seulement si, muni des lois $+$ et $\times$ induites sur B , $(B, +, \times)$ est un anneau de même neutre multiplicatif que A .

Démonstration.

Élémentaire, procéder exactement comme pour les groupes. $\square$

3.3 Morphismes d'anneaux

Les morphismes d'anneaux sont aux anneaux ce que les morphismes de groupes sont aux groupes, à un détail près.

Définition 3.3.1.

Soit $(A, +, \times)$, $(B, +, \times)$ deux anneaux. Un morphisme entre ces deux anneaux est une application

$$\varphi : A \rightarrow B$$

vérifiant les propriétés suivantes.

- $\forall x, y \in A, \varphi(x + y) = \varphi(x) + \varphi(y)$
- $\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y)$
- $\varphi(1_A) = 1_B$

Si l'anneau de départ est égal à l'anneau d'arrivée, on parle bien entendu d'endomorphisme d'anneau.

Un morphisme d'anneaux bijectif est un isomorphisme d'anneau.

Enfin, un morphisme bijectif d'un anneau sur lui-même est un automorphisme d'anneau.

Exemple 3.3.2.

Dans l'anneau $(\mathbb{C}, +, \times)$, on a les automorphismes Id et $z \mapsto \bar{z}$.

Sur l'anneau des fonctions réelles, si $a \in \mathbb{R}$, l'application d'évaluation $f \mapsto f(a)$ est un morphisme à valeurs dans l'anneau $\mathbb{R}$.

L'application nulle n'est pas un morphisme d'anneaux !

Remarque 3.3.3.

Un morphisme d'anneaux est un morphisme de groupes. La notion de noyau ne change pas : pour un morphisme φ entre deux anneaux A et B ,

$$\text{Ker}(\varphi) = \{x \in A \mid \varphi(x) = 0_B\}.$$

3. Regarder l'ensemble des suites à valeurs entières muni de l'addition et de la multiplication terme à terme

Notamment, un morphisme d'anneaux est injectif si et seulement si son noyau est réduit à l'élément nul.

Remarquons que par définition $1_A \notin \text{Ker}(\varphi)$: ainsi, le noyau d'un morphisme d'anneaux n'est JAMAIS un sous-anneau de l'anneau de départ, en dehors de l'exemple dégénéré de l'anneau nul.

Proposition 3.3.4 (transport par morphisme). Soit $(A, +, \times)$, $(B, +, \times)$ deux anneaux, soit $\varphi : A \rightarrow B$ un morphisme entre ces deux anneaux.

1. Si C est un sous-anneau de $(A, +, \times)$, alors $\varphi(C)$ est un sous-anneau de $(B, +, \times)$.
2. Si D est un sous-anneau de $(B, +, \times)$, alors $\varphi^{-1}(D)$ est un sous-anneau de $(A, +, \times)$.

Démonstration.

Élémentaire, procéder exactement comme pour les groupes. $\square$

Remarque 3.3.5.

Si φ est un morphisme entre deux anneaux A et B , alors $\text{Im}(\varphi) = \varphi(A)$ est un sous-anneau de B .

4 Structure de corps.

Définition 4.0.1.

On appelle *corps* tout anneau commutatif non nul dans lequel tout élément non nul est inversible pour $\times$.

Exemple 4.0.2.

- $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$ sont des corps. $\mathbb{N}$ et $\mathbb{Z}$ n'en sont pas.
- $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Proposition 4.0.3. (i) Un corps est intègre.

- (ii) Si $\mathbb{K}$ est un corps, on a $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ (qui est un groupe pour la loi induite par $\times$).

Démonstration. (i) Soit $(\mathbb{K}, +, \times)$ un corps. Soit $(a, b) \in \mathbb{K}^2$ vérifiant $ab = 0$. Supposons que a est non nul. Alors a est inversible donc $a^{-1} \times ab = a^{-1} \times 0$, donc $b = 0$.

On a donc $a = 0$ ou $b = 0$.

- (ii) Tout élément non nul est inversible pour $\times$ d'après la définition, d'où $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ et on sait d'après la proposition 3.1.8 que $(\mathbb{K}^*, \times)$ est un groupe. $\square$

Remarque 4.0.4.

Un corps est un anneau qui est intègre, par contre un anneau intègre n'est pas forcément un corps ! Trouvez un exemple ...

Chapitre XIV

Limite d'une fonction

Sommaire

1	Préliminaires.	198
2	Définitions de la limite d'une fonction.	199
2.1	Limite en un point.	199
2.2	Limites à gauche et à droite en un point.	202
3	Propriétés des limites de fonctions.	204
3.1	Opérations sur les limites.	204
3.2	Passage à la limite et relations d'ordre.	205
4	Théorèmes d'existence.	206
4.1	Théorèmes des gendarmes et de minoration/majoration.	206
4.2	Théorème de la limite monotone.	207
5	Cas des fonctions à valeurs complexes.	208

Dans tout ce chapitre, sauf mention expresse du contraire, I et J sont des intervalles de $\mathbb{R}$, et $f : I \rightarrow \mathbb{R}$.

1 Préliminaires.

Comme pour la notion de limite d'une suite, nous allons définir la notion de limite de fonction de manière naïve. Cela va nous amener à répéter de nombreuses fois certains énoncés. Vous unifierez cela en spé, avec la notion de voisinage.

Nous nous permettons cependant de définir quelques raccourcis de langages qui simplifieront les énoncés.

Définition 1.0.1.

On dit qu'une propriété est vraie *au voisinage* d'un point $a \in \mathbb{R}$ s'il existe un intervalle ouvert contenant a sur lequel la propriété est vérifiée.

On dit qu'une propriété est vraie *au voisinage* de $+\infty$ (resp. de $-\infty$) s'il existe un intervalle de la forme $[A, +\infty[$ (resp. $] -\infty, A]$) sur lequel la propriété est vérifiée.

Remarque 1.0.2.

On pourrait (voire même devrait) donner ces définitions avec des intervalles ouverts : c'est équivalent.

Exemple 1.0.3.

- La fonction sinus est strictement positive au voisinage de $\pi/2$.
- La fonction Arctan est supérieure à $\pi/4$ au voisinage de $+\infty$.

Remarque 1.0.4.

Si $a \in \mathbb{R}$, si P est un prédicat portant sur les réels, P est vrai au voisinage de a si et seulement si

$$\exists \varepsilon > 0, \forall t \in [a - \varepsilon, a + \varepsilon], P(t).$$

Si P n'est défini que sur un ensemble $I \subset \mathbb{R}$, la définition 1.0.1 doit alors être modifiée en remplaçant tous les intervalles par leurs intersections avec I , *i.e*

$$\exists \varepsilon > 0, \forall t \in I \cap [a - \varepsilon, a + \varepsilon], P(t),$$

ou encore

$$\exists \varepsilon > 0, \forall t \in I, t \in [a - \varepsilon, a + \varepsilon] \Rightarrow P(t),$$

On a les mêmes écritures au voisinage de $\pm\infty$.

Exemple 1.0.5.

Si on s'intéresse à la propriété « $\frac{1}{x^2} - 1 \geq 0$ », celle-ci n'a de sens que sur $D = \mathbb{R}^*$.

Dire que « $\frac{1}{x^2} - 1 \geq 0$ au voisinage de 0 » signifie qu'il existe $\varepsilon > 0$ tel que

$$\forall t \in [-\varepsilon, \varepsilon] \cap \mathbb{R}^*, \frac{1}{t^2} - 1 \geq 0.$$

Proposition 1.0.6.

Si P et Q sont vraies au voisinage de a , alors « P et Q » est vraie au voisinage de a .

Démonstration.

Montrons le dans le cas $a \in \mathbb{R}$ (les autres sont laissés au lecteur).

Soit $\alpha, \beta > 0$ tels que, pour tout $x \in \mathbb{R}$:

- si $|x - a| \leq \alpha$, alors $P(x)$;
- si $|x - a| \leq \beta$, alors $Q(x)$.

Alors, avec $\gamma = \min(\alpha, \beta) > 0$, pour tout $x \in \mathbb{R}$, si $|x - a| \leq \gamma$, on a bien simultanément $|x - a| \leq \alpha$ et $|x - a| \leq \beta$, donc $P(x)$ et $Q(x)$ sont vraies. $\square$

Remarque 1.0.7.

Dire qu'une propriété est vraie au voisinage de a est vague car on ne précise pas sur quel ensemble elle est vraie mais très pratique car on ne précise pas sur quel ensemble elle est vraie !

C'est l'exact analogue du « à partir d'un certain rang » utilisé sur les suites.

Remarque 1.0.8.

Quand on parle de plusieurs propriétés vraies « au voisinage d'un point a », il faut bien comprendre que tous ces « voisinages » ne sont pas nécessairement les mêmes.

Par exemple, pour tout $\varepsilon > 0$, la propriété « $|x| \leq \varepsilon$ » est vraie pour x au voisinage de 0 mais le « voisinage » en question dépend de ε (il s'agit de $[-\varepsilon, \varepsilon]$).

On peut remarquer d'ailleurs que, bien que pour tout $\varepsilon > 0$, la propriété « $|x| \leq \varepsilon$ » soit vraie pour x au voisinage de 0, il est faux d'affirmer que la propriété « pour tout $\varepsilon > 0$, $|x| \leq \varepsilon$ » est vraie pour x au voisinage de 0 (elle n'est vraie qu'en 0).

On va s'intéresser dans la suite à la notion de limite de fonction. Étant donné une partie E de $\mathbb{R}$, une fonction f définie sur E et $a \in \overline{\mathbb{R}}$, sans même connaître f , il est intuitivement clair que la notion de limite de f n'a pas de sens dans certains cas. Par exemple si $E = \mathbb{R}^-$, se questionner sur la limite de f en $+\infty$ ou en 1 n'a aucun sens. La définition ci-dessous va nous permettre, étant donné E , de définir précisément en quels points chercher si f admet une limite à un sens. Cet ensemble de points est appelé l'adhérence de E .

Exercice 1.0.9.

Pour les ensembles E suivants, quelles sont les valeurs sur lesquelles chercher si f admet une limite à un sens ?

1. $\mathbb{R}$	5. $]\pi, 42]$
2. $[0, +\infty[$	6. $\mathbb{R}^*$
3. $]0, +\infty[$	7. $]-\infty, -7] \cup]6, 42]$
4. $]\pi, 42[$	8. $\{0\}$

Définition 1.0.10 (HP – sera vu en MP).

Soit E un sous-ensemble de $\mathbb{R}$.

- On appelle *intérieur* de E et l'on note $\overset{\circ}{E}$ l'ensemble des $x \in \mathbb{R}$ tels que E soit un voisinage de x , c'est-à-dire l'ensemble des x appartenant à E tels que E contienne un intervalle ouvert centré en x .
- On appelle *adhérence* de E et l'on note $\overline{E}$ l'ensemble des éléments de $\overline{\mathbb{R}}$ limites de suites d'éléments de E .
- On appelle *frontière* de E l'ensemble $\overline{E} \setminus \overset{\circ}{E}$.

Exercice 1.0.11.

Vérifier que pour les exemples de l'exercice 1.0.9, cette définition donne bien la même chose.

En pratique, on pourra essentiellement se contenter de la définition suivante, en se rappelant que l'adhérence (resp. l'intérieur) de l'union d'un nombre fini d'intervalles disjoints est l'union de leurs adhérences (resp. leurs intérieurs).

Remarque 1.0.12.

E est dense dans $\mathbb{R}$ si et seulement si $\overline{E} = \mathbb{R}$.

Définition 1.0.13.

Soit I un intervalle de la forme (a, b) , avec $a, b \in \overline{\mathbb{R}}$, tels que $a \leq b$, et où les symboles (et) peuvent prendre la valeur [ou].

- On appelle *intérieur* de I , noté $\text{Int}(I)$ ou $\overset{\circ}{I}$, l'intervalle $]a, b[$, c'est-à-dire I privé de ses extrémités. C'est le plus grand intervalle ouvert contenu dans I .
- On appelle *fermeture* ou *adhérence* de I , noté $\overline{I}$, l'intervalle $[a, b]$, c'est-à-dire I augmenté de ses extrémités. C'est le plus petit intervalle fermé de $\overline{\mathbb{R}}$ contenant I .

Définition 1.0.14.

Soit I un intervalle de $\mathbb{R}$, soit $a \in \overline{\mathbb{R}}$. Si $a \in \overline{I}$, on dit que a *adhère* à I .

2 Définitions de la limite d'une fonction.

Comme pour les suites, nous allons donner différentes définitions naïves de limites de fonctions : on peut considérer la limite d'une fonction en un point réel, en $+\infty$ et en $-\infty$; on peut considérer une limite réelle ou infinie. On traite donc séparément neuf cas différents.

La notion topologique de *voisinage*, que vous verrez l'année prochaine, permet d'unifier tout cela en un seul vocabulaire : quel gain en efficacité et en élégance !

2.1 Limite en un point.

Définition 2.1.1 (Limite en un point réel).

Soit $a \in \overline{I} \cap \mathbb{R}$, soit $\ell \in \mathbb{R}$.

• On dit que f *tend vers* ℓ *en* a et l'on note $f \xrightarrow{a} \ell$ ou $f(x) \xrightarrow{x \rightarrow a} \ell$ si

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow |f(x) - \ell| \leq \varepsilon.$$

• On dit que f *tend vers* $+\infty$ *en* a et l'on note $f \xrightarrow{a} +\infty$ ou $f(x) \xrightarrow{x \rightarrow a} +\infty$ si

$$\forall A \in \mathbb{R}, \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow f(x) \geq A.$$

- On dit que f tend vers $-\infty$ en a et l'on note $f \xrightarrow[a]{-} -\infty$ ou $f(x) \xrightarrow{x \rightarrow a} -\infty$ si

$$\forall A \in \mathbb{R}, \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow f(x) \leq A.$$

Remarque 2.1.2.

On préférera parfois écrire $|x - a| \leq \alpha$ sous la forme $x \in [a - \alpha, a + \alpha]$.

Le bloc $\forall x \in I, |x - a| \leq \alpha \Rightarrow [\dots]$ s'écrit alors $\forall x \in I \cap [a - \alpha, a + \alpha], [\dots]$.

On remarquera la structure commune :

$$\forall [\dots], \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow f(x) \in [\dots].$$

Remarque 2.1.3.

On voit facilement que, si f tend vers $+\infty$ ou $-\infty$ en a , alors f n'est pas définie en a .

Définition 2.1.4 (Limite en $+\infty$).

Supposons que $\sup I = +\infty$, soit $\ell \in \mathbb{R}$.

- On dit que f tend vers ℓ en $+\infty$ et l'on note $f \xrightarrow{+\infty} \ell$ ou $f(x) \xrightarrow{x \rightarrow +\infty} \ell$ si

$$\forall \varepsilon > 0, \exists B \in \mathbb{R}, \forall x \in I, x \geq B \Rightarrow |f(x) - \ell| \leq \varepsilon.$$

- On dit que f tend vers $+\infty$ en $+\infty$ et l'on note $f \xrightarrow{+\infty} +\infty$ ou $f(x) \xrightarrow{x \rightarrow +\infty} +\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \geq B \Rightarrow f(x) \geq A.$$

- On dit que f tend vers $-\infty$ en $+\infty$ et l'on note $f \xrightarrow{+\infty} -\infty$ ou $f(x) \xrightarrow{x \rightarrow +\infty} -\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \geq B \Rightarrow f(x) \leq A.$$

Remarque 2.1.5.

On préférera parfois écrire $x \geq B$ sous la forme $x \in [B, +\infty[$.

Le bloc $\forall x \in I, x \geq B \Rightarrow [\dots]$ s'écrit alors $\forall x \in I \cap [B, +\infty[, [\dots]$.

On remarquera la structure commune :

$$\forall [\dots], \exists B \in \mathbb{R}, \forall x \in I, x \geq B \Rightarrow f(x) \in [\dots].$$

Définition 2.1.6 (Limite en $-\infty$).

Supposons que $\inf I = -\infty$, soit $\ell \in \mathbb{R}$.

- On dit que f tend vers ℓ en $-\infty$ et l'on note $f \xrightarrow{-\infty} \ell$ ou $f(x) \xrightarrow{x \rightarrow -\infty} \ell$ si

$$\forall \varepsilon > 0, \exists B \in \mathbb{R}, \forall x \in I, x \leq B \Rightarrow |f(x) - \ell| \leq \varepsilon.$$

- On dit que f tend vers $+\infty$ en $-\infty$ et l'on note $f \xrightarrow{-\infty} +\infty$ ou $f(x) \xrightarrow{x \rightarrow -\infty} +\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \leq B \Rightarrow f(x) \geq A.$$

- On dit que f tend vers $-\infty$ en $-\infty$ et l'on note $f \xrightarrow{-\infty} -\infty$ ou $f(x) \xrightarrow{x \rightarrow -\infty} -\infty$ si

$$\forall A \in \mathbb{R}, \exists B \in \mathbb{R}, \forall x \in I, x \leq B \Rightarrow f(x) \leq A.$$

Remarque 2.1.7.

On préférera parfois écrire $x \leq B$ sous la forme $x \in]-\infty, B]$.

Le bloc $\forall x \in I, x \leq B \Rightarrow [\dots]$ s'écrit alors $\forall x \in I \cap]-\infty, B], [\dots]$.

On remarquera la structure commune :

$$\forall [\dots], \exists B \in \mathbb{R}, \forall x \in I, x \leq B \Rightarrow f(x) \in [\dots].$$

Remarque 2.1.8.

On peut aussi remarquer que les trois définitions de « f tend vers $\ell \in \mathbb{R}$ » ont en commun la structure suivante.

$$\forall \varepsilon > 0, \exists [\dots], \forall x \in I, x \in [\dots] \Rightarrow |f(x) - \ell| \leq \varepsilon$$

Exercice 2.1.9.

Dégager la structure commune des trois définitions de « f tend vers $+\infty$ ». Faire de même pour $-\infty$.

Remarque 2.1.10.

Comme dans le cas des suites, on obtient des propositions équivalents en remplaçant les inégalités larges (ou certaines d'entre elles) par des inégalités strictes. En revanche, attention aux inégalités $\varepsilon > 0$ et $\alpha > 0$ qui doivent être conservées strictes.

Remarque 2.1.11.

On peut également remplacer les conditions $A \in \mathbb{R}$ par $A \in \mathbb{R}_+^*$ ou $A \in \mathbb{R}_-^*$ suivant les cas.

Remarque 2.1.12.

L'ordre des quantificateurs dans ces définitions est évidemment essentiel.

Remarque 2.1.13.

Sur les suites, le « $\forall n \geq n_0$ » devait être compris comme portant sur un n entier, de façon à ce que u_n ait un sens.

C'est le « $\forall x \in I$ » qui ici remplit ce rôle, de façon à ce que $f(x)$ soit bien défini.

Attention à ne pas l'oublier !

Remarque 2.1.14.

Remarquez que la caractérisation de la convergence d'une suite à l'aide de « $\forall \varepsilon \exists n_0 \dots$ » est très similaire à celle de l'existence d'une limite finie pour une fonction en $+\infty$, de même la caractérisation de la divergence vers $+\infty$ d'une suite est très similaire à celle du fait qu'une fonction tend vers $+\infty$ en $+\infty$.

Cette similarité n'est pas un hasard : regardez ce que donne la définition de limite de fonction (utilisant les voisinages) pour une fonction définie sur $\mathbb{N}$. Que constatez-vous ?

Remarque 2.1.15.

Pour donner la définition de limite en un point, nous avons dû traiter neuf cas différents, ce qui est assez fastidieux. Comme dans le cas des suites, la notion de voisinage permet de donner une définition unifiée, regroupant tous les cas en une seule définition. Cette définition unifiée est la suivante :

Soit $a \in \bar{I}$ et $\ell \in \bar{\mathbb{R}}$. On dit que f admet ℓ pour limite en a et on note $f \xrightarrow[a]{\ell}$ ou $f(x) \xrightarrow{x \rightarrow a} \ell$ si pour tout voisinage $V \in \mathcal{V}(\ell)$, il existe un voisinage $W \in \mathcal{V}(a)$ tel que $\forall x \in W \cap I \quad f(x) \in V$.

Cette définition étant plus abstraite et hors-programme, nous ne l'utiliserons pas en priorité dans ce cours, même si elle peut systématiquement être employée. Cependant, certaines démonstrations seront données sans la notion de voisinage, puis une seconde fois avec la notion de voisinage. Vous pourrez voir les simplifications que ces voisinages apportent et vous entraîner à réécrire d'autres démonstrations grâce aux voisinages.

Théorème 2.1.16.

Soit $a \in \bar{I}$, soit $\ell_1, \ell_2 \in \bar{\mathbb{R}}$. Si $f(x) \xrightarrow{x \rightarrow a} \ell_1$ et $f(x) \xrightarrow{x \rightarrow a} \ell_2$, alors $\ell_1 = \ell_2$.

Démonstration.

Par symétrie et en supposant que $\ell_1 \neq \ell_2$, on a trois cas possibles pour a ($a \in \mathbb{R}$, $a = +\infty$ et $a = -\infty$), et pour chaque choix de a on a quatre cas possibles :

- $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$;
- $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$;
- $\ell_1 = -\infty$ et $\ell_2 = +\infty$.

Cela donne donc douze cas à traiter. Nous ne les détaillons pas tous, le lecteur saura les retrouver sans difficulté.

Supposons $a \in \mathbb{R}$, $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$. Posons $\varepsilon = \frac{1}{3}|\ell_1 - \ell_2| > 0$. Il existe donc $\alpha_1, \alpha_2 > 0$ tels que, pour tout $x \in I$,

- si $|x - a| \leq \alpha_1$, alors $|f(x) - \ell_1| \leq \varepsilon$;
- si $|x - a| \leq \alpha_2$, alors $|f(x) - \ell_2| \leq \varepsilon$.

Soit $\alpha = \min(\alpha_1, \alpha_2) > 0$. Comme a adhère à I , il existe $x \in I$ tel que $|x - a| \leq \alpha$. Les deux conditions précédentes sont donc vérifiées, et

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - f(x) - (\ell_2 - f(x))| \\ &\leq |\ell_1 - f(x)| + |(\ell_2 - f(x))| \\ &\leq \frac{2}{3}|\ell_1 - \ell_2|. \end{aligned}$$

Cela contredit le fait que $\ell_1 \neq \ell_2$.

Supposons $a = +\infty$, $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$. Soit $A = \ell_1 + 1$ et $\varepsilon = \frac{1}{2}$. Il existe donc $B_1, B_2 \in \mathbb{R}$ tels que, pour tout $x \in I$,

- si $x \geq B_1$, alors $|f(x) - \ell_1| \leq \varepsilon$, notamment $f(x) \leq \ell_1 + \frac{1}{2} < A$;
- si $x \geq B_2$, alors $f(x) \geq A$.

Soit $B = \max(B_1, B_2)$. Comme $\sup I = +\infty$, il existe $x \in I$ tel que $x \geq B$. On a alors simultanément $f(x) < A$ et $f(x) \geq A$, ce qui est absurde. $\square$

Définition 2.1.17.

Soit $a \in \bar{I}$. S'il existe $\ell \in \bar{\mathbb{R}}$ tel que $f(x) \xrightarrow{x \rightarrow a} \ell$, alors cet élément est appelé « limite de f en a » et est noté $\lim_a f$ ou $\lim_{t \rightarrow a} f(t)$.



Le symbole $\lim_{x \rightarrow a}$ ne peut s'utiliser qu'après avoir montré l'existence de ladite limite. L'utiliser avant est une erreur grave. On préférera systématiquement utiliser l'écriture $f(x) \xrightarrow{x \rightarrow a} \ell$.

Théorème 2.1.18.

Toute fonction possédant une limite *finie* en $a \in \mathbb{R}$ est bornée au **voisinage** de a .

Démonstration.

Comme pour les suites. $\square$

Remarque 2.1.19.

Si f admet une limite infinie en $a \in \mathbb{R}$, alors f n'est pas bornée au voisinage de a .

Proposition 2.1.20.

Si $a \in I$ et si f tend vers $\ell \in \mathbb{R}$ en a , alors $\ell = f(a)$.



Il s'agit bien d'être certain que a appartient à I (et pas seulement à $\bar{I}$!).

Démonstration.

Supposons $\ell = +\infty$. soit $A = f(a) + 1$. Il existe $\alpha > 0$ tel que, pour tout $x \in I \cap [a - \alpha, a + \alpha]$, $f(x) \geq A$. Or, $a \in I \cap [a - \alpha, a + \alpha]$, donc $f(a) \geq f(a) + 1$, ce qui est absurde. De même, $\ell = -\infty$ est absurde, donc $\ell \in \mathbb{R}$.

Soit $\varepsilon > 0$, soit $\alpha > 0$ tel que, pour tout $x \in I \cap [a - \alpha, a + \alpha]$, $|f(x) - \ell| \leq \varepsilon$. Or, on a toujours $a \in I \cap [a - \alpha, a + \alpha]$, car $a \in I$. Ainsi, $|f(a) - \ell| \leq \varepsilon$.

On a donc : pour tout $\varepsilon > 0$, $|f(a) - \ell| \leq \varepsilon$. Cela implique bien que $f(a) = \ell$ (sinon, prendre $\varepsilon = \frac{1}{2}|f(a) - \ell|$). $\square$

Remarque 2.1.21.

Pour tous a et ℓ réels, on montre facilement que les assertions suivantes sont équivalentes.

- (i) $f \xrightarrow{a} \ell$
- (ii) $f - \ell \xrightarrow{a} 0$
- (iii) $|f - \ell| \xrightarrow{a} 0$
- (iv) $f(a + h) \xrightarrow{h \rightarrow 0} \ell$

Exemple 2.1.22.

Pour s'entraîner à manipuler la définition (mais ce n'est pas la meilleure méthode dans la pratique), considérons la fonction $f : \mathbb{R} \rightarrow \mathbb{R}$ Mon-

$x \mapsto x^3 + x$
trons $f(x) \xrightarrow{x \rightarrow 1} 2$.

On a, pour tout $x \in \mathbb{R}$, $f(x) - 2 = (x - 1)(x^2 + x + 2)$.

Si $x \in [0, 2]$, alors $|x| \leq 2$ et donc (inégalité triangulaire) $|x^2 + x + 2| \leq 8$.

Soit $\varepsilon > 0$. Si $x \in \left[1 - \frac{\varepsilon}{8}; 1 + \frac{\varepsilon}{8}\right]$, alors $|x - 1| \leq \frac{\varepsilon}{8}$.

Ainsi, avec $\alpha = \min\left(1; \frac{\varepsilon}{8}\right)$, si $|x - 1| \leq \alpha$, on a simultanément $|x^2 + x + 2| \leq 8$ et $|x - 1| \leq \frac{\varepsilon}{8}$.

On a alors $|f(x) - 2| \leq \varepsilon$.

Donc on a bien

$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in \mathbb{R}, |x - 1| \leq \alpha \Rightarrow |f(x) - 2| \leq \varepsilon$.

Donc $f(x) \xrightarrow{x \rightarrow 1} 2$.

Remarque 2.1.23.

Si u est une suite réelle et $\ell \in \mathbb{R}$, la définition de « $u_n \xrightarrow{n \rightarrow +\infty} \ell$ » donnée dans le chapitre sur les suites numériques correspond exactement à celle donnée ici, quand on voit u comme une fonction de $\mathbb{N}$ dans $\mathbb{R}$.

2.2 Limites à gauche et à droite en un point.**Définition 2.2.1.**

Soient $a \in \mathbb{R}$ et $\ell \in \mathbb{R}$.

- (i) Si f est définie au voisinage de a à gauche, c'est-à-dire si $a \in I \cap]-\infty, a[$, on dit que f admet ℓ pour limite à gauche en a (ou tend vers ℓ à gauche en a) si $f|_{I \cap]-\infty, a[}$ admet ℓ pour limite en a .

On note alors $f(x) \xrightarrow{x \rightarrow a^-} \ell$, $f(x) \xrightarrow{x \rightarrow a^-} \ell$ ou encore $f \xrightarrow{a^-} \ell$.

Si elle existe, la limite à gauche est unique (puisque c'est une limite) et dans ce cas elle est notée $\lim_{a^-} f$, $\lim_{x \rightarrow a^-} f(x)$ ou $\lim_{\substack{x \rightarrow a \\ x < a}} f(x)$.

- (ii) On définit de la même manière la notion de *limite à droite*.



Dans la définition de limite à gauche, c'est la fonction $f|_{I \cap]-\infty, a[}$ qu'il faut considérer, et non la fonction $f|_{I \cap]-\infty, a]}$ (intervalle fermé en a). En effet, on veut que la fonction de la figure XIV.1 ait une limite à gauche, ce qui n'est le cas qu'avec une restriction à un intervalle ouvert en a .

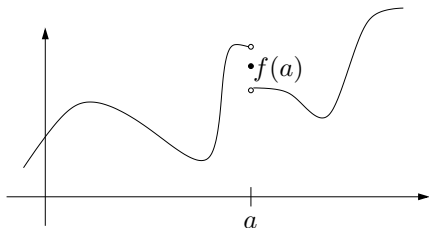


FIGURE XIV.1 – Fonction f sans limite en a , ayant des limites à droite et à gauche en a différentes.

Remarque 2.2.2.

Comme pour les limites, l'existence d'une limite à gauche / droite s'écrit avec des ε . Par exemple, dans le cas où $a, \ell \in \mathbb{R}$, f admet ℓ pour limite à gauche en a si et seulement si on a

$$\forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall x \in I \\ a - \alpha \leq x < a \Rightarrow |f(x) - \ell| \leq \varepsilon$$

On a le même genre de proposition pour les 5 autres cas (il y a au total 6 cas suivant qu'il s'agit d'une limite à gauche ou à droite d'une part et que la limite est réelle, égale à $+\infty$ ou $-\infty$ d'autre part).

Exemple 2.2.3.

On a $\frac{1}{x} \xrightarrow[x>0]{x \rightarrow 0} +\infty$ et $\frac{1}{x} \xrightarrow[x<0]{x \rightarrow 0} -\infty$.

Théorème 2.2.4.

Soit a un réel appartenant à I , et qui n'est pas une borne de I . Soit $\ell \in \mathbb{R}$. Alors $f \xrightarrow{a} \ell$ si et seulement si on a simultanément

- (i) $f \xrightarrow{a^-} \ell$
- (ii) $f \xrightarrow{a^+} \ell$
- (iii) $f(a) = \ell$.



Le point (iii) est indispensable, sinon la fonction de la figure XIV.2 aurait une limite en a .

Démonstration. $(\Rightarrow)$ Supposons d'abord $f \xrightarrow{a} \ell$.

Nous avons déjà observé que $f(a) = \ell$ est nécessaire. Il est alors immédiat d'après les définitions que $f \xrightarrow{a^-} \ell$ et $f \xrightarrow{a^+} \ell$.

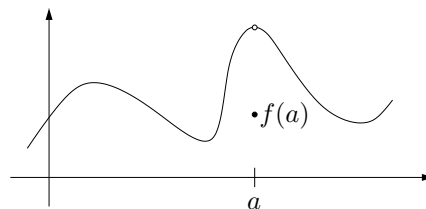


FIGURE XIV.2 – Fonction f ayant des limites à gauche et à droite en a égales, mais pas de limite en a .

$(\Leftarrow)$ Réciproquement, supposons qu'on ait les trois conditions (i), (ii) et (iii). On a $f(a) = \ell$, donc $\ell \in \mathbb{R}$. Soit $\varepsilon > 0$. Il existe $\alpha^-, \alpha^+ \in \mathbb{R}_+^*$ vérifiant

$$\begin{cases} \forall x \in I & a - \alpha^- \leq x < a \Rightarrow |f(x) - \ell| \leq \varepsilon \\ \forall x \in I & a < x \leq a + \alpha^+ \Rightarrow |f(x) - \ell| \leq \varepsilon \end{cases}$$

Posons alors $\alpha = \min\{\alpha^-, \alpha^+\}$ et montrons $\forall x \in I$ $|x - a| \leq \alpha \Rightarrow |f(x) - \ell| \leq \varepsilon$.

Soit $x \in I$ tel que $|x - a| \leq \alpha$, c'est-à-dire $a - \alpha \leq x \leq a + \alpha$. Alors

1. si $a - \alpha \leq x < a$, on a en fait $a - \alpha^- \leq x < a$ et donc $|f(x) - \ell| \leq \varepsilon$;
2. si $x = a$, $f(x) = f(a) = \ell$ et donc $|f(x) - \ell| \leq \varepsilon$;
3. si $a < x \leq a + \alpha$, on a en fait $a < x \leq a + \alpha^+$ et donc $|f(x) - \ell| \leq \varepsilon$.

Dans tous les cas on a bien $|f(x) - \ell| \leq \varepsilon$.

On a donc $f \xrightarrow{a} \ell$.

□

Exemple 2.2.5.

Le théorème précédent permet de montrer que, l'application $f : \mathbb{R} \rightarrow \mathbb{R}$

$$x \mapsto \begin{cases} e^x & \text{si } x \geq 0 \\ 1 - x & \text{si } x < 0 \end{cases}$$

tend vers 1 en 0.

Remarque 2.2.6.

On n'utilisera la caractérisation d'une limite par le théorème 2.2.4 que quand la fonction n'est pas définie de la même manière à gauche et à droite du point considéré. Sinon, cela n'a aucun intérêt et l'on travaillera directement avec la définition générale de limite, ou ses caractérisations.

Remarque 2.2.7.

On pourrait aussi définir, mais le besoin s'en fera rarement sentir, la notion de « limite épointée », que l'on noterait $f(x) \xrightarrow[x \neq a]{x \rightarrow a} \ell$, qui signifie

$$f|_{I \setminus \{a\}} \xrightarrow{a} \ell.$$

De même, les notations $f(x) \xrightarrow[x \leq a]{x \rightarrow a} \ell$ et $f(x) \xrightarrow[x \geq a]{x \rightarrow a} \ell$ ne devraient pas vous faire peur.

3 Propriétés des limites de fonctions.

3.1 Opérations sur les limites.

Les résultats usuels valables pour les limites de suite restent valables :

1. Soit $f : I \rightarrow \mathbb{R}$, $a \in \bar{I}$ et $\ell \in \mathbb{R}$. Alors

$$\begin{aligned} f \xrightarrow[a]{a} \ell &\iff f - \ell \xrightarrow[a]{a} 0 \\ f \xrightarrow[a]{a} 0 &\iff |f(x)| \xrightarrow[x \rightarrow a]{} 0 \\ f \xrightarrow[a]{a} \ell &\iff |f(x) - \ell| \xrightarrow[x \rightarrow a]{} 0 \end{aligned}$$

2. Soit $f, g : I \rightarrow \mathbb{R}$ et $a \in \bar{I}$. Si f est bornée au voisinage de a et $g \xrightarrow[a]{a} 0$, alors $f \times g \xrightarrow[a]{a} 0$.

Exemple 3.1.1.

Le deuxième point permet de montrer $\frac{\sin x}{x} \xrightarrow[x \rightarrow +\infty]{} 0$.

Pour les opérations usuelles (somme, produit et inverse), les résultats valables pour les limites de suites sont toujours valables pour les fonctions, et les démonstrations sont tout à fait similaires. Nous ne les redémontrons donc pas, mais vous devez savoir les faire sans problème.

Voyons le théorème sur la composition de deux fonctions ayant une limite :

Théorème 3.1.2.

Soient $f : I \rightarrow \mathbb{R}$ et $g : J \rightarrow \mathbb{R}$ deux applications vérifiant $f(I) \subset J$ et soit $a \in \bar{I}$, $b \in \bar{J}$ et $\ell \in \mathbb{R}$. Si $f \xrightarrow[a]{a} b$ et $g \xrightarrow[b]{b} \ell$, alors $g \circ f \xrightarrow[a]{a} \ell$.

Remarque 3.1.3.

L'hypothèse $b \in \bar{J}$ est superflue : si $f : I \rightarrow J$ a une limite b en a , alors automatiquement, $b \in \bar{J}$.

Démonstration.

On a vingt-sept cas à distinguer, selon si a , b et ℓ sont

chacun un réel, $+\infty$ ou $-\infty$. Nous ne détaillerons pas tous ces cas, le lecteur intéressé saura les retrouver facilement.

Si $a \in \mathbb{R}$, $b \in \mathbb{R}$ et $\ell \in \mathbb{R}$. Soit $\varepsilon > 0$, posons $V_\ell = [\ell - \varepsilon, \ell + \varepsilon]$. Il existe $\alpha > 0$ tel que, pour tout $y \in J \cap V_b$, avec $V_b = [b - \alpha, b + \alpha]$, on a $g(y) \in V_\ell$. Il existe donc $\eta > 0$ tel que, pour tout $x \in I \cap V_a$, avec $V_a = [a - \eta, a + \eta]$, on a $f(x) \in V_b$. Soit $x \in I \cap V_a$. On a, d'une part, $f(x) \in V_b$ et, d'autre part, $f(x) \in J$. Donc $g(f(x)) \in V_\ell$. On a bien montré $g \circ f \xrightarrow[a]{a} \ell$.

Si $a = +\infty$, $b = -\infty$ et $\ell = +\infty$. Soit $A \in \mathbb{R}$, posons $V_\ell = [A, +\infty[$. Il existe $B \in \mathbb{R}$ tel que, pour tout $y \in J \cap V_b$, avec $V_b =]-\infty, B]$, on a $g(y) \in V_\ell$. Il existe donc $C \in \mathbb{R}$ tel que, pour tout $x \in I \cap V_c$, avec $V_c = [C, +\infty[$, on a $f(x) \in V_b$. Soit $x \in I \cap V_c$. On a, d'une part, $f(x) \in V_b$ et, d'autre part, $f(x) \in J$. Donc $g(f(x)) \in V_\ell$. On a bien montré $g \circ f \xrightarrow[+\infty]{a} +\infty$. $\square$

Remarque 3.1.4.

La structure de la preuve précédente ne change pas en fonction des natures de a , b et ℓ , mais seulement les formes des intervalles V_a , V_b , V_ℓ .

À cause des vingt-sept cas à distinguer, cette démonstration est un exemple typique de démonstration où la notion de voisinage fait gagner du temps. Redémontrons donc ce résultat :

Démonstration.

Soit $V \in \mathcal{V}(\ell)$. Montrons qu'il existe un voisinage W de a vérifiant $(g \circ f)(W \cap I) \subset V$.

On a $g \xrightarrow[b]{b} \ell$, donc il existe un voisinage W' de b vérifiant $g(W' \cap J) \subset V$.

Or $f \xrightarrow[a]{a} b$, donc il existe un voisinage W de a vérifiant $f(W \cap I) \subset W'$.

Or $f(I) \subset J$, donc $f(W \cap I) \subset J$, donc $f(W \cap I) \subset W' \cap J$.

Donc $(g \circ f)(W \cap I) \subset g(W' \cap J) \subset V$.

On a donc bien $g \circ f \xrightarrow[a]{a} \ell$. $\square$

Remarque 3.1.5.

On a vu (remarque 2.1.10) que la définition de la limite d'une suite n'est qu'un cas particulier de celle de fonction. Ce théorème de composition sur les fonctions a donc pour corollaire celui qu'on a énoncé au chapitre concernant les limites de suites sur la composition d'une fonction et d'une suite.

Exemple 3.1.6.

Ce théorème permet de montrer par exemple que $\ln(\tan x^2) \xrightarrow[x \rightarrow \frac{\sqrt{\pi}}{2}]{} 0$.

Théorème 3.1.7 (Caractérisation séquentielle des limites).

Soient $a \in \bar{I}$, $\ell \in \mathbb{R}$. On a équivalence entre :

- (i) $f(x) \xrightarrow{x \rightarrow a} \ell$
- (ii) pour toute suite (u_n) telle que $u_n \in I$ et $u_n \xrightarrow{n \rightarrow +\infty} a$, on a $f(u_n) \xrightarrow{n \rightarrow +\infty} \ell$.

Démonstration.

Traitons les cas a et ℓ finis (les autres cas se traitent de manière similaire).

(i) $\Rightarrow$ (ii) C'est une conséquence immédiate du résultat de composition d'une application et d'une suite.

$\neg$ (i) $\Rightarrow$ $\neg$ (ii) Supposons $f \not\xrightarrow{a} \ell$. Alors il existe $\varepsilon > 0$ vérifiant

$$\forall \eta \in \mathbb{R}_+^* \exists x \in I \quad (x \in [a - \eta, a + \eta] \text{ et } |f(x) - \ell| > \varepsilon) \quad (\text{XIV.1})$$

Soit alors $n \in \mathbb{N}$. Comme $\frac{1}{n+1} \in \mathbb{R}_+^*$, d'après l'assertion (XIV.1), il existe $u_n \in I$ vérifiant

- (a) $u_n \in [a - \frac{1}{n+1}, a + \frac{1}{n+1}]$
- (b) et $|f(u_n) - \ell| > \varepsilon$.

On a donc construit une suite u d'éléments de I . Le point (a) nous assure qu'elle converge vers a , le second que $f(u_n)$ ne tend pas vers ℓ (une suite minorée par un réel strictement positif ne saurait tendre vers 0). $\square$

Ce théorème peut être vu comme l'analogue pour les fonctions du théorème suivant sur les suites : si une suite a une limite, toutes ses sous-suites tendent aussi vers cette limite.

Ainsi, il est particulièrement intéressant de contraposer ce résultat, ce qui nous donne des méthodes pour montrer qu'une fonction n'a pas de limite en un point :

Corollaire 3.1.8.

Soit $a \in \bar{I}$.

- (i) S'il existe une suite $(u_n) \in I^{\mathbb{N}}$ telle que $u_n \xrightarrow{n \rightarrow +\infty} a$ et $(f(u_n))$ n'a pas de limite, alors f n'a pas de limite en a .
- (ii) S'il existe deux suites $(u_n), (v_n) \in I^{\mathbb{N}}$ tendant toutes deux vers a , et telles que $(f(u_n))$ et $(f(v_n))$ ont des limites différentes, alors f n'a pas de limite en a .

Exercice 3.1.9.

La fonction $f : \mathbb{R}_+^* \rightarrow \mathbb{R}$ admet-elle
 $x \mapsto \sin(1/x)$
une limite en 0 ?

3.2 Passage à la limite et relations d'ordre.

Les théorèmes suivants sont analogues à des résultats déjà vu sur les suites.

Théorème 3.2.1.

Soit $f : I \rightarrow \mathbb{R}$, $a \in \bar{I}$ et $(m, M, \ell) \in \mathbb{R}^3$.

Supposons $f \xrightarrow{a} \ell$ et $m < \ell < M$.

Alors, au voisinage de a , on a $m < f(x) < M$.

Démonstration.

On traite le cas $a \in \mathbb{R}$, les autres cas sont laissés au lecteur.

Soit $\varepsilon = \frac{\min(\ell - m, M - \ell)}{2} > 0$. On a bien $[\ell - \varepsilon; \ell + \varepsilon] \subset]m, M[$.

Ainsi, il existe $\alpha > 0$ tel que, pour tout $x \in [a - \alpha, a + \alpha] \cap I$, on a $f(x) \in [\ell - \varepsilon; \ell + \varepsilon]$, donc $f(x) \in]m, M[$. $\square$

Avec les voisinages :

Démonstration.

$]m, M[$ est un intervalle ouvert contenant ℓ , c'est donc un voisinage de ℓ . Donc il existe un voisinage V de a tel que pour tout $x \in V \cap I$, on a $f(x) \in]m, M[$. $\square$

Remarque 3.2.2.

Le plus souvent, ce résultat s'applique sous la forme suivante :

Soit $f : I \rightarrow \mathbb{R}$, $a \in \bar{I}$ vérifiant $f \xrightarrow{a} \ell$. Alors

- (i) Soit $M \in \mathbb{R}$ vérifiant $\ell < M$. Alors au voisinage de a , $f(x) < M$.
- (ii) Soit $m \in \mathbb{R}$ vérifiant $m < \ell$. Alors au voisinage de a , $f(x) > m$.



Ce résultat est faux avec des inégalités larges : ainsi $x^2 \xrightarrow{x \rightarrow 0} 0$ et donc sa limite est négative. Mais dire que pour x au voisinage de 0 on a $x^2 \leq 0$ est faux.

Corollaire 3.2.3 (Passage à la limite dans une inégalité).

Soit $a \in \bar{I}$ et $f : I \rightarrow \mathbb{R}$ vérifiant $f \xrightarrow{a} \ell$. Soit $(m, M) \in \mathbb{R}^2$.

- (i) Si M majore f au voisinage de a , alors $\ell \leq M$.
- (ii) Si m minore f au voisinage de a , alors $m \leq \ell$.

Démonstration.

On traite le cas $a \in \mathbb{R}$, les autres cas sont laissés au lecteur.

- (i) Supposons que M majore f sur l'intersection de I et d'un intervalle $V_1 = [a - \alpha, a + \alpha]$, avec $\alpha > 0$.
Par l'absurde, supposons $\ell > M$. D'après le théorème 3.2.1, il existe $\eta > 0$ tel que, avec $V_2 = [a - \eta, a + \eta]$, pour tout $x \in V_2 \cap I$, on a $f(x) > M$.
Pour tout $x \in V_1 \cap V_2 \cap I$, on a alors $f(x) > M$ et $f(x) \leq M$.
Or $V_1 \cap V_2 \cap I$ est non vide, c'est donc absurde.
On a donc $\ell \leq M$.
- (ii) On constate qu'au voisinage de a , $-m$ majore $-f$ et l'on applique le résultat du (i) à $-f$, $-\ell$ et $-m$.

□

Corollaire 3.2.4 (Passage à la limite dans une inégalité, deuxième version).

Soit $f, g : I \rightarrow \mathbb{R}$, $a \in \bar{I}$ et $(\ell, \ell') \in \mathbb{R}^2$.

Supposons $f \xrightarrow{a} \ell$, $g \xrightarrow{a} \ell'$ et $f(x) \leq g(x)$ au voisinage de a . Alors $\ell \leq \ell'$.

Démonstration.

On a $(g - f)(x) \geq 0$ pour x au voisinage de a et $g - f \xrightarrow{a} \ell' - \ell$. Donc d'après le corollaire 3.2.3, on a $\ell' - \ell \geq 0$, donc $\ell \leq \ell'$. □



Les inégalités strictes ne sont pas conservées par passage à la limite. Par exemple, au voisinage de $+\infty$ on a $e^{-x} > 0$, mais on a $e^{-x} \xrightarrow{x \rightarrow +\infty} 0$.

4 Théorèmes d'existence.

4.1 Théorèmes des gendarmes et de minoration/majoration.

On retrouve sur les limites de fonctions les mêmes théorèmes d'encadrement que pour les suites.

Théorème 4.1.1 (Théorème d'encadrement, ou théorème des gendarmes).

Soit $f, m, M : I \rightarrow \mathbb{R}$ trois applications, $a \in \bar{I}$ et $\ell \in \mathbb{R}$.

Supposons qu'on a $m \xrightarrow{a} \ell$ et $M \xrightarrow{a} \ell$ et qu'au voisinage de a on a $m(x) \leq f(x) \leq M(x)$.

Alors, f tend vers ℓ en a .

Démonstration.

On traite le cas $a \in \mathbb{R}$. Les autres cas sont laissés au lecteur, la structure de la démonstration de changeant pas.

Soit $\varepsilon > 0$, posons $V_\ell = [\ell - \varepsilon, \ell + \varepsilon]$. Il existe $\alpha, \beta > 0$ tels que, pour tout $x \in I$,

- si $x \in V_a$, alors $m(x) \in V_\ell$;
- si $x \in V'_a$, alors $M(x) \in V_\ell$;

avec $V_a = [a - \alpha, a + \alpha]$ et $V'_a = [a - \beta, a + \beta]$. Soit enfin $\eta > 0$ tel que, pour tout $x \in I$, si $x \in I \cap V''_a$, avec $V''_a = [a - \eta, a + \eta]$, alors $m(x) \leq f(x) \leq M(x)$. Il suffit de remarquer que, si $x \in I \cap V_a \cap V'_a \cap V''_a$, alors $m(x) \leq f(x) \leq M(x)$ et $m(x), M(x) \in V_\ell$, donc $f(x) \in V_\ell$, car V_ℓ est un intervalle. On a donc bien $f \xrightarrow{a} \ell$. □

Théorème 4.1.2 (Théorème de minoration).

Soit $f, m : I \rightarrow \mathbb{R}$ deux applications, soit $a \in \bar{I}$.

Supposons qu'on a $m \xrightarrow{a} +\infty$ et qu'au voisinage de a , on a $m(x) \leq f(x)$.

Alors, f admet une limite en a et cette limite vaut $+\infty$.

Démonstration.

On traite le cas $a = -\infty$. Les autres cas sont laissés au lecteur, la structure de la démonstration de changeant pas.

Soit $A \in \mathbb{R}$, posons $V_{+\infty} = [A, +\infty[$. Il existe $B \in \mathbb{R}$ tel que, pour tout $x \in I$, avec $V_a =]-\infty, B]$, si $x \in V_a$, alors $m(x) \in V_{+\infty}$. Soit enfin $C \in \mathbb{R}$ tel que, avec $V'_a =]-\infty, C]$, pour tout $x \in I$, si $x \in V'_a$, alors $m(x) \leq f(x)$. Il suffit de remarquer que, si $x \in I \cap V_a \cap V'_a$, alors $m(x) \leq f(x)$ et $m(x) \in V_{+\infty}$, donc $f(x) \in V_{+\infty}$. On a donc bien $f \xrightarrow{a} +\infty$. □

Théorème 4.1.3 (Théorème de majoration).

Soit $f, M : I \rightarrow \mathbb{R}$ deux applications, $a \in \bar{I}$.

Supposons qu'on a $M \xrightarrow{a} -\infty$ et qu'au voisinage de a , on a $f(x) \leq M(x)$.

Alors, f admet une limite en a et cette limite vaut $-\infty$.

Démonstration.

Il suffit d'appliquer le théorème de minoration à $-f$. □

Corollaire 4.1.4.

Soient $f, g : I \rightarrow \mathbb{R}$ deux applications et $a \in \bar{I}$. Si au voisinage de a on a $|f| \leq g$ et si $g \xrightarrow{a} 0$, alors $f \xrightarrow{a} 0$.

Démonstration.

Il suffit de remarquer qu'au voisinage de a , on a $-g \leq f \leq g$. $\square$

4.2 Théorème de la limite monotone.

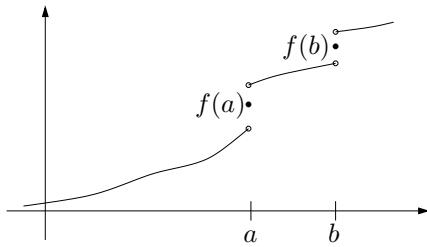


FIGURE XIV.3 – Illustration de limite monotone : à retenir !

Théorème 4.2.1.

Soit $f : I \rightarrow \mathbb{R}$ une application croissante. On note α et β les bornes inférieure et supérieure de I dans $\mathbb{R}$. Alors :

- (i) f possède une limite à gauche (resp. à droite) en tout point a de $] \alpha, \beta]$ (resp. $[\alpha, \beta [$) et l'on a, pour chaque a où ces limites ont un sens,

$$f(x) \xrightarrow[x < a]{x \rightarrow a} \sup_{I \cap]-\infty, a[} f$$

ainsi que

$$f(x) \xrightarrow[x > a]{x \rightarrow a} \inf_{I \cap]a, +\infty[} f.$$

- (ii) Soient $a, b \in \bar{I}$ tels que $a < b$. Alors,

$$\lim_{a^-} f \leq f(a) \leq \lim_{a^+} f \leq \lim_{b^-} f \leq f(b) \leq \lim_{b^+} f.$$

- (iii) Dans $\bar{\mathbb{R}}$, f admet une limite à droite en α . Si f est minorée, cette limite est finie, sinon elle vaut $-\infty$.

- (iv) Dans $\bar{\mathbb{R}}$, f admet une limite à gauche en β . Si f est majorée, cette limite est finie, sinon elle vaut $+\infty$.

Si f est décroissante, on a bien sûr des résultats analogues.

Démonstration. (i) On ne montre le résultat que pour la limite à gauche.

Soit $a \in] \alpha, \beta]$. On pose $V = f(I \cap]-\infty, a[) = \{ f(x) \mid x < a \}$. L'ensemble V est non vide puisque $I \cap]-\infty, a[$ est non vide. Posons $\ell = \sup_{x < a} f(x)$,

cette borne supérieure étant prise dans $\mathbb{R}$. On a $\ell = +\infty$ ou $\ell \in \mathbb{R}$. Distinguons ces deux cas :

- (a) $\ell = +\infty$. Alors soit M un réel fixé, il existe $y \in I \cap]-\infty, a[$ tel que $f(y) \geq M$.

Alors, puisque f est croissante, pour tout $x \in]y, a[\cap I$, on a $f(x) \geq M$.

Donc f prend ses valeurs dans $[M, +\infty[$ au voisinage de a , à gauche.

On a donc bien $f \xrightarrow{a^-} +\infty$.

- (b) $\ell \in \mathbb{R}$. Alors, soit $\varepsilon > 0$. Il existe $y \in I \cap]-\infty, a[$ tel que $f(y) \geq \ell - \varepsilon$.

Alors, pour tout $x \in]y, a[\cap I$, on a $f(x) \geq \ell - \varepsilon$, f étant croissante, et $f(x) \leq \ell$ par définition de ℓ .

On en déduit qu'au voisinage à gauche de a , f prend ses valeurs dans $[\ell - \varepsilon, \ell + \varepsilon]$.

f admet donc pour limite ℓ en a à gauche.

- (ii) Remarquons tout d'abord que, f étant croissante $\{ f(x) \mid x \in I \cap]-\infty, a[\}$ est majoré par $f(a)$, donc d'après le point (i), on a $\lim_{a^-} f \leq f(a)$.

De la même façon, on a $f(a) \leq \lim_{a^+} f$, $\lim_{b^-} f \leq f(b)$ et $f(b) \leq \lim_{b^+} f$.

Par ailleurs, $\lim_{b^-} f$ majore $f(]a, b[)$ et $\lim_{a^+} f$ minore ce même ensemble, qui est non vide. Donc $\lim_{a^+} f \leq \lim_{b^-} f$.

On a donc le résultat.

- (iii) (iii) (resp. (iv)) sont des conséquences immédiates de (i), l'existence d'un minorant (resp. majorant) étant équivalente au fait que la borne inférieure (resp. supérieure) soit finie.

Pour le cas d'une fonction décroissante, il suffit d'appliquer le résultat sur les fonctions croissantes à $-f$. $\square$

Exercice 4.2.2.

Soit f un endomorphisme croissant du groupe $(\mathbb{R}, +)$.

Déterminer $f(x)$ pour chaque $x \in \mathbb{N}$, puis $x \in \mathbb{Z}$ et $x \in \mathbb{Q}$.

Déterminer enfin f sur $\mathbb{R}$.

5 Cas des fonctions à valeurs complexes.

Dans cette partie, on considère une application complexe $f : I \rightarrow \mathbb{C}$.

Notons tout de suite que les notions de fonction complexe majorée, minorée ou monotone n'ont **aucun sens**, car il n'y a pas de relation d'ordre naturelle sur $\mathbb{C}$. Cependant, on peut définir la notion de fonction complexe bornée.

Définition 5.0.1.

On dit que f est *bornée* s'il existe $K \in \mathbb{R}^*$ tel que pour tout $x \in I$ on ait $|f(x)| \leq K$.

Remarque 5.0.2.

f est bornée si et seulement si $\operatorname{Re} f$ et $\operatorname{Im} f$ sont bornées.

Définition 5.0.3.

Soit $a \in \mathbb{C}$. Une propriété P est vraie au voisinage de a s'il existe $r > 0$ tel que, pour tout $z \in \mathbb{C}$, si $|z - a| \leq r$, alors $P(z)$ est vraie.

Remarque 5.0.4.

La notion bidimensionnelle de voisinage complexe donnée ici généralise assez bien la notion unidimensionnelle de voisinage réel, néanmoins d'autres définitions seraient possibles : on pourrait utiliser, à la place de disques fermés, des disques ouverts ou bien des rectangles (fermés ou ouverts).

Définition 5.0.5.

Soit $a \in \bar{I}$ et $\ell \in \mathbb{C}$. On dit que f *admet ℓ pour limite en a* , ou f *tend vers ℓ en a* , si $|f(x) - \ell| \xrightarrow{x \rightarrow a} 0$.

On note bien entendu ceci $f \xrightarrow{a} \ell$ ou encore $f(x) \xrightarrow{x \rightarrow a} \ell$.

Remarque 5.0.6.

Ceci nous ramène au cas d'une limite d'une fonction à valeurs réelles.

Remarque 5.0.7.

La définition quantifiée de « f tend vers ℓ en a » s'écrit comme pour une fonction réelle :

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow |f(x) - \ell| \leq \varepsilon.$$

Théorème 5.0.8.

Soit $a \in \bar{I}$ et $\ell \in \mathbb{C}$. Les deux assertions suivantes sont équivalentes :

- (i) $f \xrightarrow{a} \ell$;
- (ii) $\operatorname{Re}(f) \xrightarrow{a} \operatorname{Re}(\ell)$ et $\operatorname{Im}(f) \xrightarrow{a} \operatorname{Im}(\ell)$.

Démonstration.

Cette démonstration s'effectue comme celle du théorème équivalent concernant les suites complexes. $\square$

Exemple 5.0.9.

$$\frac{e^{ix}}{1+x^2} \xrightarrow{x \rightarrow +\infty} 0$$

Théorème 5.0.10.

Si f a une limite en un point de $\bar{I}$, cette limite est unique.

Démonstration.

Deux démonstrations sont possibles : ou bien on utilise le théorème 5.0.8, ou bien on reprend la démonstration donnée dans le cas réel (il suffit alors essentiellement de changer des $\mathbb{R}$ en $\mathbb{C}$). $\square$

Certains autres résultats établis pour les fonctions réelles sont toujours valables pour les fonctions complexes :

1. toute fonction à valeurs complexes ayant une limite en un point est bornée au voisinage de ce point,
2. les limites à gauche et à droite en un point peuvent être également définies,
3. la caractérisation séquentielle de la limite est maintenue,
4. la corollaire 4.1.4 du théorème des gendarmes se généralise aux fonctions f à valeurs complexes, ce qui permet également de montrer que le produit d'une fonction bornée au voisinage d'un point a par une fonction de limite nulle en a est une fonction de limite nulle en a .

5. les opérations sur les limites ne faisant pas intervenir de limite infinie demeurent.

Les grands théorèmes ne se généralisent pas, de nouveau à cause du manque de relation d'ordre naturelle sur $\mathbb{C}$.

Chapitre XV

Continuité

Sommaire

1	Définitions et premières propriétés. . .	212
1.1	Définitions.	212
1.2	Prolongement par continuité en un point. .	213
1.3	Caractérisation séquentielle de la continuité.	214
1.4	Opérations sur la continuité.	214
2	Les grands théorèmes.	215
2.1	Théorème des valeurs intermédiaires. .	215
2.2	Image d'un segment par une fonction continue.	217
2.3	Rappels concernant les fonctions strictement monotones.	218
2.4	Monotonie stricte, bijectivité et continuité.	218
3	Extension au cas des fonctions à valeurs complexes.	219

Dans tout ce chapitre, I et J sont des intervalles de $\mathbb{R}$, $f : I \rightarrow \mathbb{R}$ et $a \in I$, sauf mention expresse du contraire.

1 Définitions et premières propriétés.

1.1 Définitions.

Définition 1.1.1.

On dit que f est *continue en a* si f admet une limite **finie** en a . Puisque $a \in I$, on sait que dans ce cas $f \xrightarrow{a} f(a)$, et donc f est continue en a s'écrit :

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I, |x - a| \leq \alpha \Rightarrow |f(x) - f(a)| \leq \varepsilon$$

On dit que f est *continue sur I* si f est continue en tout point de I .

On note $\mathcal{C}(I, \mathbb{R})$ l'ensemble des fonctions continues de I dans $\mathbb{R}$.

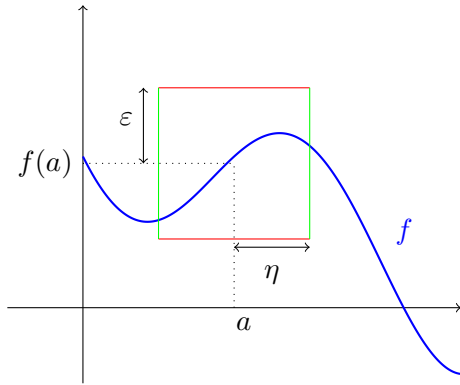


FIGURE XV.1 – Illustration de la définition d'une fonction continue en a , ε et η étant fixés.

Remarque 1.1.2. • On verra que cette définition est cohérente avec l'idée qu'une fonction est continue si et seulement si on peut en tracer le graphe sans lever le crayon.

- Attention à l'ordre des quantificateurs $\forall$ et $\exists$.

Exemple 1.1.3.

Quasiment toutes les fonctions usuelles sont continues.

- La fonction $\cos$: pour tous réels x et x_0 , on a en effet

$$\begin{aligned} |\cos x - \cos x_0| &= \left| -2 \sin \frac{x + x_0}{2} \sin \frac{x - x_0}{2} \right| \\ &\leq 2 \left| \sin \frac{x - x_0}{2} \right| \leq |x - x_0|. \end{aligned}$$

- La fonction $\sqrt{\cdot}$: En effet, d'une part elle est continue en 0, car on a

$$\forall \varepsilon > 0 \quad \forall x \in [0, \varepsilon^2] \quad \sqrt{x} \leq \varepsilon.$$

D'autre part, soit $x_0 > 0$. Alors soit $x \in \mathbb{R}^+$, on a $|\sqrt{x} - \sqrt{x_0}| = \frac{|x - x_0|}{\sqrt{x} + \sqrt{x_0}} \leq \frac{|x - x_0|}{\sqrt{x_0}}$.

En notant $C = \frac{1}{\sqrt{x_0}}$ (qui ne dépend pas de x), on a donc

$$\forall x \in \left[\frac{x_0}{2}, \frac{3x_0}{2} \right] \quad |\sqrt{x} - \sqrt{x_0}| \leq C |x - x_0|.$$

On a donc

$$\sqrt{x} \xrightarrow{x \rightarrow x_0} \sqrt{x_0}.$$

Définition 1.1.4 (Continuité à gauche et à droite).

On dit que f est *continue à gauche* (resp à droite) si $f|_{I \cap]-\infty, a]}$ (resp. $f|_{I \cap [a, +\infty[}$) est continue en a , c'est-à-dire admet une limite en a , qui est alors nécessairement $f(a)$.

Remarque 1.1.5.

Cette fois, on ferme les intervalles en a dans les restrictions de f , à l'inverse de ce que l'on faisait pour les limites à gauche et à droite.

Théorème 1.1.6.

f est continue en a si et seulement si f est continue à gauche et à droite en a .

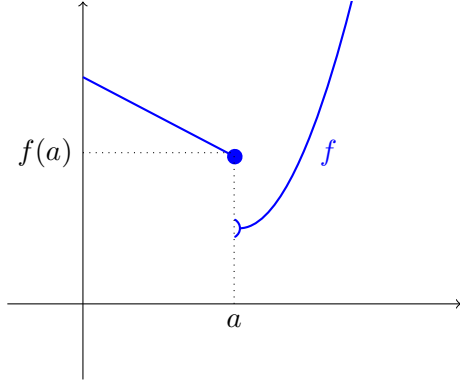


FIGURE XV.2 – Illustration d'une fonction continue à gauche en a , mais pas à droite.

Démonstration.

D'une part f continue en a si et seulement si la limite de f en a existe, ce qui est vrai si et seulement si les limites de f en a , à gauche et à droite, existent et valent $f(a)$.

D'autre part, f est continue à gauche (resp. à droite) si et seulement si la limite de f en a , à gauche (resp. à droite) existe et vaut $f(a)$. $\square$

Exemple 1.1.7. • On reprend l'exemple du chapitre précédent :

$$f : \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} e^x & \text{si } x \geq 0 \\ 1 - x & \text{sinon} \end{cases}$$

Alors f est continue en 0.

• Posons

$$g : \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} \frac{\ln(1+|x|)}{x} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

Alors g a pour limite à droite 1 en 0, mais $g(0) \neq 1$, donc g n'est pas continue en 0.

Remarque 1.1.8.

On n'utilisera cette caractérisation de la continuité par les continuités à gauche et à droite que lorsque la fonction que l'on étudie est définie différemment à gauche et à droite du point considéré. Sinon, on reviendra à la définition générale.

1.2 Prolongement par continuité en un point.

Définition 1.2.1.

Soit $a \in I$ et $f : I \setminus \{a\} \rightarrow \mathbb{R}$. On dit que f est *prolongeable par continuité en a* s'il existe une application $\tilde{f} : I \rightarrow \mathbb{R}$ qui coïncide avec f sur $I \setminus \{a\}$ (c'est-à-dire vérifiant $\tilde{f}|_{I \setminus \{a\}} = f$), et qui est continue en a .

Remarque 1.2.2.

Quand on prolonge en v une application f définie sur un intervalle $[u, v[$ ou $]u, v[$ (resp. $]v, u]$ et $]v, u[$) et qu'on prolonge f en v par continuité, on parle de prolongement par continuité à droite (resp à gauche).

Théorème 1.2.3.

Avec les mêmes hypothèses que dans la définition 1.2.1 : f est prolongeable par continuité en a si et seulement si la limite de f en a existe **et est finie**. Dans ce cas le prolongement est unique, noté $\tilde{f}$ et défini par

$$\tilde{f} : I \rightarrow \mathbb{R}, \\ x \mapsto \begin{cases} f(x) & \text{si } x \neq a, \\ \ell & \text{si } x = a, \end{cases}$$

où ℓ est la limite de f en a .

Très souvent, par abus de notation, on notera f la fonction $\tilde{f}$.

Démonstration.

Démontrons implication et réciproque :

- Soit $\tilde{f}$ un prolongement par continuité de f en a . $\tilde{f}$ est définie et continue en a , on a donc

$$\tilde{f}(x) \xrightarrow[x \neq a]{x \rightarrow a} \tilde{f}(a)$$

Or, pour tout $x \in I \setminus \{a\}$, on a $\tilde{f}(x) = f(x)$, donc

$$f(x) \xrightarrow{x \rightarrow a} \tilde{f}(a)$$

Donc $\tilde{f}(a)$ est nécessairement la limite de f en a . Cette limite est donc finie. Donc f est nécessairement l'application

$$I \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} f(x) & \text{si } x \neq a \\ \ell & \text{si } x = a \end{cases}$$

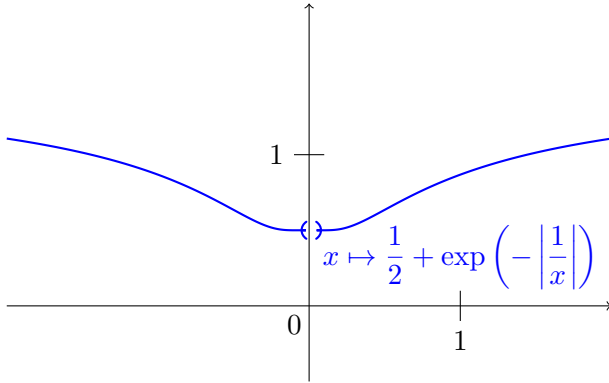


FIGURE XV.3 – Illustration d'une fonction prolongeable par continuité en 0.

Donc si f admet un prolongement par continuité alors la limite de f en a existe et est finie ; le prolongement par continuité est alors bien celui donné dans l'énoncé.

- Réciproquement, supposons que la limite de f en a existe et est finie, notons la ℓ . Alors, définissons $\tilde{f}$ comme donné dans l'énoncé. $\tilde{f}$ coïncide alors avec f sur $I \setminus \{a\}$ et on a donc

$$\tilde{f}(x) \xrightarrow[x \neq a]{x \rightarrow a} \ell$$

Donc

$$\tilde{f}(x) \xrightarrow[x \neq a]{x \rightarrow a} \tilde{f}(a)$$

$\tilde{f}$ est donc continue en a .

□

Exercice 1.2.4.

Quels sont les prolongements par continuité en 0 de

1. $\mathbb{R}^* \rightarrow \mathbb{R} \quad ?$

$$x \mapsto \frac{1}{x}$$
2. $\mathbb{R}^* \rightarrow \mathbb{R} \quad ?$

$$x \mapsto \frac{\sin(x)}{x}$$
3. $\mathbb{R}^* \rightarrow \mathbb{R} \quad ?$

$$x \mapsto \sin \frac{1}{x}$$

Ce théorème est parfois utilisé sous la forme :

Corollaire 1.2.5.

Soient $a \in \mathring{I}$ et $g : I \setminus \{a\} \rightarrow \mathbb{R}$ une application. Si les limites de g en a , à gauche et à droite, existent,

sont égales et **sont finies**, alors, en notant ℓ cette limite, il existe un unique prolongement par continuité $\tilde{g}$ de g obtenu en posant $\tilde{g}(a) = \ell$.

Démonstration.

C'est immédiat, puisqu'on sait que la limite de g en a existe si et seulement si les limites de g en a , à gauche et à droite, existent et sont égales. □

Exemple 1.2.6.

Peut-on prolonger par continuité en 0 l'application

$$f :]-1, +\infty[\setminus \{0\} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} \frac{\sin x}{x} & \text{si } x > 0 \\ \frac{\ln(1+x)}{x} & \text{si } x < 0 \end{cases}$$

Même question en -1 .

1.3 Caractérisation séquentielle de la continuité.

Théorème 1.3.1.

Les assertions suivantes sont équivalentes :

- (i) f est continue en a ;
- (ii) pour toute suite (u_n) à valeurs dans I vérifiant $u_n \xrightarrow[n \rightarrow +\infty]{} a$, on a $f(u_n) \xrightarrow[n \rightarrow +\infty]{} f(a)$.

Démonstration.

C'est une conséquence immédiate de la caractérisation séquentielle de la limite. □

1.4 Opérations sur la continuité.

Lemme 1.4.1.

Soit $g : I \rightarrow \mathbb{R}$ continue en $a \in I$ et telle que $g(a) > 0$. Alors g est strictement positive dans un voisinage de a (idem avec < 0).

Démonstration.

Il suffit de remarquer que la limite de g en a est strictement positive et d'utiliser les résultats connus sur les limites. □

Théorème 1.4.2.

Soient $\lambda \in \mathbb{R}$ et $f, g : I \rightarrow \mathbb{R}$.

- (i) Si f est continue en a alors $|f|$ et λf aussi.
- (ii) Si f et g continues en a alors $f + g$, fg , $\max(f, g)$ et $\min(f, g)$ aussi et si $g(a) \neq 0$ alors $\frac{f}{g}$ aussi.

Démonstration.

Le théorème est une conséquence immédiate des résultats sur les limites et des remarques suivantes :

1. Pour tout $x \in I$,

$$\begin{aligned}\max(f(x), g(x)) &= \frac{f(x) + g(x) + |f(x) - g(x)|}{2} \\ \min(f(x), g(x)) &= \frac{f(x) + g(x) - |f(x) - g(x)|}{2}\end{aligned}$$

2. Si $g(a) \neq 0$ et g continue en a , alors au voisinage de a , g ne s'annule pas, donc $\frac{f}{g}$ est bien définie.

□

Remarque 1.4.3.

Un corollaire immédiat de ce théorème est obtenu en remplaçant dans son énoncé «continue en a » par «continue sur I » et « $g(a) \neq 0$ » par « g ne s'annule pas sur I ».

Exemple 1.4.4.

La fonction $\tan$ et les fonctions polynomiales sont continues sur leur ensemble de définition.

Théorème 1.4.5.

Soient $g : I \rightarrow \mathbb{R}$ et $h : J \rightarrow \mathbb{R}$ deux applications, avec $g(I) \subset J$. Si g est continue en a et h est continue en $g(a)$, alors $h \circ g$ est continue en a .

Démonstration.

Immédiat avec les résultats avec les limites. □

Remarque 1.4.6.

On obtient un corollaire immédiat en remplaçant «continue en a » et «continue en $h(a)$ » respectivement par «continue sur I » et «continue sur J ».

2 Les grands théorèmes.

2.1 Théorème des valeurs intermédiaires.

Proposition 2.1.1 (Rappel).

Les intervalles de $\mathbb{R}$ sont les parties convexes de $\mathbb{R}$, c'est-à-dire les parties I de $\mathbb{R}$ telles que tout réel compris entre deux éléments de I appartient à I . Autrement dit, une partie I de $\mathbb{R}$ est un intervalle si et seulement si

$$\forall (x, y) \in I^2 \quad \forall t \in [0, 1] \quad x + t(y - x) \in I$$

Théorème 2.1.2 (TVI).

L'image d'un intervalle par une fonction continue est un intervalle.

- Remarque 2.1.3.** 1. Soit $f : I \rightarrow \mathbb{R}$, une application telle que $f(I)$ soit un intervalle. Alors pour tout $(a, b) \in I^2$, vérifiant $a < b$, $f(a)$ et $f(b)$ sont dans cet intervalle, donc tout élément compris entre $f(a)$ et $f(b)$ s'écrit sous la forme $f(c)$ avec $c \in [a, b]$.
2. Attention : le TVI assure l'existence de ce c mais absolument pas son unicité.
3. Réciproquement, le fait que pour tout a et tout b vérifiant $a < b$ et tout m compris entre $f(a)$ et $f(b)$ il existe $c \in [a, b]$ vérifiant $f(c) = m$ implique que $f(I)$ est un intervalle.

Démonstration.

Soit $f : I \rightarrow \mathbb{R}$ une application continue. D'après les remarques précédentes, il suffit de montrer que pour tout $(a, b) \in I^2$, vérifiant $a < b$, tout élément compris entre $f(a)$ et $f(b)$ s'écrit sous la forme $f(c)$ avec $c \in [a, b]$.

Soit donc $(a, b) \in I^2$ vérifiant $a < b$, et soit m compris entre $f(a)$ et $f(b)$.

Supposons, sans perte de généralité, que $f(a) \leq f(b)$ (si $f(b) \leq f(a)$, il suffit de considérer $-f$). Soit $m \in]f(a), f(b)[$ (si $m = f(a)$ ou $m = f(b)$, c'est immédiat).

Notons alors $\mathcal{E} = \{x \in [a, b] \mid f(x) \leq m\}$. On a évidemment $a \in \mathcal{E}$ et $\mathcal{E}$ est majoré par b . Donc $\mathcal{E}$ admet une borne supérieure.

Notons $c = \sup \mathcal{E}$. Comme b majore $\mathcal{E}$, $c \leq b$ et comme $a \in \mathcal{E}$, $a \leq c$, donc $c \in [a, b]$.

Ensuite, il existe une suite u à valeurs dans $\mathcal{E}$ telle que $u_n \xrightarrow{n \rightarrow +\infty} c$. Pour tout $n \in \mathbb{N}$, on a donc $f(u_n) \leq m$. Par continuité et par passage à la limite, $f(c) \leq m$.

Si $c = b$, alors $m < f(b) = f(c) \leq m$, ce qui est absurde. Donc $c < b$.

Ainsi, il existe une suite (v_n) à valeurs dans $]c, b[$ telle que $v_n \xrightarrow{n \rightarrow +\infty} c$. Pour tout $n \in \mathbb{N}$, on a donc $f(v_n) > m$.

Par continuité et par passage à la limite, $f(c) \geq m$.

On a donc bien $f(c) = m$. $\square$

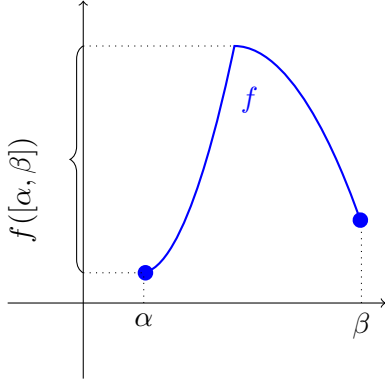


FIGURE XV.4 – Illustration du TVI pour une fonction continue, sur un intervalle.

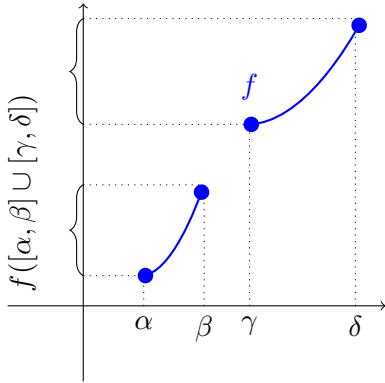


FIGURE XV.5 – Contre-exemple au TVI pour une fonction continue, non sur un intervalle.

Corollaire 2.1.4.

Soit $f \in \mathcal{C}(I)$, et $a, b \in I$ tels que $f(a) > 0$ et $f(b) < 0$. Alors il existe c entre a et b tel que $f(c) = 0$.

Remarque 2.1.5.

Une autre démonstration de ces résultats repose sur le principe de dichotomie, qui donne directement un algorithme. Voici un algorithme python.

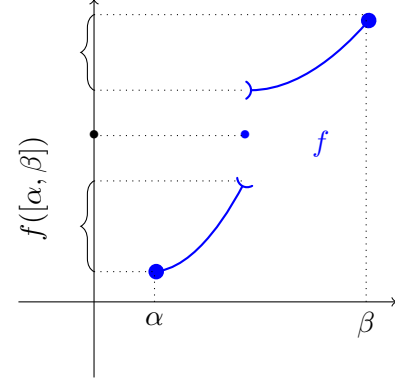


FIGURE XV.6 – Contre-exemple au TVI pour une fonction non continue, sur un intervalle.

Pour tester si l'intervalle étudié est bien un intervalle où $f(a)$ et $f(b)$ sont de signes opposés, on étudie le signe du produit $f(a)f(b)$. On s'arrête lorsque la largeur de l'intervalle est inférieure à un pas donné.

def zeros (f,a,b,p) :

""" Recherche d'un zéro de f dans l'intervalle [a,b]. Retourne le résultat avec une précision p. Précondition : f continue, a < b et f(a)*f(b) <= 0 """

g, d = a, b

[g,d] : Intervalle courant

while d-g > p :

Invariant :

f s'annule entre g et d

soit (f(g)*f(d) <= 0)

Variant : g-d est divisé

par deux à chaque étape

m = (g+d)/2 # Milieu de [g,d]

if (f(g)*f(m)) <= 0 :

d = m

On garde la moitié de gauche

else :

g = m

On garde celle de droite

return m

Il existe deux variantes du TVI, officiellement hors-programme mais très souvent utilisées.

Proposition 2.1.6 (TVI à l'infini).

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$, continue, telle que f admette une limite $\ell_1 \in \mathbb{R}$ en $-\infty$ et une limite $\ell_2 \in \mathbb{R}$ en $+\infty$. Soit y compris strictement entre ℓ_1 et ℓ_2 . Alors il existe $c \in \mathbb{R}$ tel que $f(c) = y$.

Proposition 2.1.7 (TVI aux limites).

Soit $a, b \in \mathbb{R}$ tels que $a < b$, et $f :]a, b[\rightarrow \mathbb{R}$ continue, telle que f admette une limite $\ell_1 \in \mathbb{R}$ en a et une limite $\ell_2 \in \mathbb{R}$ en b . Soit y compris strictement entre ℓ_1 et ℓ_2 . Alors il existe $c \in]a, b[$ tel que $f(c) = y$.

Démonstration.

Donnons une première démonstration générale (il suffit de poser $a = -\infty$ et $b = +\infty$). Soit y compris strictement entre ℓ_1 et ℓ_2 . Comme f tend vers ℓ_1 en a et vers ℓ_2 en b , il existe a', b' dans $]a, b[$ tels que $f(a') < y < f(b')$. Comme f est continue sur l'intervalle $]a, b[$, par le théorème des valeurs intermédiaires, il existe $c \in]a, b[$ tel que $f(c) = y$.

Démontrons d'une autre manière le premier point dans le cas $\ell_1, \ell_2 \in \mathbb{R}$, le second se montre de la même manière que la fin de la démonstration du premier point.

Utilisons l'astuce suivante : soit $\varphi :]-\pi/2, \pi/2[$, $x \mapsto f(\tan(x))$. Alors par composition, φ est continue, et elle admet ℓ_1 et ℓ_2 comme limites en moins et plus $\pi/2$. On peut alors la prolonger en une fonction continue $\tilde{\varphi}$, avec $\tilde{\varphi}(-\pi/2) = \ell_1$ et $\tilde{\varphi}(\pi/2) = \ell_2$.

Le (vrai) TVI assure alors qu'il existe $d \in]-\pi/2, \pi/2[$ tel que $\varphi(d) = y$, et il suffit de poser $c = \tan d$ pour avoir $f(c) = y$. $\square$

2.2 Image d'un segment par une fonction continue.

Dans le cas d'un segment, le TVI peut-être complété.

Théorème 2.2.1.

L'image d'un segment par une fonction continue est un segment.

Démonstration.

Notons $I = [a, b]$, $f : I \rightarrow \mathbb{R}$ continue, et $J = f(I)$. D'après le TVI, J est un intervalle. Il suffit de montrer que ses extrémités gauche et droite sont réelles et lui appartiennent.

Notons M la borne supérieure de J dans $\mathbb{R}$ et montrons $M \in J$. Tout d'abord, nous savons que l'on peut construire

une suite u de points de I vérifiant $f(u_n) \xrightarrow{n \rightarrow +\infty} M$.

Ensuite, u est à valeurs dans $[a, b]$ or $[a, b]$ est un segment donc d'après le théorème de Bolzano-Weierstrass, on peut extraire de u une suite v convergeant vers une valeur $c \in [a, b]$. Comme f est continue sur $[a, b]$, on en déduit que $(f(v_n))_{n \in \mathbb{N}}$ converge vers $f(c)$.

Or $(f(v_n))_{n \in \mathbb{N}}$ est une suite extraite de $(f(u_n))_{n \in \mathbb{N}}$, donc elle tend vers M .

On a donc $M = f(c)$, donc $M \in f([a, b]) = J$.

De la même manière, on montre $\inf(J) \in J$. $\square$

Corollaire 2.2.2 (Théorème des bornes atteintes).

Toute fonction continue sur un segment est bornée et atteint ses bornes.

Démonstration.

Soit f continue sur un segment $[a, b]$. D'après le théorème, $f([a, b])$ est un segment $[c, d]$. f est donc majorée par d , minorée par c . Or $d \in f([a, b])$ donc d possède un antécédent dans $[a, b]$ par f . f atteint donc ce majorant (qui est donc un maximum). De la même façon, f atteint son minorant c , qui est donc un minimum de f sur $[a, b]$. $\square$

Exemple 2.2.3.

C'est un résultat intuitif, voici des contre-exemples lorsque les hypothèses ne sont pas vérifiées.

- Sur un intervalle fermé, non borné : $\mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto x$ est continue, mais n'a ni maximum ni minimum.
- Sur un intervalle ouvert non fermé : $]0, 1[\rightarrow \mathbb{R}$, $x \mapsto 1/x$ est continue mais n'a pas de maximum.
- Avec une fonction non continue : sur le segment $[0, 1]$, la fonction qui a un réel associe 0, sauf aux $1/n$ avec $n \in \mathbb{N}^*$ qui leur associe n . Cette fonction est discontinue et n'a pas de maximum.

Exemple 2.2.4.

Toute fonction périodique continue et définie sur $\mathbb{R}$ est bornée et atteint ses bornes.

Démonstration.

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ T -périodique, et $x \in \mathbb{R}$. Sur $[0, T]$, f est bornée et atteint son maximum M en x_M et son minimum m en x_m .

Or pour tout $x \in \mathbb{R}$, il existe $x' \in [0, T]$ tel que $x - x'$ soit un multiple entier de T (il est suffisant (et nécessaire) de prendre pour x' la valeur $T \times (x/T - \lfloor x/T \rfloor)$). On en déduit $f(x) \in [m, M]$. f est donc bornée sur $\mathbb{R}$ et atteint ses bornes en x_M et x_m . $\square$

2.3 Rappels concernant les fonctions strictement monotones.

Dissipons d'emblée une idée populaire, mais fausse : ce n'est pas parce qu'une fonction est dérivable en un point que l'on peut dire quoi que ce soit quant au sens de variation de la fonction au voisinage de ce point.

Exemple 2.3.1.

Soit la fonction

$$f : \begin{cases} \mathbb{R} & \longrightarrow \mathbb{R}, \\ x & \longmapsto \begin{cases} x^2 \sin\left(\frac{1}{x}\right) + \frac{x}{2} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases} \end{cases}$$

Alors f est continue et dérivable sur $\mathbb{R}$, $f'(0) = 1/2$, mais f n'est monotone sur aucun voisinage de 0.

Dans la suite, nous ne parlerons pas du tout de dérivabilité.

Théorème 2.3.2.

Soit $a, b \in \overline{\mathbb{R}}$ vérifiant $a < b$. Supposons que f est continue sur I et **strictement** croissante sur I . Soit $\ell, \ell' \in \overline{\mathbb{R}}$ tels que $f \xrightarrow{a} \ell$ et $f \xrightarrow{b} \ell'$. Alors :

1. si $I = [a, b]$, alors $f(I) = [f(a), f(b)]$;
2. si $I =]a, b[$, alors $f(I) =]\ell, \ell'[$;
3. si $I = [a, b[$, alors $f(I) = [f(a), \ell'[$;
4. si $I =]a, b]$, alors $f(I) =]\ell, f(b)]$.

On a un résultat analogue lorsque f est **strictement** décroissante sur I .

Démonstration.

Remarquons que f étant strictement monotone, f admet une limite à droite en a et à gauche en b .

On se contente de donner le cas f strictement décroissante et $I =]a, b]$. On sait que $f(I)$ est un intervalle. On note $\alpha = \inf f(I)$ et $\beta = \sup f(I)$. f étant décroissante, $f(b)$ minore $f(I)$, or $f(b)$ est dans $f(I)$, donc $\alpha = f(b)$. Par ailleurs, comme f est strictement décroissante, on ne peut avoir $\beta \in f(I)$, car alors il existerait $c \in]a, b]$ vérifiant $f(c) = \beta$ et dans ce cas on aurait $f(\frac{a+c}{2}) > \beta$ et β ne majorerait plus $f(I)$, ce qui serait absurde.

Enfin, le théorème de limite monotone nous donne l'existence des limites manipulées. On en rappelle ici les arguments.

- Supposons $\beta = +\infty$, alors f n'est pas majorée, donc pour tout $M > 0$, il existe $c \in I$ tel que $f(c) > M$.

Mais f est décroissante, donc pour tout $x \in]a, c]$, $f(x) > M$. On a donc $f \xrightarrow{a} +\infty = \beta$.

- Supposons $\beta \in \mathbb{R}$, alors pour tout $\varepsilon > 0$, $\beta - \varepsilon$ ne majore pas $f(I)$, donc il existe $d \in]\beta - \varepsilon, \beta]$ tel que $d \in f(I)$, donc il existe $c \in I$ tel que $f(c) \in]\beta - \varepsilon, \beta]$. Or f est décroissante, donc pour tout $x \in]a, c]$, on a $f(x) \in]\beta - \varepsilon, \beta]$. Ainsi $f(I) = [f(b), \ell'[$ ($\beta \notin f(I)$ car f est strictement décroissante). On a donc $f \xrightarrow{a} \beta$.

Dans les deux cas, on a bien $f(I) = [f(b), \ell'[$ □

Remarque 2.3.3.

Si la fonction f n'est supposée que monotone, $f(I)$ peut être fermé alors que I est ouvert (prendre f constante, par exemple).

2.4 Monotonie stricte, bijectivité et continuité.

Explorons maintenant les liens entre ces trois notions.

Lemme 2.4.1 (Réciproque d'une application strictement monotone).

Soit D et E deux parties de $\mathbb{R}$ et $f : D \rightarrow E$ une bijection strictement monotone. Alors l'application réciproque $f^{-1} : E \rightarrow D$ est strictement monotone, de même sens de variation que f .

Démonstration.

Montrons maintenant que f^{-1} est strictement monotone, de même sens de variation que f .

- Supposons que f soit strictement croissante. Alors, soit y_1 et y_2 deux éléments de $f(D)$ vérifiant $y_1 < y_2$ et soit $x_1 = f^{-1}(y_1)$ et $x_2 = f^{-1}(y_2)$. Si on avait $x_1 \geq x_2$ alors, comme f est croissante, on aurait $f(x_1) \geq f(x_2)$, c'est-à-dire $y_1 \geq y_2$, ce qui serait absurde. Donc $x_1 < x_2$, c'est-à-dire $f^{-1}(y_1) < f^{-1}(y_2)$.
 f^{-1} est donc strictement croissante.
- Supposons que f soit strictement décroissante. De la même façon, on montre que f^{-1} est alors strictement décroissante.

Dans les deux cas, f^{-1} est strictement monotone, de même sens de variation que f . □

Le résultat suivant est une réciproque partielle au théorème des valeurs intermédiaires.

Lemme 2.4.2.

Soit I un intervalle et $f : I \rightarrow \mathbb{R}$ une application monotone telle que $f(I)$ est un intervalle.

Alors f est continue sur I .

Démonstration.

Le cas où I est un intervalle vide ou réduit à un point est trivial. Nous supposons donc par la suite que I n'est ni vide, ni réduit à un point.

Nous étudions seulement ici le cas où f est croissante. Si f est décroissante, il suffit d'appliquer ce qui suit à $-f$.

Il suffit de montrer que d'une part que pour tout point $a \in I$ qui n'est pas l'extrémité gauche de I , on a $f \xrightarrow{a^-} f(a)$ et d'autre part que pour tout point $a \in I$ qui n'est pas l'extrémité droite de I , on a $f \xrightarrow{a^+} f(a)$.

Par l'absurde, supposons que ce n'est pas le cas. Pour fixer les idées, supposons qu'il existe $a \in I$ qui n'est pas l'extrémité gauche de I vérifiant $f \not\xrightarrow{a^-} f(a)$ (l'autre cas est similaire). Notons alors α un point de I vérifiant $\alpha < a$.

Alors, f étant croissante, on sait que la limite de f en a , à gauche, existe. Notons la ℓ . Alors, $f(\alpha) \leq \ell \leq f(a)$. Puisque $f \not\xrightarrow{a^-} f(a)$, on a $\ell < f(a)$. L'intervalle $] \ell, f(a)[$ n'est donc pas vide, on peut donc y choisir un point y . On a alors $f(\alpha) \leq \ell < y < f(a)$.

Or $f(I)$ est un intervalle, donc $y \in f(I)$. Donc il existe $c \in I$ vérifiant $f(c) = y$. On a $f(c) < f(a)$ et f croissante, donc $c < a$. Donc $f(c) \leq \ell$, donc $y \leq \ell$ ce qui est absurde. $\square$

Lemme 2.4.3.

Soit I un intervalle et $f : I \rightarrow \mathbb{R}$, une application continue et injective. Alors f est strictement monotone.

Démonstration.

Supposons par l'absurde que f n'est pas strictement monotone, c'est-à-dire qu'elle n'est ni strictement croissante, ni strictement décroissante.

Comme f n'est pas strictement croissante, il existe $(x, y) \in I^2$ vérifiant $x < y$ et $f(x) \geq f(y)$.

De même, comme f n'est pas strictement décroissante, il existe $(x', y') \in I^2$ vérifiant $x' < y'$ et $f(x') \leq f(y')$.

Notons

$$\begin{aligned} \alpha : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto (1-t)x + tx' \\ \beta : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto (1-t)y + ty' \\ \varphi : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto f(\alpha(t)) - f(\beta(t)) \end{aligned}$$

I est un intervalle donc, pour tout $t \in [0, 1]$, $\alpha(t)$ et $\beta(t)$ appartiennent à I , donc φ est bien définie.

Par ailleurs, on peut remarquer que, comme $x < y$ et $x' < y'$, pour tout $t \in [0, 1]$, on a $\alpha(t) < \beta(t)$.

Enfin, on a :

- (i) φ est continue sur $[0, 1]$;
- (ii) $\varphi(0) = f(x) - f(y) \geq 0$;
- (iii) $\varphi(1) = f(x') - f(y') \leq 0$.

Donc φ s'annule en une valeur $t \in [0, 1]$. On a alors $f(\alpha(t)) = f(\beta(t))$.

Or f est injective, donc $\alpha(t) = \beta(t)$. Or $\alpha(t) < \beta(t)$, donc c'est absurde. $\square$

Théorème 2.4.4 (Théorème de la bijection strictement monotone).

Soit I un intervalle de $\mathbb{R}$ et $f : I \rightarrow \mathbb{R}$ une application. Posons $J = f(I)$. Alors si deux quelconques des trois propriétés suivantes sont vraies, la troisième l'est également :

- (i) J est un intervalle et f réalise une bijection de l'intervalle I sur l'intervalle $f(I)$.
- (ii) f est strictement monotone sur I .
- (iii) f est continue sur I .

De plus, lorsque ces conditions sont vérifiées, l'application réciproque $f^{-1} : J \rightarrow I$ est aussi une bijection continue strictement monotone.

Démonstration.

Pour ce qui est de la première partie du théorème :

- Dans le cas où (i) et (ii) sont vraies, $f(I)$ est un intervalle, f est donc continue d'après le lemme 2.4.2
- Dans le cas où (i) et (iii) sont vraies, f réalise une bijection de I sur $f(I)$ donc est injective, or elle est continue, donc strictement monotone d'après le lemme 2.4.3.
- Dans le cas où (ii) et (iii) sont vraies, f est strictement monotone donc injective, donc réalise une bijection de I sur $f(I)$. De plus, elle est continue donc $f(I)$ est un intervalle.

Pour ce qui est de la seconde partie, supposons donc ces conditions vérifiées.

Alors on sait que la bijection d'une application strictement monotone est monotone, donc $f^{-1} : J \rightarrow I$ est strictement monotone.

De plus f^{-1} réalise une bijection de l'intervalle J sur l'intervalle $f^{-1}(J) = I$.

La première partie assure donc que f^{-1} est continue. $\square$

Exemple 2.4.5.

Cela permet de montrer que les fonctions Arccos, Arcsin et Arctan sont continues.

3 Extension au cas des fonctions à valeurs complexes.

Les notions de continuité, continuité à gauche et à droite se généralisent sans problème aux fonctions à valeurs complexes, puisque c'est juste une histoire de limite. On a aussi le résultat suivant.

Théorème 3.0.1.

Soit $f : I \rightarrow \mathbb{C}$, $a \in I$. On a équivalence entre :

1. f est continue en a (resp. sur I)
2. $\operatorname{Im}(f)$ et $\operatorname{Re}(f)$ sont continues en a (resp. sur I).

La caractérisation séquentielle de la continuité est vraie comme pour les applications à valeurs dans $\mathbb{R}$, de même que toutes les résultats sur les opérations usuelles. En revanche, les grands théorèmes liés au TVI ne peuvent pas être étendus à $\mathbb{C}$: ils font appel à l'ordre $\leq$ sur $\mathbb{R}$.

Exemple 3.0.2.

Notons $f : [0, \pi] \rightarrow \mathbb{C}$. Alors f est continue

$$t \mapsto e^{it}$$

sur $[0, \pi]$, vaut 1 en 0, -1 en π mais ne s'annule pas.

Quant à l'image du segment $[0, \pi]$, il s'agit d'un demi-cercle et non d'un intervalle !

Chapitre XVI

Polynômes

Sommaire

1	$\mathbb{K}[X]$: définitions et résultats algébriques.	222
1.1	Premières définitions.	222
1.2	Somme et produit.	223
1.3	Composition.	224
1.4	Opérations et degré.	224
1.5	Fonctions polynomiales.	225
1.6	Division euclidienne.	226
1.7	L'algorithme de Horner.	228
2	Décomposition.	229
2.1	Racines, ordre de multiplicité.	229
2.2	Nombres de racines.	230
2.3	Polynômes scindés et relations coefficients-racines.	231
2.4	Le théorème fondamental de l'algèbre.	232
2.5	Décomposition en produit de facteurs irréductibles.	234
3	Dérivation des polynômes.	235
3.1	Définition.	235
3.2	Propriétés.	235
4	Arithmétique de $\mathbb{K}[X]$.	238
4.1	PGCD.	238
4.2	Polynômes premiers entre eux.	240
4.3	PGCD de n polynômes.	242
4.4	PPCM.	243
5	Formule d'interpolation de Lagrange.	243
6	Annexe : construction de $\mathbb{K}[X]$	245
7	Annexe : fonctions polynomiales à valeurs dans un anneau	247

Dans tout ce chapitre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 $\mathbb{K}[X]$: définitions et résultats algébriques.

1.1 Premières définitions.

Définition 1.1.1.

On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

- Remarque 1.1.2.** 1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.
2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse¹ (par exemple la suite $(1/n)$).

Définition 1.1.3 (Anneau des polynômes sur le corps $\mathbb{K}$).

On admet qu'on peut construire un anneau commutatif $(\mathbb{K}[X], +, \times)$ appelé *anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$* . Vérifiant les propriétés suivantes :

1. $\mathbb{K}[X]$ étend l'anneau $\mathbb{K}$, c'est-à-dire :
 - (a) $\mathbb{K} \subset \mathbb{K}[X]$
 - (b) l'addition et la multiplication de $\mathbb{K}[X]$ coïncident avec celles de $\mathbb{K}$ sur l'ensemble $\mathbb{K}$. Autrement dit : les opérations $+\mathbb{K}[X]$ et $\times\mathbb{K}[X]$ restreintes au sous-ensemble $\mathbb{K}$ sont exactement les opérations $+\mathbb{K}$ et $\times\mathbb{K}$.
 - (c) le neutre pour l'addition sur $\mathbb{K}$, noté 0, est aussi le neutre pour l'addition sur $\mathbb{K}[X]$ et le neutre pour la multiplication sur $\mathbb{K}$, noté 1, est aussi le neutre pour la multiplication sur $\mathbb{K}[X]$. Le polynôme 0 est appelé *le polynôme nul*.
2. $\mathbb{C}[X]$ étend $\mathbb{R}[X]$.

1. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

3. Il existe un polynôme, noté X (appelé *l'indéterminée* de $\mathbb{K}[X]$).
4. Les polynômes de la forme αX^k pour $k \in \mathbb{N}$ et $\alpha \in \mathbb{K}$ sont appelés *monômes*.
5. Tout polynôme P peut s'écrire de façon *unique* sous *forme normale*² (appelée aussi *forme développée réduite*) :

$$\sum_{k=0}^{+\infty} a_k X^k$$

où $(a_k)_{k \in \mathbb{N}}$ est une suite à support fini, appelée *suite des coefficients de P* (la suite des coefficients de P est donc unique).

- Remarque 1.1.4.** 1. Si on note φ l'application qui à tout polynôme P associe sa suite des coefficients et ψ l'application qui à toute suite à valeurs dans $\mathbb{K}$ à support fini u associe le polynôme $\sum_{k=0}^{+\infty} u_k X^k$, on constate que pour tout polynôme P , $(\psi \circ \varphi)(P) = P$ et que pour toute suite à support fini u , on a $(\varphi \circ \psi)(u) = u$. Ces deux applications sont donc des bijections réciproques : il y a donc une bijection (canonique) entre les suites à support fini et les polynômes.

2. Il est important de ne pas confondre X et x : $2X^3 + \sqrt{2}X + 7$ est un polynôme, $x \mapsto 2x^3 + \sqrt{2}x + 7$ désigne une fonction polynomiale (allant de $\mathbb{R}$ dans $\mathbb{R}$ ou de $\mathbb{R}$ dans $\mathbb{C}$ ou de $\mathbb{C}$ dans $\mathbb{C}$ selon le contexte). L'expression « $x^3 + \sqrt{2}x + 7$ » est une erreur si x n'a pas été introduit ou si c'est une matrice carrée de taille 42. C'est un réel si x est un réel et un complexe si x est un complexe.

Le polynôme 0 a pour suite de coefficients la suite nulle.

2. La somme est une somme finie, prise pour les valeurs de k telle que $a_k \neq 0$. On a donc $P = \sum_{\substack{k \in \mathbb{N} \\ a_k \neq 0}} a_k X^k$ mais

aussi $P = \sum_{k=0}^n a_k X^k$ si la suite (a_k) est nulle à partir du rang $n + 1$.

Pour tout $\lambda \in \mathbb{K}$, le polynôme λ a pour suite de coefficients la suite nulle partout sauf au rang 0, où elle a pour valeur λ . Les éléments de $\mathbb{K}$ sont appelés les polynômes constants.

Définition 1.1.5 (Degré).

Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$. On appelle degré de P , et note $\deg P$ la valeur

$$\sup \{ k \in \mathbb{N} \mid a_k \neq 0 \},$$

prise dans $\overline{\mathbb{R}}$.

- (i) Si P est le polynôme nul, $\deg P = -\infty$.
- (ii) Si P n'est pas le polynôme nul, le support de $(a_k)_{k \in \mathbb{N}}$ est un ensemble d'entiers non vide et majoré, donc

$$\deg P = \max \{ k \in \mathbb{N} \mid a_k \neq 0 \}.$$

- (iii) Si P est non nul, le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg P} X^{\deg P}$ est le *monôme dominant* de P .
- (iv) Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n .

Remarque 1.1.6. 1. $\mathbb{K}_n[X]$ n'est pas l'ensemble des polynômes de degré égal à n .

- 2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \dots \subset \mathbb{K}[X]$.
- 3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.
- 4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geq d$ (P est de degré au plus n), alors P peut s'écrire sous la forme $\sum_{k=0}^n a_k X^k$.

1.2 Somme et produit.

Proposition 1.2.1.

Soit P et Q deux polynômes respectivement de

la forme $\sum_{k=0}^{+\infty} a_k X^k$ et $\sum_{k=0}^{+\infty} b_k X^k$. Alors on a :

$$P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k.$$

Autrement dit, la suite des coefficients de $P+Q$ est la somme de leurs suites de coefficients respectives.

En ce qui concerne le produit, on a

$$P \times Q = \sum_{(i,j) \in \mathbb{N}^2} a_i b_j X^{i+j} = \sum_{k=0}^{+\infty} c_k X^k$$

où $(c_k)_{k \in \mathbb{N}}$ est la suite vérifiant, pour tout $k \in \mathbb{N}$,

$$c_k = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k a_{k-i} b_i.$$

Démonstration.

Il s'agit essentiellement de constater que les sommes sont en fait finies. En notant S et S' les supports respectifs des suites de coefficients de P et Q , on a

$$P = \sum_{k \in S} a_k X^k = \sum_{k \in S \cup S'} a_k X^k,$$

$$Q = \sum_{k \in S'} b_k X^k = \sum_{k \in S \cup S'} b_k X^k,$$

d'où

$$P + Q = \sum_{k \in S \cup S'} (a_k X^k + b_k X^k)$$

$$= \sum_{k \in S \cup S'} (a_k + b_k) X^k.$$

Or a_k et b_k sont nuls pour tout $k \in \mathbb{N} \setminus (S \cup S')$, donc la somme

$$\sum_{k=0}^{+\infty} (a_k + b_k) X^k$$

est finie et vaut la même chose.

Pour le produit, notons, pour tout $k \in \mathbb{N}$,

$$c_k = \sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j.$$

Il est clair que c_k est une somme finie (elle comporte $k+1$ termes) et de plus, on a

$$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^k a_{k-i} b_i.$$

Il reste à montrer qu'on a bien $P \times Q = \sum_{k=0}^{+\infty} c_k X^k$.

Posons $S'' = \{i+j \mid (i,j) \in S \times S'\}$, S'' est l'image directe de l'ensemble fini $S \times S'$ par l'application somme, donc S'' est un ensemble fini.

Remarquons tout de suite que pour $k \in \mathbb{N} \setminus S''$ et tout couple $(i,j) \in \mathbb{N}^2$ vérifiant $i+j=k$, on a $(i,j) \notin S \times S'$, donc $a_i = 0$ ou $b_j = 0$. Donc pour tout $k \in \mathbb{N} \setminus S''$, la somme $\sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j$ ne comporte que des termes nuls.

En outre

$$\begin{aligned} PQ &= \left(\sum_{i \in S} a_i X^i \right) \left(\sum_{j \in S'} b_j X^j \right) \\ &= \sum_{(i,j) \in S \times S'} a_i b_j X^{i+j} \\ &= \sum_{k \in S''} \left(\sum_{\substack{(i,j) \in S \times S' \\ i+j=k}} a_i b_j X^{i+j} \right) \\ &= \sum_{k \in S''} \left(\sum_{\substack{(i,j) \in S \times S' \\ i+j=k}} a_i b_j \right) X^k \\ &= \sum_{k \in S''} \left(\sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k \\ &= \sum_{k=0}^{+\infty} \left(\sum_{\substack{(i,j) \in \mathbb{N}^2 \\ i+j=k}} a_i b_j \right) X^k. \end{aligned}$$

d'où le résultat. $\square$

1.3 Composition.

Définition 1.3.1.

Soit P et Q deux polynômes de $\mathbb{K}[X]$. P s'écrit sous la forme

$$\sum_{k=0}^{+\infty} a_k X^k.$$

Alors, la somme

$$\sum_{k=0}^{+\infty} a_k Q^k$$

est une somme finie, appelée *composée de P et Q* (ou de Q par P) et est notée $P \circ Q$.

Proposition 1.3.2.

La composition est distributive **à droite** par rapport aux lois $+$ et $\times$ et elle est également associative, c'est-à-dire que si P , Q et R désignent trois polynômes, on a :

- (i) $(P + Q) \circ R = (P \circ R) + (Q \circ R)$;
- (ii) $(PQ) \circ R = (P \circ R) \times (Q \circ R)$;
- (iii) $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Démonstration. (i) Direct.

(ii) Traiter d'abord le cas $P = X^n$ et $Q = X^m$, puis le cas P quelconque et $Q = X^m$, puis le cas général.

(iii) Montrer par récurrence que $Q^k \circ R = (Q \circ R)^k$. $\square$



Attention à la composition à gauche, qui n'est pas distributive. Par exemple :

$$\begin{aligned} X^2 \circ (X + 2) &= (X + 2)^2 \neq X^2 + 2^2 \\ (1 \circ X) + (1 \circ 2) &= 2 \neq 1 \circ (X + 2) \\ (1 + X) \circ (X.X) &\neq ((1 + X) \circ X).((1 + X) \circ X). \end{aligned}$$

Exemple 1.3.3.

Un polynôme P est dit pair si $P \circ (-X) = P$, impair si $P \circ (-X) = -P$. Que peut-on dire des coefficients de tels polynômes ?

1.4 Opérations et degré.

Théorème 1.4.1.

Soient $P, Q \in \mathbb{K}[X]$.

- (i) $\deg(P + Q) \leq \max(\deg P, \deg Q)$;
- (ii) $\deg(PQ) = \deg P + \deg Q$;
- (iii) si Q n'est pas constant, alors $\deg(P \circ Q) = \deg P \times \deg Q$. Si Q est constant, $\deg P \circ Q = 0$ ou $-\infty$.

Remarque 1.4.2.

Méditez les exemples suivants :

- (i) $P = X - 1$ et $Q = 2 - X$;
- (iii) $P = X^2 - 1$ et $Q = 1$.

Démonstration.

Le théorème est évident si P ou Q est nul. On les supposera donc tous deux non nuls, et on pose $n = \deg P$ et $m = \deg Q$. Les polynômes P , Q et PQ s'écrivent respectivement

sous la forme $\sum_{k=0}^n a_k X^k$ et $\sum_{k=0}^m b_k X^k$ et $\sum_{k=0}^{+\infty} c_k X^k$.

(i) Facile ;

(ii) On a $c_k = \sum_{i=0}^k a_i b_{k-i}$.

Soit $k \geq m+n$. Si $i > n$, alors $a_i = 0$, et si $i < n$, alors $b_{m+n-i} = 0$.

Ainsi, si $k = m+n$, la somme définissant c_k n'a qu'un terme non nul, et $c_{m+n} = a_n b_m \neq 0$.

Si $k > m+n$, tous les termes de la somme sont nuls, donc $c_k = 0$. Ceci prouve bien le résultat.

(iii) Q non constant équivaut à $\deg Q \geq 1$. Donc si k_1 et k_2 sont deux entiers tels que $k_2 > k_1$, on a $\deg Q^{k_2} > \deg Q^{k_1}$. Ainsi $\deg P \circ Q = \deg a_n Q^n = \deg(Q^n)$. Or d'après (ii), $\deg(Q^n) = n \deg Q$.

□

Corollaire 1.4.3.

$\mathbb{K}[X]$ est intègre.

Démonstration.

Il suffit de montrer que pour tout $(P, Q) \in \mathbb{K}[X]^2$, $PQ = 0 \Rightarrow (P = 0 \text{ ou } Q = 0)$. Soit donc $(P, Q) \in \mathbb{K}[X]^2$ vérifiant $PQ = 0$. Alors d'après le point (iii) du théorème 1.4.1, $-\infty = \deg(PQ) = \deg P + \deg Q$, donc on a nécessairement $\deg P = -\infty$ ou $\deg Q = -\infty$. □

Corollaire 1.4.4.

Soient $P, A, B \in \mathbb{K}[X]$ tel que $P \neq 0$. Alors :

$$PA = PB \Leftrightarrow A = B.$$

Démonstration.

$PA = PB$ si et seulement si $P(A - B) = 0$ si et seulement si $(P = 0 \text{ ou } A - B = 0)$ si et seulement si $A - B = 0$ si et seulement si $A = B$. □

Corollaire 1.4.5.

$U(\mathbb{K}[X]) = \mathbb{K}^*$. Autrement dit, les seuls éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration.

Soient P un polynôme inversible. Il existe donc un polynôme Q tel $PQ = 1$. P et Q sont non nuls, et donc $\deg P \geq 0$ et $\deg Q \geq 0$. Mais $0 = \deg 1 = \deg PQ = \deg P + \deg Q$. Nécessairement, $\deg P = \deg Q = 0$.

Réciproquement, tout polynôme constant non nul est bien inversible. □

Il y a donc peu de polynômes inversibles. L'inversibilité est une propriété fort utile lorsqu'on veut simplifier une égalité de la forme $PA = PB$ (on multiplie alors des deux côtés par l'inverse de P) mais heureusement, elle n'est pas nécessaire pour cela, l'intégrité de $\mathbb{K}[X]$ suffit.

Définition 1.4.6.

Deux polynômes P et Q de $\mathbb{K}[X]$ sont dits associés s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$.

Remarque 1.4.7.

Ainsi, deux polynômes sont associés si et seulement si on passe de l'un à l'autre en multipliant par un polynôme inversible. On pourra effectuer un rapprochement avec les entiers ainsi qu'avec l'arithmétique sur les entiers : les éléments inversibles de $\mathbb{Z}$ sont 1 et -1 , et les objets construits en arithmétique des entiers (PGCD, nombres premiers, etc.) le sont toujours « à un élément inversible près ». Ce sera encore le cas en arithmétique des polynômes.

1.5 Fonctions polynomiales.

Dans cette section, on considère un entier naturel n fixé

Définition 1.5.1.

Soit $P \in \mathbb{K}[X]$ écrit sous forme développée réduite

$P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\tilde{P}(x)$ l'élément de $\mathbb{K}$ défini par

$$\tilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k.$$

Remarque 1.5.2.

Comme précédemment, le symbole $\sum_{k=0}^{+\infty}$ a un sens car la suite (a_k) est à support fini. Cette somme est donc finie.

Exemple 1.5.3.

On pose $P = X^2 + 2X + 3$, que vaut l'évaluation de P en -2 ?

Proposition 1.5.4.

Soit $x \in \mathbb{K}$ fixé. Alors, l'application d'évaluation en x , $\text{eval}_x : \mathbb{K}[X] \rightarrow \mathbb{K}$ est un morphisme d'anneaux ; autrement dit pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P + Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \widetilde{P}(x) \times \widetilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_{\mathbb{K}}$.

De plus, on a

$$\widetilde{P \circ Q}(x) = \widetilde{P}(\widetilde{Q}(x))$$

On note $\widetilde{P} : \mathbb{K} \rightarrow \mathbb{K}$.
 $x \mapsto \widetilde{P}(x)$

Remarque 1.5.5.

D'après ce qui précède, on a donc, pour tous polynômes P et Q :

1. $\widetilde{P + Q} = \widetilde{P} + \widetilde{Q}$;
2. $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$;
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

Exemple 1.5.6.

Posons $P = X^2 + 2X + 3$.

1. Que vaut $\widetilde{P}$?
2. A t-on $P = \widetilde{P}$?

En pratique, on note en général $P(x)$ la valeur de $\widetilde{P}(x)$. On va même parfois jusqu'à identifier P et $\widetilde{P}$, c'est-à-dire identifier les polynômes et les fonctions polynomiales. Cela se justifie par le résultat suivant :

Théorème 1.5.7.

Soient P et Q deux polynômes de $\mathbb{K}[X]$.

- (i) $\widetilde{P}$ est la fonction identiquement nulle si et seulement si $P = 0$;
- (ii) $\widetilde{P} = \widetilde{Q}$ si et seulement si $P = Q$.

Cependant, nous ne sommes pas en mesure de montrer tout de suite cette propriété. Nous nous contenterons donc pour l'instant de faire les remarques suivantes :

Remarque 1.5.8. 1. Les implications $P = 0 \Rightarrow \widetilde{P} = 0$ et $P = Q \Rightarrow \widetilde{P} = \widetilde{Q}$ sont évidentes. Il suffit donc de montrer les implications réciproques.

2. Si l'on admet pour tout P l'implication $\widetilde{P} = 0_{\mathbb{K}} \Rightarrow P = 0$ alors, pour tout couple (P, Q) , l'implication $\widetilde{P} = \widetilde{Q} \Rightarrow P = Q$ s'en déduit. En effet, il suffit de remarquer que $\widetilde{P - Q} = \widetilde{P} - \widetilde{Q}$, donc si $\widetilde{P} = \widetilde{Q}$, alors $\widetilde{P - Q}$ est nul donc $P - Q$ est nul donc $P = Q$.

Remarque 1.5.9 (à caractère culturel).

On verra que la démonstration du résultat exploite le fait que $\mathbb{K}$ est un ensemble infini. Même si seuls les cas $\mathbb{K} = \mathbb{R}$ et $\mathbb{K} = \mathbb{C}$ sont au programme, il existe des corps $\mathbb{K}$ finis et on peut définir $\mathbb{K}[X]$ pour de tels corps. Dans le cas où $\mathbb{K}$ est un corps fini, le théorème 1.5.7 n'est plus vrai.

1.6 Division euclidienne.

Définition 1.6.1.

Soit P et D deux polynômes à coefficients dans $\mathbb{K}$. On dit que D *divise* P , que P *est un multiple de* D , ou que P *est factorisable par* D et on note $D|P$ si et seulement s'il existe un polynôme Q à coefficients dans $\mathbb{K}$ vérifiant $P = D \times Q$.

Remarque 1.6.2.

Le polynôme nul est divisible par tout polynôme.

Remarque 1.6.3.

Le quotient Q , s'il existe, est unique.

Proposition 1.6.4.

Soit $P, Q \in \mathbb{K}[X]$, si $P \mid Q$ et si $Q \neq 0$, alors $\deg(P) \leq \deg(Q)$.

Démonstration.

Immédiat à partir de la définition. $\square$

On peut définir une opération de division dans $\mathbb{K}[X]$ similaire à celle de la division euclidienne dans $\mathbb{Z}$.

Rappelons tout d'abord la définition de la division euclidienne dans $\mathbb{Z}$:

Définition 1.6.5 (Division euclidienne).

Soit P et D deux entiers, avec $D \neq 0$. Alors il existe un unique couple (Q, R) d'entiers vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$
2. et $0 \leq R < |D|$.

Q et R sont respectivement appelé le quotient et le reste de la division euclidienne de P par D .

Définition 1.6.6 (Division euclidienne des polynômes).

Soit P et D deux polynômes à coefficients dans $\mathbb{K}$, avec $D \neq 0$. Alors il existe un unique couple (Q, R) de polynômes à coefficients dans $\mathbb{K}$ vérifiant les deux propriétés suivantes :

1. $P = D \times Q + R$
2. et $\deg R < \deg D$.

Q et R sont respectivement appelés le quotient et le reste de la division euclidienne de P par D .

Exemple 1.6.7.

La division euclidienne de $3X^4 - 5X^3 + 7X^2 + 8X - 1$ par $X^2 - 3X + 2$ s'écrit :

$$\begin{aligned} & 3X^4 - 5X^3 + 7X^2 + 8X - 1 \\ &= (X^2 - 3X + 2)(3X^2 + 4X + 13) + 39X - 27. \end{aligned}$$

On la pose comme suit.

$$\begin{array}{r|l} 3X^4 - 5X^3 + 7X^2 + 8X - 1 & X^2 - 3X + 2 \\ \hline -(3X^4 - 9X^3 + 6X^2) & \\ \hline 4X^3 + X^2 + 8X - 1 & \\ -(4X^3 - 12X^2 + 8X) & \\ \hline 13X^2 - 1 & \\ -(13X^2 - 39X + 26) & \\ \hline 39X - 27 & \end{array}$$



On alignera toujours les monômes de mêmes degrés pour les additionner sans commettre d'erreur.

Remarque 1.6.8.

La preuve du théorème de division euclidienne repose sur l'idée mise en œuvre dans l'algorithme donnant cette division. On cherche en effet chaque fois à annuler le monôme de plus haut degré du dividende en multipliant le diviseur par un monôme convenable.

Démonstration.

- Commençons d'abord par montrer l'unicité.

Soit (Q_1, R_1) et (Q_2, R_2) deux couples convenables. Alors

$$DQ_2 + R_2 = DQ_1 + R_1,$$

donc

$$(Q_2 - Q_1)D = R_1 - R_2$$

et donc $D \mid (R_1 - R_2)$. Si $R_1 - R_2 \neq 0$, alors nécessairement

$$\deg D \leq \deg(R_1 - R_2).$$

Or $\deg R_1 < \deg D$ et $\deg R_2 < \deg D$, donc par somme

$$\deg(R_1 - R_2) < \deg D.$$

Par conséquent $R_1 - R_2 = 0$, donc $R_1 = R_2$. Il vient ensuite $(Q_2 - Q_1)D = 0$: puisque $D \neq 0$ et que $\mathbb{K}[X]$ est intègre, alors $Q_2 - Q_1 = 0$, soit finalement $(Q_1, R_1) = (Q_2, R_2)$.

- Montrons maintenant l'existence d'un tel couple, par le principe du minimum. Soit les ensembles

$$E = \{ P - DS \mid S \in \mathbb{K}[X] \}$$

et

$$\mathcal{E} = \{ \deg A \mid A \in E \}.$$

Si $0 \in E$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = DQ$, et le couple $(Q, 0)$ est donc celui que nous cherchons.

Sinon, si $0 \notin E$, $\mathcal{E}$ est un sous-ensemble de $\mathbb{N}$. Comme il est clairement non vide, il possède un minimum, noté m . Il existe donc $Q \in \mathbb{K}[X]$ tel que $P - DQ \in \mathbb{K}[X]$, et

$$\deg(P - DQ) = m \in \mathbb{N}.$$

La seule chose à montrer est que $m < \deg D$. Posons $R = P - DQ$.

Par l'absurde, supposons que $m \geq \deg D$. Notons aX^m et bX^d les monômes dominants de R et D respectivement. On sait alors que a et b sont non nuls car R et D sont non nuls, et nous avons supposé que $d \leq m$. Posons alors

$$A = R - \frac{a}{b} \cdot D \cdot X^{m-d}.$$

Alors $\deg A < \deg R$, par annulation du monôme dominant aX^m de R . De plus

$$A = P - DQ - \frac{a}{b} \cdot D \cdot X^{m-d} = P - D\left(Q + \frac{a}{b} X^{m-d}\right),$$

donc $\deg A \in \mathcal{E}$: ceci contredit la minimalité de m , donc par l'absurde, $m < d$, et le couple (Q, R) est le couple voulu.

• On peut aussi montrer ce résultat d'existence par récurrence forte sur le degré de P . Cela a l'avantage de donner un algorithme de calcul du couple (Q, R) . Nous verrons cette méthode sur des exemples, l'idée étant à chaque fois la même : annuler le monôme dominant du dividende. $\square$

Remarque 1.6.9.

Si P et D sont à coefficients dans $\mathbb{R}$, on peut aussi les considérer comme polynômes à coefficients dans $\mathbb{C}$. Remarquer que dans les deux cas, le quotient et le reste de la division euclidienne de P par D sont les mêmes.

Remarque 1.6.10.

P est divisible par D si et seulement si le reste de la division euclidienne de P par D est nul.

Remarque 1.6.11.

En vertu de la remarque sur la division euclidienne, lorsque P et D sont deux polynômes à coefficients dans $\mathbb{R}$, P est divisible par D en tant qu'éléments de $\mathbb{R}[X]$ si et seulement si il l'est en tant qu'éléments de $\mathbb{C}[X]$.

Exemple 1.6.12.

Pour tout $n \in \mathbb{N}$ et tout $a \in \mathbb{K}$, on a

$$X - a \mid X^n - a^n.$$

Proposition 1.6.13.

Soit P et Q deux polynômes. $P \mid Q$ et $Q \mid P$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$ vérifiant $P = \lambda Q$. On dit alors que P et Q sont *associés*.

Tout polynôme P non nul est associé à un unique polynôme unitaire : $\frac{1}{c}P$, où c est le coefficient dominant de P .

Démonstration.

Le résultat est évident si P ou Q est nul (et dans ce cas $P = Q = 0$).

Soient donc P et Q deux polynômes non nuls tels que $P \mid Q$ et $Q \mid P$. Alors on a à la fois $\deg P \leq \deg Q$ et $\deg P \geq \deg Q$. Ainsi $\deg P = \deg Q$. Puisque $P \mid Q$, il existe un polynôme R tel que $PR = Q$, et comme $\deg P = \deg Q$, R est un polynôme constant : P et Q sont bien associés.

Le sens réciproque est évident. $\square$

1.7 L'algorithme de Horner.

Soit $n \in \mathbb{N}$ et $P = \sum_{k=0}^n a_k X^k$ un polynôme de degré au plus n à coefficients dans $\mathbb{K}$ et $x_0 \in \mathbb{K}$.

On a $\tilde{P}(x_0) = \sum_{k=0}^{\deg P} a_k x_0^k$. Connaissant x_0 et les

a_k pour $k \in \llbracket 0, n \rrbracket$, comment calculer $\tilde{P}(x_0)$ de façon aussi efficace que possible ?

On peut évidemment calculer toutes les valeurs x_0^k pour $k \in \llbracket 0, n \rrbracket$ (cela demande $n - 1$ multiplications) puis les produits $a_k x_0^k$ (n multiplications supplémentaires), puis calculer la somme (n additions). Total : $2n - 1$ multiplications et n additions.

On peut cependant faire mieux.

L'algorithme de Horner consiste à remarquer qu'on peut écrire $P(x_0)$ sous la forme

$$(((\dots((a_n x_0 + a_{n-1})x_0 + a_{n-2})\dots)x_0 + a_1)x_0 + a_0)$$

Autrement dit, en posant $r_n = a_n$, puis, pour k allant de $n - 1$ à 0 , $r_k = r_{k+1}x_0 + a_k$, la valeur de $P(x_0)$ est celle de r_0 .

Ainsi on a calculé $P(x_0)$ en seulement n multiplications et n additions.

Exemple 1.7.1.

Posons $P = 2X^4 - 4X^3 - 7X^2 + 2X - 1$ par $X - x_0$ et $x_0 = 3$. On exécute parfois l'algorithme de Horner en traçant un tableau. Dans le cas présent, cela donne :

k	4	3	2	1	0
a_k	2	-4	-7	2	-1
r_k	2	2	-1	-1	-4

On a donc $P(x_0) = -4$.

Associé à la proposition suivante, l'algorithme de Horner permet également d'effectuer la division

euclidienne d'un polynôme P par un polynôme de degré 1.

Proposition 1.7.2.

Soit $P \in \mathbb{K}[X]$ et $x_0 \in \mathbb{K}$. Alors il existe $Q \in \mathbb{K}[X]$ vérifiant $P = (X - x_0)Q + P(x_0)$.

Démonstration.

Nous donnerons deux démonstrations :

Première méthode Posons la division euclidienne de P par $X - x_0$: il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - x_0)Q + R$, avec $\deg R = 0$ ou $-\infty$. R est donc un polynôme constant, notons-le λ .

Évaluons l'égalité $P = (X - x_0)Q + \lambda$ en x_0 : il reste exactement $P(x_0) = \lambda$, d'où le résultat.

Deuxième méthode Cette deuxième méthode ne fait pas appel à la division euclidienne. Elle consiste à constater, en posant $n = \deg P$ et en écrivant P sous la forme $\sum_{k=0}^n a_k X^k$, où $a_k \in \mathbb{K}$ pour $k \in \llbracket 0, n \rrbracket$, que pour tout $k \in \mathbb{N}$, $X^k - x_0^k$ s'écrit $(X - x_0)Q_k$, où $Q_k = \sum_{i=0}^{k-1} x_0^{k-1-i} X^i$, donc

$$\begin{aligned} P - P(x_0) &= \sum_{k=0}^n a_k (X^k - x_0^k) \\ &= \sum_{k=0}^n a_k (X - x_0) Q_k \\ &= (X - x_0) \sum_{k=0}^n a_k Q_k \end{aligned}$$

Donc en posant $Q = \sum_{k=0}^n a_k Q_k$, on a $P = (X - x_0)Q + P(x_0)$.

□

Calculer le reste de la division est facile par la méthode de Horner. Comment calculer le quotient Q ? Q est de la forme $\sum_{k=0}^{n-1} b_k X^k$. On a alors :

$$\sum_{k=0}^n a_k X^k = (X - x_0) \sum_{k=0}^{n-1} b_k X^k + P(x_0)$$

En identifiant les termes de même degré, il vient :

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - x_0 b_{n-1} \\ &\vdots \\ a_2 &= b_1 - x_0 b_2 \\ a_1 &= b_0 - x_0 b_1 \end{aligned}$$

On en déduit :

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= a_{n-1} + x_0 b_{n-1} \\ &\vdots \\ b_1 &= a_2 + x_0 b_2 \\ b_0 &= a_1 + x_0 b_1 \end{aligned}$$

On peut remarquer que les valeurs des coefficients de Q sont exactement celles calculées pour le calcul de $P(x_0)$: on constate en effet qu'on a

$$\begin{aligned} b_{n-1} &= r_n \\ b_{n-2} &= r_{n-1} \\ &\vdots \\ b_1 &= r_2 \\ b_0 &= r_1 \end{aligned}$$

Exemple 1.7.3.

En reprenant l'exemple 1.7.1, on trouve $P = (X - 3)(2X^3 + 2X^2 - X - 1) - 4$.

2 Décomposition.

2.1 Racines, ordre de multiplicité.

Définition 2.1.1.

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est racine de P si $P(a) = 0$.

Proposition 2.1.2.

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est racine de P si et seulement si $X - a$ divise P . Autrement dit :

$$P(a) = 0 \iff X - a \mid P.$$

Démonstration.

Le sens indirect est évident.

Le sens direct découle directement de la proposition 1.7.2 avec $x_0 = a$. $\square$

Corollaire 2.1.3.

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}$ et $a_1, \dots, a_n$ n éléments de $\mathbb{K}$ distincts. Alors $a_1, \dots, a_n$ sont des racines de P si et seulement si $\prod_{k=1}^n (X - a_k)$ divise P .

Démonstration.

Là encore le sens indirect est évident.

Le sens direct se fait par récurrence sur le nombre de racines en utilisant la proposition précédente. $\square$

Définition 2.1.4.

Soit $P \in \mathbb{K}[X]$ un polynôme non nul, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. On dit que a est *racine d'ordre de multiplicité r de P* si r est le plus grand entier k tel que $(X - a)^k$ divise P . On dit que a est racine simple (resp. multiple) de P si $r = 1$ (resp. $r > 1$).

Remarque 2.1.5.

L'ensemble des k tel que $(X - a)^k \mid P$ contient 0 et est majoré par le degré de P , donc possède bien un plus grand élément.

Remarque 2.1.6.

Si a est racine d'ordre r , alors pour tout $k \in \llbracket 0, r \rrbracket$, $(X - a)^k \mid P$.

Remarque 2.1.7.

a est racine de multiplicité r si et seulement si $(X - a)^r \mid P$ et $(X - a)^{r+1} \nmid P$.

Remarque 2.1.8.

a est racine d'ordre au moins 1 si et seulement si $X - a \mid P$, c'est-à-dire si et seulement si $P(a) = 0$.

Remarque 2.1.9.

a est racine multiple si et seulement si $(X - a)^2 \mid P$.

Proposition 2.1.10.

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. a est racine d'ordre r de P si et seulement si P s'écrit sous la forme $(X - a)^r Q$ où $Q(a) \neq 0$.

Démonstration.

Supposons que a est racine d'ordre r de P . Alors P est divisible par $(X - a)^r$, donc s'écrit sous la forme $(X - a)^r Q$. Par l'absurde, supposons $Q(a) = 0$, alors $X - a \mid Q$, donc $(X - a)^{r+1} \mid P$, ce qui est absurde. Donc $Q(a) \neq 0$.

Supposons que P s'écrit sous la forme $(X - a)^r Q$ où $Q(a) \neq 0$. Alors l'ordre de multiplicité de a dans P est au moins r . Supposons par l'absurde que cet ordre soit strictement supérieur. Alors $(X - a)^{r+1}$ divise P , donc P s'écrit sous la forme $(X - a)^{r+1} R$, donc $(X - a)^{r+1} R = (X - a)^r Q$, donc $(X - a)R = Q$. Donc $Q(a) = 0$, ce qui est absurde. $\square$

2.2 Nombres de racines.

Proposition 2.2.1.

Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Alors P a au plus $\deg(P)$ racines distinctes.

Démonstration.

Soit P un polynôme non nul de degré n , et $\lambda_1, \dots, \lambda_{n+1}$ $n + 1$ racines distinctes de P . Alors P est divisible par $\prod_{k=1}^{n+1} (X - \lambda_k)$, qui est un polynôme de degré strictement supérieur au degré de P : c'est absurde. $\square$

Proposition 2.2.2.

Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Si P admet au moins $n + 1$ racines distinctes, alors P est le polynôme nul.

Démonstration.

C'est la contraposée du résultat précédent. $\square$

Corollaire 2.2.3.

On déduit de cette proposition les résultats suivants :

1. Soit $P \in \mathbb{K}[X]$. Si P admet une infinité de racines, alors P est le polynôme nul.
2. Soit $n \in \mathbb{N}$ et $(P, Q) \in \mathbb{K}_n[X]^2$. Si P et Q coïncident sur au moins $n + 1$ points, alors $P = Q$.
3. Soit $(P, Q) \in \mathbb{K}[X]^2$. Si P et Q coïncident sur une infinité de valeurs, alors $P = Q$.

Démonstration. 1. Choisir un entier n vérifiant $n > \deg P$ et appliquer la proposition précédente.

2. Appliquer la proposition précédente au polynôme $P - Q$.
3. Appliquer le premier point à un $n \in \mathbb{N}$ vérifiant $n \geq \max(\deg P, \deg Q)$ ou le second à $P - Q$.

□

En particulier, $\mathbb{K}$ étant infini, un polynôme P tel que $\tilde{P}$ est l'application nulle sur $\mathbb{K}$ est nécessairement nul et deux polynômes P et Q tels que $\tilde{P} = \tilde{Q}$ sont nécessairement égaux, ce qui permet de conclure la démonstration du théorème 1.5.7.

Remarque 2.2.4.

(à caractère culturel) Il est essentiel pour ce résultat que $\mathbb{K}$ soit infini. Dans un corps fini $\mathbb{K}$ comportant n éléments $k_1, \dots, k_n$, le polynôme $(X - k_1) \times (X - k_2) \times \dots \times (X - k_n)$ est non nul (car de degré n) mais a pour racine tous les éléments du corps.

2.3 Polynômes scindés et relations coefficients-racines.

Définition 2.3.1.

Soit $P \in \mathbb{K}[X]$.

On dit que P est *scindé* si P est nul ou peut s'écrire comme produit de polynômes de degré 1, c'est-à-dire s'il existe $n \in \mathbb{N}$, $\lambda \in \mathbb{K}$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ vérifiant

$$P = \lambda \prod_{i=1}^n (X - \alpha_i).$$

Remarque 2.3.2. 1. Dans cette écriture, si P est non nul :

- n est le degré de P
- λ est son coefficient dominant.
- $(\alpha_1, \dots, \alpha_n)$ sont les racines de P comptées avec ordre de multiplicité.

2. Un polynôme à coefficients réels peut être scindé dans $\mathbb{C}$ sans l'être dans $\mathbb{R}$: $P = X^2 + 1$.

Proposition 2.3.3 (Relations coefficients-racines.).

Démonstration.

Il suffit d'identifier $\sum_{i=0}^n a_i X^i$ et $\lambda \prod_{k=1}^n (X - \alpha_k)$. □

Définition 2.3.4.

Les scalaires σ_i , pour $i \in \llbracket 1, n \rrbracket$ sont appelés *fonctions symétriques élémentaires* des racines de P .

Toute expression polynomiale dépendant de variables $\alpha_1, \dots, \alpha_n$, symétrique en $\alpha_1, \dots, \alpha_n$ (c'est-à-dire telle que l'échange de deux de ces variables ne change pas sa valeur) est appelée *fonction symétrique* de $\alpha_1, \dots, \alpha_n$.

Remarque 2.3.5 (à caractère culturel).

Toute fonction symétrique de $\alpha_1, \dots, \alpha_n$ peut s'écrire à partir des seules fonctions symétriques élémentaires de $\alpha_1, \dots, \alpha_n$.

Exemple 2.3.6.

Soit $(x_1, x_2) \in \mathbb{C}$. On pose $v = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2 + 49x_1^2x_2^2$.

v est fonction symétrique de x_1 et x_2 . Comment l'exprimer à partir des fonctions symétriques élémentaires $\sigma_1 = x_1 + x_2$ et $\sigma_2 = x_1x_2$?

Une méthode systématique est la suivante³ :

1. On repère tout d'abord le monôme «dominant». Parmi tous les monômes, le monôme dominant fait partie de ceux dont la puissance de la dernière variable est maximale, et parmi ceux-ci, c'est celui dont la puissance de l'avant-dernière variable est maximale, etc. Ici, la puissance maximale pour x_2 est 2, et parmi les monômes x_2^2 , $14x_1x_2^2$ et $49x_1^2x_2^2$, celui dont la puissance de x_1 est maximale est $49x_1^2x_2^2$.

2. Pour éliminer un monôme $\alpha x_1^{k_1} \dots x_n^{k_n}$, on soustrait $\alpha \sigma_1^{k_n - k_{n-1}} \dots \sigma_{n-1}^{k_2 - k_1} \sigma_n^{k_1}$. Autrement dit, ici on soustrait $49\sigma_1^{2-2}\sigma_2^2$. On obtient donc $v - 49\sigma_2^2 = x_1^2 + 2x_1x_2 + 14x_1^2x_2 + x_2^2 + 14x_1x_2^2$.

3. On itère. Ici il convient donc d'éliminer le monôme $14x_1x_2^2$ et pour cela de soustraire $14\sigma_1^{2-1}\sigma_2$, ce qui donne $v - 49\sigma_2^2 - 14\sigma_1\sigma_2 = x_1^2 + 2x_1x_2 + x_2^2$.

Le plus grand monôme est alors x_2^2 ; on soustrait donc σ_1^2 , ce qui donne $v - 49\sigma_2^2 - 14\sigma_1\sigma_2 - \sigma_1^2 = 0$.

On a donc $v = 49\sigma_2^2 + 14\sigma_1\sigma_2 + \sigma_1^2$.

On remarque cependant qu'on pouvait aller beaucoup plus vite en remarquant dès le début $v = (x_1 + 7x_1x_2 + x_2)^2 = (\sigma_1 + 7\sigma_2)^2$.

NB : selon le programme officiel «Aucune connaissance spécifique sur le calcul des fonctions symétriques des racines n'est exigible».

Exercice 2.3.7.

Résoudre le système d'inconnues (x, y, z)

$$\begin{cases} x + y + z = 3 \\ x^2 + y^2 + z^2 = 11 \\ x^3 + y^3 + z^3 = 27 \end{cases}$$

3. Source : article *Elementary symmetric polynomial* sur Wikipedia (en.wikipedia.org).

2.4 Le théorème fondamental de l'algèbre.

Définition 2.4.1 (Polynômes irréductibles).

Soit $P \in \mathbb{K}[X]$, avec $\deg P \geq 1$. On dit que P est réductible dans $\mathbb{K}[X]$ s'il existe deux polynômes Q et R dans $\mathbb{K}[X]$ vérifiant

1. $\deg Q \geq 1$
2. et $\deg R \geq 1$
3. et $P = Q \times R$.

On dit que P est irréductible dans $\mathbb{K}[X]$ dans le cas contraire.

Remarque 2.4.2. 1. La notion de polynôme irréductible est comparable à celle de primalité dans $\mathbb{Z}$: un polynôme est irréductible si et seulement s'il est de degré au moins 1 et que ses seuls diviseurs sont les éléments de $\mathbb{K}^*$ et ses associés.

2. Attention : un polynôme peut être irréductible dans $\mathbb{R}[X]$ sans l'être dans $\mathbb{C}[X]$. Par exemple $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais se factorise en $(X - i)(X + i)$ dans $\mathbb{C}[X]$.
3. Tout polynôme à coefficients réels irréductible dans $\mathbb{C}[X]$ est irréductible dans $\mathbb{R}[X]$.
4. Tout polynôme de degré 1 est irréductible.
5. Tout polynôme de $\mathbb{K}[X]$ de degré supérieur ou égal à 2 admettant une racine dans $\mathbb{K}$ est réductible dans $\mathbb{K}[X]$.
6. Il existe des polynômes sans racines qui ne sont pas irréductibles. Par exemple $X^4 + 2X^2 + 1$ n'admet pas de racines réelles alors qu'il se décompose comme produit de deux polynômes de degré 2.

Proposition 2.4.3.

Tout polynôme non constant se décompose comme produit de polynômes irréductibles.

Démonstration.

Par récurrence forte sur le degré du polynôme. □

Reste au moins deux questions :

1. Cette décomposition est-elle unique ?

2. Quels sont les polynômes irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$?

On verra plus loin comment répondre au premier point. Pour le second, la réponse nous est fournie par le théorème de d'Alembert-Gauss, aussi appelé théorème fondamental de l'algèbre : comme ce dernier nom l'indique, ce résultat est effectivement d'une importance capitale en algèbre.

Théorème 2.4.4 (d'Alembert-Gauss).

Tout polynôme non constant à coefficients dans $\mathbb{C}$ admet au moins une racine dans $\mathbb{C}$.

Démonstration.

Ce résultat est admis. Pour mémoire, une démonstration possible est de considérer un polynôme P et de montrer successivement :

1. Il existe $R > 0$ tel que pour tout z vérifiant $|z| > R$, $|P(z)| \geq |P(0)|$;
2. $z \mapsto |P(z)|$ admet un minimum sur le pavé des complexes de parties réelles et imaginaires appartenant à $[-R, R]$ en un point a (montrer que la borne inférieure de $|P(z)|$ est un minimum en exploitant la compacité de ce pavé).
3. $z \mapsto |P(z)|$ admet donc un minimum sur $\mathbb{C}$ au point a .
4. Par l'absurde, on suppose $P(a) \neq 0$ et on pose $Q = \frac{1}{P(a)}(P \circ (X + a))$. Alors $Q(0)$ vaut 1 et $z \mapsto |Q(z)|$ admet un minimum (global) en 0.
5. En explicitant Q , on constate que son coefficient constant est égal à 1 et on montre qu'il existe z vérifiant $|Q(z)| < 1$, ce qui est absurde, donc $P(a) = 0$.

□

Corollaire 2.4.5.

Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration.

On sait déjà que tous les polynômes de degré 1 sont irréductibles. De plus, pour tout $n \geq 2$, tout polynôme P de degré n admet une racine complexe a , donc est le produit de $X - a$ par un polynôme de degré $n - 1$. Or $n - 1 \geq 1$, donc P est réductible. □

Remarque 2.4.6.

Ce corollaire est en fait équivalent au théorème de d'Alembert-Gauss. En effet, si l'on admet ce corollaire, on peut démontrer le théorème de d'Alembert-Gauss par une récurrence forte sur le degré du polynôme.

Corollaire 2.4.7.

Tout polynôme non constant est scindé dans $\mathbb{C}[X]$.

Démonstration.

Il suffit d'utiliser les résultats 2.4.3 et 2.4.5. □

Pour les polynômes à coefficients réels, il est intéressant de noter le résultat suivant :

Proposition 2.4.8.

Soit P un polynôme à coefficients réels et $z \in \mathbb{C}$.

Alors z et $\bar{z}$ sont des racines de P de même multiplicité.

En particulier, z est racine de P si et seulement si $\bar{z}$ est racine de P .

Les racines de P non réelles sont donc deux à deux conjuguées.

Démonstration.

On note $\bar{P}$ le polynôme conjugué de P , c'est-à-dire le polynôme dont les coefficients sont les conjugués de ceux de P . On peut alors démontrer plusieurs résultats simples :

1. Si $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, alors $\overline{P(\lambda)} = \bar{P}(\bar{\lambda})$;
2. Si $P, Q \in \mathbb{K}[X]$, $\overline{PQ} = \bar{P} \bar{Q}$;
3. P est à coefficients réels si et seulement si $\bar{P} = P$.

Soit donc P un polynôme à coefficients réels, et z une racine complexe de P , de multiplicité exactement r . Alors il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - z)^r Q$, avec $Q(z) \neq 0$. Mais alors $P = \bar{P} = \overline{(X - z)^r Q} = (X - \bar{z})^r \bar{Q}$. Donc $\bar{z}$ est racine de P multiplicité au moins r . Mais $\bar{Q}(\bar{z}) = \overline{Q(z)} \neq 0$, donc $\bar{z}$ est racine de P multiplicité exactement r .

On peut également démontrer ce résultat de la manière suivante, en utilisant le résultat 3.2.7 qui vient un peu plus loin.

Soit $z \in \mathbb{C}$. On sait que z est racine d'ordre r de P si et seulement si $r = \min \{ k \in \mathbb{N} \mid P^{(k)}(z) \neq 0 \}$ si et seulement si $r = \min \{ k \in \mathbb{N} \mid \overline{P^{(k)}(z)} \neq 0 \}$.

Or pour tout k , $\overline{P^{(k)}(z)} = \overline{P^{(k)}(\bar{z})}$ et pour P à coefficients réels, $\overline{P^{(k)}} = P^{(k)}$, donc

$$\{ k \in \mathbb{N} \mid \overline{P^{(k)}(z)} \neq 0 \} = \{ k \in \mathbb{N} \mid P^{(k)}(\bar{z}) \neq 0 \}$$

Par conséquent z est racine d'ordre r de P si et seulement si $r = \min \{ k \in \mathbb{N} \mid P^{(k)}(\bar{z}) \neq 0 \}$ si et seulement si z est racine d'ordre r de $\bar{P}$. □

On en déduit la proposition suivante

Proposition 2.4.9.

Soit P un polynôme à coefficients réels non constant n'admettant pas de racine réelle. Alors il est divisible par un polynôme à coefficients réels de degré 2.

Démonstration.

Notons a une racine complexe de P . D'après ce qui précède $\bar{a}$ est également une racine de P .

Or, $a \notin \mathbb{R}$ donc $a \neq \bar{a}$, donc $(X - a)(X - \bar{a}) \mid P$.

On voit alors que

$$(X - a)(X - \bar{a}) = X^2 - 2\operatorname{Re}(a)X + |a|^2 \in \mathbb{R}[X].$$

□

On obtient alors le résultat suivant.

Proposition 2.4.10.

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Démonstration.

Montrons déjà que les polynômes réels de degré deux sans racine réelle sont irréductibles. Soit P un tel polynôme, et Q, R deux polynômes réels tels que $P = QR$. Supposons que $\deg Q = 1$. Alors Q est de la forme $aX + b$, où a et b sont des réels, avec $a \neq 0$. Il admet donc $-\frac{b}{a}$ comme racine réelle, et donc P a une racine réelle, ce qui est absurde. Ainsi $\deg Q = 0$ ou 2, et P est irréductible.

Soit P un polynôme réel irréductible, de degré strictement supérieur à 1. S'il admet une racine réelle a , il est divisible par $X - a$ et n'est donc pas irréductible. S'il n'admet pas de racine réelle, il est divisible par un polynôme réel de degré 2. Donc si P est de degré strictement supérieur à 2, il est réductible. S'il est de degré 2, il est bien de la forme annoncée. □

2.5 Décomposition en produit de facteurs irréductibles.

Le théorème de d'Alembert-Gauss a pour corollaires immédiats les résultats suivants.

Corollaire 2.5.1.

Soit $n \in \mathbb{N}$, P un polynôme de degré n et de coefficient dominant c . Alors il existe $z_1, \dots, z_n$ des complexes vérifiant :

$$P = c \prod_{k=1}^n (X - z_k),$$

où les z_k , pour $k \in \llbracket 1, n \rrbracket$ sont les racines de P , éventuellement répétées.

Remarque 2.5.2.

Dans une telle écriture, c est forcément le coefficient dominant de P , n est le degré de P et les z_i sont les racines de P , répétées autant de fois que leurs multiplicités.

Une telle écriture est donc unique. On retrouvera l'unicité de cette décomposition ultérieurement, et de manière plus abstraite (et semblable à la démonstration donnée sur les entiers).

Corollaire 2.5.3.

Soit $n \in \mathbb{N}$, $P \in \mathbb{C}[X]$ de degré n et de coefficient dominant c . Alors, en notant p le nombre de racines distinctes de P , $z_1, \dots, z_p$ les racines distinctes de P , et $n_1, \dots, n_p$ leurs multiplicités respectives, on a :

$$P = c \prod_{k=1}^p (X - z_k)^{n_k},$$

$$n = \sum_{k=1}^p n_k.$$

Démonstration.

La première égalité découle directement du corollaire précédent, et la seconde est l'égalité des degrés dans l'égalité polynomiale précédente. □

Théorème 2.5.4.

Soit P un polynôme à coefficients réels, alors on peut écrire P sous la forme

$$P = c \prod_{k=1}^n (X - a_k) \prod_{k=1}^m (X - z_k)(X - \bar{z}_k)$$

où $a_1, \dots, a_n$ sont les racines réelles de P (répétées avec leur multiplicité), $z_1, \dots, z_m, \bar{z}_1, \dots, \bar{z}_m$ les racines complexes non réelles (répétées avec leur multiplicité), c le coefficient dominant de P , et $n + 2m = \deg(P)$.

On a donc

$$P = c \prod_{k=1}^n (X - a_k) \prod_{k=1}^m (X^2 - 2\operatorname{Re}(z_k)X + |z_k|^2)$$

Remarque 2.5.5.

On obtiendrait une décomposition semblable à celle obtenue au corollaire 2.5.3 en faisant apparaître des multiplicités.

Corollaire 2.5.6.

Tout polynôme à coefficients réels de degré impair a au moins une racine réelle.

Démonstration.

Par contraposition : un polynôme à coefficients réels n'ayant pas de racine réelle s'écrit sous la forme $c \prod_{k=1}^m (X^2 - 2\operatorname{Re}(z_k)X + |z_k|^2)$ et est donc de degré pair. $\square$

Exercice 2.5.7.

Factoriser sur $\mathbb{R}$ les polynômes $X^5 + 1$ et $X^4 + 1$.

3 Dérivation des polynômes.

On introduit maintenant la notion de dérivation formelle de polynômes. Le mot « formel » est à prendre au sens suivant : on effectue des opérations *algébriques*, qui n'ont pas forcément de sens *analytique* (même si la dérivation formelle de polynômes coïncide avec la dérivation de fonctions polynomiales).

3.1 Définition.

Définition 3.1.1.

Soit $P \in \mathbb{K}[X]$, que l'on écrit $P = \sum_{k=0}^{+\infty} a_k X^k$. Son polynôme dérivé est

$$P' = \sum_{k=1}^{+\infty} a_k k X^{k-1}.$$

Remarque 3.1.2.

- La somme ne commence qu'à l'indice 1 :



en effet, pour $k = 0$, X^{k-1} n'existe pas.

- On a également, après changement d'indice :

$$P' = \sum_{k=0}^{+\infty} a_{k+1} (k+1) X^k.$$

Cette formule est intéressante lorsqu'il s'agit de manipuler plusieurs polynômes, tous exprimés comme sommes commençant à l'indice 0.

- Sur $\mathbb{R}[X]$, cette opération coïncide avec la dérivation des applications à valeurs réelles :

$$\forall P \in \mathbb{R}[X] \quad (\widetilde{P'}) = (\tilde{P})'.$$

- Si P est de degré 0 ou $-\infty$, alors $P' = 0$. Sinon $\deg(P') = \deg(P) - 1$.

- Dans tous les cas, $\deg P' \leq \deg P - 1$, et cela est suffisant dans beaucoup de cas.

Par exemple, soit $\varphi : \mathbb{R}_n[X] \rightarrow \mathbb{R}_n[X]$, $P \mapsto X^2 P'' - (2X + 1)P' + 2P$. Montrer que l'ensemble d'arrivée de φ est bien $\mathbb{R}_n[X]$.

- P est un polynôme vérifiant $P' = \sum_{k=0}^{+\infty} a_k X^k$ si et seulement s'il existe $C \in \mathbb{K}$ vérifiant

$$P = C + \sum_{k=0}^{+\infty} \frac{a_k}{k+1} X^{k+1}$$

(donner un nom aux coefficients de P , calculer P' et utiliser l'unicité de la forme développée réduite).

- Si $P' = 0$, alors P est constant.

Définition 3.1.3.

Soit $P \in \mathbb{K}[X]$. On définit, pour $n \in \mathbb{N}$, le n -ième dérivé de P , noté $P^{(n)}$ par

$$P^{(0)} = P \\ \text{et } \forall n \in \mathbb{N} \quad P^{(n+1)} = (P^{(n)})'$$

Exercice 3.1.4.

Soit $p \in \mathbb{N}$, dériver successivement X^p .

3.2 Propriétés.

Proposition 3.2.1.

Soit $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q', \quad (\text{XVI.1})$$

$$(PQ)' = P'Q + PQ', \quad (\text{XVI.2})$$

$$(P \circ Q)' = Q' \times (P' \circ Q). \quad (\text{XVI.3})$$

Démonstration.

Écrivons P sous la forme $\sum_{k=0}^{+\infty} a_k X^k$ et Q sous la forme

$$\sum_{k=0}^{+\infty} b_k X^k.$$

Alors on a

$$\begin{aligned} (\lambda P + \mu Q)' &= \left(\sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) X^k \right)' \\ &= \sum_{k=1}^{+\infty} k(\lambda a_k + \mu b_k) X^{k-1} \\ &= \lambda \left(\sum_{k=1}^{+\infty} k a_k X^{k-1} \right) + \mu \left(\sum_{k=1}^{+\infty} k b_k X^{k-1} \right) \\ &= \lambda P' + \mu Q'. \end{aligned}$$

Le premier point est donc assuré. Il se généralise évidemment par récurrence à toute combinaison linéaire finie de polynômes.

Montrons alors le second. Notons, pour tout $i \in \mathbb{N}$, A_i le monôme X^i et remarquons que pour tout $(i, j) \in \mathbb{N}^2$, on a $(A_i A_j)' = A'_i A_j + A_i A'_j$.

En effet, c'est évidemment vrai si $i = 0$ (auquel cas $A_i = 1$ et $A'_i = 0$) ou symétriquement si $j = 0$. Si ni i ni j n'est nul, on a $i \geq 1$ et $j \geq 1$, d'où

$$\begin{aligned} (A_i A_j)' &= (X^{i+j})' \\ &= (i+j) X^{i+j-1} \\ &= i X^{i-1} X^j + X^i \times j X^{j-1} \\ &= A'_i A_j + A_i A'_j. \end{aligned}$$

On a alors successivement :

$$\begin{aligned} (PQ)' &= \left(\left(\sum_{i \in \mathbb{N}} a_i A_i \right) \left(\sum_{j \in \mathbb{N}} b_j A_j \right) \right)' \\ &= \left(\sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A_j \right)' \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j (A_i A_j)' \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j (A'_i A_j + A_i A'_j) \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A'_i A_j + \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A'_j. \end{aligned}$$

Or on a

$$\begin{aligned} \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A'_i A_j &= \left(\sum_{i \in \mathbb{N}} a_i A'_i \right) \left(\sum_{j \in \mathbb{N}} b_j A_j \right) \\ &= P' Q \\ \text{et } \sum_{(i,j) \in \mathbb{N}^2} a_i b_j A_i A'_j &= \left(\sum_{i \in \mathbb{N}} a_i A_i \right) \left(\sum_{j \in \mathbb{N}} b_j A'_j \right) \\ &= P Q', \end{aligned}$$

donc $(PQ)' = P'Q + PQ'$.

On en déduit par récurrence que pour tout entier $k \in \mathbb{N}^*$, on a $(Q^k)' = kQ' \times Q^{k-1}$. En outre, on a évidemment $(Q^0)' = (1_{\mathbb{K}[X]})' = 0$.

On a alors successivement

$$\begin{aligned} (P \circ Q)' &= \left(\sum_{k=0}^{+\infty} a_k Q^k \right)' \\ &= \sum_{k=1}^{+\infty} a_k k Q' \times Q^{k-1} \\ &= Q' \times \sum_{k=1}^{+\infty} a_k k Q^{k-1} \\ &= Q' \times \left(\left(\sum_{k=1}^{+\infty} k a_k Q^{k-1} \right) \circ Q \right) \\ &= Q' \times (P' \circ Q). \end{aligned}$$

□

Remarque 3.2.2.

Notamment, $P' = Q'$ si et seulement si il existe $C \in \mathbb{K}$ tel que $P = Q + C$.

Proposition 3.2.3 (Formule de Leibniz).

Soit $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$. Alors

$$(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Démonstration.

Elle se démontre par récurrence et est laissée en exercice au lecteur, qui remarquera une très très forte ressemblance avec la démonstration d'une formule de début d'année. □

Lemme 3.2.4 (Formule de Taylor Mac-Laurin).

Soit $n \in \mathbb{N}$ et $P \in \mathbb{K}_n[X]$. Alors

$$P = \sum_{k=0}^n \frac{P^{(k)}(0)}{k!} X^k.$$

Démonstration.

Démontrons-la par récurrence :

pour tout $n \in \mathbb{N}$, soit (H_n) : pour tout $P \in \mathbb{K}_n[X]$,

$$P = \sum_{k=0}^n \frac{P^{(k)}(0)}{k!} X^k.$$

- Pour $n = 0$, la propriété est évidente.
- Soit $n \in \mathbb{N}$ tel que la propriété soit vraie, et soit

$P \in \mathbb{K}_{n+1}[X]$. Puisque $P' \in \mathbb{K}_n[X]$, on peut lui appliquer l'hypothèse de récurrence : $P' = \sum_{k=0}^n \frac{(P')^{(k)}(0)}{k!} X^k = \sum_{k=0}^n \frac{P^{(k+1)}(0)}{k!} X^k$. Il existe donc une constante $C \in \mathbb{K}$ telle que $P = \sum_{k=0}^n \frac{P^{(k+1)}(0)}{(k+1)!} X^{k+1} + C = \sum_{k=1}^{n+1} \frac{P^{(k)}(0)}{k!} X^k + C$ après un changement d'indice. Pour calculer C , on peut étudier les fonctions polynomiales associés aux polynômes de l'égalité précédente, et les évaluer en 0 : on trouve alors $C = P(0) = \frac{P^{(k)}(0)}{k!} X^k$ avec $k = 0$, et donc H_{n+1} est bien vérifiée. $\square$

Proposition 3.2.5 (Formule de Taylor).

Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors

$$P = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Corollaire 3.2.6.

On en déduit immédiatement

$$P \circ (a + X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} X^k$$

Démonstration.

Il suffit d'effectuer une "translation" à partir du théorème précédent : posons $Q = P \circ (X + a)$.

Alors $Q = \sum_{k=0}^n \frac{Q^{(k)}(0)}{k!} X^k$. Mais on vérifie facilement que

pour tout k , $Q^{(k)} = P^{(k)} \circ (X + a)$ et donc $Q^{(k)}(0) = P^{(k)}(a)$.

Finalement, on a

$$\begin{aligned} P &= Q \circ (X - a) \\ &= \left(\sum_{k=0}^n \frac{P^{(k)}(a)}{k!} X^k \right) \circ (X - a) \\ &= \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X - a)^k \end{aligned}$$

$\square$

Proposition 3.2.7.

Soit $P \in \mathbb{K}[X]$ non nul, $r \in \mathbb{N}$ et $a \in \mathbb{K}$.

a est racine d'ordre r de P si et seulement si $P^{(r)}(a) \neq 0$ et pour tout $k \in \llbracket 0, r-1 \rrbracket$, $P^{(k)}(a) = 0$

Démonstration.

On écrit, pour un entier n supérieur ou égal à r et à $\deg(P)$:

$$P = \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!} (X-a)^k + \sum_{k=r}^n \frac{P^{(k)}(a)}{k!} (X-a)^k.$$

Si

$$P(a) = P'(a) = \dots = P^{(r-1)}(a) = 0, P^{(r)}(a) \neq 0$$

alors directement $(X-a)^r \mid P$ et $(X-a)^{r+1} \nmid P$.

Réciproquement, si $(X-a)^r \mid P$, alors

$$(X-a)^r \mid \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!} (X-a)^k.$$

Comme

$$\deg \left(\sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!} (X-a)^k \right) \leq r-1,$$

on obtient

$$\sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!} (X-a)^k = 0.$$

On écrit alors

$$\begin{aligned} 0 &= 0 \circ (X + a) \\ &= \sum_{k=0}^{r-1} \frac{P^{(k)}(a)}{k!} (X)^k. \end{aligned}$$

Par unicité des coefficients d'un polynôme, on a alors

$$P(a) = P'(a) = \dots = P^{(r-1)}(a) = 0,$$

Si de plus $(X-a)^{r+1} \nmid P$, alors $P^{(r)}(a) \neq 0$.

On a donc bien $(X-a)^r \mid P$ et $(X-a)^{r+1} \nmid P$ si et seulement si $P^{(r)}(a) \neq 0$ et pour tout $k \in \llbracket 0, r-1 \rrbracket$, $P^{(k)}(a) = 0$. $\square$

Exercice 3.2.8.

Déterminer la multiplicité de 1 en tant que racine de

$$nX^{n+1} - (n+1)X^n + 1$$

Corollaire 3.2.9.

Soit $P \in \mathbb{K}[X]$, $r \in \mathbb{N}^*$ et $a \in \mathbb{K}$.

Si a est racine d'ordre r de P , alors a est racine d'ordre $r-1$ de P' .



La réciproque est fautive ! Par exemple si $P = X^2 - 1$, alors 0 est racine de multiplicité 1 de P' , mais n'est pas racine de multiplicité 2 de P (ce n'est même pas une racine de P).

On peut cependant énoncer le résultat suivant : si a est racine d'ordre $r - 1$ de P' et si a est racine, de P , alors a est racine d'ordre r de P .

4 Arithmétique de $\mathbb{K}[X]$.

4.1 PGCD.

Dans cette partie, pour tout $a \in \mathbb{K}[X]$, on note $\mathcal{D}(a)$ l'ensemble des diviseurs de a et pour tout couple $(a, b) \in \mathbb{K}[X]$, $\mathcal{D}(a, b)$ l'ensemble des diviseurs communs à a et b . On remarquera que $\mathcal{D}(a, b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

- Remarque 4.1.1.** 1. Soit d et δ deux polynômes. $\mathcal{D}(d) = \mathcal{D}(\delta)$ si et seulement si d et δ sont associés.
2. En particulier, si on a $\mathcal{D}(d) = \mathcal{D}(\delta)$ et que d et δ sont unitaires, alors $d = \delta$ et pour tout polynôme d , il existe δ unitaire vérifiant $\mathcal{D}(\delta) = \mathcal{D}(d)$.

Lemme 4.1.2 (lemme d'Euclide).

Soient $(a, b) \in \mathbb{K}[X]^2$, avec $b \neq 0$. Notons r le reste de la division euclidienne de a par b . Alors $\mathcal{D}(a, b) = \mathcal{D}(b, r)$.

Démonstration.

Soit $d \in \mathcal{D}(a, b)$. Alors a s'écrit sous la forme $bq + r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise bq , donc divise r . Donc $\mathcal{D}(a, b) \subset \mathcal{D}(b, r)$.

Réciproquement, soit $d \in \mathcal{D}(b, r)$, alors a s'écrit sous la forme $bq + r$ or $d|b$ et $d|r$ donc d divise a . Donc $\mathcal{D}(b, r) \subset \mathcal{D}(a, b)$. $\square$

Théorème 4.1.3.

Soit $(a, b) \in \mathbb{K}[X]^2$ avec $(a, b) \neq (0, 0)$. Alors, il existe $d \in \mathbb{K}[X]$ tel que $\mathcal{D}(a, b) = \mathcal{D}(d)$.

Démonstration.

Ce résultat repose sur un algorithme, appelé algorithme d'Euclide. En utilisant les objets «polynômes» fournis par la bibliothèque python `numpy`, cet algorithme s'écrit :

```
def euclide (a,b) :
    """Précondition  $\square(a, b) \neq \square(0, 0)$  """
    R0 = abs(a)
    R1 = abs(b)
    while R1 > 0 :
        # Invariant :  $D(R0, R1) = D(a, b)$ 
        # et  $R0 \geq 0$  et  $R1 \geq 0$ 
        # et  $(R0, R1) \neq (0, 0)$ 
        # Variant :  $R1$ 
        (q, R2) = diveuclide (R0, R1)
        R0 = R1
        R1 = R2
    # Sortie de boucle :  $R1 == 0$ 
    return R0
```

Soit a et b deux polynômes non tous les deux nuls. Il est clair que l'appel `euclide(a,b)` termine. La valeur d retournée vérifie $\mathcal{D}(a, b) = \mathcal{D}(d, 0)$ et $(d, 0) \neq (0, 0)$. Or $\mathcal{D}(d, 0)$ est l'ensemble des diviseurs de d donc $\mathcal{D}(a, b)$ est bien l'ensemble des diviseurs d'un polynôme d .

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante :

$$\begin{cases} r_0 = a \\ r_1 = b \\ \forall n \in \mathbb{N}, r_{n+2} = \begin{cases} \text{diveuclide}(r_n, r_{n+1}) & \text{si } r_{n+1} \neq 0 \\ 0 & \text{sinon} \end{cases} \end{cases}$$

À partir d'un certain rang, cette suite est nulle, sinon la suite $(\deg(r_n))_{n \in \mathbb{N}}$ serait strictement décroissante (du moins, à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0, 0)$, on a $\mathcal{D}(r_n, r_{n+1}) = \mathcal{D}(a, b)$. En particulier, pour la dernière valeur non nulle r_n , on a $\mathcal{D}(r_n, 0) = \mathcal{D}(a, b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au n ème tour de boucle, R_0 contient la valeur de r_n , et R_1 celle de r_{n+1} . $\square$

Remarque 4.1.4.

D'après la remarque 4.1.1, il existe donc un unique d unitaire tel que $\mathcal{D}(a, b) = \mathcal{D}(d)$.

Définition 4.1.5.

Soit a et b deux polynômes avec $(a, b) \neq (0, 0)$, alors on appelle plus grands diviseurs communs de a et b (pgcd de a et b) les polynômes d vérifiant $\mathcal{D}(d) = \mathcal{D}(a, b)$. L'unique polynôme unitaire parmi ceux-ci est appelé le pgcd de a et b et noté $\text{PGCD}(a, b)$ ou $a \wedge b$.

On convient que $\text{PGCD}(0, 0) = 0$.

Remarque 4.1.6. 1. L'existence des pgcd assurée par le théorème 4.1.3. D'après la remarque 4.1.1, il y en a donc un nombre infini.

2. L'existence et l'unicité du pgcd unitaire est assurée par la remarque 4.1.4.
3. Les pgcd de a et b sont les polynômes de degré maximum de $\mathcal{D}(a, b)$.
4. Si a et b sont deux polynômes de $\mathbb{R}[X]$, nous avons déjà vu que leurs divisions euclidiennes dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$ sont les mêmes. Le lemme d'Euclide assure donc que le PGCD de a et b dans $\mathbb{C}[X]$ est le même que leur PGCD dans $\mathbb{R}[X]$. L'unicité du PGCD permet également de s'en assurer.
5. La relation de divisibilité $|$ n'est pas une relation d'ordre sur $\mathbb{K}[X]$, mais induit une relation d'ordre sur l'ensemble des polynômes unitaires. Le pgcd de deux polynômes unitaires a et b est alors le maximum des polynômes unitaires de $\mathcal{D}(a, b)$ pour $|$ et est donc la borne inférieure de a et b pour $|$.

On peut donner la caractérisation suivante :

Proposition 4.1.7.

Soient $(a, b, d) \in \mathbb{K}[X]^3$. d est un pgcd de a et b si et seulement si $d|a$ et $d|b$ et pour tout $n \in \mathbb{K}[X]$ vérifiant $n|a$ et $n|b$, on a $n|d$.

Démonstration.

Remarquons successivement :

1. $d|a$ et $d|b \Leftrightarrow d \in \mathcal{D}(a, b) \Leftrightarrow \mathcal{D}(d) \subset \mathcal{D}(a, b)$. La dernière équivalence peut se démontrer comme suit : le sens direct provient de la transitivité de la relation de divisibilité (si d est un diviseur de a , tout diviseur de d est un diviseur de a ; idem avec b) ; le sens indirect vient du fait que $\mathcal{D}(d)$ contient d .
2. $[\forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d] \Leftrightarrow \mathcal{D}(d) \supset \mathcal{D}(a, b)$ découle directement de la définition de $\mathcal{D}(d)$ et $\mathcal{D}(a, b)$.
3. Par conséquent, on a $[d|a \text{ et } d|b \text{ et } \forall n \in \mathbb{K}[X], (n|a \text{ et } n|b) \Rightarrow n|d]$ si et seulement si $\mathcal{D}(d) = \mathcal{D}(a, b)$, si et seulement si d est un pgcd de a et b .

□

On a également :

Proposition 4.1.8.

Soient $(a, b, c) \in \mathbb{K}[X]^3$. Alors $(ac) \wedge (bc) = \frac{1}{\lambda} c(a \wedge b)$, où λ est le coefficient dominant de c .

Démonstration.

Soit $\delta = a \wedge b$ et $\Delta = (ac) \wedge (bc)$. Il suffit de montrer que $c\delta$ et Δ sont associés, et pour cela nous allons montrer que $c\delta|\Delta$ et $\Delta|c\delta$.

1. $\delta|a$ et $\delta|b$, donc $c\delta|ac$ et $c\delta|bc$. Par suite $c\delta|\Delta$.
2. $c|ac$ et $c|bc$, donc $c|\Delta$. Ainsi il existe $p \in \mathbb{R}[X]$ tel que $\Delta = pc$. Or $\Delta|ac$ et $\Delta|bc$, i.e $pc|ac$ et $pc|bc$. Le polynôme c étant non nul, on en déduit $p|a$ et $p|b$, et donc $p|\delta$. Finalement $pc|\delta c$, soit encore $\Delta|c\delta$.

On a donc le résultat. □

Théorème 4.1.9 (Théorème de Bézout, première partie).

Soient $(a, b) \in \mathbb{K}[X]^2$. Il existe deux polynômes u et v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b .

Démonstration.

L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires (à coefficients polynomiaux) de a et b . À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b .

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0a + V_0b$ et $R_1 = U_1a + V_1b$. En python, en supposant ⁴ que l'existence d'un type des polynômes, et à condition que les notation $+$ et $*$ soient autorisées pour la somme et le produit de polynômes (et pour le produit d'un polynôme par un scalaire), cet algorithme s'écrit :

```
def euclide_etendu (a, b) :
    """Précondition  $\square(a, b) \square \square (0, 0)$  """
    R0 = abs(a)
    if a < 0 :
        U0 = -1
    else :
        U0 = 1
    V0 = 0
    # Invariant : R0 == U0*a + V0*b
    R1 = abs(b)
    U1 = 0
    if b < 0 :
        V1 = -1
    else :
        V1 = 1
    # Invariant : R1 == U1*a + V1*b
    # Invariant : D(R0, R1) == D(a, b)
    while R1 > 0 :
        # Invariants :
        # D(R0, R1) == D(a, b)
```

4. Il existe des bibliothèques pour cela (numpy par ex.) !

```

# R1>=0 et R2>=0
# (R1,R2) != (0,0)
# R0 == U0*a + V0*b
# R1 == U1*a + V1*b
# Variant : R1
(q,R2) = diveuclide(R0,R1)
# donc R2 = R0 - q*R1
U2 = U0-q*U1
V2 = V0-q*V1
# R2 = U2*a + V2*b
R0, U0, V0 = R1, U1, V1
R1, U1, V1 = R2, U2, V2
# R1 == 0
return (R0,U0,V0)

```

(attention cependant, l'algorithme ci-dessus ne retourne pas le pgcd mais un pgcd avec les coefficients de Bézout associés).

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r , u et v , où r est la suite considérée précédemment, où u et v vérifient $r_i = u_i a + v_i b$ pour $i = 0, 1$ et pour n tel que r_{n+1} soit non nul, $u_{n+2} = u_n - a q_{n+1}$ et $v_{n+2} = v_n - q v_{n+1}$, où q est le quotient de la division euclidienne de r_n par r_{n+1} . Là encore, il n'est pas difficile de montrer par récurrence double que tant que $(r_n, r_{n+1}) \neq (0, 0)$, on a $r_n = u_n a + v_n b$. $\square$



Le couple des coefficients de Bézout n'est pas unique. Par exemple on a

$$\begin{array}{rcl} 1 \times (2X^2 + X) & -2X \times X & = X \\ (X+1) \times (2X^2 + X) & -(2X^2 + 3X) \times X & = X \end{array}$$

Exemple 4.1.10.

Calcul d'un couple de Bézout pour

$$P = 2X^6 - 5X^5 + 8X^4 - 6X^3 + 3X - 2$$

et

$$Q = 2X^5 - 7X^4 + 14X^3 - 17X^2 + 12X - 4$$

4.2 Polynômes premiers entre eux.

Définition 4.2.1.

Deux polynômes a et b sont dit premiers entre eux si et seulement si $(a, b) \neq (0, 0)$ et $a \wedge b = 1$.

Remarque 4.2.2. 1. Le PGCD de deux polynômes réels étant le même dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$, alors deux polynômes réels sont premiers dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.

2. a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont les éléments inversibles de $\mathbb{K}[X]$, en d'autres termes si et seulement si $\mathcal{D}(a, b) \subset \mathbb{K}^*$ (ce qui est équivalent à $\mathcal{D}(a, b) = \mathbb{K}^*$).
3. si a et b sont irréductibles, alors ils sont soit premiers entre eux, soit associés. En particulier, si a et b sont irréductibles et unitaires, alors ils sont soit premiers entre eux, soit égaux.

Théorème 4.2.3 (Théorème de Bézout, seconde partie).

Soient $a, b \in \mathbb{K}[X]$. a et b sont premiers entre eux si et seulement s'il existe deux polynômes u et v tels que $au + bv = 1$.

Démonstration.

Le cas $(a, b) = (0, 0)$ est trivial (dans ce cas, a et b ne sont pas premiers entre eux et il n'existe pas de couple de Bézout).

Considérons donc $(a, b) \in \mathbb{K}[X]^2 \setminus \{(0, 0)\}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout première partie, on a le résultat.

Réciproquement, supposons qu'il existe deux polynômes u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathcal{D}(a, b)$. On a $d|a$ et $d|b$, donc $d|(au + bv)$, donc $d|1$, donc $d \in \mathbb{K}^*$. Donc $\mathcal{D}(a, b) \subset \mathbb{K}^*$. $\square$



$au + bv = 1$ implique $a \wedge b = 1$, mais $au + bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b) | d$.

Corollaire 4.2.4.

Soit $a, b \in \mathbb{K}[X] \setminus \{(0, 0)\}$. Alors en posant $d = a \wedge b$, a et b s'écrivent respectivement sous la forme $a_0 \times d$ et $b_0 \times d$ où $(a_0, b_0) \in \mathbb{K}[X]^2$. On a alors $a_0 \wedge b_0 = 1$.

Démonstration.

On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a_0 u + b_0 v$, donc a_0 et b_0 sont premiers entre eux. $\square$

Remarque 4.2.5.

Ce corollaire est très fréquemment utilisé.

Corollaire 4.2.6. (i) Soient a premier avec k polynômes $b_1, b_2, \dots, b_k$. Alors a est premier avec $b_1.b_2.\dots.b_k$.
(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}^*$, a^m et b^n sont également premiers entre eux.

Démonstration. (i) On traite le cas $k = 2$, le cas général s'en déduit par récurrence. Il existe u_i et v_i vérifiant $au_i + b_iv_i = 1$ pour $i \in \{1, 2\}$. En multipliant ces deux relations, il vient successivement

$$\begin{aligned} 1 &= (au_1 + b_1v_1)(au_2 + b_2v_2) \\ 1 &= a^2u_1u_2 + au_1b_2v_2 + b_1v_1au_2 + b_1v_1b_2v_2 \\ 1 &= a(au_1u_2 + u_1b_2v_2 + b_1v_1u_2) + b_1b_2(v_1v_2) \end{aligned}$$

D'où le résultat.

(ii) On applique (i) à a et $b.b.b.\dots.b$, puis (i) à b^n et $a.a.a.\dots.a$. Plus proprement, la résultat se démontre par récurrence. $\square$

Proposition 4.2.7.

Deux polynômes complexes sont premiers entre eux si et seulement s'ils n'ont aucune racine complexe en commun.

Démonstration.

Soit $A, B \in \mathbb{C}[X]$.

Supposons que $A \wedge B = 1$, par le théorème de Bézout il existe $U, V \in \mathbb{C}[X]$ tels que $AU + BV = 1$. Si A et B ont une racine en commun, il suffit d'évaluer en cette racine pour obtenir $0 = 1$, ce qui est absurde. Ainsi, A et B n'ont pas de racine complexe en commun.

Réciproquement, supposons que A et B n'ont pas de racine complexe en commun. Remarquons que si $\alpha \neq \beta$, alors $X - \alpha$ et $X - \beta$ sont premiers entre eux (il suffit de trouver une combinaison linéaire donnant 1). En utilisant les décompositions de A et de B en produits de facteurs irréductibles complexes, il suffit d'utiliser le résultat du corollaire 4.2.6 pour obtenir que A et B sont premiers entre eux. $\square$

Théorème 4.2.8 (Théorème de Gauss).

Soient $(a, b, c) \in \mathbb{K}[X]^3$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.

On a $a \wedge b = 1$ donc 1 s'écrit sous la forme $au + bv$ avec $(u, v) \in \mathbb{K}[X]^2$. Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire à coefficients dans $\mathbb{K}[X]$ de a et bc . Or bc est un multiple de a donc c est un multiple de a . $\square$

Théorème 4.2.9 (Unicité de la décomposition en facteurs irréductibles).

Tout polynôme non nul se décompose de façon unique comme produit d'un scalaire par des irréductibles unitaires, à l'ordre près des facteurs.

Démonstration.

On a déjà vu l'existence. Il reste donc à montrer l'unicité. Par l'absurde, supposons qu'il existe un polynôme admettant deux décompositions. Alors il existe un polynôme P de degré minimal admettant deux décompositions distinctes $\lambda \prod_{k=1}^a A_k$ et $\mu \prod_{k=1}^b B_k$, où $(a, b) \in \mathbb{N}^2$, $(\lambda, \mu) \in \mathbb{K}^2$ et les A_k et les B_k sont irréductibles unitaires pour k appartenant respectivement à $\llbracket 1, a \rrbracket$ et $\llbracket 1, b \rrbracket$.

Alors λ et μ sont le coefficient dominant de P , donc sont égaux.

$$\text{Donc } \prod_{k=1}^a A_k = \prod_{k=1}^b B_k.$$

On a $a \neq 0$. En effet, sinon on aurait $b = 0$ et on aurait dans les deux cas à un produit vide, il aurait donc unicité.

De même $b \neq 0$.

Remarquons que pour tout $k \in \llbracket 1, b \rrbracket$, A_a est premier avec B_k . En effet, sinon il existerait $k_0 \in \llbracket 1, b \rrbracket$ tel que A_a et B_{k_0} ne soient pas premiers entre eux. Or ils sont irréductibles et unitaires, donc ils seraient égaux. On aurait donc

$$\prod_{k=1}^{a-1} A_k = \prod_{\substack{k \in \llbracket 1, b \rrbracket \\ k \neq k_0}} B_k$$

Il existerait alors un polynôme de degré strictement plus petit que $\deg P$, admettant deux décompositions distinctes, ce qui est absurde car on a supposé que P était de degré minimal.

Donc A_a est donc premier avec $\prod_{k=1}^b B_k$, donc avec P . Or

A_a divise P et n'est pas un polynôme constant.

C'est donc absurde. $\square$

Remarque 4.2.10.

Comme pour les entiers, nous pouvons donner les résultats suivants :

- Deux polynômes sont premiers entre eux si et seulement s'ils n'ont aucun facteur irréductible en commun ;
- la notion de *valuation* d'un polynôme irréductible dans un polynôme peut se définir, et permet de calculer le PGCD de deux polynômes A et B , en considérant le minimum des valuations d'un même facteur irréductible dans A et B . En anticipant sur les paragraphes qui suivent, la valuation est

également utilisée pour le PPCM de deux polynômes, mais aussi les PGCD et PPCM d'une famille de polynômes.

4.3 PGCD de n polynômes.

Comme dans le cas de l'arithmétique sur les entiers, on introduit la notion de PGCD de plusieurs polynômes et de polynômes premiers entre eux dans leur ensemble.

Définition 4.3.1.

Soit $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, on note $\mathcal{D}(A_1, \dots, A_n) = \bigcap_{i=1}^n \mathcal{D}(A_i)$ l'ensemble des diviseurs communs à tous ces polynômes.

Proposition 4.3.2.

Soit $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, il existe un polynôme D unique à association près tel que $\mathcal{D}(A_1, \dots, A_n) = \mathcal{D}(D)$.

Démonstration.

L'unicité à association près est évidente. On montre par récurrence que $\forall n \in \mathbb{N}^*$, $\mathcal{H}_n : \forall (A_1, \dots, A_n) \in \mathbb{K}[X]^n, \exists D \in \mathbb{K}[X], \mathcal{D}(A_1, \dots, A_n) = \mathcal{D}(D)$.

Initialisation : OK.

Hérédité : Soit $n \in \mathbb{N}^*$, supposons $\mathcal{H}_n$ et montrons $\mathcal{H}_{n+1}$. Soit $(A_1, \dots, A_{n+1}) \in \mathbb{K}[X]^{n+1}$. D'après $\mathcal{H}_n$, il existe D_1 tel que $\mathcal{D}(A_1, \dots, A_n) = \mathcal{D}(D_1)$. On a alors

$$\begin{aligned} \mathcal{D}(A_1, \dots, A_{n+1}) &= \bigcap_{i=1}^{n+1} \mathcal{D}(A_i) \\ &= \mathcal{D}(A_1, \dots, A_n) \cap \mathcal{D}(A_{n+1}) \\ &= \mathcal{D}(D_1) \cap \mathcal{D}(A_{n+1}) \\ &= \mathcal{D}(D_1 \wedge A_{n+1}), \end{aligned}$$

d'où $\mathcal{H}_{n+1}$.

□

Remarque 4.3.3.

On a toujours $\mathcal{D}(A_1, \dots, A_n, 0) = \mathcal{D}(A_1, \dots, A_n)$.

Définition 4.3.4.

Soit $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, non tous nuls. On note alors $A_1 \wedge \dots \wedge A_n = \text{PGCD}(A_1, \dots, A_n)$ l'unique polynôme unitaire D vérifiant

$\mathcal{D}(A_1, \dots, A_n) = \mathcal{D}(D)$ (un polynôme non unitaire vérifiant ceci est un PGCD).

On convient que $\text{PGCD}(0, \dots, 0) = 0$.

Corollaire 4.3.5.

Soit $A_1, \dots, A_n \in \mathbb{K}[X]$, tels que les $A_1, \dots, A_{n-1}$ soient non tous nuls. On a alors $A_1 \wedge \dots \wedge A_n = (A_1 \wedge \dots \wedge A_{n-1}) \wedge A_n$.

Corollaire 4.3.6.

Soit $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, non tous nuls, soit $D \in \mathbb{K}[X]$ unitaire. Alors $D = A_1 \wedge \dots \wedge A_n$ si et seulement si

1. $\forall i \in \{1, \dots, n\}, D|A_i$;
2. $\forall P \in \mathbb{K}[X], (\forall i \in \{1, \dots, n\}, P|A_i) \Rightarrow P|D$.

Définition 4.3.7.

Des polynômes $A_1, \dots, A_n$ sont dits premiers entre eux *dans leur ensemble* si $A_1 \wedge \dots \wedge A_n = 1$, c'est-à-dire si $\mathcal{D}(A_1, \dots, A_n) = \mathbb{K}^*$.

Théorème 4.3.8 (Théorème de Bézout.).

Soit $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, non tous nuls.

1. Il existe $(U_1, \dots, U_n) \in \mathbb{K}[X]^n$ tel que

$$\sum_{i=1}^n A_i U_i = A_1 \wedge \dots \wedge A_n.$$

2. S'il existe $(U_1, \dots, U_n) \in \mathbb{K}[X]^n$ tel que $\sum_{i=1}^n A_i U_i = 1$, alors les $(A_i)_{i=1}^n$ sont premiers entre eux dans leur ensemble.

Démonstration.

Exactement comme pour les entiers, en remarquant que s'il existe D et $U_1, \dots, U_n$ vérifiant $\sum_{i=1}^n A_i U_i = D$, alors $A_1 \wedge \dots \wedge A_n | D$. □

Remarque 4.3.9.

Si une famille finie de polynômes contient deux

polynômes premiers entre eux, alors les polynômes de cette famille sont premiers entre eux dans leur ensemble.

Exemple 4.3.10.

Comme dans le cas des entiers, des polynômes qui ne sont pas premiers entre eux deux à deux peuvent être premiers entre eux dans leur ensemble. Exhiber une telle famille.

4.4 PPCM.

Pour tout polynôme a, b , l'ensemble des multiples de a est noté $a\mathbb{K}[X]$. L'ensemble des multiples communs à a et b est donc $a\mathbb{K}[X] \cap b\mathbb{K}[X]$.

Remarque 4.4.1. 1. Soit d et δ deux polynômes. $d\mathbb{K}[X] = \delta\mathbb{K}[X]$ si et seulement si d et δ sont associés.

2. En particulier, si on a $d\mathbb{K}[X] = \delta\mathbb{K}[X]$ et que d et δ sont unitaires, alors $d = \delta$ et pour tout polynôme d non nul, il existe δ unitaire vérifiant $\delta\mathbb{K}[X] = d\mathbb{K}[X]$.

Théorème 4.4.2.

Soit $(a, b) \in \mathbb{K}[X]^2$. Alors il existe $m \in \mathbb{K}[X]$ tel que $a\mathbb{K}[X] \cap b\mathbb{K}[X] = m\mathbb{K}[X]$.

Démonstration.

Dans le cas où a ou b est nul, on a évidemment $a\mathbb{K}[X] \cap b\mathbb{K}[X] = 0\mathbb{K}[X]$. On suppose donc par la suite que a et b sont tous deux non nuls.

Posons $d = a \wedge b$. Alors a (resp. b) est de la forme $a'd$ (resp. $b'd$) et a' et b' sont premiers entre eux.

Posons $m = a'b'd$. m est un multiple de a et de b , donc $m\mathbb{K}[X] \subset a\mathbb{K}[X]$ et $m\mathbb{K}[X] \subset b\mathbb{K}[X]$. Donc $m\mathbb{K}[X] \subset a\mathbb{K}[X] \cap b\mathbb{K}[X]$.

Réciproquement, soit $c \in a\mathbb{K}[X] \cap b\mathbb{K}[X]$. Comme c est multiple de a , il existe $u \in \mathbb{K}[X]$ tel que $c = ua = ua'd$. De même, c est multiple de b , il existe $v \in \mathbb{K}[X]$ tel que $c = vb = vb'd$.

On a donc, comme $d \neq 0$, $ua' = vb'$. Ainsi, $b' | ua'$. Or, a' et b' sont premiers entre eux, donc d'après le lemme de Gauss $b' | u$. Ainsi, $b'a'd | ua'd$, or $m = b'a'd$ et $c = ua'd$, donc $c \in m\mathbb{K}[X]$. $\square$

Définition 4.4.3.

Soit a et b deux polynômes. Alors on appelle plus petits communs multiples de a et b (ppcm de a et b) les polynômes d tels que l'ensemble

$a\mathbb{K}[X] \cap b\mathbb{K}[X]$ des multiples communs à a et b soit l'ensemble $d\mathbb{K}[X]$ des multiples de d .

On appelle le ppcm de a et b le seul de ces ppcm qui soit unitaire ou nul. Il est noté $\text{PPCM}(a, b)$ ou $a \vee b$.

Remarque 4.4.4. 1. Cette définition est justifiée par la remarque 4.4.1 et le théorème 4.4.2.

2. $a \vee b = 0$ si et seulement si a ou b est nul.

Remarque 4.4.5.

Sur l'ensemble des polynômes unitaires, le ppcm de deux polynômes a et b est donc la borne supérieure de a et b pour l'ordre $|$.

On peut donner la caractérisation suivante :

Proposition 4.4.6.

Soient $a, b, m \in \mathbb{K}[X]$. m est un ppcm de a et b si et seulement si on a

1. $a | m$;
2. et $b | m$;
3. et pour tout $n \in \mathbb{K}[X]$, $a | n$ et $b | n \Rightarrow m | n$.

On a également :

Proposition 4.4.7.

Soient $a, b, c \in \mathbb{K}[X]$, avec $c \neq 0$.

- (i) $(ac) \vee (bc)$ et $c(a \vee b)$ sont associés.
- (ii) ab et $(a \wedge b).(a \vee b)$ sont associés.

Exemple 4.4.8.

Calculer $X^2 - 4X + 3 \vee X^2 + X - 2$.

5 Formule d'interpolation de Lagrange.

Dans cette partie, on considère un entier n et $(x_0, y_0), \dots, (x_n, y_n)$ des couples d'éléments de $\mathbb{K}$.

On aimerait savoir s'il existe un polynôme P vérifiant

$$\forall i \in [0, n] \quad P(x_i) = y_i, \quad (\text{XVI.4})$$

dit autrement, on cherche s'il existe une fonction polynomiale dont le graphe passe par tous les points (x_i, y_i) pour $i \in \llbracket 0, n \rrbracket$.

Il est bien évident que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i = y_j$, on peut supprimer le couple (x_j, y_j) de la liste des couples considérés sans changer le problème.

Il est évident également que s'il existe i et j distincts tels que $x_i = x_j$ et $y_i \neq y_j$, il n'existe pas de solution.

C'est pourquoi, par la suite, **on suppose que** $x_0, \dots, x_n$ **sont deux à deux distincts.**

Définition 5.0.1.

On appelle *base de Lagrange associée aux points* $x_0, \dots, x_n$ le $(n+1)$ -uplet $(L_0, \dots, L_n)$ vérifiant pour tout $i \in \llbracket 0, n \rrbracket$:

$$L_i = \frac{1}{\alpha_i} \prod_{\substack{j \in \llbracket 0, n \rrbracket \\ j \neq i}} (X - x_j)$$

où

$$\alpha_i = \prod_{\substack{j \in \llbracket 0, n \rrbracket \\ j \neq i}} (x_i - x_j).$$

Proposition 5.0.2.

Pour tout $(i, j) \in \llbracket 0, n \rrbracket^2$, on a $L_i(x_i) = 1$ et $L_i(x_j) = 0$ si $j \neq i$.

Autrement dit, dans tous les cas, on a

$$L_i(x_j) = \delta_{i,j}.$$

Corollaire 5.0.3.

Soit $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$. Alors, en posant

$$P = \sum_{i=0}^n \lambda_i L_i,$$

on a pour tout $i \in \llbracket 0, n \rrbracket$:

$$P(x_i) = \lambda_i.$$

Théorème 5.0.4.

Il existe un unique polynôme P de degré au plus n vérifiant l'équation (XVI.4). Il s'agit du polynôme

$$\sum_{i=0}^n y_i L_i.$$

Démonstration. Unicité sous réserve d'existence

Soit P et Q deux polynômes de degré au plus n vérifiant la propriété demandée. Alors P et Q coïncident en $n+1$ points distincts et sont de degré au plus n donc P et Q sont égaux.

Existence Le polynôme donné dans l'énoncé vérifie évidemment l'équation (XVI.4). Par ailleurs, il s'agit d'une combinaison linéaire de polynômes qui sont tous de degré n . Il est donc de degré au plus n . $\square$

Exercice 5.0.5.

Montrer que pour tout $P \in \mathbb{K}_n[X]$, il existe un unique $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que $P = \sum_{i=0}^n \lambda_i L_i$.

Exercice 5.0.6.

Déterminer l'unique polynôme P de degré au plus 3 vérifiant $P(-1) = -9$, $P(0) = -1$, $P(1) = 5$ et $P(2) = 21$.

Corollaire 5.0.7.

L'ensemble des polynômes vérifiant l'équation (XVI.4) est

$$\{ P \times D + P_0 \mid P \in \mathbb{K}[X] \}$$

où

$$D = \prod_{i=0}^n (X - x_i),$$

$$P_0 = \sum_{i=0}^n y_i L_i.$$

Démonstration.

Remarquons tout d'abord que pour tout $i \in \llbracket 0, n \rrbracket$, on a $D(x_i) = 0$.

Analyse Soit Q un polynôme vérifiant l'équation (XVI.4). En effectuant la division euclidienne de Q par D , on peut écrire Q sous la forme $P \times D + R$ où $P \in \mathbb{K}[X]$ et $R \in \mathbb{K}[X]$ avec $\deg R < n+1$. On a donc $\deg R \leq n$.

De plus, pour tout $i \in \llbracket 0, n \rrbracket$, on a $R(x_i) = Q(x_i) - P(x_i)D(x_i) = y_i - P(x_i) \times 0 = y_i$. Donc R est nécessairement le polynôme P_0 et Q s'écrit sous la forme $P \times D + P_0$.

Synthèse Réciproquement, soit P un polynôme. Posons $Q = P \times D + P_0$. Alors pour tout $i \in \llbracket 0, n \rrbracket$, on a $Q(x_i) = P(x_i) \times 0 + P_0(x_i) = y_i$. Donc Q vérifie l'équation (XVI.4).

Conclusion L'ensemble des polynômes vérifiant l'équation (XVI.4) est

$$\{ P \times D + P_0 \mid P \in \mathbb{K}[X] \}.$$

□

Remarque 5.0.8.

En exprimant l'équation (XVI.4) sous la forme

$$(P(x_0), \dots, P(x_n)) = (y_0, \dots, y_n),$$

cet ensemble de solutions est encore un ensemble de la forme solution particulière plus l'ensemble des solutions de l'équation homogène associée.

6 Annexe : construction de $\mathbb{K}[X]$

La construction de $\mathbb{K}[X]$ n'est pas exigible, cette partie est une version alternative aux parties 1.1 et 1.2.

Définition 6.0.1.

On appelle support d'une suite u à valeurs dans $\mathbb{K}$ l'ensemble des entiers n tels que $u_n \neq 0$. Si cet ensemble est fini, u est dite à support fini.

Remarque 6.0.2. 1. Une suite u est à support fini si et seulement si elle est nulle à partir d'un certain rang.

2. Toute suite à support fini converge donc vers 0 mais la réciproque est évidemment fausse⁵.

On peut alors construire l'anneau des polynômes à coefficients dans $\mathbb{K}$ comme suit.

Définition 6.0.3.

On note $\mathbb{K}[X]$ l'ensemble des suites à support fini à valeurs dans $\mathbb{K}$.

⁵. Par ailleurs, dans ce chapitre, le fait que les suites à support fini convergent n'est d'aucun intérêt.

Définition 6.0.4.

Soit $P = (P_n)_{n \in \mathbb{N}}$ un polynôme. Si P n'est pas la suite nulle, le *degré* de P est le plus grand rang d pour lequel $P_d \neq 0$. Si P est la suite nulle, on considère que c'est $-\infty$.

Dans tous les cas, on peut écrire :

$$\deg P = \sup \{ d \in \mathbb{N}, P_d \neq 0 \}.$$

Définition 6.0.5.

L'addition sur $\mathbb{K}[X]$ est celle de $\mathbb{K}^{\mathbb{N}}$, on la notera $+$. $(\mathbb{K}[X], +)$ est alors un groupe abélien.

Remarque 6.0.6.

$\mathbb{K}[X]$ hérite aussi de la multiplication scalaire de $\mathbb{K}^{\mathbb{N}}$. On dira plus tard que c'en est un *sous-espace vectoriel*.

Remarque 6.0.7.

Par l'injection $\mathbb{K} \rightarrow \mathbb{K}[X], x \mapsto (x, 0, \dots)$, on voit $\mathbb{K}$ comme étant inclus dans $\mathbb{K}[X]$. C'en est aussi un sous-groupe (et un sous-espace vectoriel). On identifiera par exemple le réel 1 au polynôme $(1, 0, \dots)$.

Démonstration.

On montre que c'est un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. La suite nulle est bien entendu à support fini. Il suffit donc de montrer que la différence de deux polynômes est un polynôme. Soit P et Q deux polynômes de degrés p et q respectivement. Si $n \geq \max(p, q)$, alors $P_n - Q_n = 0$ donc $P - Q$ est un polynôme. □

Définition 6.0.8.

Soit $P = (P_n)$ et $Q = (Q_n)$ deux polynômes, on définit le polynôme $P \times Q$ par :

$$PQ = \left(\sum_{k=0}^n P_k Q_{n-k} \right)_{n \in \mathbb{N}}.$$

Proposition 6.0.9.

Si P et Q sont deux polynômes, PQ est un polynôme de degré $\deg P + \deg Q$.

Démonstration.

Si P ou Q sont nuls, il est évident que $PQ = 0$. Sinon, notons p et q les degrés respectifs de P et de Q . Soit $n > p + q$, soit $k \in \llbracket 0, n \rrbracket$. Si $k > p$, alors $P_k = 0$ et si $k \leq p$, $n - k \geq n - p > q$, donc $Q_{n-k} = 0$. Ainsi, si $n > p + q$, $\sum_{k=0}^n P_k Q_{n-k} = 0$ et PQ est donc bien un polynôme, de degré au plus $p + q$. Il suffit ensuite de voir que $(PQ)_{p+q} = P_p Q_q \neq 0$ pour obtenir le degré de PQ . $\square$

Théorème 6.0.10.

$(\mathbb{K}[X], +, \times)$ est un anneau.

Remarque 6.0.11.

La structure multiplicative de $\mathbb{K}[X]$ est différente de celle de $\mathbb{K}^{\mathbb{N}}$, $\mathbb{K}[X]$ n'est pas un sous-anneau (notion HP) de $\mathbb{K}^{\mathbb{N}}$.

Démonstration.

Le caractère de groupe abélien a déjà été vu, le reste des propriétés se montre de manière élémentaire, mais fastidieuse. L'écriture canonique introduite plus bas permet un peu d'alléger les notations. $\square$

Définition 6.0.12.

On note X la suite toujours nulle, sauf pour le terme de rang 1 qui vaut 1 : $X = (0, 1, 0, 0, \dots)$.

Proposition 6.0.13.

Par convention, $X^0 = 1$. De plus, si $n \geq 1$,

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ fois}}, \underbrace{1}_{(n+1)^{\text{e}} \text{ position}}, 0, \dots).$$

Plus formellement, si $k \in \mathbb{N}$,

$$(X^n)_k = \begin{cases} 1 & \text{si } k = n ; \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

On le montre aisément par récurrence sur n , en remarquant que pour tout polynôme P le k^{e} coefficient de PX est le $(k-1)^{\text{e}}$ coefficient de P . $\square$

On obtient donc la représentation usuelle des polynômes.

Corollaire 6.0.14.

Soit $P = (P_n)_{n \in \mathbb{N}}$ un polynôme de degré d . On a alors

$$P = \sum_{n=0}^d P_n X^n.$$

De plus, pour tout entier $d' \geq d$,

$$P = \sum_{n=0}^{d'} P_n X^n.$$

On s'autorise donc à écrire

$$P = \sum_{n=0}^{+\infty} P_n X^n$$

et, pour tout polynôme $Q = \sum_{n=0}^d P_n X^n$, on a bien

$$P + Q = \sum_{n=0}^{+\infty} (P_n + Q_n) X^n$$

ainsi que

$$P \times Q = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^n P_k Q_{n-k} \right) X^n.$$

Enfin, on retrouve les mêmes notations que classiquement.

Définition 6.0.15.

Soit P un polynôme de la forme $\sum_{k=0}^{+\infty} a_k X^k$, non nul.

Le coefficient $a_{\deg P}$ est appelé *coefficient dominant* de P et on dit que $a_{\deg P} X^{\deg P}$ est le *monôme dominant* de P .

Si le coefficient dominant de P vaut 1 on dit que P est *unitaire*.

Pour tout entier $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n .

Remarque 6.0.16. 1. $\mathbb{K}_n[X]$ n'est pas l'ensemble des polynômes de degré égal à n .

2. $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}_1[X] \subset \mathbb{K}_2[X] \subset \cdots \subset \mathbb{K}[X]$.
3. $\mathbb{K}_n[X]$ est un sous-groupe de $(\mathbb{K}[X], +)$.
4. Soit P un polynôme de degré d et $n \in \mathbb{N}$ vérifiant $n \geq d$ alors P peut s'écrire sous la forme $\sum_{k=0}^n a_k X^k$.

7 Annexe : fonctions polynomiales à valeurs dans un anneau

Dans cette section, on considère un entier naturel n fixé et on pose $A = \mathbb{K}$ ou $A = \mathcal{M}_n(\mathbb{K})$. Dans tous les cas, A , muni de l'addition et de la multiplication usuelle est un anneau. Notons 0_A et 1_A les neutres respectifs pour l'addition et la multiplication dans A . Il s'agit de 0 et 1 si $A = \mathbb{K}$ et de $0_{\mathcal{M}_n(\mathbb{K})}$ et I_n si $A = \mathcal{M}_n(\mathbb{K})$.

Dans les deux cas, on dispose d'une loi de composition externe, que nous noterons $\cdot : \mathbb{K} \times A \rightarrow A$. C'est la multiplication usuelle dans $\mathbb{K}$ si $A = \mathbb{K}$ et la multiplication d'une matrice par un scalaire si $A = \mathcal{M}_n(\mathbb{K})$.

Dans les deux cas, on a d'une part les propriétés suivantes⁶ :

1. La loi $\cdot$ est distributive à gauche par rapport à l'addition dans A et à droite par rapport à l'addition dans $\mathbb{K}$.
2. Elle vérifie la propriété d'associativité mixte par rapport à la multiplication dans $\mathbb{K}$.
3. l'élément neutre de $\mathbb{K}$ est neutre à gauche pour $\cdot$.

Autrement dit, pour tout $(\lambda, \mu) \in \mathbb{K}^2$ et tout $(x, y) \in A^2$:

1. $\lambda \cdot (x +_A y) = \lambda \cdot x +_A \lambda \cdot y$ et $(\lambda +_{\mathbb{K}} \mu) \cdot x = \lambda \cdot x +_A \mu \cdot x$.
2. $(\lambda \times_{\mathbb{K}} \mu) \cdot x = \lambda \cdot (\mu \cdot x)$.
3. $1 \cdot x = x$.

Dans les deux cas, on a de plus la propriété additionnelle⁷ que pour tout (λ, μ) et tout (x, y) ,

6. On dit que $(A, +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel.

7. Un anneau $(A, +, \times)$ tel que $(A, +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel et qui vérifie cette propriété est appelé une $\mathbb{K}$ -algèbre.

on a :

$$(\lambda \cdot x) \times_A (\mu \cdot y) = (\lambda \times_{\mathbb{K}} \mu) \cdot (x \times_A y)$$

Si on met l'accent sur ces seules propriétés, c'est parce qu'elles sont suffisantes pour montrer tout ce dont nous aurons besoin dans cette partie, sans plus avoir besoin de distinguer le cas $A = \mathbb{K}$ du cas $A = \mathcal{M}_n(\mathbb{K})$. Par exemple, le fait que pour élément x de A on a $0 \cdot x$ peut se montrer en remarquant qu'on a $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$.

Définition 7.0.1.

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme et x un élément de $\mathbb{K}$.

On appelle *évaluation du polynôme P en x* et on note $\tilde{P}(x)$ l'élément de A défini par

$$\tilde{P}(x) = \sum_{k=0}^{+\infty} a_k \cdot x^k$$

Exemple 7.0.2.

On pose $P = X^2 + 2X + 3$

1. Que vaut l'évaluation de P en -2 ?
2. Que vaut l'évaluation de P en $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$?

Proposition 7.0.3.

Soit $x \in A$ fixé. Alors l'application d'évaluation en x , $\text{eval}_x : \mathbb{K}[X] \rightarrow A$ est un

$$P \mapsto \tilde{P}(x)$$

morphisme d'anneau ; autrement dit pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a

1. $\widetilde{P + Q}(x) = \tilde{P}(x) + \tilde{Q}(x)$;
2. $\widetilde{P \times Q}(x) = \tilde{P}(x) \times \tilde{Q}(x)$;
3. $\widetilde{1_{\mathbb{K}[X]}}(x) = 1_A$.

De plus, on a

$$\widetilde{P \circ Q}(x) = P(\tilde{Q}(x))$$

La suite du cours considère uniquement le cas $A = \mathbb{K}$, le cas $A = \mathcal{M}_n(\mathbb{K})$ fera l'objet d'une étude plus approfondie en spé.

Chapitre XVII

Dérivabilité

Sommaire

1	Définitions et premières propriétés. . .	250
1.1	Taux d'accroissement.	250
1.2	Définitions.	250
1.3	Opérations sur la dérivabilité.	252
1.4	Dérivées successives.	254
2	Les grands théorèmes.	256
2.1	Extremums locaux.	256
2.2	Le théorème de Rolle.	257
2.3	Égalité et inégalité des accroissements finis.	258
2.4	Dérivabilité et sens de variation. . . .	259
2.5	Limite de la dérivée.	260
2.6	Théorème des accroissements finis et suites récurrentes.	261
3	Extension au cas des fonctions com- plexes.	262
4	Convexité.	263
4.1	Parties convexes de $\mathbb{R}^2$ (HP).	263
4.2	Fonctions convexes.	264
4.3	Régularité des fonctions convexes. . . .	267

Sauf mention du contraire, I et J sont deux intervalles de $\mathbb{R}$ et $f : I \rightarrow \mathbb{R}$, et $a \in I$.

1 Définitions et premières propriétés.

1.1 Taux d'accroissement.

Rappel 1.1.1.

Soit $x \neq y \in I$.

La *corde* à la courbe de f reliant les points d'abscisses x et y est le segment reliant les points de coordonnées $(x, f(x))$ et $(y, f(y))$.

La *sécante* à la courbe de f reliant les points d'abscisses x et y est la droite passant par les points de coordonnées $(x, f(x))$ et $(y, f(y))$.

Définition 1.1.2.

Soit $x, y \in I$ avec $x \neq y$, on note $\tau_f(x, y)$ le *taux d'accroissement* de f entre x et y , défini comme le réel $\frac{f(y) - f(x)}{y - x}$. Pour x fixé, on notera

$$\begin{aligned} \tau_{f,x} : I \setminus \{x\} &\rightarrow \mathbb{R} \\ t &\mapsto \tau_f(x, t) \end{aligned}.$$

Remarque 1.1.3.

On a toujours $\tau_f(x, y) = \tau_f(y, x)$.

Remarque 1.1.4.

$\tau_f(x, y)$ est la pente de la corde de la courbe f reliant les points d'abscisses x et y .

1.2 Définitions.

Définition 1.2.1.

Soit $a \in I$. On dit que f est *dérivable en a* si $\tau_{f,a}$ admet une limite finie en a . On appelle alors *dérivée de f en a* ou *nombre dérivé de f en a* cette limite, que l'on note $f'(a)$.

Remarque 1.2.2.

$\tau_{f,a}$ admet une limite finie en a si et seulement si $\frac{f(a+h) - f(a)}{h}$ admet une limite finie quand h tend vers 0 et ces deux limites sont alors égales.

Exemple 1.2.3. 1. Si f est constante, $f'(a) = 0$ pour tout $a \in I$.

2. Dérivée de $x \mapsto x^{n+1}$ en a , pour n entier naturel : pour tout $x \in \mathbb{R} \setminus \{a\}$,

$$x^{n+1} - a^{n+1} = (x - a) \sum_{k=0}^n x^k a^{n-k}, \text{ donc}$$

$$\frac{x^{n+1} - a^{n+1}}{x - a} = \sum_{k=0}^n x^k a^{n-k}. \text{ Il suffit alors de passer à la limite.}$$

Définition 1.2.4.

Si f est dérivable en tout point de I , on dit qu'elle est *dérivable sur I* . On appelle alors *fonction dérivée de f* et on note f' , voire Df ou $\frac{df}{dx}$, l'application $x \mapsto f'(x)$.

Proposition 1.2.5.

Soit ℓ un réel. Les propositions suivantes sont toutes équivalentes.

- (i) f est dérivable en a et $f'(a) = \ell$;
- (ii) $\tau_{f,a}$ admet pour limite ℓ en a ;
- (iii) on peut prolonger $\tau_{f,a}$ par continuité en a et son prolongement est

$$\begin{aligned} \hat{\tau}_{f,a} : I &\rightarrow \mathbb{R} \\ x &\mapsto \begin{cases} \tau_{f,a}(x) & \text{si } x \neq a \\ \ell & \text{si } x = a \end{cases} \end{aligned}$$

- (iv) il existe une application $\varphi_{f,a} : I \rightarrow \mathbb{R}$ continue en a , vérifiant $\varphi_{f,a}(a) = \ell$ et

$$\forall x \in I \quad f(x) = f(a) + (x - a)\varphi_{f,a}(x)$$

- (v) il existe une fonction $\varepsilon : I \rightarrow \mathbb{R}$, de limite nulle en a , telle que pour tout $x \in I$,

$$f(x) = f(a) + (x - a) \cdot \ell + (x - a)\varepsilon(x).$$

Remarque 1.2.6.

On traduira plus tard le point (v) comme suit : « f admet, au voisinage de a , le développement limité $f(x) = f(a) + (x - a) \cdot \ell + o(x - a)$ ».

Démonstration.

On a évidemment (i) $\iff$ (ii) d'après la définition de la dérivée. Montrons les autres équivalences par implications successives.

(ii) $\implies$ (iii) C'est immédiat à partir de la définition de prolongement par continuité.

(iii) $\implies$ (iv) Supposons (iii). Posons $\varphi_{f,a} = \hat{\tau}_{f,a}$. Alors, $\varphi_{f,a}$ est continue en a et on a bien $\varphi_{f,a}(a) = \ell$.

Enfin, soit $x \in I$. Si $x = a$, on a clairement $f(x) = f(a) + (x - a)\varphi_{f,a}(x)$. Si $x \neq a$, on a $\varphi_{f,a}(x) = \frac{f(x) - f(a)}{x - a}$, d'où $f(x) - f(a) = (x - a)\varphi_{f,a}(x)$.

On a donc

$$\forall x \in I \quad f(x) = f(a) + (x - a)\varphi_{f,a}(x)$$

(iv) $\implies$ (v) Supposons (iv). $\varphi_{f,a}$ est continue en a donc tend vers $\varphi_{f,a}(a) = \ell$ en a . Il suffit alors de poser $\varepsilon = \varphi_{f,a} - \ell$.

(v) $\implies$ (ii) Supposons (v). Alors, pour $x \in I \setminus \{a\}$, on a successivement :

$$\begin{aligned} f(x) &= f(a) + (x - a) \cdot \ell + (x - a)\varepsilon(x), \\ \frac{f(x) - f(a)}{x - a} &= \ell + \varepsilon(x), \\ \tau_{f,a}(x) &= \ell + \varepsilon(x). \end{aligned}$$

Donc $\tau_{f,a}(x) \xrightarrow{x \rightarrow a} \ell$.

□

Remarque 1.2.7. 1. La caractérisation (iv) est parfois appelée caractérisation de Carathéodory.

2. Lorsque f est dérivable en a , la fonction $\varphi_{f,a}$ de la caractérisation de Carathéodory coïncide nécessairement avec le taux d'accroissement $\tau_{f,a}$ sur $I \setminus \{a\}$ et est continue en a , c'est donc le prolongement par continuité $\hat{\tau}_{f,a}$ du taux d'accroissement en a .

3. La caractérisation (v) est parfois appelée caractérisation de Hilbert.

4. Sous la forme donnée plus haut, la caractérisation de Carathéodory et celles de Hilbert sont utiles lorsqu'on veut *utiliser* une hypothèse disant que f est dérivable en a . Lorsqu'on veut les utiliser pour *montrer* que f est dérivable en a , on les utilisera plutôt sous les formes

$$\begin{aligned} \forall x \in I \quad f(x) - f(a) &= (x - a)\varphi_{f,a}(x) \\ f(x) - f(a) &= (x - a) \cdot \ell + o(x - a) \end{aligned}$$

Théorème 1.2.8.

Si f est dérivable en a , alors f est continue en a .

Démonstration.

C'est une conséquence directe de la caractérisation de Carathéodory (et de celle de Hilbert). □



La réciproque est fausse :

1. L'application valeur absolue n'est pas dérivable en 0, son taux d'accroissement en 0 ayant des limites à gauche et à droite distinctes en 0.
2. L'application racine carrée n'est pas dérivable en 0, son taux d'accroissement tendant vers $+\infty$ en 0.

Cela nous amène à la notion de dérivabilité à gauche et à droite :

Définition 1.2.9.

On dit que f est *dérivable à gauche en a* (resp. à droite en a) si la fonction $f|_{]-\infty, a] \cap I}$ (resp. $f|_{[a, +\infty[\cap I}$) est dérivable en a , c'est-à-dire si le taux d'accroissement $\tau_{f,a}$ de f en a admet une limite finie à gauche (resp. une limite finie à droite).

Dans ce cas, cette limite est appelée *dérivée à gauche* (resp. à droite) de f en a et est notée $f'_g(a)$ (resp. $f'_d(a)$).

Exemple 1.2.10.

L'application valeur absolue est dérivable à gauche en 0 (de dérivée à gauche -1), ainsi qu'à droite (de dérivée à droite 1).

Remarque 1.2.11.

Si f est dérivable à droite (resp. à gauche) alors elle est continue à droite (resp. à gauche).

Définition 1.2.12 (Interprétation géométrique).

Si f est dérivable (resp. dérivable à gauche, resp. dérivable à droite) en a , on appelle *tangente à f en a* (resp. *demi-tangente à f à gauche en a* , resp. *demi-tangente à f à droite en a*) la droite d'équation

$$y = f(a) + f'(a)(x - a)$$

(resp. la demi-droite d'équation $y = f(a) + f'_g(a)(x - a)$ et $x \leq a$, resp. la demi-droite d'équation $y = f(a) + f'_d(a)(x - a)$ et $x \geq a$).

Remarque 1.2.13.

Le membre droit de cette équation n'est autre que la partie linéaire du développement limité donné par la caractérisation de Hilbert.

Théorème 1.2.14.

f est dérivable en a si et seulement si f est dérivable à gauche et à droite en a **et** $f'_g(a) = f'_d(a)$.

Démonstration.

C'est une conséquence directe des résultats sur les limites de fonction : le taux d'accroissement $\tau_{f,a}$ de f en a , qui n'est pas défini en a admet une limite en a si et seulement s'il admet des limites à gauche et à droite en a et que ces limites sont égales. $\square$

Exemple 1.2.15.

1. Valeur absolue en 0.
2. La fonction

$$f : \begin{cases} \mathbb{R} & \longrightarrow \mathbb{R} \\ x & \longmapsto \begin{cases} \ln(1+2x) & \text{si } x \geq 0 \\ 2e^x - 2 & \text{si } x < 0 \end{cases} \end{cases}$$

est-elle dérivable en 0 ?

On calcule les dérivées à gauche et à droite en revenant à la définition : à gauche, on constate $\frac{2(e^x - 1)}{x} \xrightarrow{x \rightarrow 0^-} 2$, à droite, $\frac{\ln(1+2x)}{x} \xrightarrow{x \rightarrow 0^+} 2$, donc f est dérivable en 0 et $f'(0) = 2$.

3. Les fonctions

$$f_n : \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} x^n \sin \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

pour $n \in \mathbb{N}$, sont-elles dérivables en 0 ?

1.3 Opérations sur la dérivabilité.

Théorème 1.3.1.

si $f, g : I \rightarrow \mathbb{R}$ sont dérivables en a , alors :

1. $f + g$ aussi, et $(f + g)'(a) = f'(a) + g'(a)$;
2. $f \times g$ aussi, et $(f \times g)'(a) = f'(a) \times g(a) + f(a) \times g'(a)$;
3. Pour $\lambda \in \mathbb{R}$, λf est dérivable en a et $(\lambda f)'(a) = \lambda f'(a)$;
4. si g ne s'annule pas au voisinage de a , alors $1/g$ est dérivable au voisinage de a et $\left(\frac{1}{g}\right)'(a) = -\frac{g'(a)}{g(a)^2}$
5. si g ne s'annule pas au voisinage de a , alors f/g est aussi dérivable en a et

$$(f/g)'(a) = \frac{f'(a)g(a) - g'(a)f(a)}{(g(a))^2}$$

Démonstration.

On donne une première démonstration en utilisant directement la définition de la dérivée. Supposons f et g dérivable en a .

1. Soit $x \in I \setminus \{a\}$, Alors $\frac{(f+g)(x) - (f+g)(a)}{x-a} = \frac{f(x) - f(a)}{x-a} + \frac{g(x) - g(a)}{x-a}$, d'où le résultat par passage à la limite en a .
2. Soit $x \in I \setminus \{a\}$, Alors

$$\begin{aligned} & \frac{(f \times g)(x) - (f \times g)(a)}{x-a} \\ &= f(x) \left(\frac{g(x) - g(a)}{x-a} \right) + g(a) \left(\frac{f(x) - f(a)}{x-a} \right) \end{aligned}$$

d'où le résultat par passage à la limite en a .

3. Ce cas est une conséquence directe du précédent (en considérant le réel λ comme la fonction constante de valeur λ).
4. Supposons que g ne s'annule pas au voisinage de a , alors pour x au voisinage épointé de a , on a

$$\frac{1/g(x) - 1/g(a)}{x-a} = -\frac{1}{g(x)g(a)} \times \frac{g(x) - g(a)}{x-a}$$

Lorsque x tend vers a , le membre droit de cette égalité tend vers $-g'(a)/g(a)^2$, d'où le résultat.

5. Ce résultat se déduit cas du produit appliqué à f et $1/g$: En effet, supposons que g ne s'annule pas au voisinage de a . Alors $1/g$ est dérivable en a d'après le point précédent, donc $f \times 1/g$ est dérivable en a . De plus

$$(f \times 1/g)'(a) = f'(a) \times 1/g(a) + f(a) \times \left(-\frac{g'(a)}{g(a)^2} \right)$$

$$= \frac{f'(a)g(a) - g'(a)f(a)}{g(a)^2}$$

□

La démonstration ci-dessus a l'avantage de n'utiliser que la définition de la dérivée. Elle a deux inconvénients : d'une part, le cas du produit n'est pas évident à retrouver ; d'autre part cette méthode ne marchera pas dans le cas de la composition.

Voici une autre méthode qui n'a pas l'inconvénient précédent :

Démonstration.

Supposons f et g dérivables en a et notons $\varphi_{f,a}$ et $\varphi_{g,a}$ leurs taux d'accroissement en a respectifs, prolongés en a par continuité. Soit alors $x \in I$, on a

$$\begin{aligned} f(x) &= f(a) + (x-a)\varphi_{f,a}(x) \\ g(x) &= g(a) + (x-a)\varphi_{g,a}(x) \end{aligned}$$

1. On a donc

$$(f+g)(x) - (f+g)(a) = (x-a)(\varphi_{f,a} + \varphi_{g,a})(x)$$

Or $\varphi_{f,a} + \varphi_{g,a}$ a pour limite $f'(a) + g'(a)$ en a , donc c'est une application continue, donc d'après la caractérisation de Carathéodory, $f+g$ est dérivable en a , de dérivée $f'(a) + g'(a)$.

2. On a

$$\begin{aligned} & (f \times g)(x) - (f \times g)(a) \\ &= (f(a) + (x-a)\varphi_{f,a}(x)) \times (g(a) + (x-a)\varphi_{g,a}(x)) \\ & \quad - f(a)g(a) \\ &= (x-a)\varphi_{f,a}(x)g(a) + f(a)(x-a)\varphi_{g,a}(x) \\ & \quad + (x-a)^2\varphi_{f,a}(x)\varphi_{g,a}(x) \\ &= (x-a) \left(\varphi_{f,a}(x)g(a) + f(a)\varphi_{g,a}(x) \right. \\ & \quad \left. + (x-a)\varphi_{f,a}(x)\varphi_{g,a}(x) \right) \end{aligned}$$

Or, lorsque x tend vers a , $\varphi_{f,a}(x)g(a) + f(a)\varphi_{g,a}(x) + (x-a)\varphi_{f,a}(x)\varphi_{g,a}(x)$ tend vers $f'(a)g(a) + f(a)g'(a)$. Donc $f \times g$ est dérivable en a , de dérivée $f'(a)g(a) + f(a)g'(a)$.

3. On a

$$(\lambda f)(x) - (\lambda f)(a) = (x-a)(\lambda\varphi_{f,a})(x)$$

4.

$$\begin{aligned} \text{On a } \frac{1}{g(x)} - \frac{1}{g(a)} &= \frac{g(a) - g(x)}{g(a)g(x)} = -\frac{(x-a)\psi_{g,a}(x)}{g(a)g(x)} \\ \text{et } -\frac{\psi_{f,a}(x)}{g(a)g(x)} &\xrightarrow{x \rightarrow a} -\frac{g'(a)}{g(a)^2} \end{aligned}$$

□

Remarque 1.3.2.

On peut également effectuer cette démonstration en utilisant la caractérisation de Hilbert plutôt que celle de Carathéodory.

Théorème 1.3.3.

Soit $g : J \rightarrow \mathbb{R}$, $f : I \rightarrow \mathbb{R}$ vérifiant $f(I) \subset J$ et $a \in I$.

1. Si f est dérivable en a et g dérivable en $f(a)$, alors $g \circ f$ est dérivable en a et

$$(g \circ f)'(a) = f'(a) \times g'(f(a))$$

2. Si g est dérivable sur J et f sur I , alors $g \circ f$ est dérivable sur I et

$$(g \circ f)' = f' \times (g' \circ f)$$

Le second point est évidemment une conséquence immédiate du premier.

Démonstration (Erronée).

f est dérivable en a donc continue en a , donc $f(x) \xrightarrow{x \rightarrow a} f(a)$.

Par composition, on a donc

$$\frac{g(f(x)) - g(f(a))}{f(x) - f(a)} \xrightarrow{x \rightarrow a} g'(f(a))$$

De plus

$$\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a} f'(a)$$

Par produit, on obtient bien le résultat voulu. □

Remarque 1.3.4.

La démonstration précédente est erronée, car elle utilise une hypothèse implicite sur f qui n'est pas nécessairement vérifiée. Laquelle ?

Démonstration.

Supposons f (resp. g) étant dérivable en a (resp. en $f(a)$) ; on note alors φ (resp. ψ) son taux d'accroissement en a (resp. en $f(a)$) prolongé par continuité en a (resp. en $f(a)$). On a alors, pour tout $x \in I$

$$\begin{aligned} (g \circ f)(x) - (g \circ f)(a) &= (f(x) - f(a))\psi(f(x)) \\ &= (x-a)\varphi(x)\psi(f(x)) \end{aligned}$$

f étant dérivable en a , elle est nécessairement continue en a ; on en déduit

$$\varphi(x)\psi(f(x)) \xrightarrow{x \rightarrow a} f'(a) \times g'(f(a))$$

D'où le résultat. □

Théorème 1.3.5.

Soit $f : I \rightarrow J$ bijective continue (de réciproque $f^{-1} : J \rightarrow I$). Soit $a \in I$, on note $f(a) = b$. Si f est dérivable en a (resp. sur I) et si f' ne s'annule pas en a (resp. sur I), alors f^{-1} est dérivable en b (resp. sur J) et $(f^{-1})'(b) = \frac{1}{f'(a)}$ (resp. $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$).

Remarque 1.3.6. 1. Moyen mnémotechnique :

$f \circ f^{-1} = \text{Id}$, donc est dérivable de dérivée 1. Or on sait d'après le th. de composition, $(f \circ f^{-1})' = (f^{-1})' \times f' \circ f^{-1}$.

2. Ce résultat est faux sans l'hypothèse de continuité. Considérer par exemple

$$f : [0, 2[\rightarrow [-1, 1[\\ x \mapsto x - 2 \lfloor x \rfloor$$

f est bijective et dérivable en 0 de dérivée 1 mais sa réciproque n'est même pas continue en $f(0)$. En effet il s'agit de

$$f^{-1} : [-1, 1[\rightarrow [0, 2[\\ x \mapsto x - 2 \lfloor x \rfloor$$

On peut même construire des contre-exemples où a n'est pas une extrémité de l'intervalle.

3. Le graphe de f^{-1} étant le symétrique de celui de f par rapport à la droite d'équation $y = x$, la tangente à f^{-1} en un point $f(a)$, si elle existe, est la symétrique de la tangente à f en a par rapport à la droite d'équation $y = x$. Par conséquent, si $f'(a) = 0$, f^{-1} a une tangente verticale en $f(a)$, et sa dérivée en ce point n'existe pas.

Démonstration.

Supposons f dérivable en a de dérivée $f'(a)$ non nulle. Notons alors φ le prolongement par continuité en a de son taux d'accroissement en a .

On a, pour tout $x \in I$, $f(x) - f(a) = (x - a)\varphi(x)$.

Soit alors $y \in J$. Alors on a $f(f^{-1}(y)) - f(a) = (f^{-1}(y) - a)\varphi(f^{-1}(y))$, donc

$$y - b = (f^{-1}(y) - f^{-1}(b))\varphi(f^{-1}(y))$$

Si $y \neq b$, on a $y - b \neq 0$, donc $\varphi(f^{-1}(y)) \neq 0$, et si $y = b$, on sait déjà que $\varphi(f^{-1}(y)) \neq 0$. Donc dans les deux cas,

on a :

$$(f^{-1}(y) - f^{-1}(b)) = (y - b) \frac{1}{\varphi(f^{-1}(y))}$$

On sait $\frac{1}{\varphi(f^{-1}(b))} = \frac{1}{f'(a)}$, donc pour conclure, il suffit de montrer que $y \mapsto \frac{1}{\varphi(f^{-1}(y))}$ est continue en b .

Or f est une bijection continue de I sur J donc f^{-1} est également continue sur J donc en particulier en b et vaut a en b . Par ailleurs on sait déjà que φ est continue en a . On en déduit donc le résultat. $\square$

Exemple 1.3.7.

On admet que $\exp$ et $\sin$ sont dérivables. Grâce aux résultats précédents, on peut montrer les résultats connus de dérivabilité de toutes les fonctions usuelles ($\ln$, $\cos$, $\tan$, Arctan , Arcsin , Arccos , ch , sh , th , Argth , Argch , Argsh).

Exercice 1.3.8.

Se faire un formulaire reprenant tout ça sur un intervalle, ainsi notamment que les cas de $(f + g)'$, $(fg)'$, $(f^n)'$, $(f \circ g)'$, $(1/f)'$, $(f^{-1})'$, $(\ln \circ f)'$, $(\exp \circ f)'$.

1.4 Dérivées successives.

Définition 1.4.1.

On définit les dérivées successives par récurrence. si $f : I \rightarrow \mathbb{R}$, on commence par définir $f^{(0)} = f$. Pour tout $n \in \mathbb{N}$, si $f^{(n)}$ est définie et dérivable, on pose

$$f^{(n+1)} = [f^{(n)}]'$$

Si $f^{(n)}$ existe, on dit que f est n -fois dérivable.

Définition 1.4.2 (Classes de régularité).

On note pour tout $n \in \mathbb{N}$

$$\mathcal{D}^n(I, \mathbb{R}) = \left\{ f : I \rightarrow \mathbb{R} \mid f^{(n)} \text{ existe} \right\};$$

$$\mathcal{C}^n(I, \mathbb{R}) = \left\{ f \in \mathcal{D}^n \mid f^{(n)} \text{ est continue} \right\};$$

$$\mathcal{C}^\infty(I, \mathbb{R}) = \bigcap_{n=0}^{+\infty} \mathcal{C}^n(I, \mathbb{R}).$$

Si $f \in \mathcal{C}^n(I, \mathbb{R})$, on dit que f est n -fois continuellement dérivable (ou de classe $\mathcal{C}^n$) sur I .

Si $f \in \mathcal{C}^\infty(I, \mathbb{R})$, on dit que f est infiniment dérivable (ou de classe $\mathcal{C}^\infty$) sur I .

Proposition 1.4.3.

Soit I un intervalle non vide, non réduit à un point. Pour tout $n \in \mathbb{N}$,

$$\mathcal{C}^{n+1}(I, \mathbb{R}) \subsetneq \mathcal{D}^{n+1}(I, \mathbb{R}) \subsetneq \mathcal{C}^n(I, \mathbb{R}).$$

Démonstration.

Les inclusions sont immédiates. On obtient le caractère strict en primitivant n fois l'exemple suivant, ainsi que la fonction valeur absolue, après avoir opéré une translation pour se ramener de 0 en un point à l'intérieur de I . $\square$

Exemple 1.4.4 (Exemple fondamental).

Soit $f : x \mapsto x^2 \sin\left(\frac{1}{x}\right)$, prolongée par continuité en 0 en posant $f(0) = 0$. Alors f est dérivable en 0 (ainsi que sur $\mathbb{R}$), mais sa dérivée n'est pas continue en 0.

Exercice 1.4.5.

Soit $n \in \mathbb{Z}$, soit

$$\begin{aligned} f_n : \mathbb{R}_+^* &\rightarrow \mathbb{R}_+^* \\ x &\mapsto x^n \end{aligned}$$

Déterminer $f_n^{(k)}$ pour tout $k \in \mathbb{N}$.

Théorème 1.4.6.

Soit $n \in \mathbb{N}$. Soient $f, g \in \mathcal{C}^n(I, \mathbb{R})$ et $\lambda \in \mathbb{R}$.

1. $(f + g) \in \mathcal{C}^n(I, \mathbb{R})$ et $(f + g)^{(n)} = f^{(n)} + g^{(n)}$.
2. $\lambda f \in \mathcal{C}^n(I, \mathbb{R})$ et $(\lambda f)^{(n)} = \lambda f^{(n)}$.
3. $(fg) \in \mathcal{C}^n(I, \mathbb{R})$ et (formule de Leibniz) :

$$(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(k)} g^{(n-k)}.$$

4. Si g ne s'annule pas, $(f/g) \in \mathcal{C}^n(I, \mathbb{R})$.

Démonstration. 1. Facile par récurrence, en notant pour f et g fixées et pour tout $n \in \mathbb{N}$, (H_n) l'assertion «si f et g appartiennent à $\mathcal{C}^n(I, \mathbb{R})$ alors $(f + g) \in \mathcal{C}^n(I, \mathbb{R})$ et $(f + g)^{(n)} = f^{(n)} + g^{(n)}$ ».

3. On fait encore une démonstration par récurrence, en notant (H_n) l'assertion «si f et g appartiennent à $\mathcal{C}^n(I, \mathbb{R})$ alors $(fg) \in \mathcal{C}^n(I, \mathbb{R})$ et $(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(k)} g^{(n-k)}$ » :
- (H_0) est évidemment vraie.

- L'hérédité se démontre à l'aide de la formule 2 du théorème 1.3.1, et se conduit de la même manière que la démonstration de la formule du binôme de Newton.

4. Encore une récurrence, mais plus subtile car cette fois on ne fixe pas f et g . Pour $n \in \mathbb{N}$, on note (H_n) l'assertion «pour toutes $f, g \in \mathcal{C}^n(I, \mathbb{R})$ telles que g ne s'annule pas, on a $f/g \in \mathcal{C}^n$ ».

- De nouveau (H_0) se démontre aisément.
- Soit $n \in \mathbb{N}$. Supposons (H_n) et montrons (H_{n+1}) . Soit $f, g \in \mathcal{C}^{n+1}(I, \mathbb{R})$, g ne s'annulant pas. Alors on sait que f/g est dérivable et $(f/g)' = \frac{f'g - fg'}{g^2}$. Mais $f'g - fg'$ est de classe $\mathcal{C}^n$, ainsi que g^2 , et g^2 ne s'annule pas. On peut donc appliquer l'hypothèse de récurrence (H_n) à $f'g - fg'$ et g^2 et en déduire que $(f/g)'$ est de classe $\mathcal{C}^n$, donc que f/g est de classe $\mathcal{C}^{n+1}$. $\square$

Théorème 1.4.7.

Soit $n \in \mathbb{N}^*$. Soient $f \in \mathcal{C}^n(I, \mathbb{R})$ et $g \in \mathcal{C}^n(J, I)$. Alors $(f \circ g) \in \mathcal{C}^n(J, \mathbb{R})$.

Démonstration.

(non exigible). La démonstration se fait là encore par récurrence, avec la même subtilité que dans la démonstration précédente. Pour $n \in \mathbb{N}$, on note (H_n) l'assertion «pour toutes $f \in \mathcal{C}^n(I, \mathbb{R})$ et $g \in \mathcal{C}^n(J, I)$, on a $(f \circ g) \in \mathcal{C}^n(J, \mathbb{R})$ ».

- De nouveau (H_0) est triviale.
- Soit $n \in \mathbb{N}$. Supposons (H_n) et montrons (H_{n+1}) . Soit $f \in \mathcal{C}^{n+1}(I, \mathbb{R})$ et $g \in \mathcal{C}^{n+1}(J, I)$. Alors on sait que $f \circ g$ est dérivable et que $(f \circ g)' = g' \cdot f' \circ g$. Or f' est de classe $\mathcal{C}^n$, ainsi que g . En appliquant l'hypothèse de récurrence (H_n) à f' et g , on obtient que $f' \circ g$ est de classe $\mathcal{C}^n$. Or g' est aussi de classe $\mathcal{C}^n$, donc le produit $g' \cdot f' \circ g$ est de classe $\mathcal{C}^n$. Ainsi $(f \circ g)'$ est de classe $\mathcal{C}^n$, donc $f \circ g$ est de classe $\mathcal{C}^{n+1}$. $\square$

Théorème 1.4.8.

Soit $n \in \mathbb{N}^*$. Soit $f \in \mathcal{C}^n(I, J)$. Si f est bijective et f' ne s'annule pas alors $f^{-1} \in \mathcal{C}^n(J, I)$.

Démonstration.

(non exigible). La démonstration se fait par récurrence de la même manière que les deux démonstrations précédentes. $\square$

2 Les grands théorèmes.

2.1 Extremums locaux.

Définition 2.1.1.

On dit que f a un *minimum* (resp. *maximum*) *local* en a s'il existe un voisinage V de a tel que pour tout $x \in V \cap I$, $f(x) \geq f(a)$ (resp. $f(x) \leq f(a)$). On dit que f a un *extremum local* en a si f a un minimum ou un maximum local en a .

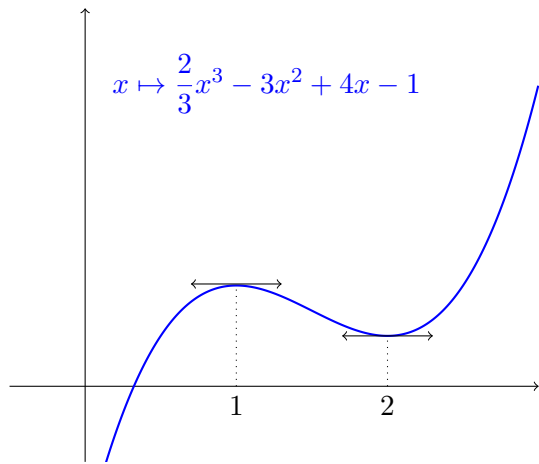


FIGURE XVII.1 – Exemple de fonction possédant des extremums locaux, mais non globaux.

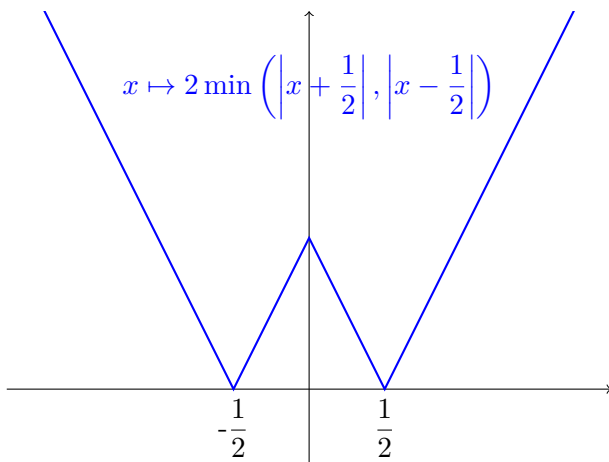


FIGURE XVII.2 – Exemple de fonction possédant des minimums globaux non uniques.

Remarque 2.1.2. 1. La condition $\forall x \in V \cap I \quad f(a) \geq f(x)$ est équivalente à chacune des assertions suivantes :

- (i) $f|_{V \cap I}$ admet un maximum global en a ;
- (ii) f est majorée par $f(a)$ sur $V \cap I$;
- (iii) $f(V \cap I)$ est majoré par $f(a)$;
- (iv) $f(a) = \sup_{x \in V \cap I} f(x)$;
- (v) $f(a) = \max_{x \in V \cap I} f(x)$.

2. Une fonction peut avoir un minimum en un point a sans qu'elle ne soit croissante sur un voisinage à droite ni décroissante sur un voisinage à gauche. Considérons par exemple l'application

$$f: \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} 0 & \text{si } x = 0 \\ x^2[\sin(1/x) + 1] & \text{sinon} \end{cases}$$

Théorème 2.1.3.

Soit $a \in \overset{\circ}{I}$. Si f possède un extremum local en a et si f est dérivable en a , alors $f'(a) = 0$.

Remarque 2.1.4. 1. Il est essentiel que a appartienne à l'intérieur de I . Si a est une extrémité de I , on peut considérer le contre-exemple $\text{Id}_{[0,1]}$, qui possède un minimum global en 0 et un maximum global en 1 et est dérivable sur $[0,1]$ mais dont la dérivée ne s'annule ni en 0 ni en 1.

2. La réciproque est fautive. Ainsi $x \mapsto x^3$ a une dérivée nulle en 0 sans avoir d'extremum.

Démonstration.

Sans perte de généralité, on suppose que f admet un maximum local en a . Il existe donc un voisinage V_1 de a tel que f soit majorée par $f(a)$ sur $V_1 \cap I$.

a étant intérieur à I , il existe un voisinage V_2 de a inclus dans I .

On a alors $V_1 \cap V_2 \subset V_1 \cap I$, f est donc majorée par $f(a)$ sur $V_1 \cap V_2$.

De plus, $V_1 \cap V_2$ est un voisinage donc contient un segment $[a - \varepsilon, a + \varepsilon]$ où $\varepsilon > 0$.

On a alors, pour tout $x \in [a - \varepsilon, a + \varepsilon]$, $f(x) - f(a) \leq 0$.

Donc d'une part

$$\forall x \in [a - \varepsilon, a[\quad \frac{f(x) - f(a)}{x - a} \geq 0$$

donc par passage à la limite $f'(a) \geq 0$.

Et d'autre part,

$$\forall x \in]a, a + \varepsilon] \quad \frac{f(x) - f(a)}{x - a} \leq 0$$

donc par passage à la limite $f'(a) \leq 0$.

Donc $f'(a) = 0$. $\square$

Définition 2.1.5.

Supposons f dérivable, un point $a \in I$ est un *point critique* de f si $f'(a) = 0$.

Remarque 2.1.6.

Le théorème 2.1.3 s'énonce donc ainsi : tous les extremums locaux d'une fonction dérivable à l'intérieur de son ensemble de définition sont des points critiques de cette fonction. Ou bien : une condition nécessaire pour qu'un point a , à l'intérieur de l'ensemble de définition d'une fonction f dérivable, soit un extremum local de f est que a soit un point critique de f .

Remarque 2.1.7.

Cette condition nécessaire n'est pas suffisante, comme le montre le contre-exemple $x \mapsto x^3$ en 0.

L'étude des extremums (locaux ou globaux) d'une fonction dérivable commencera donc la plupart du temps par une étude systématique de ses points critiques.

2.2 Le théorème de Rolle.

Théorème 2.2.1 (Théorème de Rolle).

Soient $a, b \in I$ avec $a < b$ et $f \in \mathcal{C}^0([a, b], \mathbb{R}) \cap \mathcal{D}(]a, b[, \mathbb{R})$ vérifiant $f(a) = f(b)$, alors il existe $c \in]a, b[$ tel que $f'(c) = 0$.

Remarque 2.2.2.

Toutes les hypothèses sont importantes. On pourra considérer les applications suivantes qui sont toutes des contre-exemples correspondant à l'oubli d'une hypothèse :

$$\begin{aligned} f_1 : [0, 1] &\rightarrow \mathbb{R} \\ x &\mapsto x \end{aligned}$$

$$\begin{aligned} f_2 : [0, 1] &\rightarrow \mathbb{R} \\ x &\mapsto x - \lfloor x \rfloor \end{aligned}$$

$$\begin{aligned} f_3 : [-1, 1] &\rightarrow \mathbb{R} \\ x &\mapsto |x| \end{aligned}$$

Démonstration.

f est continue sur $[a, b]$, donc elle est bornée et atteint ses bornes. On note m son minimum et M son maximum.

- Si $f(a) = f(b) \neq m$, alors $m < f(a)$ et $m < f(b)$, et donc m est atteint sur $]a, b[$, donc f' s'annule en ce point.
- Même raisonnement si $f(a) = f(b) \neq M$.
- Sinon, cela signifie que $f(a) = f(b) = m = M$, et donc f est nécessairement constante sur $]a, b[$. f' y est donc identiquement nulle. $\square$

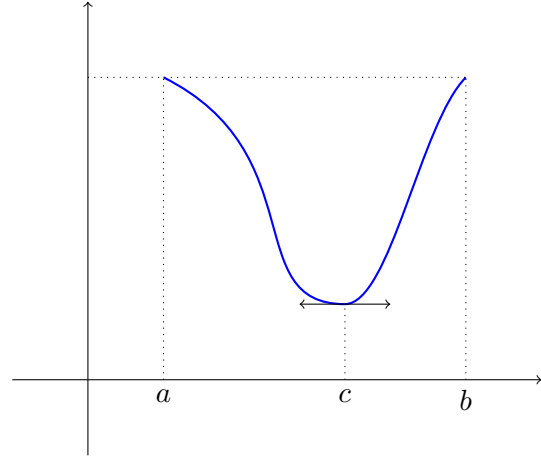


FIGURE XVII.3 – Illustration du théorème de Rolle (existence d'une tangente horizontale, d'un point critique).

2.3 Égalité et inégalité des accroissements finis.

Théorème 2.3.1 (Égalité des accroissements finis, ou TAF).

Soient $(a, b) \in I^2$ avec $a < b$ et $f \in \mathcal{C}^0([a, b], \mathbb{R}) \cap \mathcal{D}(]a, b[, \mathbb{R})$. Alors il existe $c \in]a, b[$ tel que

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Remarque 2.3.2. 1. Ce théorème est une généralisation du théorème de Rolle : les hypothèses sont les mêmes, à l'exception de l'hypothèse $f(a) = f(b)$, qui n'est ici pas nécessaire, et la conclusion est la même que celle du théorème de Rolle dans le cas où $f(a) = f(b)$.

2. Cependant, on va utiliser le théorème de Rolle pour démontrer le théorème des accroissements finis. Dans ces conditions affirmer que le théorème de Rolle n'est qu'un corollaire du TAF laisserait croire que l'on n'a pas bien saisi l'enchaînement des démonstrations.

3. Un autre énoncé de ce théorème est le suivant : Soient $(a, b) \in I^2$ avec $a \neq b$ et f continue sur l'intervalle $[a, b]$ (ou $[b, a]$ si $b < a$) et dérivable sur l'intérieur de ce même intervalle. Alors il existe $\theta \in]0, 1[$ tel que

$$f'(a + \theta(b - a)) = \frac{f(b) - f(a)}{b - a}.$$

Démonstration.

Posons $p = \frac{f(b) - f(a)}{b - a}$ et

$$\begin{aligned} \varphi : [a, b] &\rightarrow \mathbb{R} \\ x &\mapsto f(x) - px \end{aligned}$$

Alors $\varphi(b) - \varphi(a) = f(b) - f(a) - p(b - a) = 0$, donc $\varphi(a) = \varphi(b)$.

De plus, φ est continue sur $[a, b]$ et dérivable sur $]a, b[$. Donc d'après le théorème de Rolle, il existe $c \in]a, b[$ vérifiant $\varphi'(c) = 0$. Or $\varphi'(c) = f'(c) - p$, donc $f'(c) = p = \frac{f(b) - f(a)}{b - a}$. $\square$

Pour montrer le TAF, on se ramène à Rolle par une transformation géométrique $(x, y) \mapsto (x, y - px)$. Où p est la pente de la droite D passant par les points $(a, f(a))$ et $(b, f(b))$. En effet, on

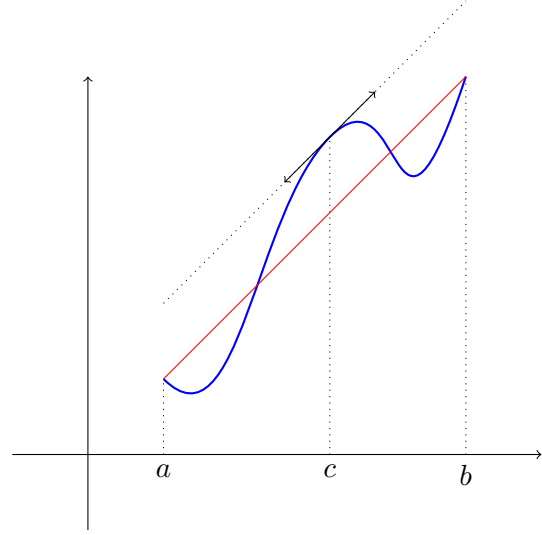


FIGURE XVII.4 – Illustration du théorème des accroissements finis (existence d'une tangente de même pente que la corde).

peut remarquer que D est parallèle au graphe de $p\text{Id}$, donc $f(a) - pa = f(b) - pb$. On peut alors appliquer le théorème de Rolle à l'application $f - p\text{Id}$.

Théorème 2.3.3 (Inégalité des accroissements finis, ou IAF).

Soient $(a, b) \in I^2$ avec $a < b$ et $f \in \mathcal{C}^0([a, b], \mathbb{R}) \cap \mathcal{D}(]a, b[, \mathbb{R})$.

1. Si f' est minorée par un réel m sur $]a, b[$, alors $m(b - a) \leq f(b) - f(a)$.
2. Si f' est majorée par un réel M sur $]a, b[$, alors $f(b) - f(a) \leq M(b - a)$.
3. Si $|f'|$ est majorée par $K > 0$, alors $|f(b) - f(a)| \leq K|b - a|$.

Démonstration.

Par application du TAF à f , on sait qu'il existe $c \in]a, b[$ vérifiant $f'(c) = \frac{f(b) - f(a)}{b - a}$

1. Sous les hypothèses données, on a $m \leq f'(c) = \frac{f(b) - f(a)}{b - a}$, d'où le résultat.
2. De même, on a $\frac{f(b) - f(a)}{b - a} = f'(c) \leq M$, d'où le résultat.

3. De même, $\frac{|f(b) - f(a)|}{|b - a|} = |f'(c)| \leq K$, d'où le résultat.

Notez que l'hypothèse $a < b$ n'est ici pas nécessaire : dans le cas où $a = b$ le résultat est évident ; dans le cas où $a > b$, il suffit d'échanger les rôles de a et b .

□

Définition 2.3.4.

Soit $K \in \mathbb{R}_+^*$. On dit que f est K -lipschitzienne si $\forall (x, y) \in I^2$, $|f(x) - f(y)| \leq K|x - y|$.

Remarque 2.3.5.

Si $x \neq y$, on a donc $\left| \frac{f(x) - f(y)}{x - y} \right| \leq K$, donc les pentes des cordes du graphe de f sont bornées par K .

Proposition 2.3.6.

Toute fonction lipschitzienne est continue.

Démonstration.

Direct en revenant aux définitions.

□

Exemple 2.3.7.

La fonction

$$\begin{aligned} f : [1, +\infty[&\rightarrow \mathbb{R} \\ x &\mapsto \frac{1}{x} \end{aligned}$$

est 1-lipschitzienne. En effet, si $x, y \geq 1$,

$$\left| \frac{1}{x} - \frac{1}{y} \right| = \left| \frac{x - y}{xy} \right| \leq 1 \times |x - y|.$$

On retrouve cela par l'inégalité des accroissements finis.

- Corollaire 2.3.8.** 1. Soit $f \in \mathcal{D}(I, \mathbb{R})$. Si $|f'|$ est bornée par K sur I , alors f est K -lipschitzienne sur I
2. Si $f \in \mathcal{C}^1([a, b], \mathbb{R})$, alors f est lipschitzienne sur $[a, b]$.

Démonstration. 1. Immédiat avec le second point de l'IAF.

2. f' est continue sur un segment, donc bornée sur ce segment, et on peut donc appliquer le premier point.

□

Exemple 2.3.9.

Utiliser l'IAF permet de montrer aisément que pour tout $x \in \mathbb{R}$, $|\sin x| \leq |x|$.

Exercice 2.3.10.

En utilisant l'inégalité des accroissements finis, montrer que pour tout $x > 0$:

$$\frac{1}{x+1} \leq \ln \left(1 + \frac{1}{x} \right) \leq \frac{1}{x}.$$

En déduire une minoration et la limite lorsque $n \rightarrow +\infty$ de

$$H_n = \sum_{k=1}^n \frac{1}{k}.$$

2.4 Dérivabilité et sens de variation.

Résultats déjà connus, que l'on précise et démontre. On rappelle l'hypothèse primordiale : I est un intervalle de $\mathbb{R}$.

Théorème 2.4.1.

Soit I un intervalle de $\mathbb{R}$ et $f \in \mathcal{D}(I, \mathbb{R})$.

1. f est croissante sur I si et seulement si $f' \geq 0$ sur I .
2. f est constante sur I si et seulement si $f' = 0$ sur I .
3. f est strictement croissante sur I si et seulement si $f' \geq 0$ et l'ensemble $\{x \in I, f'(x) = 0\}$ ne contient aucun intervalle non trivial (non vide et non réduit à un point).

On obtient les mêmes résultats pour des fonctions décroissantes *mutatis mutandis*.

Démonstration.

On ne traite que les cas où f est croissante.

1. ($\Rightarrow$) On suppose f croissante sur I , alors son taux d'accroissement en tout point fixé $a \in I$ est positif. Par passage à la limite, on obtient $f'(a) \geq 0$. ($\Leftarrow$) On suppose $f' \geq 0$. Soit alors $(x, y) \in I^2$ avec $x < y$. Par application de l'IAF à f entre x et y , nous avons directement $f(y) - f(x) \geq 0$. Donc f est croissante.
2. f est constante si et seulement si f est croissante et décroissante. On conclut par utilisation du point précédent.

3. ($\Rightarrow$) On suppose f strictement croissante. On sait déjà que $f' \geq 0$. On pose $\mathcal{E} = \{x \in I \mid f'(x) = 0\}$. Soit $(a, b) \in I^2$, $a \leq b$, tel que $[a, b] \subset \mathcal{E}$. Il suffit de montrer que $a = b$. On a $f'|_{[a, b]} = 0$ donc $f|_{[a, b]}$ est constante. En particulier $f(a) = f(b)$. Or f est strictement croissante, donc on ne peut pas avoir $a < b$, donc $a = b$.
- ($\Leftarrow$) Supposons que l'ensemble des points où f' s'annule ne contient aucun intervalle non trivial. Alors f est croissante. Par l'absurde, supposons que f n'est pas strictement croissante. Alors il existe $(x, y) \in I^2$ avec $x < y$ et $f(x) = f(y)$. Alors puisque f est croissante, f est constante sur $[x, y]$, et donc $f'|_{[x, y]} = 0$. Mais alors par hypothèse, $x = y$, ce qui est absurde. Donc f est strictement croissante. $\square$

Remarque 2.4.2. 1. On a $f' > 0 \Rightarrow f$ strictement croissante, mais pas la réciproque : une fonction strictement croissante peut avoir une dérivée qui s'annule (mais pas n'importe comment), ex : $x \mapsto x^3$ (il s'agit souvent d'un point d'inflexion).

2. I doit être un intervalle. Le théorème est faux dans le cas où I est une réunion d'intervalles disjoints (considérer par exemple l'application $x \mapsto 1/x$, de $] -\infty, 0[\cup]0, +\infty[$ dans $\mathbb{R}$).

3. Si on suppose seulement $f'(a) > 0$, alors f n'est pas nécessairement strictement croissante au voisinage de a . Exemple :

$$f : \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} 0 & \text{si } x = 0 \\ x^2 \sin 1/x + (x/2) & \text{sinon} \end{cases}$$

En calculant la limite du taux d'accroissement de f en zéro, on obtient $f'(0) = 1/2$, mais pour $x \neq 0$, $f'(x) = 1/2 + 2x \sin 1/x - \cos 1/x$, et cette expression prend des valeurs négatives dans tout voisinage de 0.

4. En général, pour étudier les variations de f sur I avec ce théorème, il suffit que f soit dérivable sur l'intérieur de I et continue sur I tout entier. En effet, si une application f continue sur I est croissante (resp. strictement croissante, resp. décroissante, resp. strictement décroissante) sur $\overset{\circ}{I}$ alors elle l'est aussi sur I .

2.5 Limite de la dérivée.

Théorème 2.5.1 (de la limite de la dérivée).

Soit $a < b$, $f : I \rightarrow \mathbb{R}$ et $\ell \in \overline{\mathbb{R}}$. On suppose

1. f continue sur $[a, b]$
2. et f dérivable sur $]a, b[$
3. et $f'(x) \xrightarrow{x \rightarrow a^+} \ell$.

Alors $\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a^+} \ell$. En particulier

- dans le cas où $\ell = +\infty$ (resp. $\ell = -\infty$), f n'admet pas de dérivée à droite en a et son graphe admet une demi-tangente verticale en $(a, f(a))$ dirigée vers le haut (resp. vers le bas) ;
- dans le cas où ℓ est réel, on a
 1. f est dérivable (à droite) en a
 2. et $f'(a) = \ell = \lim_{x \rightarrow a^+} f'(x)$
 3. et f' est continue (à droite) en a .

On a le même résultat à gauche en un point (inverser haut et bas dans le cas des limite infinies) et des deux côtés (limite globale) en un même point.

Démonstration.

La difficulté est de montrer $\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a^+} \ell$, le reste s'en déduisant immédiatement.

Pour tout $x \in]a, b[$, f est dérivable sur $]a, x[$ et continue sur $[a, x]$ donc il existe $c \in]a, x[$ vérifiant $f'(c) = \frac{f(x) - f(a)}{x - a}$.

On peut ainsi définir une application $g :]a, b[\rightarrow]a, b[$, vérifiant pour tout $x \in]a, b[$, $g(x) \in]a, x[$ et $f'(g(x)) = \frac{f(x) - f(a)}{x - a}$.

Donc $g(x) \xrightarrow{x \rightarrow a^+} a$. Or $f' \xrightarrow{a^+} \ell$ donc $f'(g(x)) \xrightarrow{x \rightarrow a^+} \ell$.

Donc $\frac{f(x) - f(a)}{x - a} \xrightarrow{x \rightarrow a^+} \ell$. $\square$

Remarque 2.5.2.

Ce théorème permet de conclure sur la dérivabilité ou non-dérivabilité de f en a dans le cas où la dérivée au voisinage épointé de a admet une limite (finie ou infinie) en a . En revanche il ne permet pas de dire quoi que ce soit dans le cas où la dérivée n'admet pas de limite.

Exemple 2.5.3.

On considère les fonctions f_n pour $n \in \mathbb{N}$ définies

au point 3 de l'exemple 1.2.15. Pour $n \geq 1$, f_n est continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R}^*$. De plus

$$\forall x \in \mathbb{R}^*, f'_n(x) = nx^{n-1} \sin\left(\frac{1}{x}\right) - x^{n-2} \cos\left(\frac{1}{x}\right)$$

Pour $n \geq 3$, $f'_n(x) \xrightarrow[x \neq 0]{x \rightarrow 0} 0$. Donc, d'après le théorème ci-dessus, pour tout $n \geq 3$, f_n est dérivable en 0, de dérivée égale à 0 et on a même $f_n \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$.

Pour $n \in \{1, 2\}$, f'_n n'a pas de limite en 0. Le théorème précédent ne permet alors de conclure ni à la dérivabilité, ni à la non-dérivabilité de f_n en 0. Et pour cause : f_2 est bien dérivable en 0, de dérivée nulle tandis que f_1 ne l'est pas. En effet, le taux d'accroissement de f_n en 0 est l'application $x \mapsto x^{n-1} \sin\left(\frac{1}{x}\right)$, qui tend vers 0 en 0 si $n = 2$ et n'a pas de limite en 0 si $n = 1$.

Exemple 2.5.4.

Notons f l'application racine carrée de $\mathbb{R}_+$ dans $\mathbb{R}$. f est dérivable sur $\mathbb{R}_+^*$ et pour tout $x \in \mathbb{R}_+^*$, $f'(x) = \frac{1}{2\sqrt{x}}$.

Donc $f'(x) \xrightarrow{x \rightarrow 0^+} +\infty$, donc $\frac{f(x)-f(0)}{x-0} \xrightarrow{x \rightarrow 0^+} +\infty$, donc f n'est pas dérivable en 0.

Remarquez cependant qu'il était ici tout aussi aisé de calculer directement le taux d'accroissement de f en 0 et de vérifier qu'il ne convergeait pas.

Remarque 2.5.5.

On voit sur ces exemples qu'il est erroné de croire que la non-dérivabilité de f en a implique que f' n'a pas de limite en a (cas de la racine carrée).

Il est tout aussi erroné de croire que l'absence de limite pour f' en a implique que f n'est pas dérivable en a (cas de f_2).

Exercice 2.5.6.

Soient $a, b \in \mathbb{R}$, et $f : \mathbb{R} \rightarrow \mathbb{R}$:

$$x \mapsto \begin{cases} e^x & \text{si } x \leq 1 \\ x^2 + ax + b & \text{si } x > 1 \end{cases} \quad \text{Trouver les valeurs de } a \text{ et } b \text{ pour lesquelles } f \text{ est de classe } \mathcal{C}^1.$$

Correction.

Remarquons que f est dérivable sur $\mathbb{R} \setminus \{1\}$ et que sa dérivée est continue sur $\mathbb{R} \setminus \{1\}$.

De plus f est continue à gauche et dérivable à gauche en 1, de dérivée à gauche $f'_g(1) = e$.

Analyse Supposons $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$. Alors f est continue, donc $f(x) \xrightarrow{x \rightarrow 1^+} f(1)$, donc $1 + a + b = e$.

De plus f est dérivable. Sa dérivée à gauche en 1 est e . Pour $x > 1$, on a $f'(x) = 2x + a$, donc $f'(x) \xrightarrow{x \rightarrow 1^+} 2 + a$, donc f' est dérivable à droite en 1, de dérivée $2 + a$.

f étant dérivable en 1, on a $e = f'_g(1) = f'_d(1) = 2 + a$.

Donc $a = e - 2$ et $b = 1$.

Synthèse Supposons $a = e - 2$ et $b = 1$. Par les calculs précédents, f est continue à droite en 1, donc f est continue en 1.

De plus, f est dérivable en tout $x \in]1, +\infty[$, et $f'(x) = 2x + a$, donc $f'(x) \xrightarrow{x \rightarrow 1^+} 2 + a$, donc grâce au théorème de la limite de la dérivée, f est dérivable à droite en 1 et $f'_d(1) = 2 + a = e$.

Ainsi, f est dérivable en 1, de dérivée e . f est donc dérivable sur $\mathbb{R}$.

De plus f' est continue à droite et à gauche en 1, donc f' est continue en 1, donc sur $\mathbb{R}$.

Donc $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$.

Conclusion $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{R})$ si et seulement si $a = e - 2$ et $b = 1$.

2.6 Théorème des accroissements finis et suites récurrentes.

Le TAF fournit un outil supplémentaire pour étudier les suites récurrentes. Si une telle suite converge, elle converge vers un point fixe de f , et se prête à une approximation des points fixes de f .

Le TAF, dans certaines conditions, assure qu'une telle suite converge (1er résultat) sans avoir à étudier la monotonie de f ni celle de (u_n) , et assure que la convergence est rapide (2eme résultat).

Exemple 2.6.1.

$f : I \rightarrow \mathbb{R}$, I stable par f , et $\ell \in I$ un point fixe de f . Soit $u_0 \in I$. On considère la suite $u_{n+1} = f(u_n)$.

Si f est dérivable et si $|f'|$ est majorée par M tel que $0 \leq M < 1$, alors pour tout n , $|u_n - \ell| \leq M^n |u_0 - \ell|$ (le montrer par récurrence). Et donc $|u_n - \ell| \rightarrow 0$. De plus, la convergence est géométrique ce qui est rapide. Par exemple, si $M = \frac{1}{10}$, alors on gagne une décimale de précision à chaque étape.

Exemple 2.6.2.

Trouver une approximation du point fixe de $f : \mathbb{R}_+ \rightarrow \mathbb{R}$, $x \mapsto \frac{1}{1+x}$ à 10^{-2} . $\mathbb{R}_+$ est stable par f , f est dérivable sur $\mathbb{R}_+$, de dérivée $x \mapsto -\frac{1}{(1+x)^2}$ bornée par 1.

Malheureusement cette borne est insuffisante pour appliquer les idées vues ci-dessus : on aimerait avoir une borne K strictement inférieure à 1.

Pour cela, on va chercher un intervalle stable par f sur lequel f' est bornée par un $K < 1$. f' étant strictement croissante et à valeurs négatives, il suffit de trouver un intervalle de la forme $[a, b]$ avec $a < b$ et $a > -1$.

Le point fixe de f est par calcul $\alpha = \frac{-1 + \sqrt{5}}{2}$. On peut constater que $f(1) = 1/2$, et comme $\alpha \leq 1$, en déduire que $1/2 \leq f(\alpha) = \alpha$.

On peut alors constater aisément que $[1/2, 1]$ est stable par f . On peut choisir une valeur arbitraire dans $[1/2, 1]$. En itérant f sur cette valeur on obtient des approximations successives de α convergeant vers α .

Exercice 2.6.3.

On considère une suite u définie par

$$u_0 \in [-1, 1] \text{ et } \forall n \in \mathbb{N}, u_{n+1} = \sqrt{2 - u_n}.$$

Déterminer un segment I sur lequel appliquer l'IAF permet de montrer que si $u_0 \in I$, alors $u_n \xrightarrow[n \rightarrow +\infty]{} 1$.

Remarque 2.6.4.

Supposons maintenant que $f : I \rightarrow I$ est dérivable et que sa dérivée est bornée par $K < 1$.

Par récurrence, on montre facilement que pour tout $n \in \mathbb{N}$, $|u_{n+1} - u_n| \leq K^n |u_1 - u_0|$. Alors, si

$n \in \mathbb{N}$,

$$\begin{aligned} |u_n - u_0| &= \left| \sum_{k=0}^{n-1} u_{k+1} - u_k \right| \\ &\leq \sum_{k=0}^{n-1} |u_{k+1} - u_k| \\ &\leq |u_1 - u_0| \sum_{k=0}^{n-1} K^k \\ &\leq \frac{1}{1-K} |u_1 - u_0|. \end{aligned}$$

Ainsi, (u_n) est bornée.

3 Extension au cas des fonctions complexes.

Soit $f : I \rightarrow \mathbb{C}$, où I est un intervalle de $\mathbb{R}$.

- La définition de dérivée en a est exactement la même que pour les fonctions réelles, mais la dérivée est à valeurs dans $\mathbb{C}$. On a aussi le résultat (simple) suivant.

Proposition 3.0.1.

La fonction f est dérivable (en un point ou sur I) si et seulement si $\operatorname{Re}(f)$ et $\operatorname{Im}(f)$ le sont aussi. Dans ce cas, on a $f' = \operatorname{Re}(f)' + i \operatorname{Im}(f)'$.

- Les résultats concernant les opérations sur la dérivabilité se généralisent : $+$, $\times$, $/$.

- Par contre, attention à la composition : dériver $f \circ g$ n'a de sens (dans notre cadre) que si g est à valeurs réelles, et f peut être à valeurs complexes ! Dans ce cas, on a le même résultat que dans le cas réel.

- Pour démontrer tout cela, on utilise la proposition 3.0.1.

- Les grands théorèmes :

- le théorème de Rolle ne se généralise pas.
Ex : $\mathbb{R} \rightarrow \mathbb{C}$, $x \mapsto e^{ix}$.

- TAF : faux aussi (normal, cela impliquerait le théorème de Rolle).

- IAF : On peut le formuler comme suit.

Théorème 3.0.2 (IAF version complexe).

Soit $(a, b) \in \mathbb{R}^2$ avec $a < b$ et $f \in \mathcal{C}^0([a, b], \mathbb{C}) \cap \mathcal{D}(]a, b[, \mathbb{C})$ tel qu'il existe $K > 0$ vérifiant $\forall x \in]a, b[\quad |f'(x)| \leq K$. Alors $|f(b) - f(a)| \leq K(b - a)$.

Démonstration. 1. On va d'abord s'intéresser au cas particulier où $f(b) - f(a)$ est un réel. Dans ce cas, considérons l'application $\text{Re}(f) : [a, b] \rightarrow \mathbb{R}$. Elle est continue sur $[a, b]$ et dérivable sur $]a, b[$. De plus, pour tout $x \in]a, b[$, on a $|\text{Re}(f)'(x)| = |\text{Re}(f'(x))| \leq |f'(x)| \leq K$. Donc on peut appliquer l'IAF à $\text{Re}(f)$ et en déduire : $|\text{Re}(f)(b) - \text{Re}(f)(a)| \leq K(b - a)$. Or $\text{Re}(f)(b) - \text{Re}(f)(a) = \text{Re}(f(b) - f(a)) = f(b) - f(a)$. On a donc le résultat.

2. Montrons maintenant le cas général. $f(b) - f(a)$ est de la forme $e^{i\theta} |f(b) - f(a)|$. Notons alors

$$\begin{aligned} \varphi : [a, b] &\rightarrow \mathbb{C} \\ x &\mapsto e^{-i\theta} f(x) \end{aligned}$$

φ est clairement dérivable sur $]a, b[$ et continue sur $[a, b]$. De plus pour tout $x \in]a, b[$, $\varphi'(x) = e^{-i\theta} f'(x)$, donc $|\varphi'(x)| = |f'(x)| \leq K$.

De plus $\varphi(b) - \varphi(a) = e^{-i\theta} (f(b) - f(a)) = |f(b) - f(a)|$.

$\varphi(b) - \varphi(a)$ est donc réel, donc on peut appliquer le point ci-dessus à $\varphi : |\varphi(b) - \varphi(a)| \leq K|b - a|$.

Or $|\varphi(b) - \varphi(a)| = |f(b) - f(a)|$, d'où le résultat. $\square$

Les notions de monotonie d'une fonction f ou de signe de f' n'ont évidemment pas de sens dans le cas des fonctions à valeurs complexes, mais on a cependant le résultat suivant.

Théorème 3.0.3.

Soit $f \in \mathcal{D}(I, \mathbb{C})$. Alors f est constante si et seulement si $f' = 0$.

Démonstration.

La fonction f est constante si et seulement si $\text{Re}(f)$ et $\text{Im}(f)$ sont constantes, ce qui équivaut à $(\text{Re}(f))' = (\text{Im}(f))' = 0$, ce qui équivaut à $(\text{Re}(f))' + i(\text{Im}(f))' = 0$, c'est-à-dire à $f' = 0$. $\square$

4 Convexité.

4.1 Parties convexes de $\mathbb{R}^2$ (HP).

Cette partie est hors du programme de MPSI (mais au programme en MP), et est présente ici à but d'illustration.

Rappel 4.1.1.

Soit A, B des points du plan de $\mathbb{R}^2$ d'affixes respectives a, b , soit M un autre point du plan. On note $[A, B]$ le segment reliant les points A et B . On a alors

$$\begin{aligned} M \in [A, B] &\Leftrightarrow \exists \lambda \in [0, 1], \overrightarrow{AM} = \lambda \overrightarrow{AB} \\ &\Leftrightarrow \exists \lambda \in [0, 1], \overrightarrow{OM} = (1 - \lambda) \overrightarrow{OA} + \lambda \overrightarrow{OB} \end{aligned}$$

Notamment, ce segment a pour paramétrisation complexe

$$\{ (1 - \lambda)a + b\lambda \mid \lambda \in [0, 1] \}.$$

Définition 4.1.2.

Une partie $\mathcal{C} \subset \mathbb{R}^2$ est dite convexe si pour tout $A, B \in \mathcal{C}$, $[A, B] \subset \mathcal{C}$, c'est-à-dire si cette partie contient tous les segments reliant ses points (voir figure XVII.5).

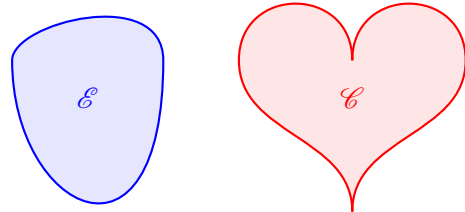


FIGURE XVII.5 – $\mathcal{E}$ est convexe, $\mathcal{C}$ ne l'est pas.

Remarque 4.1.3.

On peut donner la même définition dans $\mathbb{R}$. Les parties convexes de $\mathbb{R}$ sont alors les intervalles de $\mathbb{R}$.

Si $a < b < c \in \mathbb{R}$, on écrit $b = (1 - \lambda)a + \lambda c$, avec $\lambda = \frac{b - a}{c - a} \in]0, 1[$.

Exemple 4.1.4.

Un demi-plan est une partie convexe de $\mathbb{R}^2$.

Exercice 4.1.5.

Montrer qu'un disque est une partie convexe de $\mathbb{R}^2$.

4.2 Fonctions convexes.

Définition 4.2.1. 1. On dit que $f : I \rightarrow \mathbb{R}$ est *convexe* si

$$\forall x, y \in I, \forall \lambda \in [0, 1], \\ f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y).$$

2. On dit que f est *concave* si

$$\forall x, y \in I, \forall \lambda \in [0, 1], \\ f(\lambda x + (1 - \lambda)y) \geq \lambda f(x) + (1 - \lambda)f(y)$$

Remarque 4.2.2 (voir figure XVII.6).

Nous avons vu que $(\lambda x + (1 - \lambda)y, \lambda f(x) + (1 - \lambda)f(y))$ est une paramétrisation de la corde à la courbe de f reliant les points d'abscisses x et y .

Ainsi, f est convexe si et seulement si ses cordes sont toutes au dessus des arcs de courbes correspondants, et concave si et seulement si ses cordes sont toutes au dessous des arcs de courbes correspondants.

Remarque 4.2.3.

Cette définition est symétrique en x, y . On pourra donc toujours supposer, sans perte de généralité, que $x < y$.

Remarque 4.2.4 ().

« concave » n'est pas le contraire de « convexe ».

Il existe des fonctions ni concaves, ni convexes (par exemple, $x \mapsto x^3$) ; il existe des fonctions concaves et convexes (par exemple, les fonctions constantes).

Exercice 4.2.5.

Caractériser les fonctions à la fois concaves et convexes.

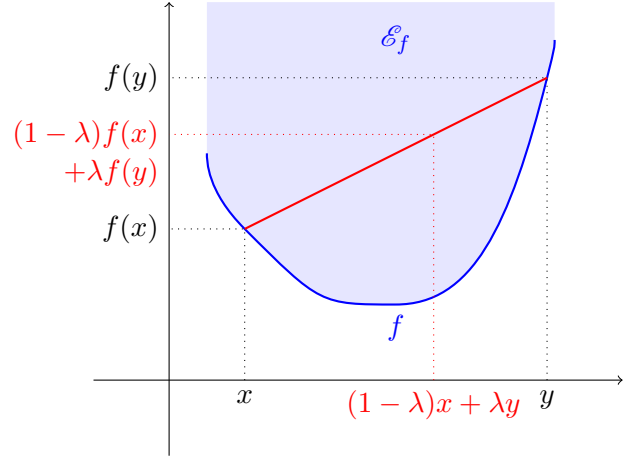


FIGURE XVII.6 – Exemple de fonction f convexe, une de ses cordes et son épigraphe $\mathcal{E}_f$.

Proposition 4.2.6.

Soit $f : I \rightarrow \mathbb{R}$, alors f est convexe si et seulement si $-f$ est concave.

Démonstration.

Élémentaire. □

Remarque 4.2.7.

Tous les résultats sur les fonctions concaves s'obtiennent donc par symétrie à partir de ceux obtenus sur les fonctions convexes. Nous nous intéresserons donc principalement aux fonctions convexes par la suite.

Définition 4.2.8.

On appelle *épigraphe* de f l'ensemble

$$\{ (x, y) \mid x \in I \text{ et } y \geq f(x) \}.$$

Proposition 4.2.9 (Interprétation géométrique, voir figure XVII.6).

Une fonction est convexe si et seulement si son épigraphe est une partie convexe de $\mathbb{R}^2$.

Démonstration.

Soit $f : I \rightarrow \mathbb{R}$ convexe, soit (x, y) et (x', y') deux points

de l'épigraphe de $f : x, x' \in I, y \geq f(x)$ et $y' \geq f(x')$. Soit $\lambda \in [0, 1]$. Comme $1 - \lambda \geq 0$ et $\lambda \geq 0$, on a

$$(1 - \lambda)y + \lambda y' \geq (1 - \lambda)f(x) + \lambda f(x').$$

Comme I est un intervalle, on a $(1 - \lambda)x + \lambda x' \in I$. Comme f est convexe, on a $(1 - \lambda)f(x) + \lambda f(x') \geq f((1 - \lambda)x + \lambda x')$, donc

$$(1 - \lambda)y + \lambda y' \geq f((1 - \lambda)x + \lambda x').$$

Ainsi, $((1 - \lambda)x + \lambda x', (1 - \lambda)y + \lambda y')$ appartient à l'épigraphe de f , donc cet épigraphe est bien convexe.

Réciproquement, supposons que l'épigraphe de f est convexe. Si $x, y \in I$, on a bien entendu $f(x) \geq f(x)$ (*idem* pour y), donc $(x, f(x))$ et $(y, f(y))$ sont deux points de l'épigraphe de f . Ainsi, si $\lambda \in [0, 1]$, alors $((1 - \lambda)x + \lambda y, (1 - \lambda)f(x) + \lambda f(y))$ est dans l'épigraphe de f , ce qui signifie exactement que

$$f((1 - \lambda)x + \lambda y) \leq (1 - \lambda)f(x) + \lambda f(y).$$

Ainsi, f est convexe. $\square$

Proposition 4.2.10 (Inégalité de Jensen).

Soit $f : I \rightarrow \mathbb{R}$ convexe. Alors pour tout $x_1, \dots, x_n \in I$ et pour tout $\lambda_1, \dots, \lambda_n \geq 0$ vérifiant $\lambda_1 + \dots + \lambda_n = 1$, on a

$$f(\lambda_1 x_1 + \dots + \lambda_n x_n) \leq \lambda_1 f(x_1) + \dots + \lambda_n f(x_n).$$

Démonstration.

On le montre par récurrence.

Pour $n = 1$, il n'y a rien à faire.

Pour $n = 2$, c'est la définition de la convexité. En effet, si $\lambda_1 + \lambda_2 = 1$, on a alors $\lambda_2 = 1 - \lambda_1$.

Soit $n \geq 1$, supposons l'inégalité de Jensen vérifiée pour n points et paramètres quelconques. Soit $x_1, \dots, x_{n+1} \in I$ et $\lambda_1, \dots, \lambda_{n+1} \geq 0$ vérifiant $\lambda_1 + \dots + \lambda_{n+1} = 1$.

Remarquons que si $\lambda_{n+1} = 0$, le résultat est assuré par hypothèse de récurrence, et si $\lambda_{n+1} = 1$, on a $\lambda_1 = \dots = \lambda_n = 0$, et le résultat est immédiat.

On peut donc supposer que $0 < \lambda_{n+1} < 1$.

On pose $\mu = \lambda_1 + \dots + \lambda_n = 1 - \lambda_{n+1} \in]0, 1[$. Posons aussi

$$S = \frac{\lambda_1}{\mu} x_1 + \dots + \frac{\lambda_n}{\mu} x_n,$$

de sorte que

$$\lambda_1 x_1 + \dots + \lambda_{n+1} x_{n+1} = \mu S + \lambda_{n+1} x_{n+1},$$

où $\mu + \lambda_{n+1} = 1$.

Comme $\frac{\lambda_1}{\mu} + \dots + \frac{\lambda_n}{\mu} = \frac{\mu}{\mu} = 1$ et comme ces nombres sont tous positifs, par convexité de I on a $S \in I$ (cela se montre aisément par une récurrence similaire à celle-ci, laissée au lecteur – ou à la lectrice).

On a alors par convexité de f :

$$f(\lambda_1 x_1 + \dots + \lambda_{n+1} x_{n+1}) \leq \mu f(S) + \lambda_{n+1} f(x_{n+1}).$$

Par hypothèse de récurrence, on a

$$f(S) \leq \frac{\lambda_1}{\mu} f(x_1) + \dots + \frac{\lambda_n}{\mu} f(x_n),$$

de sorte que l'on obtient bien

$$f(\lambda_1 x_1 + \dots + \lambda_{n+1} x_{n+1}) \leq \lambda_1 f(x_1) + \dots + \lambda_{n+1} f(x_{n+1}).$$

Le résultat est donc bien établi par récurrence. $\square$

Théorème 4.2.11.

Soit $f : I \rightarrow \mathbb{R}$. Alors, f est convexe si et seulement si, pour tout $a \in I$, la fonction

$$\tau_{f,a} : \begin{cases} I \setminus \{a\} & \longrightarrow \mathbb{R} \\ x & \longmapsto \frac{f(x) - f(a)}{x - a} \end{cases}$$

est croissante.

Démonstration.

Supposons que f est convexe, soit $a \in I$, montrons que $\tau_{f,a}$ est croissante.

Soit $x, y \in I \setminus \{a\}$ vérifiant $x < y$, montrons que $\tau_{f,a}(x) \leq \tau_{f,a}(y)$.

On procède par disjonction de cas, suivant la position de a .

• Si $a < x < y$, il existe $\lambda \in]0, 1[$ tel que $x = (1 - \lambda)a + \lambda y$: $\lambda = \frac{x - a}{y - a}$. On a alors par convexité de f :

$$f(x) \leq (1 - \lambda)f(a) + \lambda f(y),$$

donc

$$f(x) - f(a) \leq \lambda(f(y) - f(a))$$

Avec la valeur de λ trouvée précédemment, on obtient

$$\frac{f(x) - f(a)}{x - a} \leq \frac{f(y) - f(a)}{y - a},$$

soit exactement $\tau_{f,a}(x) \leq \tau_{f,a}(y)$.

On pourrait procéder de même dans les deux autres cas, mais ces derniers sont équivalents (voir la remarque 4.2.13 pour plus de détails).

• Si $x < a < y$, on a par ce qui précède :

$$\frac{f(a) - f(x)}{a - x} \leq \frac{f(y) - f(x)}{y - x}.$$

Après avoir multiplié par $(a - x)(y - x) \geq 0$ et réordonné cela, on retrouve $\tau_{f,a}(x) \leq \tau_{f,a}(y)$.

• Si $x < y < a$, on a de même

$$\frac{f(y) - f(x)}{y - x} \leq \frac{f(a) - f(x)}{a - x}$$

et l'on retrouve de la même manière (après des manipulations élémentaires) : $\tau_{f,a}(x) \leq \tau_{f,a}(y)$.

Ainsi, par disjonction de cas, $\tau_{f,a}$ est croissante.

Réciproquement, supposons que, pour tout $a \in I$, $\tau_{f,a}$ est croissante sur $I \setminus \{a\}$.

Soit $x, y \in I$, supposons sans perte de généralité que $x < y$. Soit $\lambda \in]0, 1[$, montrons que $f((1 - \lambda)x + \lambda y) \leq (1 - \lambda)f(x) + \lambda f(y)$. Posons $a = (1 - \lambda)x + \lambda y \in]x, y[$. Notamment, $\lambda = \frac{a - x}{y - x}$ et $1 - \lambda = \frac{y - a}{y - x}$. On a par croissance de $\tau_{f,a}$:

$$\tau_{f,a}(x) \leq \tau_{f,a}(y),$$

soit

$$\frac{f(a) - f(x)}{a - x} \leq \frac{f(y) - f(a)}{y - a},$$

ou l'on a prit soin de n'écrire que des membres positifs. On a donc

$$(y - a)(f(a) - f(x)) \leq (a - x)(f(y) - f(a)),$$

soit

$$(y - x)f(a) \leq (a - x)f(y) + (y - a)f(x),$$

soit exactement

$$f((1 - \lambda)x + \lambda y) \leq (1 - \lambda)f(x) + \lambda f(y).$$

Ainsi, f est convexe. $\square$

Corollaire 4.2.12 (Théorème des trois pentes, voir figure XVII.7).

Soit $f : I \rightarrow \mathbb{R}$. Alors, f est convexe si et seulement si, pour tout $a < b < c \in I$, on a

$$\frac{f(a) - f(b)}{a - b} \leq \frac{f(a) - f(c)}{a - c} \leq \frac{f(b) - f(c)}{b - c}.$$

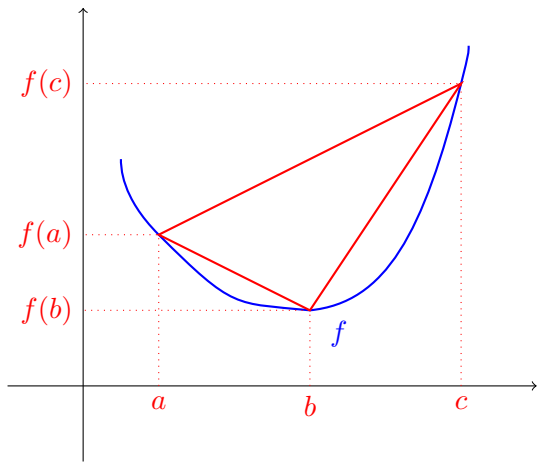


FIGURE XVII.7 – Les trois cordes du théorème des trois pentes.

Démonstration.

Si f est convexe, cela se lit $\tau_{f,a}(b) \leq \tau_{f,a}(c)$ et $\tau_{f,c}(a) \leq \tau_{f,c}(b)$, ce qui est vrai par les croissances de $\tau_{f,a}$ et de $\tau_{f,c}$.

Réciproquement, si l'inégalité des trois pentes est toujours vraie, on lit que la fonction $\tau_{f,a}$ est croissante sur $I \cap]a, +\infty[$ et que la fonction $\tau_{f,c}$ est croissante sur $I \cap]-\infty, c[$.

Comme a et c sont quelconques, $\tau_{f,b}$ est croissante sur $I \cap]-\infty, b[$ et sur $I \cap]b, +\infty[$. Or si $a < b < c$, on lit $\tau_{f,b}(a) \leq \tau_{f,b}(c)$, donc $\tau_{f,b}$ est croissante, donc f est convexe. $\square$

Remarque 4.2.13.

Les trois inégalités

$$\begin{aligned} \frac{f(a) - f(b)}{a - b} &\leq \frac{f(a) - f(c)}{a - c} \\ \frac{f(a) - f(c)}{a - c} &\leq \frac{f(b) - f(c)}{b - c} \\ \frac{f(a) - f(b)}{a - b} &\leq \frac{f(b) - f(c)}{b - c} \end{aligned}$$

sont toutes les trois équivalentes à l'inégalité

$$(a - b)f(c) + (b - c)f(a) + (c - a)f(b) \leq 0.$$

Corollaire 4.2.14 (voir la figure XVII.8).

Si $f : I \rightarrow \mathbb{R}$ est convexe, considérons une sécante à la courbe de f :

- la corde ainsi construite est au dessus de la courbe de f ;
- en dehors de la corde, la sécante est en dessous de la courbe de f .

Démonstration.

Nous savons déjà que la corde à la courbe de f est au dessus de sa courbe. Soit $a < b \in I$, notons $\mathcal{S}$ la sécante à la courbe de f passant par les points d'abscisses a et b . Soit $x \in I$ vérifiant $x < a$. Le point d'abscisse x se trouvant sur $\mathcal{S}$ a pour ordonnée

$$f(a) + \tau_{f,a}(b)(x - a)$$

et le point d'abscisse x se trouvant sur la courbe de f a pour ordonnée

$$f(x) = f(a) + \tau_{f,a}(x)(x - a).$$

Par croissance de $\tau_{f,a}$, on a $\tau_{f,a}(b) \geq \tau_{f,a}(x)$. Comme $x - a < 0$, on obtient bien

$$f(a) + \tau_{f,a}(b)(x - a) \leq f(x),$$

ce qui permet de conclure.

Le cas $x > b$ est strictement identique. $\square$

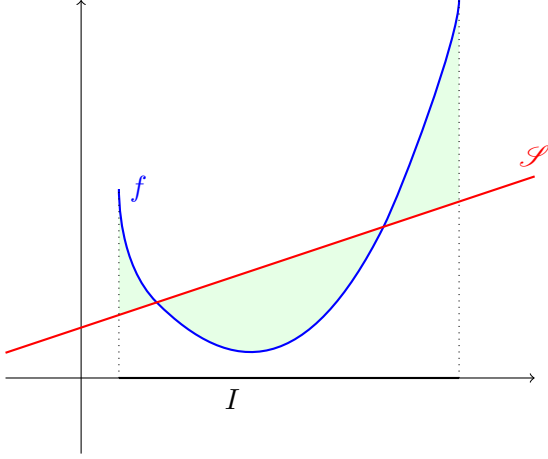


FIGURE XVII.8 – Position d'une sécante $\mathcal{S}$ par rapport à la courbe d'une fonction convexe f .

4.3 Régularité des fonctions convexes.

Rappel 4.3.1.

Soit $I \subset \mathbb{R}$ un intervalle, de bornes inférieures et supérieures $a, b \in \bar{\mathbb{R}}$.

L'intérieur de I est l'intervalle ouvert $\overset{\circ}{I} =]a, b[$. Pour $x \in \mathbb{R}$, on a la caractérisation

$$x \in \overset{\circ}{I} \Leftrightarrow \exists \varepsilon > 0, [x - \varepsilon, x + \varepsilon] \subset I.$$

Théorème 4.3.2 (HP, mais important).

Soit $f : I \rightarrow \mathbb{R}$ convexe.

Pour tout $a \in \overset{\circ}{I}$, f est dérivable à gauche et à droite en a et $f'_g(a) \leq f'_d(a)$.

De plus, f est continue sur $\overset{\circ}{I}$.

Démonstration.

La clef de ce théorème est le résultat de croissance des pentes démontré précédemment. Soit $x < a < y \in \overset{\circ}{I}$. Alors, par croissance de $\tau_{f,a}$:

$$\tau_f(x, a) \leq \tau_f(a, y).$$

Par limite monotone, $\tau_{f,a}$ admet donc une limite finie à gauche en a , donc f est dérivable à gauche en a et

$$f'_g(a) \leq \tau_f(a, y).$$

De même, $\tau_{f,a}$ admet une limite finie à droite en a , donc f est dérivable à droite en a et

$$f'_d(a) \leq f'_g(a).$$

Comme f est dérivable à gauche et à droite en a , f est continue à gauche et à droite en a , donc continue en a . $\square$

Remarque 4.3.3.

Il existe des fonctions convexes non continues, les discontinuités se trouvant alors au bord de l'intervalle de définition. On peut démontrer qu'une fonction convexe admet des limites (éventuellement infinies) à gauche ou à droite au bord son intervalle de définition.

Il existe aussi des fonctions convexes non dérivables.

Exercice 4.3.4.

Montrer que la fonction valeur absolue est convexe.

Théorème 4.3.5.

Soit $f : I \rightarrow \mathbb{R}$ dérivable. Alors, f est convexe si et seulement si f' est croissante.

Démonstration.

Supposons que f est convexe. Soit $a < b \in I$, soit $x \in]a, b[$. Par le théorème des trois pentes (corollaire 4.2.12) :

$$\tau_f(a, x) \leq \tau_f(a, b) \leq \tau_f(b, x).$$

Par passage à la limite lorsque x tend vers a , puis vers b , on obtient

$$f'(a) \leq \tau_f(a, b) \leq f'(b),$$

donc f' est croissante.

Réciproquement, supposons que f' est croissante. Soit $a < b < c \in I$. Par l'égalité des accroissements finis appliqués sur $[a, b]$ et $[b, c]$, il existe $x \in]a, b[$ et $y \in]b, c[$ tels que $\frac{f(b) - f(a)}{b - a} = f'(x)$ et $\frac{f(c) - f(b)}{c - b} = f'(y)$. Comme $x < y$, on a donc

$$\frac{f(b) - f(a)}{b - a} \leq \frac{f(c) - f(b)}{c - b},$$

ce qui s'écrit en multipliant par $(b - a)(c - b) > 0$ et en simplifiant :

$$(c - a)f(b) + (b - c)f(a) + (a - b)f(c) \leq 0.$$

On en déduit immédiatement la condition du théorème des trois pentes, donc f est convexe. $\square$

Remarque 4.3.6.

On démontre de même que, si f est convexe, f'_g et f'_d sont croissantes sur $\overset{\circ}{I}$, et ce sans hypothèse de dérivabilité.

Corollaire 4.3.7.

Soit $f : I \rightarrow \mathbb{R}$ deux fois dérivable. Alors, f est convexe si et seulement si f'' est positive.

Démonstration.

Immédiat.

□

Exemple 4.3.8.

La fonction exponentielle est convexe. Si $\alpha \geq 1$, $x \mapsto x^\alpha$ est convexe sur $\mathbb{R}_+^*$.

Théorème 4.3.9 (voir la figure XVII.9).

Soit $f : I \rightarrow \mathbb{R}$ dérivable. Alors, f est convexe si et seulement si la courbe de f est au dessus de toutes ses tangentes.

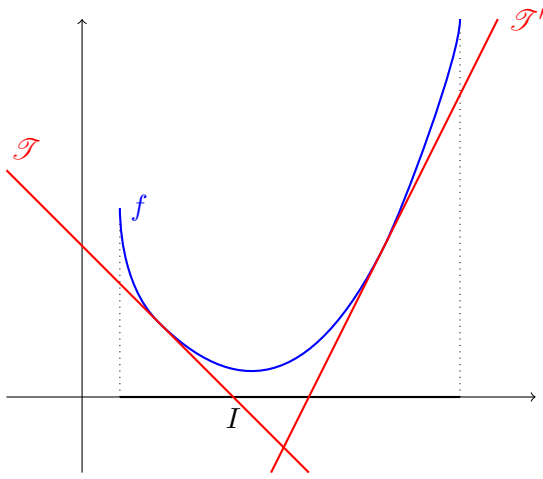


FIGURE XVII.9 – Position de deux tangentes $\mathcal{T}$ et $\mathcal{T}'$ par rapport à la courbe d'une fonction convexe f .

Démonstration.

On démontre que f est convexe si et seulement si, pour tout $a, x \in I$,

$$f(x) \geq f(a) + (x - a)f'(a).$$

Supposons f convexe. Soit $x, a \in I$. Si $x = a$, on a $f(x) = f(a) + (x - a)f'(a)$. Si $x \neq a$, on peut appliquer l'égalité des accroissements finis : il existe c entre a et x tel que

$$\frac{f(x) - f(a)}{x - a} = f'(c).$$

- Si $x > a$, on a $x - a > 0$ et par croissance de f' , on a $f'(c) \geq f'(a)$.
- Si $x < a$, on a $x - a < 0$ et par croissance de f' , on a $f'(c) \leq f'(a)$.

Dans les deux cas, on a bien $f(x) \geq f(a) + (x - a)f'(a)$.

Réciproquement, supposons que la courbe de f est au dessus de toutes ses tangentes. Soit $(x, y) \in I^2$, soit $\lambda \in [0, 1]$. On pose $a = \lambda x + (1 - \lambda)y \in I$. Le graphe de f est

au-dessus de sa tangente en $(a, f(a))$, donc on a les deux inégalités

$$f(x) \geq f(a) + f'(a)(x - a),$$

$$f(y) \geq f(a) + f'(a)(y - a).$$

En effectuant leur combinaison linéaire avec les coefficients $\lambda \geq 0$ et $(1 - \lambda) \geq 0$, on obtient

$$\lambda f(x) + (1 - \lambda)f(y) \geq f(a) + f'(a)(\lambda x + (1 - \lambda)y - a),$$

ce qui donne exactement

$$\lambda f(x) + (1 - \lambda)f(y) \geq f(a).$$

Ainsi, f est convexe. □

Corollaire 4.3.10 (Caractérisations de la concavité).

Soit $f : I \rightarrow \mathbb{R}$.

Si f est dérivable, alors f est concave si et seulement si f' est décroissante, et si et seulement si la courbe de f est en dessous de toutes ses tangentes.

Si f est deux fois dérivable, alors f est concave si et seulement si f'' est négative.

Démonstration.

Immédiat avec la proposition 4.2.6. □

Exemple 4.3.11.

La fonction $\ln$ est concave.

Définition 4.3.12.

Soit $f : I \rightarrow \mathbb{R}$ continue, soit $a \in I$. Alors, a est un *point d'inflexion* pour f si la courbe de f change de concavité en a , c'est-à-dire s'il existe $\varepsilon > 0$ tel que $f|_{[a-\varepsilon, a]}$ et $f|_{[a, a+\varepsilon]}$ soient de concavités opposées (l'une est convexe et l'autre est concave).

Proposition 4.3.13.

Soit $f : I \rightarrow \mathbb{R}$ deux fois dérivable. Alors tout point d'annulation de f'' où f'' change de signe est un point d'inflexion de f .

Si a est un point d'inflexion de f , la tangente à la courbe de f en a traverse la courbe de f , en a .

Exemple 4.3.14.

Les fonction $\tan$, $\sin$ et $\sh$ ont chacune un point d'inflexion en 0.

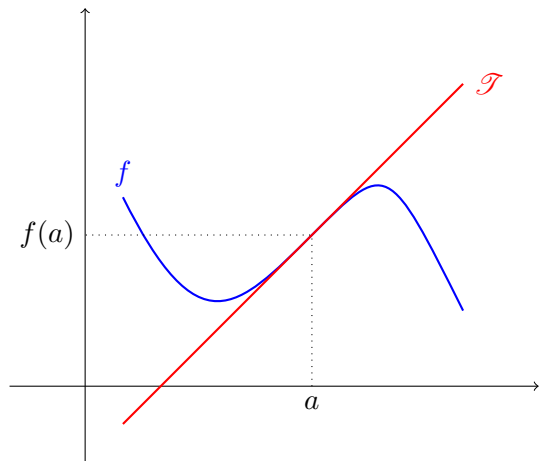


FIGURE XVII.10 – Exemple de point d’inflexion a pour une fonction f . La tangente $\mathcal{T}$ traverse la courbe de f .

Chapitre XVIII

Fractions rationnelles

Sommaire

1	Corps des fractions rationnelles $\mathbb{K}(X)$.	272
1.1	Définitions.	272
1.2	Fonctions rationnelles.	273
1.3	Dérivées, degrés et pôles.	273
1.4	Zéros et pôles.	275
2	Étude locale d'une fraction rationnelle.	275
2.1	Partie entière.	275
2.2	Partie polaire associée à un pôle.	276
2.3	Décomposition en éléments simples dans $\mathbb{C}(X)$.	276
2.4	Décomposition en éléments simples dans $\mathbb{R}(X)$.	276
2.5	Quelques méthodes de calcul.	277
a	Avant même de commencer.	277
b	Simplification par symétrie, parité et imparité.	277
c	Simplification par conjugaison de fractions rationnelles réelles.	277
d	Méthode de base.	278
e	Résidus.	279
f	Un exemple.	279
g	Évaluation en un point différent d'un pôle.	279
h	Identification.	279
i	Développements limités.	280
2.6	Décomposition de P'/P .	280
3	Application au calcul intégral.	281
3.1	Si $\mathbb{K} = \mathbb{C}$.	281
3.2	Si $\mathbb{K} = \mathbb{R}$.	281

Dans ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
 Nous allons étudier un nouveau corps : $\mathbb{K}(X)$, qui est le corps des *fractions rationnelles*. Sa construction est hors-programme, mais on peut mentionner que l'on obtient $\mathbb{K}(X)$ à partir de $\mathbb{K}[X]$ de la même manière que l'on obtient $\mathbb{Q}$ à partir de $\mathbb{Z}$: on rajoute de nouveaux éléments qui seront les inverses pour la loi $\times$ de tous les éléments non nuls, c'est-à-dire que l'on introduit les éléments $\frac{1}{P}$, où $P \in \mathbb{K}[X] \setminus \{0\}$. Ainsi, $\mathbb{K}(X)$ est le corps contenant les fractions de polynômes.

1 Corps des fractions rationnelles $\mathbb{K}(X)$.

1.1 Définitions.

La construction de l'ensemble des fractions rationnelles étant hors-programme, on introduit celui-ci de façon axiomatique.

Définition 1.1.1.

Il existe un ensemble $\mathbb{K}(X)$ vérifiant :

- (i) À tout couple $(A, B) \in \mathbb{K}[X]^2$ tel que $B \neq 0$, on peut associer un élément de $\mathbb{K}(X)$ noté $\frac{A}{B}$;
- (ii) Réciproquement, tout élément de $\mathbb{K}(X)$ s'écrit $\frac{A}{B}$, avec $A, B \in \mathbb{K}[X]$, $B \neq 0$;
- (iii) Si $A, B, C, D \in \mathbb{K}[X]$ tels que B et D soient non nuls, on a : $\frac{A}{B} = \frac{C}{D} \Leftrightarrow AD = BC$.

Cette définition permet de donner sans ambiguïté tous les éléments de $\mathbb{K}(X)$: ce n'est qu'une définition ensembliste.

Cet ensemble est appelé *l'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$* .



L'écriture (ii) n'est pas unique !

Remarque 1.1.2.

Remarquons que cette définition dit notamment que pour toute fraction rationnelle $\frac{A}{B}$ et tout polynôme non nul C , les fractions rationnelles $\frac{AC}{BC}$ sont égales (en effet $AC \times B = A \times BC$).

Définition 1.1.3.

Soit $R \in \mathbb{K}(X)$, un couple $(A, B) \in \mathbb{K}[X]^2$ tel que $R = \frac{A}{B}$ est appelé *représentant* de la fraction rationnelle R .

Passons maintenant à des définitions algébriques.

Définition 1.1.4 (Lois sur $\mathbb{K}(X)$).

On définit trois lois sur $\mathbb{K}(X)$, les deux premières sont des lois internes, la troisième est une loi externe.

$$\text{Addition } + : \begin{cases} \mathbb{K}(X) \times \mathbb{K}(X) & \longrightarrow \mathbb{K}(X) \\ \left(\frac{A}{B}, \frac{C}{D} \right) & \longmapsto \frac{AD + BC}{BD} \end{cases}$$

$$\text{Produit } \times : \begin{cases} \mathbb{K}(X) \times \mathbb{K}(X) & \longrightarrow \mathbb{K}(X) \\ \left(\frac{A}{B}, \frac{C}{D} \right) & \longmapsto \frac{AC}{BD} \end{cases}$$

Multiplication par un scalaire :

$$\begin{cases} \mathbb{K} \times \mathbb{K}(X) & \longrightarrow \mathbb{K}(X) \\ \left(\lambda, \frac{A}{B} \right) & \longmapsto \frac{\lambda A}{B} \end{cases}$$

Alors $(\mathbb{K}(X), +, \times)$ est un corps.

De plus, tout polynôme de $\mathbb{K}[X]$ s'identifie à l'élément $\frac{P}{1}$ de $\mathbb{K}(X)$. Cette identification permet de considérer $(\mathbb{K}[X], +, \times)$ comme un sous-anneau de $(\mathbb{K}(X), +, \times)$.

Le neutre de la loi $+$ est 0, celui de la loi $\times$ est 1. L'opposé de $\frac{A}{B}$ est $\frac{-A}{B}$, son inverse est $\frac{B}{A}$.

Remarque 1.1.5.

On verra bientôt que $(\mathbb{K}(X), +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel.

Démonstration.



Les définitions ci-dessus sont a priori ambiguës : par exemple lorsqu'on veut additionner deux fractions rationnelles R_1 et R_2 , on dispose de plusieurs représentants pour R_1 et de plusieurs représentants pour R_2 (il y en a même une infinité). Lesquels choisir pour appliquer la définition ? On peut en fait montrer que le résultat ne dépend pas du choix des représentants. En effet, considérons deux représentants $\frac{A_1}{B_1}$ et $\frac{C_1}{D_1}$ pour R_1 et deux représentants $\frac{A_2}{B_2}$ et $\frac{C_2}{D_2}$ pour R_2 .

On a $A_i D_i = B_i C_i$ pour $i = 1, 2$. Montrons alors qu'on a $\frac{A_1 B_2 + A_2 B_1}{B_1 B_2} = \frac{C_1 D_2 + C_2 D_1}{D_1 D_2}$.
Il suffit de remarquer qu'on a successivement :

$$\begin{aligned} (A_1 B_2 + A_2 B_1) D_1 D_2 &= (A_1 D_1) B_2 D_2 + (A_2 D_2) B_1 D_1 \\ &= (B_1 C_1) B_2 D_2 + (B_2 C_2) B_1 D_1 \\ &= (C_1 D_2 + C_2 D_1) B_1 B_2 \end{aligned}$$

On a aisément de même $\frac{A_1 A_2}{B_1 B_2} = \frac{C_1 C_2}{D_1 D_2}$ et $\frac{\lambda A_1}{B_1} = \frac{\lambda C_1}{D_1}$.

On procède de même (mais plus simplement) pour le produit et la multiplication scalaire. $\square$

1.2 Fonctions rationnelles.

Définition 1.2.1.

Soit $R \in \mathbb{K}(X)$. On appelle *forme irréductible* de R toute écriture de R de la forme $R = \frac{P}{Q}$ avec $P, Q \in \mathbb{K}[X]$ tels que $P \wedge Q = 1$.

Exemple 1.2.2.

$\frac{X^2 - 1}{X(X - 1)}$ n'est pas irréductible, mais $\frac{X + 1}{X}$ l'est.

Remarque 1.2.3.



Il existe une infinité de formes irréductibles : ainsi $\frac{1}{X}$, $\frac{2}{2X}$ et $\frac{3}{3X}$ sont trois formes irréductibles d'une même fraction rationnelle.

Cependant, si $\frac{A}{B}$ et $\frac{C}{D}$ sont deux formes irréductibles d'une même fraction rationnelle, alors il existe $\lambda \in \mathbb{K}^*$ vérifiant $C = \lambda A$ et $D = \lambda B$. (en effet, on a alors $AD = BC$ donc $D|BC$ or D et C sont premiers entre eux, donc D divise B ; de même $B|AD$ donc $B|D$, B et D sont donc associés, il existe donc λ non nul vérifiant $D = \lambda B$, donc $\lambda AB = BC$, or $B \neq 0$ donc $C = \lambda A$).

Définition 1.2.4.

Soient $R \in \mathbb{K}(X)$ et $\frac{A}{B}$ une forme irréductible de R . Alors si $\tilde{A}$ et $\tilde{B}$ sont les fonctions polynomiales associées à A et B , on appelle *fonction rationnelle associée à R* la fonction $\tilde{R} : \mathbb{K} \setminus \mathcal{A} \rightarrow \mathbb{K}$,

$$x \mapsto \frac{\tilde{A}(x)}{\tilde{B}(x)}$$

où $\mathcal{A}$ est l'ensemble des racines de B .

Remarque 1.2.5. 1. Ce problème du domaine de définition explique pourquoi l'on travaille avec des formes irréductibles : avec une forme réductible, le domaine de définition serait encore plus restreint (et en tout cas différent, donc pas très pratique), car le dénominateur aurait encore plus de racines. Par exemple, pour $R = 1$ si l'on écrit $R = \frac{X}{X}$, la fonction rationnelle associée ne serait pas définie en 0, ce qui est idiot pour une fonction constante.

2. La remarque 1.2.3 permet de conclure que $\tilde{R}$ ne dépend pas de la forme irréductible choisie.

Proposition 1.2.6.

Soient R_1, R_2 deux fractions rationnelles. Alors $R_1 = R_2 \Leftrightarrow \tilde{R}_1 = \tilde{R}_2$.

Démonstration.

Le sens direct découle des propriétés de l'égalité en mathématiques.

Étudions le sens indirect : on note $R_1 = \frac{P}{Q}$ et $R_2 = \frac{A}{B}$, deux formes irréductibles. Alors les fonctions $\frac{\tilde{P}}{\tilde{Q}}$ et $\frac{\tilde{A}}{\tilde{B}}$ coïncident sur leur ensemble de définition D , d'où $\tilde{P}\tilde{B}$ et $\tilde{A}\tilde{Q}$, qui sont deux fonctions polynomiales, coïncident sur D , qui est infini. Donc les polynômes sous-jacents sont égaux, i.e. $P\tilde{B} = A\tilde{Q}$. Donc on a $R_1 = R_2$. $\square$

1.3 Dérivées, degrés et pôles.

Définition 1.3.1.

Soit $R = \frac{A}{B}$. On appelle *dérivée* de R la fraction rationnelle $\frac{A'B - B'A}{B^2}$. Cette fraction rationnelle ne dépend pas du choix de A et de B , et est donc bien définie.

On a alors les propriétés suivantes, pour $R_1, R_2 \in \mathbb{K}(X)$ et $\lambda \in \mathbb{K}$:

- (i) $(R_1 + \lambda R_2)' = R_1' + \lambda R_2'$
- (ii) $(R_1 \times R_2)' = R_1' R_2 + R_1 R_2'$
- (iii) si $R_2 \neq 0$, $\left(\frac{R_1}{R_2}\right)' = \frac{R_1' R_2 - R_1 R_2'}{R_2^2}$.

Démonstration. • Montrons que R' ne dépend pas du choix de A et B : si $R = \frac{P}{Q} = \frac{A}{B}$, avec $\frac{A}{B}$ irréductible. Alors $PB = AQ$, donc $B|AQ$ et, avec le lemme de Gauss, $B|Q$, d'où il existe $C \in \mathbb{K}[X]$ tel que $Q = BC$, et par suite $PB = ABC$ avec $B \neq 0$, donc $P = AC$. Dans ce cas,

$$\begin{aligned} \left(\frac{P}{Q}\right)' &= \frac{P'Q - Q'P}{Q^2} \\ &= \frac{(A'C + AC')BC - (B'C + BC')AC}{B^2C^2} \\ &= \frac{C^2(A'B - AB')}{C^2B^2} \\ &= \frac{A'B - AB'}{B^2} \\ &= \left(\frac{A}{B}\right)'. \end{aligned}$$

- Il suffit de remplacer les expressions par leurs définitions et d'un simple calcul pour vérifier les propriétés énoncées. $\square$

Remarque 1.3.2.

La dérivation sur $\mathbb{K}(X)$ prolonge celle sur $\mathbb{K}[X]$.

Définition 1.3.3 (Degré).

Soit $R = \frac{A}{B}$, avec $A, B \in \mathbb{K}[X]$, $B \neq 0$. On appelle *degré* de R , noté $\deg R$, la quantité $\deg R = \deg A - \deg B$. Si $A \neq 0$, il s'agit d'un entier relatif. Sinon, $\deg R = -\infty$. Cette définition ne dépend là encore pas du représentant choisi.

Démonstration.

Si $R = \frac{A}{B} = \frac{C}{D}$, alors $AD = BC$, donc $\deg(AD) = \deg(BC)$, soit $\deg(A) + \deg(D) = \deg(B) + \deg(C)$. On obtient donc $\deg(A) - \deg(B) = \deg(C) - \deg(D)$. $\square$

Remarque 1.3.4.

Le degré sur $\mathbb{K}(X)$ prolonge celui sur $\mathbb{K}[X]$.

Remarque 1.3.5.

La fraction rationnelle nulle est la seule à ne pas avoir pour degré un entier.

Exemple 1.3.6.

$$\begin{aligned} \deg\left(\frac{X^4}{X(X-1)}\right) &= 4 - 2 = 2 \\ \deg\left(\frac{X(X^2+5)}{X^3(X^2+X-2)}\right) &= 3 - 5 = -2 \\ \deg\left(\frac{X^2(X+1)}{X^3-2X+3}\right) &= 3 - 3 = 0 \end{aligned}$$

On voit là qu'une fraction rationnelle de degré nul n'est pas forcément constante.

Proposition 1.3.7.

Soient $R_1, R_2 \in \mathbb{K}(X)$.

- (i) $\deg(R_1 + R_2) \leq \max(\deg R_1, \deg R_2)$
- (ii) $\deg(R_1 R_2) = \deg R_1 + \deg R_2$
- (iii) Si $R_2 \neq 0$, $\deg \frac{R_1}{R_2} = \deg R_1 - \deg R_2$.
- (iv) Si $\deg R_1 \neq 0$, alors $\deg R'_1 = \deg R_1 - 1$.
- (v) Si $R_1 \neq 0$, alors $\deg R'_1 < \deg R_1$.

Démonstration.

On note $R_1 = \frac{P}{Q}$ et $R_2 = \frac{A}{B}$.

- (i) On a : $R_1 + R_2 = \frac{PB + AQ}{QB}$. Donc

$$\begin{aligned} \deg(R_1 + R_2) &= \deg(PB + AQ) - \deg(QB) \\ &\leq \max(\deg(PB), \deg(AQ)) - \deg Q - \deg B \\ &\leq \max(\deg P + \deg B, \deg A + \deg Q) - \deg Q - \deg B \\ &\leq \max(\deg P + \deg B - \deg Q - \deg B, \\ &\quad \deg A + \deg Q - \deg Q - \deg B) \\ &\leq \max(\deg P - \deg Q, \deg A - \deg B) \\ &\leq \max(\deg(P/Q), \deg A/B) \\ &\leq \max(\deg(R_1), \deg(R_2)). \end{aligned}$$

- (ii) Simple calcul.
- (iii) Idem.
- (iv) On note $d = \deg P$, $e = \deg Q$, p le coefficient dominant de P et q celui de Q .
 - Si $e = 0$, alors R_1 est un polynôme et le résultat est alors connu.
 - Si $d = 0$ et $e \neq 0$, alors $\deg R_1 = -e$ et $R'_1 = -p \frac{Q'}{Q^2}$, dont le degré est $e - 1 - 2e = -e - 1 = \deg R_1 - 1$.
 - Si $d \neq 0$ et $e \neq 0$, alors on a $R'_1 = \frac{P'Q - Q'P}{Q^2}$, donc $\deg P'Q = \deg PQ' = \deg P + \deg Q - 1 = d + e - 1$. Le coefficient de degré $d + e - 1$ de $P'Q - Q'P$ est

$dpq - epq = (d - e)pq \neq 0$ car $d - e = \deg R_1 \neq 0$, donc $\deg R'_1 = d + e - 1 - \deg(Q^2) = d + e - 1 - 2e = d - e - 1 = \deg R_1 - 1$.

- (v) En reprenant le calcul précédent : $\deg(R'_1) \leq \max(\deg(P'Q), \deg(PQ')) - 2\deg(Q) < d + e - 2e$. $\square$



si $\deg R = 0$, on peut juste dire $\deg R' < \deg R - 1$, car avec les notations de la démonstration on a $e = d$.

Exemple 1.3.8.

- si $R = 1$, $\deg R' = -\infty$.
- si $R = \frac{1}{X}$, $R' = -\frac{1}{X^2}$ donc $\deg R' = \deg R - 1$.
- si $R = \frac{X}{X+1} = 1 - \frac{1}{X+1}$, $R' = \frac{1}{(X+1)^2}$, donc $\deg R' = \deg R - 2$.
- De manière générale, si $n \in \mathbb{N}^*$ et $R = \frac{X^n}{X^n + 1}$, alors $\deg R' = \deg R - (n + 1)$.

1.4 Zéros et pôles.

Définition 1.4.1.

Soit $R = \frac{A}{B}$, irréductible.

1. Toute racine de A est appelée *racine* ou *zéro* de R . Si elle est de multiplicité m dans A , on dira aussi qu'elle est de multiplicité m dans R .
2. Toute racine de B est appelée *pôle* de R . Si elle est de multiplicité m dans B , on dira aussi qu'elle est de multiplicité m dans R .

On utilise les expressions *pôle ou racine simple* ou *double* quand la multiplicité vaut 1 ou 2.



À nouveau, la multiplicité n'est bien définie que si la fraction est irréductible : 1 n'a pas la même multiplicité dans les dénominateurs de $\frac{X(X-1)}{(X-1)^2}$ et $\frac{X}{X-1}$. De plus 1 n'est pas racine de ces fractions rationnelles, car 1 n'est pas racine de la forme irréductible.

En allant encore plus loin, soit $R = \frac{A}{B}$ une fraction rationnelle. Alors $R = \frac{A(X-\lambda)^n}{B(X-\lambda)^n}$, et ce

pour tous $\lambda \in \mathbb{K}$ et $n \in \mathbb{N}$. Donc, si on oubliait l'hypothèse « forme irréductible », on pourrait montrer que tout scalaire est racine et pôle de toute fraction rationnelle, avec n'importe quelle multiplicité.

Remarque 1.4.2.

On pourra, si besoin, considérer la convention suivante : un scalaire est racine (resp. pôle) de multiplicité zéro de $R = A/B$ s'il n'est pas racine de A (resp. B).

2 Étude locale d'une fraction rationnelle.

2.1 Partie entière.

Théorème 2.1.1.

Soit $R \in \mathbb{K}(X)$. Alors il existe un unique couple $(E, Q) \in \mathbb{K}[X] \times \mathbb{K}(X)$ tel que $\deg Q < 0$ et $R = E + Q$. Le polynôme E est appelé la *partie entière* de R .

Démonstration.

On note $R = \frac{A}{B}$.

Existence On effectue la division euclidienne de A par B , qui donne $A = EB + T$, avec $\deg T < \deg B$. Ainsi $R = \frac{EB + T}{B} = E + Q$, avec $Q = \frac{T}{B}$: on a bien $\deg Q < 0$.

Unicité Soient (E, Q) et (D, U) deux couples convenables. Alors $E + Q = D + U$, soit $E - D = U - Q$. Si $E - D \neq 0$, on a $\deg(E - D) \geq 0$. Or $\deg(U - Q) \leq \max(\deg Q, \deg U) < 0$. Ceci est contradictoire, donc $E - D = 0$, i.e. $E = D$. Il s'ensuit que $Q = U$. $\square$

Exemple 2.1.2.

Après division euclidienne, on obtient $\frac{X^6 + X^3 + X^2 - 1}{X^2 + 3} = X^4 - 3X^2 + X + 10 + \frac{-3X - 31}{X^2 + 3}$, et ainsi la partie entière de $\frac{X^6 + X^3 + X^2 - 1}{X^2 + 3}$ est $X^4 - 3X^2 + X + 10$.

2.2 Partie polaire associée à un pôle.

Définition 2.2.1.

Soit $m \in \mathbb{N}$, $R \in \mathbb{K}(X)$, et λ un pôle de R de multiplicité m . Alors il existe une unique famille $a_1, \dots, a_m \in \mathbb{K}$ et une unique fraction rationnelle S n'ayant pas λ pour pôle vérifiant

$$R = \sum_{k=1}^m \frac{a_k}{(X - \lambda)^k} + S.$$

La somme $\sum_{k=1}^m \frac{a_k}{(X - \lambda)^k}$ est appelée *partie polaire de R associée au pôle λ* .

De plus :

1. le coefficient a_m est non nul ;
2. les autres pôles de R sont exactement les pôles de S , avec la même multiplicité.

Démonstration.

Hors-programme. $\square$

Exemple 2.2.2.

Par exemple, il existe $a, b, c \in \mathbb{R}$ et $P \in \mathbb{K}[X]$ uniques tels que

$$\frac{X+1}{(X-1)^3(X-2)^2} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{(X-1)^3} + \frac{P}{(X-2)^2}$$

2.3 Décomposition en éléments simples dans $\mathbb{C}(X)$.

Théorème 2.3.1 (Décomposition dans $\mathbb{C}(X)$).

Soit $R \in \mathbb{C}(X)$. Alors R est la somme de sa partie entière et de ses parties polaires. Cette décomposition s'appelle la *décomposition en éléments simples de R* .

Plus précisément : si $\lambda_1, \dots, \lambda_n$ sont les pôles de R , de multiplicités respectives $m_1, \dots, m_n$, alors il existe une unique famille d'éléments de $\mathbb{C}$ $a_{1,1}, \dots, a_{1,m_1}, \dots, a_{n,1}, \dots, a_{n,m_n}$ (le premier indice représentant le pôle et le second indice allant de 1 à la multiplicité de ce pôle), vérifiant

$$R = E + \sum_{k=1}^n \left(\sum_{j=1}^{m_k} \frac{a_{k,j}}{(X - \lambda_k)^j} \right)$$

où E est la partie entière de R .

Démonstration.

Hors programme. $\square$

Exemple 2.3.2.

$\frac{X^5 + X^2 - 3}{(X-1)^3(X-2)^2}$ s'écrit de manière unique sous la forme

$$1 + \frac{a_1}{X-1} + \frac{a_2}{(X-1)^2} + \frac{a_3}{(X-1)^3} + \frac{b_1}{X-2} + \frac{b_2}{(X-2)^2}$$

2.4 Décomposition en éléments simples dans $\mathbb{R}(X)$.

Dans $\mathbb{R}(X)$, le dénominateur d'une fraction rationnelle n'est pas nécessairement scindé ce qui complique la décomposition en éléments simples des fractions rationnelles. Nous commençons par donner un énoncé valable à la fois dans $\mathbb{C}(X)$ et $\mathbb{R}(X)$ et nous verrons ensuite ce qu'il donne dans le cas particulier de $\mathbb{C}(X)$.

Théorème 2.4.1 (Décomposition dans $\mathbb{K}(X)$).

Soit $R \in \mathbb{K}(X)$. R s'écrit sous forme irréductible $\frac{P}{Q}$ avec Q unitaire. Le polynôme Q s'écrit alors sous la forme $H_1^{n_1} \dots H_p^{n_p}$ où $H_1, \dots, H_p$ sont des polynômes irréductibles unitaires distincts et $n_1, \dots, n_p$ des naturels non nuls.

Alors R se décompose de façon unique sous la forme

$$R = E + F_1 + \dots + F_p$$

où E est un polynôme et pour tout $k \in \llbracket 1, p \rrbracket$, F_k s'écrit sous la forme $\sum_{j=1}^{n_k} \frac{J_{k,j}}{H_k^j}$, où pour tout $j \in \llbracket 1, n_k \rrbracket$, on a $\deg J_{k,j} < \deg H_k$. Cette décomposition s'appelle la *décomposition en éléments simples de R dans $\mathbb{K}(X)$* .

De plus E est nécessairement la partie entière de R .

Démonstration.

Hors programme. $\square$

Remarque 2.4.2. 1. Dans $\mathbb{C}(X)$, les irréductibles sont de degré 1 et les $J_{k,j}$ sont donc tous des polynômes constants : on retrouve l'énoncé donné spécifiquement pour $\mathbb{C}(X)$.

2. Dans $\mathbb{R}(X)$, les irréductibles sont de degré 1 ou 2, d'où l'énoncé qui suit.

Théorème 2.4.3 (Décomposition dans $\mathbb{R}(X)$). Soit $R \in \mathbb{R}(X)$. R s'écrit sous forme irréductible $\frac{P}{Q}$ avec Q unitaire. Le polynôme Q s'écrit alors sous la forme $\prod_{i=1}^q (X - \lambda_i)^{m_i} \times \prod_{i=1}^p H_i^{n_i}$, où $\lambda_1, \dots, \lambda_q$ sont les racines (deux à deux distinctes) de Q et $H_1, \dots, H_p$ sont des polynômes de degré deux sans racines réelles.

Alors R se décompose de façon unique sous la forme

$$R = E + \sum_{k=1}^q \sum_{j=1}^{m_k} \frac{a_{k,j}}{(X - \lambda_k)^j} + \sum_{k=1}^p \sum_{j=1}^{n_k} \frac{b_{k,j}X + c_{k,j}}{H_k^j}$$

où E est un polynôme et tous les $a_{k,j}$, les $b_{k,j}$ et les $c_{k,j}$ sont des réels.

Cette décomposition s'appelle la *décomposition en éléments simples de R dans $\mathbb{R}(X)$* .

De plus E est nécessairement la partie entière de R .

2.5 Quelques méthodes de calcul.

L'objectif est d'obtenir le plus rapidement possible la décomposition en éléments simples d'une fraction rationnelle, bien entendu sans faire d'erreurs de calculs. Il est donc *fortement conseillé* de suivre les méthodes suivantes, en essayant d'utiliser les méthodes les plus appropriées dans le contexte.

Enfin, si vous en avez le temps, pensez bien à vérifier vos calculs, par exemple en recomposant la fraction rationnelle.

a Avant même de commencer.

Pour décomposer une fraction rationnelle F , on commence par l'écrire sous forme $E + R$ où $\deg R < 0$ et E est sa partie entière.

Toutes les méthodes ci-dessous s'appliquent à la fraction rationnelle R qui est de degré strictement négatif.

b Simplification par symétrie, parité et imparité.

Il convient à chaque fois de simplifier au maximum le problème posé en réduisant le nombre de coefficients à chercher. Pour cela, on exploite les symétries repérées dans la fraction rationnelle.

Traitions un exemple : la fraction rationnelle

$$R = \frac{1}{(X-1)^2(X+1)^2}$$

est paire, car $R(-X) = R(X)$. Mais on sait qu'il existe $a, b, c, d \in \mathbb{R}$ tels que

$$R = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1} + \frac{d}{(X+1)^2}.$$

Et donc

$$R(-X) = -\frac{a}{X+1} + \frac{b}{(X+1)^2} - \frac{c}{X-1} + \frac{d}{(X-1)^2}.$$

Par unicité des coefficients de la décomposition en éléments simples, on en déduit que $a = -c$ et $b = d$: le calcul de a et b suffit donc (deux coefficients au lieu de quatre !).

On a la même chose avec les fractions rationnelles impaires.

On pourra aussi exploiter d'autres types de symétries. En voici un exemple : $F = \frac{1}{X(X-1)}$. Les pôles (0 et 1) sont « symétriques » par rapport à $\frac{1}{2}$, ce qui se voit par $F(X) = F(1-X)$. Si l'on écrit $F = \frac{\alpha}{X} + \frac{\beta}{X-1}$, on obtient alors $F(1-X) = \frac{-\beta}{X} + \frac{-\alpha}{X-1}$, ce qui donne $\alpha = -\beta$.

c Simplification par conjugaison de fractions rationnelles réelles.

Soit $R \in \mathbb{R}(X)$, et soit $\lambda \in \mathbb{C} \setminus \mathbb{R}$ un pôle complexe non réel de R , de multiplicité m . Alors $\bar{\lambda}$ est aussi un pôle de R de multiplicité m . On a donc :

$$R = \frac{a_1}{X - \lambda} + \frac{a_2}{(X - \lambda)^2} + \dots + \frac{a_m}{(X - \lambda)^m} + \frac{b_1}{X - \bar{\lambda}} + \frac{b_2}{(X - \bar{\lambda})^2} + \dots + \frac{b_m}{(X - \bar{\lambda})^m} + G,$$

où G n'admet ni λ ni $\bar{\lambda}$ pour pôle. Mais on a $\bar{R} = R$, et donc

$$\begin{aligned} \bar{R} &= \frac{\bar{a}_1}{X - \bar{\lambda}} + \frac{\bar{a}_2}{(X - \bar{\lambda})^2} + \dots + \frac{\bar{a}_m}{(X - \bar{\lambda})^m} \\ &+ \frac{\bar{b}_1}{X - \lambda} + \frac{\bar{b}_2}{(X - \lambda)^2} + \dots + \frac{\bar{b}_m}{(X - \lambda)^m} + \bar{G}. \end{aligned}$$

Par unicité des coefficients on obtient donc : $a_1 = \bar{b}_1, \dots, a_m = \bar{b}_m$ et $G = \bar{G}$ (i.e. $G \in \mathbb{R}(X)$). Là encore, cela permet de réduire le nombre de coefficients à calculer.

d Méthode de base.

Soit $R = \frac{A}{B}$ avec $\deg R < 0$ à décomposer, avec A et B deux polynômes non nuls, B étant de la forme $C \times (X - \lambda)^m$ où λ n'est pas racine de C .

R s'écrit $\sum_{k=1}^m \frac{a_k}{(X - \lambda)^k} + S$. On peut trouver le coefficient a_m (et seulement celui-là !) en multipliant R par $(X - \lambda)^m$ et en évaluant le résultat en λ .

En effet, on a

$$\begin{aligned} \frac{A}{C} &= (X - \lambda)^m R \\ &= \sum_{k=1}^m a_k (X - \lambda)^{m-k} + (X - \lambda)^m S \\ &= \sum_{h=0}^{m-1} a_{m-h} (X - \lambda)^h + (X - \lambda)^m S \\ &= a_m + \sum_{h=1}^{m-1} a_{m-h} (X - \lambda)^h + (X - \lambda)^m S \end{aligned}$$

D'où :

$$\frac{A(\lambda)}{C(\lambda)} = a_m + 0$$

On a donc trouvé a_m :

$$a_m = \frac{A(\lambda)}{C(\lambda)}$$

On calcule alors $T = R - \frac{a_m}{(X - \lambda)^m}$, et on continue en cherchant à décomposer T .

Remarque 2.5.1.

On a la garantie que, soit λ n'est pas pôle de T (c'est le cas si $m = 1$ ou si les coefficients $a_1, \dots, a_{m-1}$ sont tous nuls), soit λ est pôle pour T de multiplicité strictement plus petite que m . En itérant l'algorithme on va donc terminer la décomposition pour la partie polaire associée à λ . On peut s'intéresser ensuite à un autre pôle, soit en partant de la dernière fraction obtenue, soit en repartant de la fraction initiale.

Remarque 2.5.2 (Cas d'un pôle simple).

Dans le cas où $m = 1$, on a

$$a_1 = \frac{A(\lambda)}{C(\lambda)}$$

Si on ne connaît pas C mais juste B , plutôt que factoriser B par $X - \lambda$, on peut remarquer $B' = (X - \lambda)C' + C$, donc $B'(\lambda) = C(\lambda)$, donc

$$a_1 = \frac{A(\lambda)}{B'(\lambda)}$$

Il est souvent plus simple dans des exercices abstraits de calculer B' , plutôt que de décomposer B en $(X - \lambda)C$, d'où l'intérêt de cette remarque.

Exemple 2.5.3.

Si

$$R = \frac{X^2 - X - 2}{4X^{10} - X^8 + 6X^3 - 9X^2 + 3X - 3} = \frac{A}{B}.$$

On remarque que $B(1) = 0$, mais

$$\begin{aligned} B'(1) &= (40X^9 - 8X^7 + 18X^2 - 18X + 3)(1) \\ &= 35 \\ &\neq 0, \end{aligned}$$

donc 1 est pôle simple de R . Or

$$\frac{A(1)}{B'(1)} = \frac{-2}{35},$$

donc $R = -\frac{2/35}{X - 1} + S$, et S n'a pas 1 pour pôle.

Remarque 2.5.4.

La méthode de base est **celle à privilégier** car elle fonctionne dans tous les cas et est souvent la plus rapide. Mais on peut la conjuguer ponctuellement à d'autres méthodes pour accélérer les calculs.

e Résidus.

Soit λ un pôle de R : on appelle *résidu* de R en λ le coefficient du terme $\frac{1}{X-\lambda}$. C'est en pratique le terme de la partie polaire associée à λ le plus compliqué à calculer, car c'est le dernier terme que l'on peut calculer avec la méthode de base. On note ce résidu $\text{Res}(R, \lambda)$, et on note R_λ la partie polaire de R associée au pôle λ .

Alors, quelle que soit la multiplicité de λ , on a :

$$xR_\lambda(x) \xrightarrow{x \rightarrow +\infty} \text{Res}(R, \lambda).$$

En sommant cette relation sur tous les pôles de R , on obtient, dans le cas où $\lim_{x \rightarrow +\infty} xR(x)$ est finie (*i.e.* $\deg R \leq -1$) :

$$xR(x) \xrightarrow{x \rightarrow +\infty} \sum_{\lambda \text{ pôle de } R} \text{Res}(R, \lambda)$$

Ainsi, si $\deg R \leq -2$, on a

$$\sum_{\lambda \text{ pôle de } R} \text{Res}(R, \lambda) = 0.$$

Par exemple, si

$$\begin{aligned} R &= \frac{1}{(X-1)^2(X+1)} \\ &= \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1}, \end{aligned}$$

on a $c = \frac{1}{(-1-1)^2} = \frac{1}{4}$, et $b = \frac{1}{(1+1)} = \frac{1}{2}$.

Mais $xR(x) \xrightarrow{x \rightarrow +\infty} 0$, donc $a + c = 0$, et ainsi

$$a = -\frac{1}{4}.$$

f Un exemple.

Exercice 2.5.5.

Décomposer en éléments simples sur $\mathbb{R}$:

$$R = \frac{2X}{X^5 - 7X^4 + 16X^3 - 16X^2 + 15X - 9}.$$

Les méthodes suivantes sont souvent peu efficaces (pour les deux premières) ou hors de votre portée pour l'instant (pour la troisième).

g Évaluation en un point différent d'un pôle.

Si nous avons n coefficients à calculer, on peut écrire l'égalité entre la fraction rationnelle et sa décomposition (aux coefficients inconnus) et évaluer les deux membres de cette égalité en n points deux à deux distincts qui ne sont pas des pôles. On obtient alors n équations à n inconnues qui permettent de calculer les n coefficients voulus.

Cette méthode est surtout efficace quand il ne reste qu'un (ou deux) coefficients à calculer, qui ne sont pas des coefficients associés à des pôles simples, sinon la méthode de base est plus rapide.

Par exemple, décomposons

$$\frac{X-2}{(X+1)(X+2)^3}$$

sous la forme

$$\frac{a}{X+1} + \frac{b}{(X+2)^3} + \frac{c}{(X+2)^2} + \frac{d}{X+2}.$$

La méthode de base nous donne immédiatement $a = -3$ et $b = 4$. Par ailleurs, la méthode des résidus nous donne $a + d = 0$, donc $d = 3$.

En évaluant alors, par exemple en 2, on obtient :

$$\begin{aligned} 0 &= \frac{-3}{2+1} + \frac{4}{(2+2)^3} + \frac{c}{(2+2)^2} + \frac{3}{2+2} \\ &= \frac{-3}{16} + \frac{c}{16} \end{aligned}$$

d'où $c = 3$.

On aurait bien sûr pu évaluer en un autre point, par exemple, en évaluant en -3 , on obtient :

$$\frac{-5}{2} = \frac{-3}{-2} + \frac{4}{-1} + \frac{c}{1} + \frac{3}{-1}$$

d'où $c = 3$.

h Identification.

C'est la méthode la plus naïve, mais elle doit vraiment être réservée au cas où la fraction rationnelle a au plus deux ou trois pôles avec multiplicité, sinon elle est trop lourde.

Par exemple on sait qu'il existe $a, b \in \mathbb{R}$ tels que $\frac{1}{X(X+1)} = \frac{a}{X} + \frac{b}{X+1}$. Or $\frac{a}{X} + \frac{b}{X+1} = \frac{(a+b)X+a}{X(X+1)}$, donc on doit avoir $a+b=0$ et $a=1$, soit $a=1$ et $b=-1$.

i Développements limités.

Prenons l'exemple d'une fraction rationnelle R admettant un pôle double.

Alors $R = \frac{a}{X - \lambda} + \frac{b}{(X - \lambda)^2} + G$, où G est une fraction rationnelle n'admettant pas λ pour pôle.

Pour h au voisinage épointé de 0,

$$h^2 R(\lambda + h) = b + ah + h^2 G(\lambda + h)$$

Or G n'a pas pour pôle λ , donc G est bornée au voisinage de λ .

Donc $h^2 R(\lambda + h)$ admet le développement limité $b + ah + o(h)$ pour h au voisinage de 0. Les développements limités étant uniques (sous réserve d'existence), il suffit de calculer le développement limité de $h^2 R(\lambda + h)$ pour obtenir a et b .

Cette méthode s'applique aussi très bien à des pôles de multiplicité supérieure à 2, quitte à développer assez loin.

Par exemple posons

$$R = \frac{3X - 1}{(X - 1)^2(X^2 + 1)}$$

et cherchons la partie polaire de R associée à 1. Pour h au voisinage de 0,

$$\begin{aligned} h^2 R(1 + h) &= \frac{3(h + 1) - 1}{(h + 1)^2 + 1} \\ &= \frac{3h + 2}{2 + 2h + h^2} \\ &= \frac{1}{2} \cdot \frac{3h + 2}{1 + h + h^2/2} \\ &= \frac{1}{2} (3h + 2)(1 - h + o(h)) \\ &= \frac{1}{2} (3h + 2 - 2h + o(h)) \\ &= 1 + h/2 + o(h) \end{aligned}$$

donc la partie polaire associée à 1 est

$$\frac{1}{2(X - 1)} + \frac{1}{(X - 1)^2}.$$

2.6 Décomposition de P'/P .

Proposition 2.6.1.

Soit $P \in \mathbb{C}[X]$ un polynôme non nul. Alors, en notant $a_1, \dots, a_n$ les n racines distinctes de P et $r_1, \dots, r_n$ leurs ordres respectifs, on a

$$\frac{P'}{P} = \sum_{k=1}^n \frac{r_k}{X - a_k}.$$

Démonstration.

Remarquons tout d'abord que $\frac{P'}{P}$ est de degré strictement négatif, donc sa partie entière est nulle.

Les seuls pôles possibles pour $\frac{P'}{P}$ sont les racines de P . Soit a une racine de P ; notons r sa multiplicité. Alors P s'écrit $(X - a)^r A$ où A est un polynôme dont a n'est pas racine. Alors on a

$$\begin{aligned} \frac{P'}{P} &= \frac{r(X - a)^{r-1} A + (X - a)^r A'}{(X - a)^r A} \\ &= \frac{r}{X - a} + \frac{A'}{A} \end{aligned}$$

et a n'est pas un pôle de $\frac{A'}{A}$. Donc $\frac{r}{X - a}$ est la partie polaire de $\frac{P'}{P}$ associée au pôle a (a est donc un pôle simple).

$\frac{P'}{P}$ étant la somme de sa partie entière et de ses parties polaires, on en déduit le résultat. $\square$

Proposition 2.6.2.

Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors P s'écrit

$$\lambda \prod_{k=1}^n H_k^{p_k},$$

où $\lambda \in \mathbb{R}$ et où les H_k , pour $k = 1, \dots, n$ sont des polynômes irréductibles deux à deux distincts et $p_1, \dots, p_k$ sont des entiers naturels non nuls.

Alors

$$\frac{P'}{P} = \sum_{k=1}^n \frac{p_k H'_k}{H_k}.$$

Cet énoncé est une simple généralisation de l'énoncé précédent. Il est en fait vrai dans $\mathbb{R}(X)$ comme dans $\mathbb{C}(X)$.

Démonstration.

Remarquons tout d'abord que $\frac{P'}{P}$ est de degré strictement négatif, donc sa partie entière est nulle.

Les seuls facteurs irréductibles du dénominateur sont les H_k , pour $k = 1, \dots, n$, donc ce sont les seuls à considérer pour décomposer $\frac{P'}{P}$.

Soit $k \in \llbracket 1, n \rrbracket$. Alors P s'écrit $H_k^{p_k} A_k$, où A_k est un polynôme dont H_k n'est pas un facteur. Alors on a

$$\begin{aligned} \frac{P'}{P} &= \frac{p_k H_k' H_k^{p_k-1} A_k + H_k^{p_k} A_k'}{H_k^{p_k} A_k} \\ &= \frac{p_k H_k'}{H_k} + \frac{A_k'}{A_k} \end{aligned}$$

et H_k n'est pas un facteur de A_k . Donc $\frac{p_k H_k'}{H_k}$ est la partie de la décomposition de $\frac{P'}{P}$ associée au facteur H_k .

$\frac{P'}{P}$ étant la somme de sa partie entière et des parties associées aux facteurs irréductibles du dénominateur, on en déduit le résultat. $\square$

3 Application au calcul intégral.

On va voir ici comment la décomposition en éléments simples permet de calculer $\int^x R(t) dt$, où $R \in \mathbb{K}(X)$, mais aussi de calculer simplement les $R^{(k)}$.

3.1 Si $\mathbb{K} = \mathbb{C}$

C'est le cas le plus simple. On commence par décomposer R en éléments simples. Il suffit alors de savoir intégrer les polynômes ainsi que toute fonction de la forme $t \mapsto \frac{1}{(t-\lambda)^k}$, avec $k \in \mathbb{N}^*$. Traitons différents cas :

Si $k = 1$ on sépare alors la partie réelle et la partie imaginaire de $\frac{1}{(t-\lambda)^k}$, puis on intègre.

Si on note $\lambda = \alpha + i\beta$, cela donne :

$$\begin{aligned} \frac{1}{t-\lambda} &= \frac{t-\alpha+i\beta}{(t-\alpha)^2+\beta^2} \\ &= \frac{t-\alpha}{(t-\alpha)^2+\beta^2} + \frac{i\beta}{(t-\alpha)^2+\beta^2}. \end{aligned}$$

Or

$$\begin{aligned} \int^x \frac{t-\alpha}{(t-\alpha)^2+\beta^2} dt &= \frac{1}{2} \ln((x-\alpha)^2+\beta^2) \\ \text{et } \int^x \frac{\beta}{(t-\alpha)^2+\beta^2} dt &= \text{Arctan}\left(\frac{x-\alpha}{\beta}\right). \end{aligned}$$

Si $k > 1$ alors

$$\int^x \frac{1}{(t-\lambda)^k} dt = -\frac{1}{k-1} \times \frac{1}{(x-\lambda)^{k-1}}.$$

3.2 Si $\mathbb{K} = \mathbb{R}$

Il s'agit de savoir intégrer d'une part les $\frac{1}{(t-\lambda)^k}$, ce qu'on sait déjà faire et d'autre part les termes de la forme $t \mapsto \frac{at+b}{(t^2+\beta t+\gamma)^n}$ où a , b , β et γ sont des constantes réelles, où n est un naturel non nul et où le polynôme $X^2+\beta X+\gamma$ n'admet pas de racine réelle.

On se limitera au cas où $n = 1$. Pour gérer les autres cas, on peut décomposer R en éléments simple dans $\mathbb{C}(X)$ et calculer l'intégrale par les méthodes données ci-dessus.

En posant $\Delta = \beta^2 - 4\gamma$, on a donc $\Delta < 0$.

On écrit alors

$$\frac{at+b}{t^2+\beta t+\gamma} = \frac{a}{2} \frac{2t+\beta}{t^2+\beta t+\gamma} + \frac{b-\frac{a\beta}{2}}{t^2+\beta t+\gamma}.$$

Le premier terme est un rapport de la forme u'/u :

$$\int^x \frac{a}{2} \frac{2t+\beta}{t^2+\beta t+\gamma} dt = \frac{a}{2} \ln|x^2+\beta x+\gamma|$$

et la valeur absolue s'enlève sans problème car $X^2+\beta X+\gamma$ étant irréductible, il n'a pas de racine et est donc de signe constant.

Le second terme se réécrit quant à lui

$$\frac{b-\frac{a\beta}{2}}{t^2+\beta t+\gamma} = \frac{b-\frac{a\beta}{2}}{(t+\beta/2)^2+(\gamma-\beta^2/4)}.$$

Or, comme $\Delta < 0$,

$$\gamma - \beta^2/4 = -\Delta/4 = \left(\frac{1}{2}\sqrt{-\Delta}\right)^2.$$

En posant alors $\theta = \frac{1}{2}\sqrt{-\Delta}$, on a $\theta > 0$ et

$$\int^x \frac{b-\frac{a\beta}{2}}{(t+\beta/2)^2+\theta^2} dt = \frac{b-\frac{a\beta}{2}}{\theta} \text{Arctan}\left(\frac{x+\beta/2}{\theta}\right)$$

Remarque 3.2.1.

Ces formules ne sont en aucun cas à apprendre par cœur, mais il convient de savoir mener ces calculs sur des exemples concrets.

Chapitre XIX

Espaces vectoriels

Sommaire

1	Espaces vectoriels et combinaisons linéaires.	284
1.1	Définitions.	284
1.2	Règles de calcul.	284
1.3	Exemples.	285
1.4	Combinaisons linéaires.	286
2	Sous-espaces vectoriels.	286
2.1	Définitions.	286
2.2	Exemples.	287
2.3	Opérations sur les sous-espaces vectoriels.	288
a	Intersection.	288
b	Sous-espace vectoriel engendré par une partie.	288
c	Sous-espace vectoriel engendré par une famille finie.	290
d	Somme.	291
2.4	Somme directe et supplémentaires.	291
3	Translations, sous-espaces affines.	293
3.1	Translations.	293
3.2	Sous-espaces affines.	293
3.3	Barycentres (hors programme)	294
3.4	Convexité (hors programme)	296

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'important est que $\mathbb{K}$ soit un corps, mais le programme se limite à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 Espaces vectoriels et combinaisons linéaires.

1.1 Définitions.

Définition 1.1.1.

On appelle $\mathbb{K}$ -*espace vectoriel* ou *espace vectoriel sur $\mathbb{K}$* (noté $\mathbb{K}$ -ev) tout triplet $(E, +, \cdot)$ où E est un ensemble muni d'une loi interne $+$ appelée addition et d'une loi externe $\cdot$, i.e. une application $\cdot : \mathbb{K} \times E \rightarrow E$, vérifiant :

- (i) $(E, +)$ est un groupe commutatif dont le neutre est noté 0 ;
- (ii) En notant 1 (ou $1_{\mathbb{K}}$) le neutre de $\mathbb{K}$ pour la multiplication, on a $\forall x \in E \quad 1 \cdot x = x$;
- (iii) $\forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall x \in E \quad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$ (distributivité à droite) ;
- (iv) $\forall \lambda \in \mathbb{K} \quad \forall x, y \in E \quad \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$ (distributivité à gauche) ;
- (v) $\forall \lambda, \mu \in \mathbb{K} \quad \forall x \in E \quad (\lambda \times \mu) \cdot x = \lambda \cdot (\mu \cdot x)$ (associativité mixte).

Les éléments de E sont appelés *vecteurs*, et ceux de $\mathbb{K}$ sont appelés *scalaires*.

Remarque 1.1.2.

Les vecteurs mathématiques étant des objets mathématiques comme les autres, on ne les marquera plus d'une flèche comme c'est traditionnellement l'usage dans le secondaire (cet usage est d'ailleurs réservé à la géométrie euclidienne, alors qu'on verra de nombreux exemples d'espaces vectoriels où les vecteurs ne sont ni ceux du plan, ni ceux de l'espace euclidien).

Remarque 1.1.3.

On omet souvent, pour alléger les notations, de noter le $\cdot$ de la multiplication scalaire. Ainsi, on pourra écrire λx au lieu de $\lambda \cdot x$, pour un scalaire λ et un vecteur x .

Exemple 1.1.4. 1. L'ensemble des vecteurs du plan euclidien, celui des vecteurs de l'espace

euclidien, ou de façon équivalente¹ $(\mathbb{R}^2, +, \cdot)$ et $(\mathbb{R}^3, +, \cdot)$, d'où les mots «vecteur» et «scalaire». De manière générale, tous les $\mathbb{R}^n$.

- 2. $(\mathbb{R}, +, \times)$ est un $\mathbb{R}$ -espace vectoriel. Remarquez que la loi $\times$ est à la fois loi interne et externe sur $\mathbb{R}$ (c'est aussi un $\mathbb{Q}$ -espace vectoriel).
- 3. $(\mathbb{C}, +, \times)$ est à la fois un $\mathbb{C}$ -espace vectoriel et un $\mathbb{R}$ -espace vectoriel (et également un $\mathbb{Q}$ -espace vectoriel).
- 4. $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ ne sont pas des espaces vectoriels ni sur $\mathbb{R}$ ni sur $\mathbb{C}$ avec les opérations usuelles².
- 5. $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{R}(X)$ et $\mathbb{C}(X)$ sont des espaces vectoriels (sur quels corps ?)
- 6. $\mathcal{M}_{n,p}(\mathbb{K})$ est un $\mathbb{K}$ -ev.

Remarque 1.1.5.

Tout $\mathbb{C}$ -espace vectoriel est aussi un $\mathbb{R}$ -espace vectoriel. La réciproque est fautive : $\mathbb{R}$ n'est pas un $\mathbb{C}$ -espace vectoriel, du moins pas avec les lois usuelles³.

Dans toute la suite, $(E, +, \cdot)$ désigne un $\mathbb{K}$ -ev.

1.2 Règles de calcul.

Théorème 1.2.1 (Règles de calcul).

Soit $\lambda \in \mathbb{K}$ et $x \in E$.

- (i) $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0_{\mathbb{K}}$ ou $x = 0_E$ et, en particulier, $0_{\mathbb{K}} \cdot x = 0_E$ et $\lambda \cdot 0_E = 0_E$.
- (ii) $-x = (-1) \cdot x$ (l'opposé de x dans $(E, +)$ est égal à l'opposé de 1 dans $(\mathbb{K}, +, \times)$ multiplié par x).

Démonstration. (i) (a) Remarquons tout d'abord qu'on a $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$ et donc par simplification dans $(E, +)$, donc $0 \cdot x = 0$.

1. Il conviendrait, en anticipant un peu, de dire plutôt : «de façon isomorphe».

2. En fait, c'est même vrai quelle que soit la loi qu'on essaie d'y définir. Pourquoi ?

3. Il y aurait moyen d'en définir une, qui serait complètement «tordue» en utilisant le fait que $\mathbb{R}$ et $\mathbb{C}$ peuvent être mis en bijection mais ça n'aurait vraisemblablement aucun intérêt.

(b) Remarquons ensuite qu'on a $\lambda \cdot 0 = \lambda(0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$, d'où $\lambda \cdot 0 = 0$.

(c) On en déduit $\lambda = 0_{\mathbb{K}}$ ou $x = 0_E \Rightarrow \lambda \cdot x = 0_E$.

(d) Réciproquement, supposons $\lambda \cdot x = 0$. Alors, si $\lambda \neq 0$, on a $x = 1 \cdot x = \left(\lambda \times \frac{1}{\lambda}\right) \cdot x = \frac{1}{\lambda} \cdot (\lambda \cdot x) = \frac{1}{\lambda} \cdot 0 = 0$

(ii) On a $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 - 1) \cdot x = 0 \cdot x = 0$. Donc $(-1) \cdot x$ est bien l'opposé de x dans $(E, +)$. $\square$

1.3 Exemples.

Théorème 1.3.1 (Espace vectoriel produit).

Soient $n \in \mathbb{N}^*$ et $(E_1, +_1, \cdot_1) \dots (E_n, +_n, \cdot_n)$ des $\mathbb{K}$ -ev. On considère l'ensemble produit $E = E_1 \times \dots \times E_n$ que l'on munit des deux lois $+$: $E \times E \rightarrow E$ et $\cdot$: $\mathbb{K} \times E \rightarrow E$ définies, par les relations suivantes pour toutes familles $(x_k)_{k \in [1, n]}$ et $(y_k)_{k \in [1, n]}$ et tout $\lambda \in \mathbb{K}$:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 +_1 y_1, \dots, x_n +_n y_n) \\ \lambda \cdot (x_1, \dots, x_n) = (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n)$$

Alors, $(E, +, \cdot)$ est un $\mathbb{K}$ -ev appelé *espace vectoriel produit*.

Démonstration.

Il suffit de vérifier les 5 points de la définition d'espace vectoriel :

- (i) $(E, +)$ est un groupe (cf. exercices sur les groupes produits vu en TD), et commutatif car tous les E_i le sont.
- (ii) Soit $(x_1, \dots, x_n) \in E$, on a $1 \cdot (x_1, \dots, x_n) = (1 \cdot_1 x_1, \dots, 1 \cdot_n x_n) = (x_1, \dots, x_n)$.
- (iii) Soit $(\lambda, \mu) \in \mathbb{K}^2$, $(x_1, \dots, x_n) \in E$. En posant

$$z = (\lambda + \mu) \cdot (x_1, \dots, x_n)$$

on a successivement :

$$\begin{aligned} z &= ((\lambda + \mu) \cdot_1 x_1, \dots, (\lambda + \mu) \cdot_n x_n) \\ &= (\lambda \cdot_1 x_1 + \mu \cdot_1 x_1, \dots, \lambda \cdot_n x_n + \mu \cdot_n x_n) \\ &= (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n) + (\mu \cdot_1 x_1, \dots, \mu \cdot_n x_n) \\ &= \lambda \cdot (x_1, \dots, x_n) + \mu \cdot (x_1, \dots, x_n). \end{aligned}$$

- (iv) Soit $\lambda \in \mathbb{K}$, $(x_1, \dots, x_n) \in E$ et $(y_1, \dots, y_n) \in E$. En posant

$$z = \lambda \cdot (x_1 +_1 y_1, \dots, x_n +_n y_n)$$

on a successivement :

$$\begin{aligned} z &= (\lambda \cdot (x_1 +_1 y_1), \dots, \lambda \cdot (x_n +_n y_n)) \\ &= (\lambda \cdot_1 x_1 + \lambda \cdot_1 y_1, \dots, \lambda \cdot_n x_n + \lambda \cdot_n y_n) \\ &= (\lambda \cdot_1 x_1, \dots, \lambda \cdot_n x_n) + (\lambda \cdot_1 y_1, \dots, \lambda \cdot_n y_n) \\ &= \lambda \cdot (x_1, \dots, x_n) + \lambda \cdot (y_1, \dots, y_n). \end{aligned}$$

- (v) Soit $(\lambda, \mu) \in \mathbb{K}^2$ et $(x_1, \dots, x_n) \in E$. On a successivement :

$$\begin{aligned} (\lambda \times \mu) \cdot (x_1, \dots, x_n) &= ((\lambda \times \mu) \cdot_1 x_1, \dots, (\lambda \times \mu) \cdot_n x_n) \\ &= (\lambda \cdot_1 (\mu \cdot_1 x_1), \dots, \lambda \cdot_n (\mu \cdot_n x_n)) \\ &= \lambda \cdot (\mu \cdot_1 x_1, \dots, \mu \cdot_n x_n) \\ &= \lambda \cdot [\mu \cdot (x_1, \dots, x_n)]. \end{aligned}$$

$\square$

Remarque 1.3.2.

Cas particuliers :

1. Déjà vu : $\mathbb{R}^2$.
2. Se généralise à tous les $\mathbb{R}^n$, $n \in \mathbb{N}^*$. Exemple de calcul dans $\mathbb{R}^6$.

Théorème 1.3.3 (Espaces d'applications).

Soit X un ensemble non vide et E un $\mathbb{K}$ -ev. On considère $\mathcal{F} = E^X$, que l'on munit de deux lois :

$$+ : \begin{cases} \mathcal{F} \times \mathcal{F} & \longrightarrow \mathcal{F} \\ (f, g) & \longmapsto \begin{cases} X & \rightarrow E \\ x & \mapsto f(x) + g(x) \end{cases} \end{cases}$$

et

$$\cdot : \begin{cases} \mathbb{K} \times \mathcal{F} & \longrightarrow \mathcal{F} \\ (\lambda, f) & \longmapsto \begin{cases} X & \rightarrow E \\ x & \mapsto \lambda \cdot (f(x)) \end{cases} \end{cases}.$$

Alors $(\mathcal{F}, +, \cdot)$ est un $\mathbb{K}$ -ev.

Démonstration.

Il suffit de vérifier les 5 points de la définition d'ev. On a déjà vu que $(E^X, +)$ était un groupe commutatif. Le lecteur saura vérifier les points (ii) à (v). $\square$

Exemple 1.3.4. 1. Soit I un intervalle, alors $(\mathbb{R}^I, +, \times)$ est un $\mathbb{R}$ -espace vectoriel, $(\mathbb{C}^I, +, \times)$ est à la fois un $\mathbb{R}$ -espace vectoriel et un $\mathbb{C}$ -espace vectoriel.

2. L'ensemble des suites à valeurs réelles $\mathbb{R}^{\mathbb{N}}$ est un $\mathbb{R}$ -espace vectoriel, celui des suites à valeurs complexes est à la fois un $\mathbb{R}$ -espace vectoriel et un $\mathbb{C}$ -espace vectoriel.

1.4 Combinaisons linéaires.

Définition 1.4.1.

Soient $u_1, \dots, u_n$ des vecteurs de E , avec $n \in \mathbb{N}$. On appelle *combinaison linéaire* de $u_1, \dots, u_n$ tout vecteur de la forme $u = \sum_{k=1}^n \lambda_k \cdot u_k = \lambda_1 \cdot u_1 + \dots + \lambda_n \cdot u_n$, avec $\lambda_1, \dots, \lambda_n \in \mathbb{K}$.

Par convention la combinaison linéaire de 0 vecteur vaut 0_E .

Exemple 1.4.2. 1. 0 est toujours combinaison linéaire de deux vecteurs quelconques u et v car $0_E = 0_{\mathbb{K}}u + 0_{\mathbb{K}}v$.

2. Décomposition dans une base dans le plan ou l'espace.

Remarque 1.4.3.

Attention : il n'y a pas nécessairement unicité des λ_i . Exemple :

$$(1, 1) = 1 \cdot (1, 0) + 1 \cdot (1, 3) + 1 \cdot (-1, -2)$$

$$(1, 1) = \frac{1}{2} \cdot (1, 0) + 0 \cdot (1, 3) - \frac{1}{2} \cdot (-1, -2)$$

Exemple 1.4.4.

Exemples menant, comme souvent, à la résolution d'un système :

1. $(3, -3, 0)$ est-il combinaison linéaire de $(1, 0, 0)$, $(0, -1, 2)$ et $(1, 0, -3)$?
2. $(-1, 2, 3)$ est-il combinaison linéaire de $(1, 1, 0)$ et $(-1, 1, 3)$?
3. $(0, 3+3i)$ est-il combinaison linéaire de $(i, 1-i)$ et $(1-i, 1)$?

Remarque 1.4.5.

Pour la deuxième question, on sait y répondre avec le déterminant. Pour l'instant ce n'est possible que pour les vecteurs du plan mais bientôt... (à suivre).

On peut généraliser la définition précédente au cas des familles quelconques.

Définition 1.4.6.

Soit I un ensemble $(x_i)_{i \in I}$ une famille de vecteurs

indexées par I . On appelle *combinaison linéaire* de la famille $(x_i)_{i \in I}$ tout vecteur de la forme

$$\sum_{i \in I} \lambda_i \cdot x_i$$

où $(\lambda_i)_{i \in I}$ est une famille de scalaire à **support fini** c'est-à-dire telle que l'ensemble des $i \in I$ tels que $\lambda_i \neq 0$ soit **fini**.

Exemple 1.4.7.

Quelles sont les combinaisons linéaires de la famille $(X^k)_{k \in \mathbb{N}}$ dans $\mathbb{R}[X]$? et de la famille $(X^{2k})_{k \in \mathbb{N}}$ dans $\mathbb{R}[X]$?

Remarque 1.4.8 (Opérations sur les combinaisons linéaires).

Une combinaison linéaire de combinaisons linéaires d'une famille de vecteurs est une combinaison linéaire des vecteurs de cette famille.

On montre en effet très simplement les points suivants.

- La somme de deux combinaisons linéaires d'une même famille est encore une combinaison linéaire de cette famille.
- Le produit par un scalaire d'une combinaison linéaire d'une famille est encore une combinaison linéaire de cette famille.

2 Sous-espaces vectoriels.

Dorénavant, nous omettrons d'écrire le $\cdot$ de la multiplication scalaire.

2.1 Définitions.

Définition 2.1.1.

Soit $F \subset E$. On dit que F est un *sous-espace vectoriel* (sev) de E si :

- (i) $0 \in F$;
- (ii) F est stable par combinaisons linéaires quelconques de deux vecteurs, *i.e.* pour tout $\lambda, \mu \in \mathbb{K}$, et pour tous $x, y \in F$, $\lambda x + \mu y \in F$.

Remarque 2.1.2.

Il est clair que tout sous-espace vectoriel est stable par multiplication externe ainsi que par l'addition. Par récurrence, on en déduit que, pour tout $n \in \mathbb{N}$, toute combinaison linéaire de n vecteurs d'un sous-espace vectoriel appartient encore à ce sous-espace vectoriel. Donc tout sous-espace vectoriel est stable par toute combinaison linéaire de ses vecteurs.

Proposition 2.1.3.

Soit $F \subset E$. Toutes les propositions suivantes sont équivalentes :

- (i) F est un sous-espace vectoriel de E ;
- (ii) F est non vide, stable par addition et par multiplication externe ;
- (iii) F est un sous-groupe de E stable par multiplication externe ;
- (iv) F est non vide et $\forall \lambda, \mu \in \mathbb{K} \quad \forall (x, y) \in F^2 \quad \lambda x + \mu y \in F$.
- (v) F est non vide et $\forall \lambda \in \mathbb{K} \quad \forall (x, y) \in F^2 \quad \lambda x + y \in F$;
- (vi) $0_E \in F$ et $\forall \lambda \in \mathbb{K} \quad \forall (x, y) \in F^2 \quad \lambda x + y \in F$.

Démonstration.

On remarque successivement :

- (i) $\Rightarrow$ (ii) Il suffit de prendre $\lambda = 1$ pour la stabilité par addition et $y = 0$ pour la stabilité par multiplication externe.
- (ii) $\Rightarrow$ (iii) Supposons (ii). Alors F est stable par multiplication externe, donc en particulier $\forall x \in F \quad (-1) \cdot x \in F$. Ainsi, F est stable par opposé. Par ailleurs, F est non vide et stable par addition, c'est donc un sous-groupe de E .
- (iii) $\Rightarrow$ (iv) Supposons (iii). Alors F est un sous-groupe donc n'est pas vide. Soit $\lambda, \mu \in \mathbb{K}$ et $(x, y) \in F^2$. F est stable par multiplication externe, donc $\lambda x \in F$ et $\mu y \in F$. F est un sous-groupe de E , donc $\lambda x + \mu y \in F$.
- (iv) $\Rightarrow$ (v) Direct avec $\mu = 1$.
- (v) $\Rightarrow$ (vi) Supposons (v). Alors F est non vide et contient donc un élément x_0 , donc contient 0_E car $0_E = (-1) \cdot x_0 + x_0$. On en déduit (vi).
- (vi) $\Rightarrow$ (i) Supposons (vi). Alors, pour tout $(x, y) \in F^2$ et pour tout $(\lambda, \mu) \in \mathbb{K}^2$, $\lambda x = \lambda x + 0$ donc $\lambda x \in F$. De plus, $\lambda x + \mu y = \mu y + (\lambda x)$, qui appartient donc bien à F avec (vi), et l'on a (i).

□

Remarque 2.1.4.

En pratique pour montrer qu'un sous-ensemble de E est un sous-espace vectoriel, on utilisera (iv) ou (v), qui est généralement le plus rapide à démontrer.

Exemple 2.1.5.

E et $\{0\}$ sont des sev de E , dits *triviaux*.

Exemple 2.1.6.

L'ensemble des solutions d'une équation différentielle linéaire homogène dont la variable est une fonction de I dans $\mathbb{R}$ est un sev de $\mathbb{R}^I$.

Théorème 2.1.7.

Soit F un sous-ensemble de E . Alors F muni des lois induites de E est un $\mathbb{K}$ -espace vectoriel si et seulement si F est un sous-espace vectoriel de E .

Démonstration.

- Supposons que F muni des lois de E soit un $\mathbb{K}$ -espace vectoriel. Alors $(F, +)$ est un groupe abélien donc c'est un sous-groupe de $(E, +)$. De plus, F est stable par multiplication externe, donc c'est bien un sous-espace vectoriel de E .
- Réciproquement, si F est un sous-espace vectoriel de E , on sait qu'il s'agit d'un sous-groupe de $(E, +)$, donc $(F, +)$ est un groupe abélien. De plus, F est stable par multiplication externe, donc la multiplication externe de E induit bien une multiplication externe sur F . On peut aisément vérifier que les propriétés (ii) à (v) des espaces vectoriels sont alors vérifiées par les lois induites sur F .

□

Remarque 2.1.8.

En pratique, pour montrer qu'un ensemble est un espace vectoriel, il est plus rapide de montrer que c'est un sous-espace vectoriel d'un espace vectoriel plus gros : on le fera donc quasiment **TOUJOURS**, et l'on ne reviendra presque **JAMAIS** à la définition complète.

2.2 Exemples.

Exemples géométriques :

Droites dans $\mathbb{R}^2$ Soient $(a, b, c) \in \mathbb{R}^3$, avec $(a, b) \neq (0, 0)$. À quelle condition la droite d'équation $ax + by = c$ est-elle un sous-espace vectoriel de $\mathbb{R}^2$?

Plans dans $\mathbb{R}^3$ Même question pour un plan d'équation $ax + by + cz + d = 0$.

Cercles dans $\mathbb{R}^2$ Même question pour un cercle dans le plan.

Exemples avec polynômes et fractions rationnelles : quels sont les liens entre $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}_n[X]$, $\mathbb{C}_n[X]$, $\mathbb{R}(X)$, $\mathbb{C}(X)$?

Exemples avec les fonctions : soit I un intervalle et n un entier naturel, $\mathcal{C}^n(I, \mathbb{K})$ est un sous-espace vectoriel de $\mathbb{K}^I$.

2.3 Opérations sur les sous-espaces vectoriels.

Dans toute la suite du chapitre, F et G sont deux sous-espaces vectoriels de E .

a Intersection.

Théorème 2.3.1. 1. $F \cap G$ est un sous-espace vectoriel de E .

2. $F \cup G$ est un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

Démonstration. 1. On a évidemment $0 \in F \cap G$. On vérifie aisément que pour tout $(x, y) \in (F \cap G)^2$ et tout $\lambda \in \mathbb{K}$, on a $\lambda x + y \in F \cap G$.

2. Si un des deux espaces vectoriels est inclus dans l'autre, alors $F \cup G$ est trivialement un sous-espace vectoriel de E .

Supposons à l'inverse qu'aucun des deux sous-espaces vectoriels ne soit inclus dans l'autre et montrons qu'alors $F \cup G$ n'est pas un sous-espace vectoriel. $F \setminus G$ contient au moins un élément x , et $G \setminus F$ au moins un élément y . Posons alors $z = x + y$. Si z appartenait à F , on aurait $y = z - x \in F$ ce qui n'est pas le cas. De même, on ne peut avoir $z \in G$. Donc $z \notin F \cup G$, donc $F \cup G$ n'est pas stable par addition. $\square$

Exemple 2.3.2.

Dans l'espace, toute droite passant par 0 est l'intersection de deux plans passant par 0, donc est un sous-espace vectoriel.

Cette propriété se généralise en fait à une intersection d'une famille quelconque de sous-espaces vectoriels :

Théorème 2.3.3.

Soit $(F_i)_{i \in I}$ (resp. $\mathcal{F}$) une famille (resp. un ensemble) de sous-espaces vectoriels de E . Alors

$$\bigcap_{i \in I} F_i \quad \text{resp.} \quad \bigcap_{F \in \mathcal{F}} F$$

est un sous-espace vectoriel de E .

Démonstration.

Remarquons que le cas de l'intersection d'un ensemble se traite comme le cas particulier d'une famille : il s'agit de l'intersection de la famille des $(F_i)_{F \in \mathcal{F}}$ où $I = \mathcal{F}$ et pour tout $G \in I$, $F_G = G$.

La démonstration s'effectue alors comme la précédente. Notons F l'intersection des F_i pour $i \in I$.

1. On a évidemment $0 \in F_i$ pour tout $i \in I$, donc $0 \in F$.
2. Pour tout $(x, y) \in F^2$ et tout $\lambda \in \mathbb{K}$, on a successivement :

$$\begin{aligned} \forall i \in I \quad (x, y) &\in F_i^2 \\ \forall i \in I \quad \lambda x + y &\in F_i \\ \lambda x + y &\in \bigcap_{i \in I} F_i \end{aligned}$$

$\square$

Un exemple important d'intersection a priori infinie est donnée dans la partie suivante.

b Sous-espace vectoriel engendré par une partie.

Définition 2.3.4 (Sous-espace vectoriel engendré par une partie).

Soit X une partie (quelconque) du $\mathbb{K}$ -espace vectoriel E . On appelle $\mathbb{K}$ -sous-espace vectoriel engendré par X et on note $\text{Vect}_{\mathbb{K}}(X)$ (ou $\text{Vect}(X)$ lorsqu'il n'y a pas d'ambiguïté) le plus petit sous-espace vectoriel de E contenant X (« plus petit » est à entendre au sens de l'inclusion).

Démonstration.

Cette définition présuppose qu'un tel sous-espace existe et qu'il est unique. L'unicité sous réserve d'existence du plus petit élément d'un ensemble muni d'une relation d'ordre est connue. Montrons l'existence.

Notons $\mathcal{F}$ l'ensemble des F tels que :

1. F est un sous-espace vectoriel de E ;
2. et $X \subset F$.

On veut montrer que cet ensemble $\mathcal{F}$ possède un plus petit élément pour l'inclusion.

Posons alors

$$V = \bigcap_{F \in \mathcal{F}} F$$

et montrons que V est ce plus petit élément.

Comme $E \in \mathcal{F}$, on a $F \neq \emptyset$, donc V est bien défini.

Montrons tout d'abord $V \in \mathcal{F}$.

Pour tout $F \in \mathcal{F}$, on a $X \subset F$, donc

$$X \subset \bigcap_{F \in \mathcal{F}} F = V$$

De plus, V est une intersection de sous-espaces vectoriels de E donc c'est un sous-espace vectoriel de E .

Donc on a $V \in \mathcal{F}$.

Il suffit donc maintenant de montrer que V est un mineur de $\mathcal{F}$, c'est-à-dire que pour tout $F \in \mathcal{F}$, on a $V \subset F$.

Soit $F \in \mathcal{F}$. On a

$$V = \bigcap_{G \in \mathcal{F}} G$$

donc tout élément de V appartient à tout élément de $\mathcal{F}$, donc en particulier à F . On a donc $V \subset F$.

V minore donc $\mathcal{F}$ pour l'inclusion.

V est donc un élément de $\mathcal{F}$ qui minore $\mathcal{F}$: c'est donc son plus petit élément. $\square$

Remarque 2.3.5. 1. Tout sous-espace vectoriel de E contenant X contient donc $\text{Vect}(X)$.

2. Si F est un sous-espace vectoriel de E , alors F est le plus petit sous-espace vectoriel contenant F , donc $\text{Vect}(F) = F$.

Remarque 2.3.6.

Soit I un ensemble et $(x_i)_{i \in I}$ une famille de vecteurs de E . On notera $\text{Vect}((x_i)_{i \in I})$ le sous-espace $\text{Vect}(\{x_i \mid i \in I\})$. En particulier si I est de la forme $\llbracket 1, n \rrbracket$, on notera $\text{Vect}(x_1, \dots, x_n)$ le sous-espace $\text{Vect}(\{x_1, \dots, x_n\})$.

Le procédé de construction de $\text{Vect}(X)$ présenté plus haut est très élégant et peut s'utiliser dans de nombreuses situations. En revanche, il est assez peu concret. Heureusement, le théorème suivant nous dit très précisément ce que contient $\text{Vect}(X)$.

Théorème 2.3.7.

Soit X une partie de E . Alors $\text{Vect}(X)$ est exactement l'ensemble de toutes les combinaisons linéaires d'éléments de X . Autrement dit :

1. Toute combinaison linéaire d'éléments de X appartient à $\text{Vect}(X)$.

2. Pour tout élément x de $\text{Vect}(X)$, il existe une famille de coefficients $(\lambda_\alpha)_{\alpha \in X}$ à support fini telle qu'on a

$$x = \sum_{\alpha \in X} \lambda_\alpha \alpha.$$

Dit autrement : il existe un entier $n \in \mathbb{N}$, des vecteurs $u_1, \dots, u_n$ de X ($\forall k \in \llbracket 1, n \rrbracket, u_k \in X$) et des scalaires $\lambda_1, \dots, \lambda_n$ tels qu'on a

$$x = \sum_{k=1}^n \lambda_k u_k.$$

Démonstration.

Notons V l'ensemble des combinaisons linéaires d'éléments de X .

Pour montrer $V = \text{Vect}(X)$, nous allons montrer que V est le plus petit sous-espace vectoriel de E contenant X .

1. V est un sous-espace vectoriel de E . En effet :

- (a) il contient 0_E (combinaison linéaire de 0 vecteur de X) ;
- (b) il est stable par addition car la somme d'une combinaison linéaire de p vecteurs de X et d'une combinaison linéaire de q vecteurs de X est une combinaison linéaire (d'au plus) $p + q$ vecteurs de X ;
- (c) il est stable par multiplication par un scalaire car le produit par un scalaire λ d'une combinaison linéaire de n vecteurs de X est la combinaison linéaire de ces mêmes vecteurs où les coefficients ont tous été multipliés par λ .

2. V contient X . En effet pour tout $x \in X$, x est la combinaison linéaire $1 \cdot x$, donc appartient à V . Donc $X \subset V$.

3. V minore l'ensemble des sous-espaces vectoriels de E contenant X . En effet, soit F un sous-espace vectoriel de E contenant X . Montrons $V \subset F$.

Soit $x \in V$ alors x est combinaison linéaire d'éléments de X . Or F contient X et est un sous-espace-vectoriel donc est stable par combinaison linéaire. Il contient donc x en particulier. On a donc $\forall x \in V \quad x \in F$.

Donc $V \subset F$.

Donc V est le plus petit sous-espace vectoriel de E contenant X . $\square$

Remarque 2.3.8.

En particulier, pour toute famille finie de vecteurs $x_1, \dots, x_n$, $\text{Vect}(x_1, \dots, x_n)$ est l'ensemble

$$\left\{ \sum_{k=1}^n \lambda_k x_k \mid (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \right\}.$$

Exemple 2.3.9. 1. Pour $\alpha \in \mathbb{R}$, on note

$$f_\alpha : \begin{cases} \mathbb{R} & \longrightarrow \mathbb{R} \\ x & \longmapsto e^{\alpha x} \end{cases}.$$

Alors $\text{Vect}((f_\alpha)_{\alpha \in \mathbb{R}})$ est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{R}}$ qui contient les fonctions sh, ch mais pas sin ni p (indication : il suffit de remarquer que les seules fonctions bornées de ce sous-espace vectoriel sont les fonctions constantes).

2. En géométrie dans $\mathbb{R}^2$, si $(\vec{v}, \vec{j})$ est une base, tout vecteur de $\mathbb{R}^2$ est combinaison linéaire de $\vec{v}$ et $\vec{j}$, donc $\mathbb{R}^2 = \text{Vect}(\vec{v}, \vec{j})$.
3. Dans $\mathbb{R}^3$, si $\mathcal{D}$ est une droite vectorielle de vecteur directeur u , alors $\mathcal{D} = \{\lambda u \mid \lambda \in \mathbb{K}\} = \text{Vect}(u)$. Si $\mathcal{P}$ est un plan vectoriel de vecteurs directeurs $u = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$ et $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, alors en écrivant une équation paramétrique de $\mathcal{P}$, on voit que tout point P de l'espace est dans $\mathcal{P}$ si et seulement s'il existe $t_1, t_2 \in \mathbb{R}$ tel que $P = t_1 u + t_2 v$, donc $\mathcal{P} = \text{Vect}(u, v)$. Exemple avec $2x - y + z = 0$.
4. $\mathbb{R} = \text{Vect}_{\mathbb{R}}(1)$ et $\mathbb{C} = \text{Vect}_{\mathbb{C}}(1) = \text{Vect}_{\mathbb{R}}(1, i)$.
5. $E = (\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ est un ev. On note les fonctions suivantes, définies sur $\mathbb{R}$ par $\exp : x \mapsto e^x$; $\widetilde{\exp} : x \mapsto e^{-x}$; $f : x \mapsto x \sin(2x)$ et $g : x \mapsto x \sin(3x)$. Avec $F = \text{Vect}(\exp, \widetilde{\exp})$ et $G = \text{Vect}(f, g)$, on a $\text{ch} \in F$ mais $\sin \notin G$.
6. L'ensemble des solutions de l'équation différentielle $y'' + y' - 2y = 0$ est $\text{Vect}(f, g)$ avec $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto e^{-2x}$ et $g = \exp$.

Proposition 2.3.10.

Soit X et Y deux parties de E . Alors :

1. $X \subset Y \Rightarrow \text{Vect}(X) \subset \text{Vect}(Y)$;
2. $\text{Vect}(\text{Vect}(X)) = \text{Vect}(X)$.

Démonstration. 1. Supposons $X \subset Y$. Alors $X \subset Y \subset \text{Vect}(Y)$. Donc $\text{Vect}(Y)$ est un sous-espace vectoriel de E contenant X donc contient $\text{Vect}(X)$.

2. Posons $F = \text{Vect}(X)$. F est un sous-espace vectoriel de E . Donc d'après la remarque faite plus haut, $\text{Vect}(F) = F$.

□

c Sous-espace vectoriel engendré par une famille finie.

Dans cette sous-partie, on s'intéressera exclusivement au cas où $I = \llbracket 1, n \rrbracket$. La famille $(x_i)_{i \in I}$ est donc le n -uplet $(x_1, \dots, x_n)$.

Proposition 2.3.11. 1. $\text{Vect}(x_1, \dots, x_n)$ n'est pas modifié si l'on permute deux vecteurs de $(x_1, \dots, x_n)$.

2. si pour un $i \in \llbracket 1, n \rrbracket$ on a x_i qui est combinaison linéaire des autres vecteurs (en particulier, si $x_i = 0$), alors $\text{Vect}(x_1, \dots, x_n) = \text{Vect}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$, c'est-à-dire que l'on peut ôter x_i de la famille sans modifier le sev engendré.
3. $\text{Vect}(x_1, \dots, x_n)$ n'est pas modifié si l'on remplace un des x_i par une combinaison linéaire en $x_1, \dots, x_n$ dont le coefficient en x_i est non nul.

Démonstration. 1. C'est une conséquence directe du fait que $\text{Vect}(x_1, \dots, x_n) = \text{Vect}\{x_1, \dots, x_n\}$.

2. C'est une conséquence du fait que pour toutes parties X et Y de E , si $X \subset Y \subset \text{Vect}(X)$, alors

$$\text{Vect}(X) \subset \text{Vect}(Y) \subset \text{Vect}(\text{Vect}(X)) = \text{Vect}(X).$$

3. Quitte à permuter les vecteurs, on peut supposer que $i = n$. Considérons un vecteur x' obtenu par combinaison linéaire des x_k pour $k \in \llbracket 1, n \rrbracket$ dont le coefficient de x_n est non nul. Posons $V = \text{Vect}(x_1, \dots, x_n)$ et $V' = \text{Vect}(x_1, \dots, x_{n-1}, x')$ et montrons $V = V'$. Posons $V'' = \text{Vect}(x_1, \dots, x_{n-1}, x_n, x')$. x' étant combinaison linéaire des x_k pour $k \in \llbracket 1, n \rrbracket$, on a $V'' = V$ d'après le point précédent.

De plus, le coefficient de x_n dans cette combinaison linéaire est non nul, donc x_n peut s'exprimer comme combinaison linéaire de $x_1, \dots, x_{n-1}$ et x' . Donc, toujours d'après le point précédent, $V'' = V'$. On a donc $V = V'' = V'$.

□

Remarque 2.3.12.

0_E est toujours combinaison linéaire de toute famille de vecteurs : on peut donc « l'enlever » d'une famille sans modifier le sev engendré par cette famille.

Exemple 2.3.13.

Dans $\mathbb{R}^3$, avec $u_1 = (1, 0, 0)$, $u_2 = (0, 1, 0)$ et $u_3 = (1, 1, 0)$.

1.

$$\begin{aligned}\text{Vect}(u_1, u_2, u_3) &= \text{Vect}(u_1, u_2) \\ &= \text{Vect}(u_1, u_3).\end{aligned}$$

 2. Déterminer une CNS sur $w \in \mathbb{R}^3$ pour que $\text{Vect}(u_1, u_2, u_3, w) \neq \text{Vect}(u_1, u_2, u_3)$.

d Somme.

Définition 2.3.14.

On appelle *somme de F et G* l'ensemble de E noté $F + G$ défini par $F + G = \{x + y \mid x \in F, y \in G\}$.

Théorème 2.3.15. 1. $F + G$ est un sev de E .

2. $F + G$ est le plus petit sev qui contient F et G :

$$F + G = \text{Vect}(F \cup G).$$

Démonstration. 1. Immédiat.

2. Montrons d'abord que $F \subset F + G$: soit $f \in F$, alors $f = f + 0$, et $0 \in G$, donc $f \in F + G$. On montre bien sûr de même que $G \subset F + G$. On a donc $(F \cup G) \subset (F + G)$.

Il suffit ensuite de montrer que pour tout sous-espace vectoriel H de E contenant $F \cup G$, on a $(F + G) \subset H$. Soit H un sous-espace vectoriel de E . Supposons $F \subset H$ et $G \subset H$. Montrons $(F + G) \subset H$.

Soit $z \in F + G$. Alors il existe $x \in F$ et $y \in G$ vérifiant $z = x + y$. On a alors $x \in H$ et $y \in H$ donc $x + y \in H$, donc $z \in H$.

Donc $F + G \subset H$. □

Remarque 2.3.16.

Par conséquent,

$$\begin{aligned}F + G &= \text{Vect}(F) + \text{Vect}(G) \\ &= \text{Vect}(F \cup G) \\ &= \text{Vect}(G \cup F) \\ &= G + F.\end{aligned}$$

Remarque 2.3.17.

Si $A = F + G$ et $a \in A$, il n'y a pas forcément unicité de la décomposition $a = f + g$, avec $f \in F$ et $g \in G$, loin de là ! Considérer par exemple le cas $F + F$.

Exemple 2.3.18.

Si $F \subset G$, alors $F + G = G$.



$F + G \neq F \cup G$ (sauf si $F \subset G$ ou $G \subset F$).

Exemple 2.3.19.

Soit $\mathcal{D}$ et $\mathcal{D}'$ deux droites du plan passant par 0 et non confondues. Alors $\mathbb{R}^2 = \mathcal{D} + \mathcal{D}'$.

Exercice 2.3.20.

Soit $\mathcal{P}_1$ le plan de représentation cartésienne $x + 3z = 0$ et $\mathcal{P}_2$ le plan de représentation cartésienne $x + y + z = 0$.

Montrer que $\mathbb{R}^3 = \mathcal{P}_1 + \mathcal{P}_2$.

Lemme 2.3.21.

Soit X et Y des parties de E . Alors

$$\text{Vect}(X) + \text{Vect}(Y) = \text{Vect}(X \cup Y).$$

Démonstration.

$\text{Vect}(X \cup Y)$ est un sous-espace vectoriel contenant $X \cup Y$, donc contient X . Or tout espace vectoriel contenant X contient $\text{Vect}(X)$, donc $\text{Vect}(X \cup Y)$ contient $\text{Vect}(X)$. De même, il contient $\text{Vect}(Y)$. $\text{Vect}(X \cup Y)$ est donc un espace vectoriel contenant les deux sous-espaces vectoriels $\text{Vect}(X)$ et $\text{Vect}(Y)$, donc il contient leur somme. On a donc $\text{Vect}(X) + \text{Vect}(Y) \subset \text{Vect}(X \cup Y)$.

Par ailleurs, $\text{Vect}(X) + \text{Vect}(Y)$ contient $\text{Vect}(X)$, donc contient X . De même, il contient Y . Il contient donc $X \cup Y$. Or $\text{Vect}(X) + \text{Vect}(Y)$ est un sous-espace vectoriel, donc il contient $\text{Vect}(X \cup Y)$. On a donc $\text{Vect}(X \cup Y) \subset \text{Vect}(X) + \text{Vect}(Y)$.

On a donc $\text{Vect}(X \cup Y) = \text{Vect}(X) + \text{Vect}(Y)$. □

Remarque 2.3.22.

On peut aussi définir la notion de somme de plus de deux sev.

2.4 Somme directe et supplémentaires.

Étant donné des sous-espaces vectoriels F, G de E , $F + G$ est l'ensemble des vecteurs x de E pouvant s'écrire au moins d'une façon sous la forme $f + g$ avec, $f \in F$ et $g \in G$.

On va s'intéresser ici au cas où, pour tout x , la décomposition est unique.

Définition 2.4.1 (Somme directe).

Soit F, G deux sev de E , on dit que la somme $F + G$ est *directe* si

$$\forall x \in F + G, \exists!(f, g) \in F \times G, x = f + g.$$

Dans ce cas, le sous-espace vectoriel $F + G$ est noté

$$F \oplus G.$$

Remarque 2.4.2.

On peut de même définir la notion de somme directe pour plus de deux sev.

Proposition 2.4.3 (Caractérisation d'une somme directe de deux sev).

Soit F, G deux sev de E . Les trois propositions suivantes sont équivalentes.

1. $F + G$ est directe.
2. $\forall f \in F, \forall g \in G, f + g = 0_E \Rightarrow f = g = 0_E$.
3. $F \cap G = \{0_E\}$.

Démonstration.

Supposons que $F + G$ est directe. Soit $f \in F, g \in G$ vérifiant $f + g = 0_E$. Alors,

$$\underbrace{f}_{\in F} + \underbrace{g}_{\in G} = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G},$$

donc par unicité on a $f = g = 0_E$.

Supposons que $\forall f \in F, \forall g \in G, f + g = 0_E \Rightarrow f = g = 0_E$. Soit $x \in F \cap G$, alors

$$\underbrace{x}_{\in F} + \underbrace{-x}_{\in G} = 0_E,$$

donc $x = 0_E$. Comme $F \cap G$ est un sev de E , $0_E \in F \cap G$, donc $F \cap G = \{0_E\}$.

Supposons que $F \cap G = \{0_E\}$, montrons que $F + G$ est directe. Soit $x \in F + G$, soit $f, f' \in F, g, g' \in G$ vérifiant

$$x = f + g = f' + g'.$$

Alors,

$$f - f' = g' - g \in F \cap G$$

donc $0_E = f - f' = g' - g$, donc $f = f'$ et $g = g'$, donc $F + G$ est directe. $\square$

Définition 2.4.4.

On dit que F est *un supplémentaire* de G (ou que F et G sont *supplémentaires*) si

$$E = F \oplus G,$$

i.e. si les deux conditions suivantes sont remplies :

1. la somme $F + G$ est directe ;
2. $E = F + G$.

Proposition 2.4.5.

F et G sont supplémentaires si et seulement si tout élément de E s'écrit *de manière unique* comme somme d'un élément de F et d'un élément de G .

Démonstration.

Direct d'après les définitions. $\square$

Exemple 2.4.6.

Montrons que dans $\mathbb{R}^2$, deux droites passant par 0 et non confondues sont toujours supplémentaires.

Exercice 2.4.7.

Dans $\mathbb{R}^2$, on note $\mathcal{D} : x + y = 0$, $\mathcal{D}' : x - y = 0$ et $\mathcal{D}'' : x - 2y = 0$.

1. Montrer $\mathbb{R}^2 = \mathcal{D} \oplus \mathcal{D}'$
2. Montrer $\mathbb{R}^2 = \mathcal{D} \oplus \mathcal{D}''$

Remarquez qu'il n'y a donc pas unicité du supplémentaire (croire le contraire est une faute classique et très grave !).

Remarque 2.4.8.

On peut montrer de même que dans $\mathbb{R}^3$, un plan et une droite passant par 0 et tel que le plan ne contienne pas la droite sont toujours supplémentaires.

Exemple 2.4.9.

$\mathcal{P} : x - y + z = 0$ et $\mathcal{D} : x = t + 1, y = 0, z = 2t + 2$. On montre que $(\vec{I}, \vec{J}, \vec{K})$ est une base de $\mathbb{R}^3$, avec $\vec{I}$ vecteur directeur de $\mathcal{D}$ et $(\vec{J}, \vec{K})$ base de $\mathcal{P}$.

Exemple 2.4.10.

$\mathbb{R}$ et $i\mathbb{R}$ dans $\mathbb{C}$.

Exercice 2.4.11.

On note E l'ensemble des applications de $\mathbb{R}$ dans

$\mathbb{R}$, I celui des applications impaires, et P celui des applications paires.

Montrer $E = I \oplus P$.

3 Translations, sous-espaces affines.

Les sous-espaces affines (sea) généralisent la notion de sev, en s'affranchissant de la contrainte « passer par 0 ». Ainsi, dans la théorie des ev, un sev passe toujours par 0.

Là encore on pourra identifier points et vecteurs, mais on essaiera de noter les points avec des majuscules et les vecteurs avec des minuscules, comme en géométrie, mais nous passerons souvent d'un point de vue à l'autre.

Définition 3.0.1.

Soit $A, B \in E$, on note $\overrightarrow{AB} = B - A$.

Remarque 3.0.2.

La loi $+$ des ev permet de donner un sens à $B - A$, vus comme points, qui vaut alors $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$.

3.1 Translations.

Définition 3.1.1.

Soit un vecteur $u \in E$. On appelle *translation* de vecteur u l'application $E \rightarrow E$:

$$x \mapsto x + u$$

3.2 Sous-espaces affines.

Définition 3.2.1.

On appelle *sous-espace affine* de E toute partie de E qui est le translaté d'un sev de E , i.e. toute partie $\mathcal{F}$ de la forme $\mathcal{F} = u + F = \{u + x \mid x \in F\}$, où F est un sev de E et u est un vecteur de E , ensemble que l'on note aussi $u + F$.

L'ensemble $\{b - a \mid (a, b) \in \mathcal{F}^2\}$ est appelé la *direction* de $\mathcal{F}$ et ses éléments sont appelés les *vecteurs directeurs* de $\mathcal{F}$.

Proposition 3.2.2.

Soit $u \in E$, F un sous-espace vectoriel de E . Alors la direction du sous-espace affine $u + F$ est F . En particulier cette direction est un espace vectoriel.

Démonstration.

Notons D la direction de $u + F$.

On a

$$\begin{aligned} D &= \{b - a \mid (a, b) \in \mathcal{F}^2\} \\ &= \{(u + x) - (u + y) \mid (x, y) \in F^2\} \\ &= \{x - y \mid (x, y) \in F^2\}. \end{aligned}$$

Or on a directement

$$F \subset \{x - 0 \mid x \in F\} \subset \{x - y \mid (x, y) \in F^2\} \subset F,$$

donc $D = F$. $\square$

Remarque 3.2.3.

Notation fréquente : $\mathcal{F}$ étant un sea de E , on note F ou $\vec{\mathcal{F}}$ sa direction.

Exemple 3.2.4.

Tout sev est un sea.

Exemple 3.2.5.

Dessin dans l'espace.

Exemple 3.2.6.

$E = \mathbb{R}^{\mathbb{R}}$. On considère l'équation différentielle $y' + 3y = x^2$ (E). Montrer que l'ensemble $\mathcal{S}_0$ des solutions de l'équation homogène forme un sev de E , et l'ensemble $\mathcal{S}$ des solutions de (E) forme un sea de direction $\mathcal{S}_0$.

Théorème 3.2.7.

Soit $\mathcal{F}$ un sea de direction F .

(i) $\mathcal{F}$ est le translaté de sa direction par n'importe lequel de ses points : $\forall a \in \mathcal{F} \quad \mathcal{F} = a + F$.

(ii) Soit $a \in \mathcal{F}$ et $b \in E$. Alors on a

$$b \in \mathcal{F} \iff a - b \in F.$$

Démonstration.

$\mathcal{F}$ est de la forme $c + F$, où $c \in E$.

(i) Soit $a \in \mathcal{F}$. On a alors $a \in c + F$, il existe donc $u \in F$ tel que $a = c + u$.

Si $v \in F$, alors $a + v = c + (u + v) \in c + F$, donc $a + F \subset \mathcal{F}$.

Réciproquement, si $v \in F$, alors $c+v = a+(v-u) \in a+F$, donc $\mathcal{F} \subset a+F$.

Ainsi, $a+F = \mathcal{F}$.

(ii) On a donc $\mathcal{F} = a+F$.

Si $b \in \mathcal{F}$, alors par définition de la direction $a-b \in F$.

Réciproquement, si $a-b \in F$, alors $b-a \in F$ et $b = a+(b-a) \in a+F$, donc $b \in \mathcal{F}$.

On a donc bien $b \in \mathcal{F} \iff a-b \in F$.

□

Remarque 3.2.8.

Tout sea contenant 0 est donc un sev.

Corollaire 3.2.9.

Deux sea sont égaux si et seulement s'ils ont même direction et un point en commun.

Démonstration.

$\Rightarrow$: évident.

$\Leftarrow$: soient $\mathcal{F}_1$ et $\mathcal{F}_2$ de même direction F et $a \in \mathcal{F}_1 \cap \mathcal{F}_2$. Alors d'après le théorème précédent, $\mathcal{F}_1 = a+F = \mathcal{F}_2$. □

Définition 3.2.10.

Soient $\mathcal{F}$ et $\mathcal{G}$ deux sea de directions F et G .

- (i) On dit que $\mathcal{F}$ est parallèle à $\mathcal{G}$ si $F \subset G$.
- (ii) On dit que $\mathcal{F}$ et $\mathcal{G}$ sont parallèles si $F = G$.



Vocabulaire : « être parallèle à » n'est pas une relation symétrique.

Exemple 3.2.11.

Une droite est parallèle à un plan, mais certainement pas l'inverse.

Théorème 3.2.12 (Intersections de sea).

Soient $\mathcal{F}$ et $\mathcal{G}$ deux sea de directions F et G . Si $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, alors on dit que $\mathcal{F}$ et $\mathcal{G}$ sont *concourants* ou *sécants*, et dans ce cas $\mathcal{F} \cap \mathcal{G}$ est un sea de direction $F \cap G$.

Démonstration.

Supposons $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, alors il existe $a \in \mathcal{F} \cap \mathcal{G}$. Donc $\mathcal{F} = a+F$ et $\mathcal{G} = a+G$.

Montrons alors que $\mathcal{F} \cap \mathcal{G} = a+F \cap G$:

Soit $b \in E$. On a successivement :

$$\begin{aligned} b \in \mathcal{F} \cap \mathcal{G} &\iff b \in \mathcal{F} \text{ et } b \in \mathcal{G} \\ &\iff b-a \in F \text{ et } b-a \in G \\ &\iff b-a \in F \cap G \\ &\iff b \in a+F \cap G \end{aligned}$$

D'où le résultat. □

Théorème 3.2.13 (Parallélisme et intersection).

Si $\mathcal{F}$ est parallèle à $\mathcal{G}$, alors soit $\mathcal{F} \cap \mathcal{G} = \emptyset$, soit $\mathcal{F} \subset \mathcal{G}$.

En particulier si $\mathcal{F}$ et $\mathcal{G}$ sont parallèles, alors soit $\mathcal{F} \cap \mathcal{G} = \emptyset$, soit $\mathcal{F} = \mathcal{G}$.

Démonstration.

Supposons $F \subset G$. Si $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, alors il existe $a \in \mathcal{F} \cap \mathcal{G}$, donc $\mathcal{F} = a+F$, or $F \subset G$, donc $a+F \subset a+G = \mathcal{G}$.

Dans le cas particulier où $\mathcal{F}$ et $\mathcal{G}$ sont parallèles, on a $\mathcal{F} \subset \mathcal{G}$ et $\mathcal{G} \subset \mathcal{F}$, d'où $\mathcal{F} = \mathcal{G}$. □

3.3 Barycentres (hors programme)

Le barycentre est maintenant hors-programme. Cette partie ne sera pas nécessairement traitée en cours mais est laissée :

- à titre culturel ;
- parce qu'elle peut être utile en sciences physiques.

Définition 3.3.1.

• On appelle *système pondéré* toute famille de la forme $((A_1, \lambda_1), \dots, (A_n, \lambda_n))$, où chaque élément (A_i, λ_i) est appelé *point pondéré*, avec $n \in \mathbb{N}^*$, $A_1, \dots, A_n$ n points de E , et $\lambda_1, \dots, \lambda_n$ n scalaires de $\mathbb{K}$.

• Avec les notations précédentes, on pose $\Lambda = \sum_{k=1}^n \lambda_k$.

(i) Si $\Lambda = 0$, alors le vecteur $\sum_{k=1}^n \lambda_k \overrightarrow{MA_k}$ ne dépend pas du point M .

(ii) Si $\Lambda \neq 0$, il existe un unique point G tel que $\sum_{k=1}^n \lambda_k \overrightarrow{GA_k} = 0$. Ce point est appelé le *barycentre* du système pondéré $(A_i, \lambda_i)_{i \in [1, n]}$

et il vérifie $G = \frac{1}{\Lambda} \sum_{k=1}^n \lambda_k A_k$.

Démonstration. (i) Supposons $\Lambda = 0$. Soit $(M, N) \in E^2$. On a

$$\begin{aligned} \sum_{k=1}^n \lambda_k \overrightarrow{MA_k} &= \sum_{k=1}^n \lambda_k \overrightarrow{MA_k} + \sum_{k=1}^n \lambda_k \overrightarrow{NM} \\ &= \sum_{k=1}^n \lambda_k (\overrightarrow{NM} + \overrightarrow{MA_k}) \\ &= \sum_{k=1}^n \lambda_k \overrightarrow{NA_k} \end{aligned}$$

(ii) Supposons $\Lambda \neq 0$. On a successivement :

$$\begin{aligned} \sum_{k=1}^n \lambda_k \overrightarrow{GA_k} = 0 &\Leftrightarrow \sum_{k=1}^n \lambda_k (A_k - G) = 0 \\ &\Leftrightarrow \sum_{k=1}^n \lambda_k A_k - \left(\sum_{k=1}^n \lambda_k \right) G = 0 \\ &\Leftrightarrow G = \frac{1}{\Lambda} \sum_{k=1}^n \lambda_k A_k \end{aligned}$$

□

Définition 3.3.2.

Soit I un ensemble. On appelle *partition finie* de I tout k -uplet, pour $k \in \mathbb{N}$, $(I_1, \dots, I_k)$ où les I_i sont des ensembles vérifiant $I_j \cap I_i = \emptyset$ si $i \neq j$ et $\bigcup_{1 \leq i \leq k} I_i = I$. Autrement dit, une partition est un ensemble de parties de I deux à deux disjointes, dont la réunion est I (on parle aussi de recouvrement de I par des parties deux à deux disjointes).

Exemple 3.3.3. • La partition de l'Europe par le traité de Verdun en 843 est une partition à trois éléments de l'ensemble des points de l'empire de Charlemagne.

- Notons C_0 , C_1 et C_2 les parties de $\mathbb{Z}$ contenant respectivement les entiers congrus à 0, 1 et 2 modulo 3. Alors (C_0, C_1, C_2) est une partition de $\mathbb{Z}$.

Théorème 3.3.4 (Associativité du barycentre). Soient I un ensemble non vide, $(A_i, \lambda_i)_{i \in I}$ un système de points pondérés de somme non nulle, et soit $(I_1, \dots, I_n)$ une partition de I . Pour tout $k \in \llbracket 1, n \rrbracket$, on note $\Lambda_k = \sum_{i \in I_k} \lambda_i$, on suppose que

Λ_k est non nul et on note alors G_k le barycentre du système pondéré $(A_i, \lambda_i)_{i \in I_k}$.

Alors le barycentre G de $(A_i, \lambda_i)_{i \in I}$ est aussi le barycentre du système pondéré $(G_k, \Lambda_k)_{k \in \llbracket 1, n \rrbracket}$.

Démonstration.

On sait que $G = \frac{1}{\Lambda} \sum_{i \in I} \lambda_i A_i$ et $\Lambda_k G_k = \sum_{i \in I_k} \lambda_i A_i$, donc

$$G = \frac{1}{\Lambda} \sum_{k=1}^n \left(\sum_{i \in I_k} \lambda_i A_i \right) = \frac{1}{\Lambda} \sum_{k=1}^n \Lambda_k G_k, \text{ et } \Lambda = \sum_{k=1}^n \Lambda_k. \quad \square$$

Exercice 3.3.5.

En déduire :

1. que les médianes d'un triangle sont concourantes au centre de gravité ;
2. que les droites reliant les milieux des arêtes opposées d'un tétraèdre et les droites reliant les centre de gravité des faces au sommet opposé sont toutes concourantes en un même point qu'on précisera.

Centre de gravité d'un triangle (ABC) = isobarycentre. Si I est le milieu de $[A, B]$, alors $G = \text{bar}((C, 1), (I, 2))$.

Théorème 3.3.6.

Un sea contient tous les barycentres obtenus à partir de ses points.

Démonstration.

Soit $\mathcal{F}$ un sea, $A_1 \dots A_n$ n points de $\mathcal{F}$, et $\lambda_1 \dots \lambda_n$ les poids correspondants, $\Lambda = \sum_{k=1}^n \lambda_k \neq 0$. On note $G = \text{bar}((A_k, \lambda_k))$.

$A_1 \in \mathcal{F}$ donc $\mathcal{F} = A_1 + F$. Donc $G \in \mathcal{F}$ ssi $G - A_1 \in F$.

Or $G - A_1 = \frac{1}{\Lambda} \sum_{k=1}^n \lambda_k (A_k - A_1)$, et tous les membres de cette somme sont dans F . □

Théorème 3.3.7.

Réciproquement, tout sous-ensemble non vide de E stable par barycentre (et même seulement par barycentre de deux points) est un sea.

Démonstration.

Soit $\mathcal{F}$ un sous-ensemble non vide de E et a un de ses points. Posons $F = \{ b - a \mid b \in \mathcal{F} \}$. On a $\mathcal{F} = a + F$, il

suffit donc de montrer que F est un sous-espace vectoriel de E .

F est une partie de E non vide car $0 \in F$.

Soit $x \in F$ et $\lambda \in \mathbb{K}$. Alors $a+x$ et a sont deux éléments de $\mathcal{F}$, donc leur barycentre $\lambda(a+x) + (1-\lambda)a$ appartient aussi à $\mathcal{F}$. Or ce barycentre est $a + \lambda x$, donc $\lambda x \in F$. F est donc stable par multiplication externe.

Soit $(x, y) \in F$. Alors, $\mathcal{F}$ étant stable par barycentre, $\frac{1}{2}((a+x) + (a+y)) \in \mathcal{F}$, donc $a + \frac{1}{2}(x+y) \in \mathcal{F}$, donc $\frac{1}{2}(x+y) \in F$. D'après ce qui précède, on a alors $x+y = 2 \times \frac{1}{2}(x+y) \in F$. Donc F est stable par addition.

Donc F est un sous-espace vectoriel de E . Donc $\mathcal{F}$ est un sous-espace affine de E . $\square$

3.4 Convexité (hors programme)

Cette partie est laissée à titre culturel mais ne sera pas nécessairement traitée en cours.

Dans ce paragraphe, on prend $\mathbb{K} = \mathbb{R}$.

Définition 3.4.1.

On appelle *segment* de E tout ensemble de la forme $\{\lambda A + (1-\lambda)B, \lambda \in [0, 1]\}$ avec $A, B \in E$. Ce segment est noté $[AB]$ ou $[A, B]$.

Remarque 3.4.2.

$[AB]$ est l'ensemble des barycentres de A et B avec des poids positifs (facultatif : dont la somme est 1). Faire un dessin.

Définition 3.4.3.

Soit $\mathcal{P}$ une partie de E . On dit que $\mathcal{P}$ est *convexe* si $\forall (A, B) \in \mathcal{P}^2 \quad [AB] \subset \mathcal{P}$.

Exemple 3.4.4.

Faire des dessins dans $\mathbb{R}^2$, puis dans $\mathbb{R}^3$.

Théorème 3.4.5.

Tout sea est convexe.

Démonstration.

Immédiat avec le théorème 3.3.6. $\square$

Exemple 3.4.6.

On reprend un exemple ancien : pour montrer qu'un cercle n'est pas un sea (ou un sev), on peut montrer qu'il n'est pas convexe.



La réciproque est fausse, même si le convexe contient 0. Par exemple, considérons $[-1, 1]$ dans $\mathbb{R}$.

Exemple 3.4.7.

Dans $\mathbb{C}$, tout disque (fermé ou ouvert) est convexe. Se fait avec inégalité triangulaire en revenant à la définition.

Théorème 3.4.8.

Toute intersection de convexes est convexe.

Démonstration.

Soit I un ensemble et $(\mathcal{P}_i)_{i \in I}$ une famille de convexes.

Posons $\mathcal{P} = \bigcap_{i \in I} \mathcal{P}_i$ l'intersection de cette famille et montrons qu'elle est convexe, c'est-à-dire

$$\forall (A, B) \in \mathcal{P}^2 \quad [AB] \subset \mathcal{P}$$

Soit $(A, B) \in \mathcal{P}^2$. Il suffit de montrer que pour tout $i \in I$, $[AB] \subset \mathcal{P}_i$.

Soit $i \in I$. On a $A \in \mathcal{P}$, donc $A \in \mathcal{P}_i$. De même $B \in \mathcal{P}_i$. Donc $[AB] \subset \mathcal{P}_i$.

On a donc $\forall i \in I \quad [AB] \subset \mathcal{P}_i$, donc $[AB] \in \bigcap_{i \in I} \mathcal{P}_i$. $\square$

Chapitre XX

Analyse asymptotique

Sommaire

1	Comparaison asymptotique de suites. . .	298
1.1	Définitions : notations de Landau. . .	298
1.2	Opérations.	299
a	o et O	299
b	Équivalents.	299
1.3	Exemples classiques (formulaire). . .	300
1.4	Formule de Stirling.	301
2	Comparaison de fonctions.	301
2.1	Définitions.	301
a	o et O	301
b	Équivalents.	302
2.2	Opérations.	302
a	o et O	302
b	Équivalents.	303
3	Développements limités.	303
3.1	Définition et premières propriétés. . .	304
3.2	Opérations sur les DL.	305
a	Somme.	305
b	Produit.	306
c	Composition.	307
d	Quotient.	307
3.3	Intégration et dérivation.	308
3.4	Formule de Taylor-Young.	309
3.5	Étude locale d'une fonction.	309
a	Allure d'une courbe au voisinage d'un point.	309
b	Prolongement de fonction.	310
c	Développements asymptotiques. .	311
d	Branche infinie d'une courbe d'équation $y = f(x)$	311
4	Théorèmes de comparaison pour les séries.	311

1 Comparaison asymptotique de suites.

Une première manière de comparer deux suites est de regarder si elles ont ou pas une limite, et si ces limites sont égales. Si deux suites n'ont pas la même limite, on peut dire que ces deux suites n'ont pas le même comportement. Mais si elles ont la même limite, on ne peut rien dire : exemple : $u_n = n$ et $v_n = e^n$, 0 , $1/n$ et $(-1)^n/n$. Même limite, mais pas du tout le même comportement. Pour une analyse plus fine, on utilise des outils de comparaison.

Dans tout cette section, (u_n) , (v_n) , (u'_n) , (v'_n) et (w_n) sont des suites réelles.

1.1 Définitions : notations de Landau.

Définition 1.1.1.

Soient (u_n) et (v_n) deux suites. Les définitions suivantes vont être données dans le cas particulier où (v_n) **ne s'annule pas**. Il existe des définitions plus générales des relations de comparaison, dans le cas où (v_n) s'annule, mais elles ne sont pas au programme.

- (i) On dit que (u_n) est *dominée* par (v_n) , ce qui se note $u_n = O(v_n)$, et se lit « (u_n) est un grand O de (v_n) », si la suite (u_n/v_n) est bornée.
- (ii) On dit que (u_n) est *négligeable* devant (v_n) , ce qui se note $u_n = o(v_n)$, et se lit « (u_n) est un petit o de (v_n) », si $u_n/v_n \rightarrow 0$.

Remarque 1.1.2.

- Petit o implique évidemment grand O .
- Une suite est un $O(1)$ si et seulement si elle est bornée, et est un $o(1)$ si et seulement si elle tend vers 0 .
- À l'écrit, prenez soin de bien différencier les tailles de o et O .

Remarque 1.1.3.

On traduira souvent la relation $u_n = o(v_n)$ par : il existe une suite (ε_n) telle que

- $\varepsilon_n \xrightarrow{n \rightarrow +\infty} 0$;

- $\forall n \in \mathbb{N}, u_n = \varepsilon_n v_n$.

Exemple 1.1.4. 1. $n = o(e^n)$.

2. $0 = o(1/n)$.

3. $1/n = O((-1)^n/n)$.

4. $\sin n = O(1)$ et $1/n = o(1)$.

5. $v_n = \frac{n^4 + n^2}{n + 1}$ et $u_n = \frac{n^2 + n}{n + 2}$. On calcule u_n/v_n , ça tend vers 0 .

Exemple 1.1.5.

Les croissances comparées vues lors du chapitre sur les suites peuvent se réécrire grâce au symbole o :

- 1. pour tous $\alpha, \beta \in \mathbb{R}$, si $\alpha < \beta$ alors $n^\alpha = o(n^\beta)$.
- 2. pour tous $\alpha, \beta, \gamma \in \mathbb{R}_+^*$, $\ln^\beta(n) = o(n^\alpha)$ et $n^\alpha = o(e^{\gamma n})$.



En accord avec l'hypothèse essentielle de la définition 1.1.1, écrire $u_n = o(0)$ ou $u_n = O(0)$ n'a aucun sens.

Remarque 1.1.6.

Une utilisation fondamentale des relations de comparaison repose sur l'écriture suivante : $u_n = v_n + o(w_n)$, qui signifie $u_n - v_n = o(w_n)$. L'égalité $u_n = v_n + o(w_n)$ exprime que v_n est une approximation de u_n , et que l'erreur de cette approximation est une quantité négligeable devant w_n . Cette égalité est intéressante si u_n est une suite « compliquée », que v_n est une suite « plus simple », et que w_n est elle-même « petite devant u_n et v_n ». Approcher une suite par une autre qui a un comportement plus difficile à étudier n'a en effet aucun intérêt, même si cela peut être tout à fait correct. De même que dire qu'un objet mesure environ 10 cm, au mètre près.

Exemple 1.1.7.

$e^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + o(1/n^2)$. Si on veut être plus précis, on écrit $e^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{1}{6n^3} + o(1/n^3)$, et on a bien $\frac{1}{6n^3} + o(1/n^3) = o(1/n^2)$. Attention, écrire $e^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{1}{6n^3} + o(1/n^2)$ est juste mais n'apporte rien de plus que $e^{1/n} =$

$1 + \frac{1}{n} + \frac{1}{2n^2} + o(1/n^2)$. Pire : $e^{1/n} = 1 + \frac{1}{n} + \frac{1}{2n^2} + \frac{40000}{n^3} + o(1/n^2)$ est juste aussi !

Définition 1.1.8.

Soient (u_n) et (v_n) deux suites. Là encore la définition donnée n'est valable que dans le cas particulier où (v_n) **ne s'annule pas**.

On dit que (u_n) est *équivalente* à (v_n) , ce qui se note $u_n \sim v_n$, si $u_n/v_n \rightarrow 1$.



Là encore, $u_n \sim 0$ n'a aucun sens.

Remarque 1.1.9.

On traduira souvent la relation $u_n \sim v_n$ par : il existe une suite (ε_n) telle que

- $\varepsilon_n \xrightarrow{n \rightarrow +\infty} 1$;
- $\forall n \in \mathbb{N}, u_n = \varepsilon_n v_n$.

Proposition 1.1.10.

Les propositions suivantes sont équivalentes :

(i) $u_n \sim v_n$	(iii) $u_n = v_n + o(v_n)$
(ii) $u_n - v_n = o(v_n)$	(iv) $v_n = u_n + o(u_n)$

Démonstration.

- (i) implique (ii) : $u_n/v_n \rightarrow 1$ et $v_n/v_n \rightarrow 1$, donc $(u_n - v_n)/v_n \rightarrow 0$.
 (ii) implique (i) : même raisonnement.
 (iii) et (iv) ne sont que des reformulations des points précédents. □

Exemple 1.1.11.

- $1/n \sim 1/n + 1/n^2$.
- $n \not\sim e^n$.
- On traduit la limite usuelle

$$\frac{e^{1/n} - 1}{1/n} \xrightarrow{n \rightarrow +\infty} 1$$

par

$$[e^{1/n} - 1] \sim \frac{1}{n}$$

ou, mieux, par

$$e^{1/n} = 1 + \frac{1}{n} + o\left(\frac{1}{n}\right).$$

1.2 Opérations.

a o et O .

Théorème 1.2.1.

Soit $\lambda \in \mathbb{R}^*$, φ une extractrice.

- (i) Multiplication par un réel non nul : si $u_n = o(v_n)$ alors $u_n = o(\lambda v_n)$ et $\lambda u_n = o(v_n)$.
- (ii) Somme : si $u_n = o(v_n)$ et $w_n = o(v_n)$ alors $u_n + w_n = o(v_n)$.



Ce sont des petits o de la même suite.

- (iii) Transitivité : si $u_n = o(v_n)$ et $v_n = o(w_n)$, alors $u_n = o(w_n)$.
- (iv) Transitivité mixte : si $u_n = o(v_n)$ et $v_n = O(w_n)$ (resp. $u_n = O(v_n)$ et $v_n = o(w_n)$), alors $u_n = o(w_n)$.
- (v) Produit 1 : si $u_n = o(v_n)$, alors $w_n u_n = o(w_n v_n)$.
- (vi) Produit 2 : si $u_n = o(v_n)$ et $u'_n = o(v'_n)$ alors $u_n u'_n = o(v_n v'_n)$.
- (vii) Suites extraites : si $u_n = o(v_n)$ alors $u_{\varphi(n)} = o(v_{\varphi(n)})$.
- (viii) Tout reste vrai en remplaçant les o par des grands O .

Démonstration.

Simple : revenir à la définition. □



Deux opérations sur les o sont formellement INTERDITES :

- Sommer deux égalités en o si les suites dans les o ne sont pas les mêmes. Ex : $1/n = o(1)$ et $1/n = o(-1)$, mais $2/n \neq o(0)$.
- Composer une égalité en o par une fonction : $u_n = o(v_n) \not\Rightarrow f(u_n) = o(f(v_n))$. Ex : $f(x) = 1/x$, $1/n = o(1)$ mais $n \neq o(1)$. De même, $1/n^2 = o(1/n)$ mais $e^{1/n^2} \neq o(e^{1/n})$.

b Équivalents.

Théorème 1.2.2.

Soit φ une extractrice.

- (i) La relation $\sim$ est une relation d'équivalence (a : réflexive, b : symétrique, c : transitive).
- (ii) Dans un petit o , on peut remplacer la suite par toute suite équivalente : si $u_n = o(v_n)$ et $v_n \underset{n \rightarrow +\infty}{\sim} w_n$, alors $u_n = o(w_n)$.
- (iii) Deux suites équivalentes ont le même signe à partir d'un certain rang.
- (iv) Produit : si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ et $u'_n \underset{n \rightarrow +\infty}{\sim} v'_n$ alors $u_n u'_n \underset{n \rightarrow +\infty}{\sim} v_n v'_n$.
- (v) Passage à l'inverse : si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ alors $1/u_n \sim 1/v_n$.
- (vi) Puissances : si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ et si $u_n > 0$ à partir d'un certain rang, alors pour tout $a \in \mathbb{R}$, $u_n^a \underset{n \rightarrow +\infty}{\sim} v_n^a$.
- (vii) Suites extraites : si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ alors $u_{\varphi(n)} \underset{n \rightarrow +\infty}{\sim} v_{\varphi(n)}$.

Démonstration.

Simple : revenir aux définitions.

□


 Trois opérations sur les équivalents sont INTERDITES :

- Sommer des équivalents. Ex : $n \underset{n \rightarrow +\infty}{\sim} n$, $-n + 1 \underset{n \rightarrow +\infty}{\sim} -n$ mais $-1 \not\sim 0$.
- Composer par une fonction. Ex : $n^2 \underset{n \rightarrow +\infty}{\sim} n^2 + n$ mais $e^{n^2} \not\sim e^{n^2 + n}$.
- Élever un équivalent à une puissance dépendant de n : $1 + \frac{1}{n} \sim 1$ mais $\left(1 + \frac{1}{n}\right)^n \sim e$. Remarquons que c'est un cas particulier de composition.

Théorème 1.2.3.

 Soit $\ell \in \mathbb{R}$.

- (i) $u_n \rightarrow \ell \in \mathbb{R}^*$ si et seulement si $u_n \underset{n \rightarrow +\infty}{\sim} \ell$.
- (ii) Si $u_n \underset{n \rightarrow +\infty}{\sim} v_n$, alors (u_n) a une limite dans $\overline{\mathbb{R}}$ ssi (v_n) en a une aussi. Dans le cas d'existence de la limite, ces deux limites sont égales. La réciproque est fausse, sauf si $u_n \xrightarrow[n \rightarrow +\infty]{} \ell \in \mathbb{R}^*$.

Démonstration.

Simple : revenir aux définitions.

□


 La réciproque de (ii) est fausse. Ex : $n \rightarrow +\infty$, $n^2 \rightarrow +\infty$, $1/n \rightarrow 0$, $1/n^2 \rightarrow 0$. Pire : $u_n \not\sim u_{n+1}$ si $u_n = (1/2)^n$.

 Il est tentant d'utiliser les symboles $\sim$ et o à tort et à travers, ce qui mène souvent à de graves erreurs.

- Il est interdit de les utiliser simultanément.
- On s'interdira le plus souvent d'écrire une équivalence à une somme, on préférera dans ce cas l'écriture en o .

1.3 Exemples classiques (formulaire).

- Les exemples donnés dans le formulaire sont à connaître par cœur.
- Ne pas oublier l'hypothèse $u_n \xrightarrow[n \rightarrow +\infty]{} 0$.
- Les formules en $\underset{n \rightarrow +\infty}{\sim}$ ne sont pas des doublons de celles en o . Il est faux d'écrire $(1 + u_n)^a \underset{n \rightarrow +\infty}{\sim} 1 + au_n + o(u_n)$ et idiot d'écrire $(1 + u_n)^a \underset{n \rightarrow +\infty}{\sim} 1 + au_n$ (pourquoi ?).

Démonstration.

Démontrons les formules du formulaire.

 La technique générale est la suivante : on part d'une fonction f définie et dérivable au voisinage de 0, et on utilise

$$f'(0) = \lim_{t \rightarrow 0} \frac{f(t) - f(0)}{t},$$
 ce qui, en composant avec u_n donne $\frac{f(u_n) - f(0)}{u_n} = f'(0) + o(1)$, et finalement, $f(u_n) = f(0) + f'(0)u_n + o(u_n)$.

 Pour $\cos$ et ch , une autre méthode est nécessaire : pour $\cos$ on utilise $\cos(2x) = 1 - 2\sin^2(x)$, et on l'applique à $x = \frac{u_n}{2}$.

 Idem avec ch avec $\text{ch}(2x) = 1 + 2\text{sh}^2(x)$.

□

Exemple 1.3.1.

Voici des exemples d'utilisation des relations d'équivalence :

- Donner un équivalent de $\left(\frac{\ln(n+1)}{\ln n}\right)^n - 1$.
- Calculer la limite de la suite $u_n = \left(2 - \cos \frac{1}{n}\right)^n$.
- Calculer la limite de $u_n = e^{-n} \text{ch} \sqrt[4]{n^4 + 1}$.

1.4 Formule de Stirling.

Voici un équivalent célèbre, qui sera démontré en DM.

Proposition 1.4.1 (Formule de Stirling).

$$n! \sim \sqrt{2n\pi} \left(\frac{n}{e}\right)^n$$

Corollaire 1.4.2.

On a le développement asymptotique

$$\ln(n!) \underset{n \rightarrow +\infty}{=} n \ln(n) - n + \frac{1}{2} \ln(n) + \frac{1}{2} \ln(2\pi) + o(1).$$

Démonstration.

Il suffit de voir par la formule de Stirling que

$$\ln \left(\frac{n!}{\sqrt{n} \left(\frac{n}{e}\right)^n} \right) \xrightarrow{n \rightarrow +\infty} \ln \sqrt{2\pi},$$

ce qui s'écrit exactement

$$\ln(n!) - \left(n \ln(n) - n + \frac{1}{2} \ln(n) \right) \underset{n \rightarrow +\infty}{=} \frac{1}{2} \ln(2\pi) + o(1).$$

□

2 Comparaison de fonctions.

Nous allons maintenant adapter les outils de la section précédente aux fonctions.

Dans toute cette section, I et J sont des intervalles de $\mathbb{R}$, $f, g, h, k : I \rightarrow \mathbb{R}$ sont quatre applications, et $a \in \bar{I}$.

2.1 Définitions.

a o et O .

Définition 2.1.1.

Nous supposons que la fonction g ne s'annule pas au voisinage de a , sauf éventuellement en a .

(i) On dit que f est *dominée par g au voisinage de a* , ce qui se note $f =_a O(g)$ ou $f(x) \underset{x \rightarrow a}{=} O(g(x))$, et se lit « f est un grand O de g au voisinage de a », si f/g est bornée au voisinage de a .

Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I \setminus \{a\}$.

(ii) On dit que f est *négligeable devant g au voisinage de a* , ce qui se note $f =_a o(g)$ ou $f(x) \underset{x \rightarrow a}{=} o(g(x))$, et se lit « f est un petit o de g au voisinage de a », si $\lim_a f/g = 0$.

Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I \setminus \{a\}$.

Remarque 2.1.2.

Ces définitions sont les mêmes que pour les suites, à ceci près que pour des fonctions il faut spécifier un point au voisinage duquel ces relations sont valables. Pour les suites, il s'agissait toujours de $+\infty$.

Remarque 2.1.3.

Comme pour les suites, on traduira souvent $f \underset{x \rightarrow a}{=} o(g)$ par : il existe $\varepsilon : I \rightarrow \mathbb{R}$ vérifiant

- $\varepsilon(x) \xrightarrow{x \rightarrow a} 0$;
- $\forall x \in I, f(x) = \varepsilon(x)g(x)$.

Remarque 2.1.4.

- Comme pour les suites, $f =_a o(0)$ ou $f =_a O(0)$ n'ont pas de sens.
- Comme pour les suites, petit o implique O .
- $f =_a O(1)$ signifie que f est bornée au voisinage de a , et $f =_a o(1)$ signifie que $f \xrightarrow{a} 0$.

Exemple 2.1.5.

Fondamental : les croissances comparées s'expriment ainsi.

En $+\infty$:

1. Soient $\alpha, \beta \in \mathbb{R}$ tels que $\alpha < \beta$. Alors $x^\alpha \underset{x \rightarrow +\infty}{=} o(x^\beta)$.
2. Soient $a, b \in \mathbb{R}$ tels que $0 < a < b$. Alors $a^x \underset{x \rightarrow +\infty}{=} o(b^x)$.
3. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$. Alors $(\ln x)^\beta \underset{x \rightarrow +\infty}{=} o(x^\alpha)$.

4. Soient $a, \alpha \in \mathbb{R}$ avec $a > 1$. Alors $x^\alpha \underset{x \rightarrow +\infty}{=} o(a^x)$.

En 0 :

1. Soient $\alpha, \beta \in \mathbb{R}$ tels que $\alpha < \beta$. Alors $x^\beta \underset{x \rightarrow 0}{=} o(x^\alpha)$.
2. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$. Alors $|\ln x|^\beta \underset{x \rightarrow 0}{=} o(x^{-\alpha})$.
3. Soient $\alpha, \beta \in \mathbb{R}$ avec $\alpha > 0$. Alors $x^\alpha \underset{x \rightarrow 0}{=} o(|\ln x|^\beta)$.

Exemple 2.1.6. 1. $x^2 \underset{x \rightarrow +\infty}{=} o(x^4)$, et $x^4 \underset{x \rightarrow 0}{=} o(x^2)$.

2. $1/x^4 \underset{x \rightarrow +\infty}{=} o(1/x^2)$, et $1/x^2 \underset{x \rightarrow 0}{=} o(1/x^4)$.

b Équivalents.

Définition 2.1.7.

Nous supposons que la fonction g ne s'annule pas au voisinage de a , sauf éventuellement en a .

On dit que f est *équivalente* à g au voisinage de a , ce qui se note $f \sim_a g$ ou $f(x) \underset{x \rightarrow a}{\sim} g(x)$, et se lit « f est équivalente à g au voisinage de a », si $f/g \underset{a}{\rightarrow} 1$.

Cette définition se généralise au cas où f et g ne sont pas définies en a : il suffit de remplacer tous les I par des $I \setminus \{a\}$.



$f \sim_a 0$ n'a pas de sens.

Remarque 2.1.8.

Comme pour les suites, on traduira souvent $f \underset{x \rightarrow a}{\sim} (g)$ par : il existe $\varepsilon : I \rightarrow \mathbb{R}$ vérifiant

- $\varepsilon(x) \underset{x \rightarrow a}{\rightarrow} 1$;
- $\forall x \in I, f(x) = \varepsilon(x)g(x)$.

Remarque 2.1.9.

Comme pour les suites, $\sim$ implique O .

Théorème 2.1.10.

$f \sim_a g$ si et seulement si $f - g =_a o(g)$ si et seulement si $f - g =_a o(f)$.



Les propositions « $\lim_{x \rightarrow a} \frac{f(x)}{g(x)} = 1$ » et « $(f(x) - g(x)) \underset{x \rightarrow a}{\rightarrow} 0$ » ne sont en aucun cas équivalentes : aucune n'implique l'autre !

Avec le théorème précédent, on voit en effet que $\frac{f(x)}{g(x)} \underset{x \rightarrow a}{\rightarrow} 1$ signifie $f - g =_a o(g)$ tandis que $(f(x) - g(x)) \underset{x \rightarrow a}{\rightarrow} 0$ signifie $f - g =_a o(1)$.

Par exemple, $x + 1 \underset{x \rightarrow +\infty}{\sim} x$, mais $(x + 1) - x \not\underset{x \rightarrow +\infty}{\rightarrow} 0$.

Exemple 2.1.11. 1. $\frac{1}{x} \underset{x \rightarrow +\infty}{\sim} \frac{1}{x} + \frac{1}{x^2}$.

2. $x \not\underset{x \rightarrow +\infty}{\sim} e^x$.

Théorème 2.1.12. (i) Si $f \sim_a g$, alors soit f et g ont toutes les deux une même limite dans $\overline{\mathbb{R}}$ en a , soit aucune des deux n'a de limite en a .

- (ii) $f(x) \underset{x \rightarrow a}{\rightarrow} \ell \in \mathbb{R}^*$ si et seulement si $f(x) \underset{x \rightarrow a}{\sim} \ell$.

2.2 Opérations.

a o et O .

Théorème 2.2.1.

Soit $\lambda \in \mathbb{R}^*$.

- (i) Multiplication par un réel non nul : si $f =_a o(g)$, alors $f =_a o(\lambda g)$ et $\lambda f =_a o(g)$.
- (ii) Somme : si $f =_a o(g)$ et $h =_a o(g)$, alors $f + h =_a o(g)$.



Ce sont des o de la même fonction.

- (iii) Transitivité : si $f =_a o(g)$ et $g =_a o(h)$, alors $f =_a o(h)$.
- (iv) Produit 1 : si $f =_a o(g)$, alors $fh =_a o(gh)$.
- (v) Produit 2 : si $f =_a o(g)$ et $h =_a o(k)$, alors $fh =_a o(gk)$.
- (vi) Composition à droite : si $b \in \overline{\mathbb{R}}$, et si φ est une fonction définie au voisinage de b à

valeurs dans I et telle que $\varphi \xrightarrow{b} a$, alors si $f =_a o(g)$, on a aussi $f \circ \varphi =_b o(g \circ \varphi)$.

- (vii) Tout ceci reste vrai en remplaçant les o par des grands O .

Démonstration.

Simple : revenir aux définitions. $\square$



Deux opérations sont formellement INTERDITES :

1. Les sommes des deux côtés : $f =_a o(g)$ et $h =_a o(k) \not\Rightarrow f + h =_a o(g + k)$.
2. La composition à gauche : si ψ est une application de $\mathbb{R}$ dans $\mathbb{R}$ $f =_a o(g) \not\Rightarrow \psi \circ f =_{\psi(a)} o(\psi \circ g)$. Par exemple $x^2 \underset{x \rightarrow 0}{=} o(x)$, mais $e^{x^2} \underset{x \rightarrow 0}{\neq} o(e^x)$.

Remarque 2.2.2.

Le point (vi) permet de faire des translations : par exemple, $x^4 \underset{x \rightarrow 0}{=} o(x^2)$ donc $(x - 1)^4 \underset{x \rightarrow 1}{=} o((x - 1)^2)$.

Il permet aussi de passer d'une relation au voisinage de 0 à une relation au voisinage de $\pm\infty$, et vice-versa. Par exemple, $x^5 \underset{x \rightarrow 0}{=} o(x)$ implique

$$\frac{1}{x^5} \underset{x \rightarrow +\infty}{=} o\left(\frac{1}{x}\right).$$

Remarque 2.2.3.

Comme avec les suites, écrire $f = g + o(h)$ signifie que $f - g = o(h)$. Cela permet de faire des développements, comme avec les suites.

b Équivalents.

Théorème 2.2.4.

Soit $\lambda \in \mathbb{R}$.

- (i) La relation $\sim$ est une relation d'équivalence (a : réflexive, b : symétrique, c : transitive).
- (ii) Dans un petit o , on peut remplacer la fonction par toute fonction équivalente : si $f =_a o(g)$ et $g \sim_a h$, alors $f =_a o(h)$.
- (iii) Deux fonctions équivalentes au voisinage de a ont le même signe sur un voisinage de a .

- (iv) Produit : si $f \sim_a g$ et $h \sim_a k$, alors $fh \sim_a gk$.

- (v) Inverse : si $f \sim_a g$, alors $\frac{1}{f} \sim_a \frac{1}{g}$.

- (vi) Puissances : pour tout $\alpha \in \mathbb{R}$, si $f \sim_a g$ et si $f > 0$ au voisinage de a , alors $f^\alpha \sim_a g^\alpha$.

- (vii) Composition à droite : si $b \in \bar{\mathbb{R}}$, et si φ est une fonction définie au voisinage de b à valeurs dans I et telle que $\varphi \xrightarrow{b} a$, alors si $f \sim_a g$, on a aussi $f \circ \varphi \sim_b g \circ \varphi$.

Démonstration.

Simple : revenir aux définitions. $\square$



Trois opérations sont formellement INTERDITES :

1. Les sommes d'équivalents : $f \sim_a g$ et $h \sim_a k \not\Rightarrow f + h \sim_a g + k$.
2. La composition à gauche : si ψ est une application de $\mathbb{R}$ dans $\mathbb{R}$ $f \sim_a g \not\Rightarrow \psi \circ f \sim_{\psi(a)} \psi \circ g$. Par exemple $x \underset{x \rightarrow +\infty}{\sim} x + 1$, mais $e^x \underset{x \rightarrow +\infty}{\not\sim} e^{x+1}$.
3. Élever un équivalent à une puissance dépendant de x (cas particulier de la composition à gauche) : $1 + x \underset{x \rightarrow 0}{\sim} 1$ mais $(1 + x)^{1/x} \underset{x \rightarrow 0}{\not\sim} e$.

Exemple 2.2.5.

Donner la limite en 0 de $x \mapsto \frac{\ln(1 + \tan(2x))}{\sin(4x)}$.

3 Développements limités.

Nous allons maintenant utiliser les relations de comparaison dans un cas particulier : celui du développement limité, qui est une approximation d'une fonction en un point par un polynôme.

Dans tout ce chapitre, n est un entier naturel, I et J sont deux intervalles de $\mathbb{R}$, f est une fonction de I dans $\mathbb{R}$ et x_0 un point de I .

3.1 Définition et premières propriétés.

Définition 3.1.1.

On dit que f admet un **développement limité d'ordre n au voisinage d'un point** $x_0 \in I$ s'il existe des réels $a_0 \dots a_n$ tels que

$$f(x) \underset{x \rightarrow x_0}{=} a_0 + a_1(x - x_0) + a_2(x - x_0)^2 + \dots + a_n(x - x_0)^n + o((x - x_0)^n).$$

On dit que le polynôme

$$a_0 + a_1(x - x_0) + a_2(x - x_0)^2 + \dots + a_n(x - x_0)^n$$

est la **partie principale** ou **régulière** du DL, et que le terme $o((x - x_0)^n)$ est son **reste**.

L'écriture

$$f(x) \underset{x \rightarrow x_0}{=} (x - x_0)^p \left(a_0 + a_1(x - x_0) + a_2(x - x_0)^2 + \dots + a_n(x - x_0)^n + o((x - x_0)^n) \right)$$

avec $a_0 \neq 0$ est appelée **forme normalisée** du DL, c'est aussi

$$f(x) \underset{x \rightarrow x_0}{=} a_0(x - x_0)^p + a_1(x - x_0)^{p+1} + a_2(x - x_0)^{p+2} + \dots + a_n(x - x_0)^{p+n} + o((x - x_0)^{p+n}).$$

L'entier p est alors la **valuation** du DL : c'est le degré du premier terme non nul du DL.

Remarque 3.1.2.

Dans la suite on utilisera la notation « f admet un DL(x_0, n) » (ou $DL_n(x_0)$) pour dire que f admet un DL d'ordre n en x_0 .



Cette notation n'a **rien** d'officiel et ne devra **en aucun cas** être utilisée ailleurs qu'en cours et en TD.

Exemple 3.1.3.

La fonction $x \mapsto \frac{1}{1-x}$ admet un DL($0, n$) pour

tout n , et l'on en connaît explicitement le reste, à savoir : $\frac{1}{1-x} \underset{x \rightarrow 0}{=} 1 + x + x^2 + x^3 + \dots + x^n + \frac{x^{n+1}}{1-x}$,

et en 0 on a bien $\frac{x^{n+1}}{1-x} \underset{x \rightarrow 0}{=} o(x^n)$.

Remarque 3.1.4.

f admet un DL(x_0, n) si et seulement si $h \mapsto f(x_0 + h)$ admet un DL($0, n$). Autrement dit, en posant $h = x - x_0$, on peut toujours se ramener à un DL en zéro.

Remarque 3.1.5.

Si f admet un DL d'ordre n en x_0 , et si $m \in \mathbb{N}$ est inférieur à n , alors f admet un DL d'ordre m en x_0 . En effet, il suffit de ne garder que les termes de degré inférieur à m : on réalise ainsi une **troncature** du DL. En particulier, le premier terme non nul d'un DL fournit un équivalent de f . Par exemple, si

$$f(x) \underset{x \rightarrow x_0}{=} 2(x - x_0)^2 - (x - x_0)^3 + o((x - x_0)^3),$$

alors $f(x) \underset{x \rightarrow x_0}{\sim} 2(x - x_0)^2$.

Théorème 3.1.6 (unicité du DL).

La partie principale d'un DL(x_0, n) de f est unique, c'est-à-dire : si $a_0 \dots a_n$ et $b_0 \dots b_n$ sont tels que

$$f(x) \underset{x \rightarrow x_0}{=} a_0 + a_1(x - x_0) + a_2(x - x_0)^2 + \dots + a_n(x - x_0)^n + o((x - x_0)^n)$$

et $f(x) \underset{x \rightarrow x_0}{=} b_0 + b_1(x - x_0) + b_2(x - x_0)^2 + \dots + b_n(x - x_0)^n + o((x - x_0)^n)$

alors $\forall i \in \{0, \dots, n\}, a_i = b_i$.

Démonstration.

En effet, en faisant la différence des deux développements, on a

$$(a_0 - b_0) + (a_1 - b_1)(x - x_0) + \dots + (a_n - b_n)(x - x_0)^n = o((x - x_0)^n).$$

Si on considère le plus petit entier $k \in \{0, \dots, n\}$ tel que $a_k \neq b_k$ alors, en divisant par $(x - x_0)^k$, on a

$$(a_k - b_k) + \sum_{i=k+1}^n (a_i - b_i)(x - x_0)^{i-k} = o((x - x_0)^{n-k}).$$

Par passage à la limite en x_0 , $a_k = b_k$. □

Corollaire 3.1.7.

Si f est paire (resp. impaire) et admet un DL(0, n), alors la partie principale de ce DL est un polynôme pair (resp. impair).

Démonstration.

Traisons le cas où f est paire, le cas où f est impaire se traitant de la même manière. On a $f(x) \underset{x \rightarrow 0}{=} a_0 + a_1x + a_2x^2 + \dots + a_nx^n + o(x^n)$.

En écrivant que $f(x) = f(-x)$, on obtient que $a_0 - a_1x + a_2x^2 - a_3x^3 + \dots + (-1)^n a_nx^n + o(x^n)$ est aussi un DL(0, n) de f . Par unicité de ce DL, on peut identifier tous les coefficients, ce qui assure que les coefficients des termes de degré impair sont nuls. $\square$

Théorème 3.1.8. (i) f est continue en x_0 ssi f admet un DL(x_0 , 0). En effet, on a alors $f(x) \underset{x \rightarrow x_0}{=} f(x_0) + o(1)$. Le coefficient constant d'un DL(x_0 , n) de f donne toujours la valeur de f en x_0 .

(ii) f est dérivable en x_0 ssi f admet un DL(x_0 , 1). En effet, si

$$f(x) \underset{x \rightarrow x_0}{=} f(x_0) + f'(x_0)(x - x_0) + o(x - x_0)$$

alors le coefficient du terme de degré 1 d'un DL(x_0 , n) de f donne toujours la valeur de f' en x_0 .



Attention ! Les termes de degrés supérieurs ne donnent pas les dérivées suivantes de f . Et même pire : une fonction peut admettre un DL(x_0 , 2) et ne pas être deux fois dérivable en x_0 .

Exemple 3.1.9.

$$x \mapsto x^3 \mathbf{1}_{\mathbb{Q}}(x)$$

Exemple 3.1.10.

$$x \mapsto \begin{cases} x^3 \sin \frac{1}{x^3} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

Exemple 3.1.11.

Notons $f : \mathbb{R} \rightarrow \mathbb{R}$

$$x \mapsto \begin{cases} e^{-\frac{1}{x^2}} \sin \left(e^{\frac{1}{x^2}} \right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

• Montrons que f admet un DL(0, n) pour tout n : on a $\left| \frac{f(x)}{x^n} \right| \leq \frac{e^{-\frac{1}{x^2}}}{|x|^n} = \left(\frac{2}{nx^2} e^{-\frac{2}{nx^2}} \right)^{\frac{n}{2}} \left(\frac{n}{2} \right)^{\frac{n}{2}}$.

Or $ue^{-u} \xrightarrow{u \rightarrow +\infty} 0$ donc $\frac{f(x)}{x^n} \xrightarrow{x \rightarrow 0} 0$, ce qui montre bien que $f(x) \underset{x \rightarrow 0}{=} o(x^n)$. f admet donc bien un DL en 0 à tout ordre, de partie principale nulle.

• Ceci implique donc que $f(0) = 0$ et $f'(0) = 0$. f est donc dérivable en 0, mais montrons que f' n'est pas continue en 0. Ainsi f n'est pas deux fois dérivable en 0. On calcule pour $x \neq 0$:

$$f'(x) = \frac{2f(x)}{x^3} - \frac{2}{x^3} \cos \left(e^{\frac{1}{x^2}} \right)$$

D'après ce qui précède, $\frac{2f(x)}{x^3} \xrightarrow{x \rightarrow 0} 0$. Montrons que

$$\frac{2}{x^3} \cos \left(e^{\frac{1}{x^2}} \right)$$

n'a pas 0 pour limite en 0 : ainsi on aura bien $f'(x) \not\xrightarrow{x \rightarrow 0} f'(0)$. Si l'on pose $u_n = \frac{1}{\sqrt{\ln(2n\pi)}}$,

on a : $\frac{2}{u_n^3} \cos \left(e^{\frac{1}{u_n^2}} \right) = \frac{2}{u_n^3} = \left(\ln(2n\pi) \right)^{\frac{3}{2}}$, qui a pour limite $+\infty$ quand n tend vers $+\infty$. On conclut avec l'argument de composition de limites.

3.2 Opérations sur les DL.

Nous allons maintenant voir comment effectuer des opérations sur les DL. Le point délicat n'est pas tant d'effectuer les calculs, mais d'anticiper le degré du DL obtenu, connaissant les degrés des DL initiaux intervenant dans les calculs.

Au cours des calculs, plusieurs restes vont apparaître, mais à chaque étape, les restes les plus petits, ou les plus précis, s'effacent devant le reste dominant. C'est le degré de ce reste dominant qu'il faut savoir déterminer a fortiori.

a Somme.**Proposition 3.2.1.**

Si f et g admettent un DL en x_0 , respectivement d'ordre n et m , alors $f + g$ admet un DL en x_0 , d'ordre $\min(n, m)$, obtenu en faisant la somme des DL de f et g .

Démonstration.

Les parties principales des deux DL donnent un polynôme. À ce polynôme s'ajoutent deux restes : l'un d'ordre n et l'autre d'ordre m . C'est le plus petit exposant, i.e. $\min(n, m)$ qui désigne le reste dominant. $\square$



L'ordre du DL d'une somme est le min des ordres des deux DL. En additionnant un DL d'ordre 3 à un DL d'ordre 2, on n'a aucune chance de récupérer un DL d'ordre 3 !

Exemple 3.2.2.

On a les DL suivants,

$$\begin{aligned}\cos(x) &= 1 - \frac{1}{2}x^2 + o(x^2) \\ \exp(x) &= 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + o(x^3) \\ &= 1 + x + \frac{1}{2}x^2 + o(x^2)\end{aligned}$$

donc on obtient de DL à l'ordre 2 :

$$\cos(x) + \exp(x) = 2 + x + o(x^2).$$

Remarque 3.2.3.

On prendra soin, en additionnant deux DL, d'aligner verticalement les termes de mêmes degrés.

b Produit.

Étudions d'abord un cas particulier :

Proposition 3.2.4.

Soient f et g admettant chacune un DL en x_0 , respectivement d'ordre n et m . Supposons que les termes constants de ces deux DL sont non nuls. Alors fg admet un DL en x_0 , d'ordre exactement $\min(n, m)$, obtenu en faisant le produit des DL de f et g , dont on ne garde que les termes de degré inférieur à $\min(n, m)$.

Démonstration.

Lorsque l'on développe le produit de ces deux DL, il apparaît plusieurs restes. Parmi ces restes il y a le terme constant du DL de f fois le reste du DL de g , et le terme constant du DL de g fois le reste du DL de f . L'un de ces deux restes est forcément le terme dominant du DL du produit. $\square$

Exemple 3.2.5.

Avec

$$\begin{aligned}f(x) &= 2 - x + 3x^2 + o(x^2) \\ g(x) &= 1 + 2x - 3x^2 + x^3 + o(x^3) \\ &= 1 + 2x - 3x^2 + o(x^2)\end{aligned}$$

on a

$$\begin{aligned}f(x)g(x) &= 2 + 4x - 6x^2 + o(x^2) \\ &\quad - x - 2x^2 + o(x^2) \\ &\quad + 3x^2 + o(x^2) \\ &= 2 + 3x - 5x^2 + o(x^2).\end{aligned}$$

Traitons maintenant le cas général :

Proposition 3.2.6.

Soient f et g admettant chacune un DL en x_0 , respectivement d'ordre n et m , et de valuation p et q . Alors fg admet un DL en x_0 , d'ordre exactement $\min(n-p, m-q) + p + q$ ($> \min(n, m)$ si p et q sont non nuls).

Démonstration.

Écrivons les formes normalisées des deux DL :

$$\begin{aligned}f(x) &= (x - x_0)^p \left(a_0 + a_1(x - x_0) \right. \\ &\quad \left. + a_2(x - x_0)^2 + \dots \right. \\ &\quad \left. + a_{n-p}(x - x_0)^{n-p} + o((x - x_0)^{n-p}) \right)\end{aligned}$$

et

$$\begin{aligned}g(x) &= (x - x_0)^q \left(b_0 + b_1(x - x_0) \right. \\ &\quad \left. + b_2(x - x_0)^2 + \dots \right. \\ &\quad \left. + b_{m-q}(x - x_0)^{m-q} + o((x - x_0)^{m-q}) \right)\end{aligned}$$

Le produit de ces deux DL est donc

$$\begin{aligned}(x - x_0)^{p+q} &\left((a_0 + \dots + o((x - x_0)^{n-p})) \right. \\ &\quad \left. (b_0 + \dots + o((x - x_0)^{m-q})) \right)\end{aligned}$$

Le DL entre les grandes parenthèses est le produit de deux DL dont les termes constants sont non nuls. Son degré est donc $\min(n-p, m-q)$ d'après 3.2.4. $\square$

Exemple 3.2.7.

Avec $f(x) = x - 2x^2 + o(x^2)$ et $g(x) = x +$

$x^2 + o(x^2)$, on a

$$\begin{aligned} f(x)g(x) &\underset{x \rightarrow 0}{=} x^2(1 - 2x + o(x))(1 + x + o(x)) \\ &\underset{x \rightarrow 0}{=} x^2(1 - x + o(x)) \\ &\underset{x \rightarrow 0}{=} x^2 - x^3 + o(x^3), \end{aligned}$$

qui est bien un DL d'ordre 3.

c Composition.

Proposition 3.2.8.

Soit f admettant un $DL(0, n)$, de partie principale F , dont le terme constant est nul, c'est-à-dire vérifiant $f(0) = 0$, et soit g admettant un $DL(0, n)$, de partie principale G . Alors $g \circ f$ admet un $DL(0, n)$ dont la partie principale est $G \circ F$ dont on a retiré les termes de degré strictement supérieur à n .

Démonstration.

Le résultat est immédiat si $n = 0$ (par composition de limites). Supposons que $n \geq 1$. On a $f(x) \underset{x \rightarrow 0}{=} F(x) + o(x^n)$ et $g(x) \underset{x \rightarrow 0}{=} G(x) + o(x^n)$.

Comme f est continue en 0 et comme $f(0) = 0$, on a $f(x) \xrightarrow{x \rightarrow 0} 0$, donc

$$g(f(x)) \underset{x \rightarrow 0}{=} G(f(x)) + o(f^n(x)).$$

Comme f admet un développement limité à l'ordre 1 de la forme $f(x) \underset{x \rightarrow 0}{=} ax + o(x)$, on peut écrire $f(x) \underset{x \rightarrow 0}{=} O(x)$, donc $f^n(x) \underset{x \rightarrow 0}{=} O(x^n)$, donc

$$g(f(x)) \underset{x \rightarrow 0}{=} G(f(x)) + o(x^n).$$

Un calcul simple (par exemple avec le binôme de Newton, ou une récurrence sur k en utilisant la propriété de produit de deux DL) assure que, si $k \geq 1$:

$$\begin{aligned} f^k(x) &\underset{x \rightarrow 0}{=} (F(x) + o(x^n))^k \\ &\underset{x \rightarrow 0}{=} F^k(x) + o(x^n). \end{aligned}$$

En écrivant sous forme développée-réduite $G = b_0 + b_1X + \dots + b_nX^n$, on a donc

$$\begin{aligned} g(f(x)) &\underset{x \rightarrow 0}{=} b_0 + \sum_{k=1}^n b_k f^k(x) + o(x^n) \\ &\underset{x \rightarrow 0}{=} b_0 + \sum_{k=1}^n b_k F^k(x) + o(x^n) \\ &\underset{x \rightarrow 0}{=} G(F(x)) + o(x^n). \end{aligned}$$

□

Remarque 3.2.9.

Ce résultat s'étend tout à fait au cas où f admet un $DL(x_0, n)$ avec $f(x_0) = a_0$, et où g admet un $DL(a_0, n)$: il suffit alors de composer les DL en ne gardant que les termes de degré inférieur ou égal à n .

Exemple 3.2.10.

Trouver un $DL(0, 4)$ de $e^{\cos x}$: on a

$$\cos x \underset{x \rightarrow 0}{=} 1 - x^2/2 + x^4/24 + o(x^4) = 1 + X.$$

D'où

$$e^{\cos x} \underset{x \rightarrow 0}{=} e^{1+X} \underset{x \rightarrow 0}{=} e \cdot e^X \underset{x \rightarrow 0}{=} e(1 + X + X^2/2 + o(X^2)).$$

Il suffit en effet de s'arrêter au terme de degré 2 dans le DL de l'exponentielle, car $X \sim \frac{-1}{2}x^2$, donc les termes négligeables devant X^2 (le $o(X^2)$) seront négligeables devant x^4 . On calcule alors, avec

$$X \underset{x \rightarrow 0}{=} \frac{-x^2}{2} + \frac{x^4}{24} + o(x^4),$$

et on obtient

$$e^{\cos x} \underset{x \rightarrow 0}{=} e(1 - x^2/2 + x^4/6) + o(x^4).$$

d Quotient.

Traisons un premier cas :

Proposition 3.2.11.

Si g admet un $DL(x_0, n)$ de valuation $p = 0$ (ainsi le terme constant de g n'est pas nul), alors $1/g$ admet aussi un $DL(x_0, n)$.

Démonstration.

On écrit

$$\begin{aligned} g(x) &\underset{x \rightarrow x_0}{=} b_0 + b_1(x - x_0) + b_2(x - x_0)^2 + \dots + \\ &b_n(x - x_0)^n + o((x - x_0)^n) \underset{x \rightarrow x_0}{=} b_0(1 - u) \text{ avec } u = \\ &\frac{b_1(x - x_0) + b_2(x - x_0)^2 + \dots + b_n(x - x_0)^n + o((x - x_0)^n)}{b_0}. \end{aligned}$$

Il suffit de composer ce DL avec celui de $\frac{1}{1-u}$. □

Proposition 3.2.12.

Si f et g admettent un $DL(x_0, n)$ et si le terme constant de g n'est pas nul, alors f/g admet aussi un $DL(x_0, n)$.

Démonstration.

Il suffit de multiplier le DL(x_0, n) de f avec celui de $1/g$. $\square$

Exemple 3.2.13.

$$\begin{aligned}\tan x &= \frac{\sin x}{\cos x} \\ &= \frac{x - x^3/6 + x^5/120 + o(x^5)}{1 - x^2/2 + x^4/24 + o(x^5)} \\ &= \left(x - x^3/6 + x^5/120 + o(x^5)\right) \times \left(1 + u(x) + u(x)^2 + o(u(x)^2)\right) \\ &\quad \text{où } u(x) = x^2/2 - x^4/24 + o(x^5)\end{aligned}$$

Il est inutile de calculer u^3 qui donnera des termes en x^6 . En effet, $u(x) \underset{x \rightarrow 0}{\sim} \frac{x^2}{2}$, donc $o(u(x)^3) \subset o(x^5)$. Donc

$$\begin{aligned}\tan x &\underset{x \rightarrow 0}{=} \left(x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5)\right) \\ &\quad \times \left(1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + o(x^5)\right) \\ &\underset{x \rightarrow 0}{=} x \left(1 - \frac{x^2}{6} + \frac{x^4}{120} + o(x^4)\right) \\ &\quad \times \left(1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + o(x^4)\right) \\ &\underset{x \rightarrow 0}{=} x + \frac{x^3}{3} + \frac{2x^5}{15} + o(x^5)\end{aligned}$$

Et le cas général :

Proposition 3.2.14.

Soit f admettant un DL en x_0 d'ordre n et de valuation p . Alors $1/f$ admet en x_0 un développement de la forme $\frac{P(x - x_0) + o((x - x_0)^{n-p})}{(x - x_0)^p}$, où P est un polynôme de terme constant non nul. Si $p > 0$, ce développement est dit *asymptotique*.

Démonstration.

Il suffit d'écrire le DL de f sous forme normalisée : $f(x) = (x - x_0)^p \cdot (F(x - x_0) + o((x - x_0)^{n-p}))$, où F est un polynôme de terme constant non nul. Alors $1/f = \frac{1}{(x - x_0)^p \cdot (F(x - x_0) + o((x - x_0)^{n-p}))}$, et d'après 3.2.12, $\frac{1}{F(x - x_0) + o((x - x_0)^{n-p})}$ admet un DL à l'ordre $n - p$, d'où l'existence du polynôme P de l'énoncé. Mais comme

le terme constant de P n'est pas nul, si $p > 0$, $\frac{P(x - x_0)}{(x - x_0)^p}$ n'est pas un polynôme mais une fraction rationnelle qui tend vers l'infini (en valeur absolue) en x_0 , et le développement est dit asymptotique. $\square$

Exemple 3.2.15.

Donner un développement asymptotique de $\frac{1}{x^2 + 2x^3 - x^4 + o(x^5)}$ en 0.

3.3 Intégration et dérivation.
Proposition 3.3.1.

Si f est continue et dérivable au voisinage de x_0 et si f' admet un DL(x_0, n), alors f admet un DL($x_0, n + 1$) dont la partie principale est la primitive de la partie principale du DL de f' qui vaut $f(x_0)$ en x_0 .

Démonstration.

Donnons la démonstration dans le cas $x_0 = 0$. On a

$$f'(x) \underset{x \rightarrow 0}{=} a_0 + a_1x + a_2x^2 + \dots + a_nx^n + o(x^n)$$

Posons

$$\begin{aligned}F : I &\rightarrow \mathbb{R} \\ x &\mapsto f(x) - f(0) - a_0x - \frac{a_1}{2}x^2 - \dots - \frac{a_n}{n+1}x^{n+1}\end{aligned}$$

Alors $F(0) = 0$ et

$$\forall x \in I \quad F'(x) = f'(x) - a_0 - a_1x - a_2x^2 - \dots - a_nx^n$$

On a donc $F'(x) \underset{x \rightarrow 0}{=} o(x^n)$. En appliquant le TAF entre 0 et x on obtient : il existe $\theta_x \in]0, 1[$ tel que

$$\begin{aligned}F(x) - F(0) &= xF'(\theta_x x) \\ \text{d'où } F(x) &\underset{x \rightarrow 0}{=} xo(\theta_x^n x^n) \\ \text{donc } F(x) &\underset{x \rightarrow 0}{=} o(x^{n+1})\end{aligned}$$

On a donc

$$f(x) \underset{x \rightarrow 0}{=} f(0) + a_0x + \frac{a_1}{2}x^2 + \dots + \frac{a_n}{n+1}x^{n+1} + o(x^{n+1})$$

$\square$

Exemple 3.3.2.

Cette proposition permet de déterminer les DL de $\ln(1 - x)$, $\ln(1 + x)$ et $\text{Arctan } x$, en primitivant les DL de $-1/(1 - x)$, $1/(1 + x)$ et $1/(1 + x^2)$.

Proposition 3.3.3.

Si f admet un DL(x_0, n) et si l'on sait que f' admet un DL($x_0, n-1$) (par exemple parce que f est de classe $\mathcal{C}^n$), alors le DL de f' s'obtient en dérivant celui de f .

Exemple 3.3.4.

Le DL de $\sqrt{1+x}$ redonne celui de $\frac{1}{\sqrt{1+x}}$.

Le DL de $\frac{1}{1+x}$ donne celui de $\frac{1}{(1+x)^2}$.

3.4 Formule de Taylor-Young.**Théorème 3.4.1** (Formule de Taylor-Young).

Si f est de classe $\mathcal{C}^n$ sur I , alors f possède un DL(x_0, n) donné par la formule de Taylor-Young :

$$f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^n),$$

soit

$$f(x) \underset{x \rightarrow x_0}{=} f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2}(x - x_0)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n + o((x - x_0)^n).$$

Démonstration.

Démontrons le résultat par récurrence. Pour $n \in \mathbb{N}$, on note $P(n)$ l'assertion « $\forall f \in \mathcal{C}^n(I, \mathbb{R})$ $f(x) \underset{x \rightarrow x_0}{=} \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^n)$ ».

$$\sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^n).$$

$P(0)$ est vrai d'après les résultats sur les fonctions continues.

Montrons $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.

Soit $n \in \mathbb{N}$, supposons $P(n)$. Montrons $P(n+1)$. Soit f de classe $\mathcal{C}^{n+1}$. Alors f' est de classe $\mathcal{C}^n$, donc par $P(n)$,

$$\begin{aligned} f'(x) &\underset{x \rightarrow x_0}{=} \sum_{k=0}^n \frac{(f')^{(k)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^n) \\ &= \sum_{k=0}^n \frac{f^{(k+1)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^n) \end{aligned}$$

D'après la proposition 3.3.1, on a donc :

$$\begin{aligned} f(x) &\underset{x \rightarrow x_0}{=} f(x_0) + \sum_{k=0}^n \frac{f^{(k+1)}(x_0)}{(k+1)k!} (x - x_0)^{k+1} \\ &\quad + o((x - x_0)^{n+1}) \\ &\underset{x \rightarrow x_0}{=} f(x_0) + \sum_{k=0}^n \frac{f^{(k+1)}(x_0)}{(k+1)!} (x - x_0)^{k+1} + o((x - x_0)^{n+1}) \\ &\underset{x \rightarrow x_0}{=} f(x_0) + \sum_{k=1}^{n+1} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k \\ &\quad + o((x - x_0)^{n+1}) \\ &\underset{x \rightarrow x_0}{=} \sum_{k=0}^{n+1} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + o((x - x_0)^{n+1}). \end{aligned}$$

□

Exemple 3.4.2.

La formule de Taylor-Young permet d'obtenir les DL des fonctions exp, sin, cos, $x \mapsto (1+x)^\alpha$, sh et ch.

Ils sont à savoir par cœur : vous les trouverez dans le formulaire déjà distribué.

3.5 Étude locale d'une fonction.**a Allure d'une courbe au voisinage d'un point.****Proposition 3.5.1.**

Si f admet en x_0 un DL de la forme $f(x) = a_0 + a_1(x - x_0) + a_k(x - x_0)^k + o((x - x_0)^k)$, où $k \geq 2$ et a_k est non nul, alors f est dérivable en x_0 , de dérivée a_1 .

La tangente à sa courbe en $(x_0, f(x_0))$ a pour équation $y = a_1(x - x_0) + a_0$ et la position de sa courbe par rapport à cette tangente est donnée par le signe du terme $a_k(x - x_0)^k$.

Les quatre positions possibles au voisinage de x_0 sont illustrées dans les figures XX.1, XX.2, XX.3 et XX.4.

En particulier, la courbe traverse la tangente (on dit qu'on a un point d'inflexion) si et seulement si k est impair.

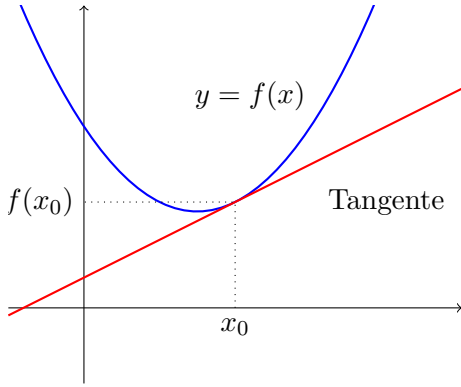


FIGURE XX.1 – Cas k pair, $a_k > 0$

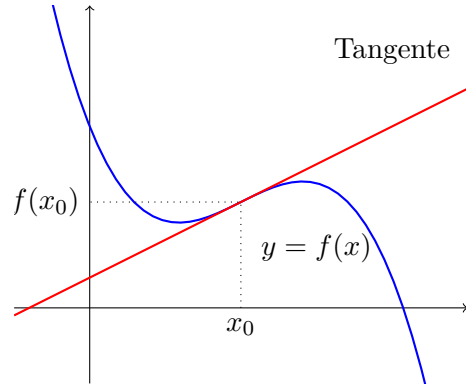


FIGURE XX.4 – Cas k impair, $a_k < 0$

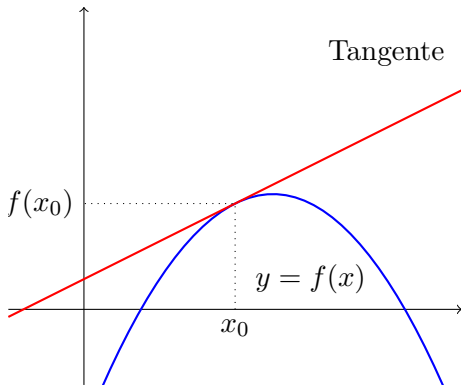


FIGURE XX.2 – Cas k pair, $a_k < 0$

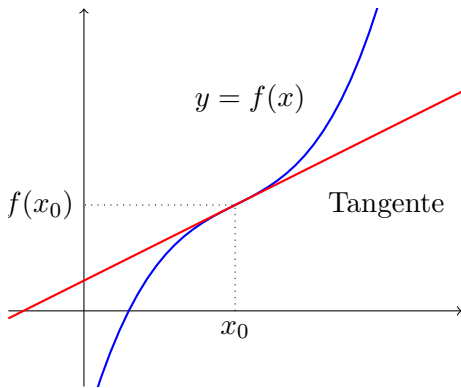


FIGURE XX.3 – Cas k impair, $a_k > 0$

Exemple 3.5.2.

Considérer les applications $x \mapsto x^3$, $x \mapsto x^2$, $x \mapsto x^4$, $\sin$, $x \mapsto x \cos x$ et $x \mapsto x(1 + \sin^3 x)$ en 0

Corollaire 3.5.3.

Si f , de classe $\mathcal{C}^2$ admet un point d'inflexion en x_0 , on a nécessairement $f''(x_0) = 0$.

Remarque 3.5.4.

On pourra regarder ce que donne cette condition sur les exemples précédents. En particulier, on verra clairement que la réciproque est fausse.

Nous savons déjà que si f a un extremum local en a , alors $f'(a) = 0$, mais la réciproque est fausse. Allons plus loin, en utilisant la proposition 3.5.1 :

Corollaire 3.5.5.

Soit f telle que $f'(a) = 0$. Si $f''(a) \neq 0$, f a un extremum local en a .

Démonstration.

$f'(a) = 0$, donc la tangente de f en a est horizontale. De plus la première dérivée non nulle en a est d'ordre 2, donc le graphe de f , dans un certain voisinage de a , est en-dessous ou au-dessus de la tangente en a . Ceci s'écrit : (pour tout t dans ce voisinage, $f(t) \geq f(a)$) ou (pour tout t dans ce voisinage, $f(t) \leq f(a)$). Donc f a un extremum local en a . $\square$

b Prolongement de fonction.

On considère une fonction f non définie en a mais définie au voisinage épointé de a .

Proposition 3.5.6.

Soit $n \in \mathbb{N}$. Si f admet un développement limité d'ordre n en a , alors elle est prolongeable par continuité en a en une fonction $\hat{f}$ et la valeur de $\hat{f}$ en a est le terme constant du développement limité de f . De plus, $\hat{f}$ admet en a le même développement limité que f .

Corollaire 3.5.7.

En particulier si f admet un DL d'ordre au moins 1 en a , alors $\hat{f}$ est dérivable en a .

Exercice 3.5.8.

Étudier la fonction f en 0 (continuité, dérivabilité, position) :

$$f(t) = \frac{1}{t} - \frac{1}{\sin t}$$

c Développements asymptotiques.

Nous avons déjà vu dans la Proposition 3.2.14 de la Partie 3.2.11 un exemple de développement asymptotique.

Plus généralement, un développement asymptotique a ceci en commun avec un DL d'être une approximation d'une fonction, que l'on présente également comme une somme de fonctions, allant de la plus « grosse » à la plus « petite », et d'un reste, négligeable devant tous les autres termes de la somme. C'est ce que l'on appelle une *échelle de comparaison*. Ces fonctions sont de nature quelconque, alors qu'un DL ne contient que des termes polynomiaux (on travaille avec des échelles de comparaisons polynomiales).

Exemple 3.5.9.

Dans l'échelle de comparaison $\{x \mapsto x^k, k \in \mathbb{Z}\}$, ordonnée par l'ordre usuel au voisinage de $+\infty$, on peut écrire :

$$\begin{aligned} \frac{3x^2 + 2}{x - 1} &\underset{x \rightarrow +\infty}{=} 3x + \frac{3x + 2}{x - 1} = 3x + o(x) \\ &\underset{x \rightarrow +\infty}{=} 3x + 3 + \frac{5}{x - 1} = 3x + 3 + o(1) \\ &\underset{x \rightarrow +\infty}{=} 3x + 3 + \frac{5}{x} + o\left(\frac{1}{x}\right). \end{aligned}$$

Notamment,

$$\frac{5}{x - 1} = \frac{5}{x} \times \frac{1}{1 - \frac{1}{x}} \underset{x \rightarrow +\infty}{=} \frac{5}{x} (1 + o(1)) \underset{x \rightarrow +\infty}{=} \frac{5}{x} + o\left(\frac{1}{x}\right).$$

Exemple 3.5.10.

Dans l'échelle de comparaison $\{x \mapsto x^\alpha \ln^\beta x, (\alpha, \beta) \in \mathbb{R}^2\}$ au voisinage de $+\infty$, ordonnée par l'ordre lexicographique sur (α, β) , on peut écrire en développant le carré :

$$\begin{aligned} \left(x + \ln x + \frac{1}{\ln x}\right)^2 &\underset{x \rightarrow +\infty}{=} x^2 + o(x^2) \\ &\underset{x \rightarrow +\infty}{=} x^2 + 2x \ln x + o(x \ln(x)) \\ &\underset{x \rightarrow +\infty}{=} x^2 + 2x \ln x + 2\frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right). \end{aligned}$$

d Branche infinie d'une courbe d'équation

$$y = f(x).$$

Principe : écrire un développement asymptotique de f au voisinage de l'infini, en général en exprimant $f(x)$ en fonction de $1/x$:

Exercice 3.5.11.

Étudier les branches infinies de

$$\begin{aligned} f : \mathbb{R} \setminus \{0, -1\} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{x^2 - x + 2}{x + 1} e^{-\frac{1}{x}}. \end{aligned}$$

4 Théorèmes de comparaison pour les séries.**Proposition 4.0.1.**

Soit (u_n) une suite à valeurs positives et $S_n = \sum_{k=0}^n u_k$. Alors la suite (S_n) est croissante et converge donc si et seulement si elle est majorée.

Démonstration.

Tout simplement, $S_{n+1} - S_n = u_{n+1} \geq 0$. $\square$

Proposition 4.0.2.

Soient (u_n) et (v_n) deux suites réelles telles que pour tout $n \in \mathbb{N}$, $0 \leq u_n \leq v_n$.

- (i) Si $\left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$ converge, alors $\left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$ également et
- $$0 \leq \lim_{N \rightarrow +\infty} \sum_{n=0}^N u_n \leq \lim_{N \rightarrow +\infty} \sum_{n=0}^N v_n.$$
- (ii) Si $\left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$ diverge, alors $\left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$ également.

Démonstration.

Il suffit de remarquer que si $(S_N)_{N \in \mathbb{N}} = \left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$ et $(S'_N)_{N \in \mathbb{N}} = \left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$, alors pour tout $N \in \mathbb{N}$, $0 \leq S_N \leq S'_N$.

(i) (S'_N) converge, donc est majorée, donc (S_N) est également majorée, et comme elle est croissante, elle converge également. Il reste alors à passer à la limite dans la relation $0 \leq S_N \leq S'_N$.

(ii) c'est le théorème de minoration.

□

Remarque 4.0.3.

La condition de positivité des suites est **PRI-MORDIALE**. Considérons par exemple les suites constantes $u_n = -1$ et $v_n = 0$.

Remarque 4.0.4.

Si la comparaison n'est valide qu'à partir d'un certain rang, le résultat de convergence est toujours vrai, mais pas la comparaison des limites.

Exercice 4.0.5.

En considérant $u_n = \frac{1}{n(n+1)}$ et $v_n = \frac{1}{(n+1)^2}$, montrer que $\left(\sum_{n=0}^N \frac{1}{(n+1)^2}\right)_{N \in \mathbb{N}}$ converge et majorer sa limite.

Corollaire 4.0.6.

Soient (u_n) et (v_n) deux suites réelles **positives**, (v_n) ne s'annulant pas à partir d'un certain rang.

- (i) Si $u_n = O(v_n)$, alors la convergence de $\left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$ entraîne celle de $\left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$.
- (ii) Si $u_n = o(v_n)$, alors la convergence de $\left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$ entraîne celle de $\left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$.
- (iii) Si $u_n \sim v_n$ (donc (u_n) ne s'annule pas à partir d'un certain rang), alors $\left(\sum_{n=0}^N v_n\right)_{N \in \mathbb{N}}$ et $\left(\sum_{n=0}^N u_n\right)_{N \in \mathbb{N}}$ sont de même nature.

Démonstration. (i) $\frac{u_n}{v_n}$ est bornée par un certain réel $M > 0$, donc à partir d'un certain rang, $0 \leq u_n \leq M v_n$ car (u_n) et (v_n) sont positives. On conclut donc avec 4.0.2.

(ii) si $u_n = o(v_n)$, alors en particulier $u_n = O(v_n)$.

(iii) si $u_n \sim v_n$, alors $u_n = O(v_n)$ et $v_n = O(u_n)$.

□

Exemple 4.0.7.

Puisque $\sin\left(\frac{1}{2^n}\right) \sim \frac{1}{2^n}$, d'après le résultat sur les séries géométriques, $\left(\sum_{n=0}^N \sin\left(\frac{1}{2^n}\right)\right)_{N \in \mathbb{N}}$ converge.

Pour pouvoir utiliser le dernier corollaire, nous avons besoin de « séries étalon » dont la nature est bien connue, et auxquelles on compare les séries à étudier. Les quelques exemples déjà étudiés font partie de ces séries de référence standard, mais la famille de séries la plus utilisée est celle des *séries de Riemann*, dont font partie la *série harmonique* et la série $\left(\sum_{n=0}^N \frac{1}{(n+1)^2}\right)_{N \in \mathbb{N}}$.

Théorème 4.0.8.

Soit $\alpha \in \mathbb{R}$. La suite $\left(\sum_{n=1}^N \frac{1}{n^\alpha}\right)_{N \in \mathbb{N}}$ converge si et seulement si $\alpha > 1$.

Démonstration.

Si $\alpha = 1$, remarquons que $\frac{1}{n} \sim \ln(n+1) - \ln n$. Donc $\left(\sum_{n=1}^N \frac{1}{n}\right)_{N \in \mathbb{N}}$ est de même nature que $\left(\sum_{n=1}^N (\ln(n+1) - \ln n)\right)_{N \in \mathbb{N}}$, qui elle-même est de même nature que la suite $(\ln n)$ par sommation télescopique, d'où la divergence.

Si $\alpha \neq 1$, $\frac{1}{n^\alpha} \sim \frac{1}{\alpha-1} \left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}} \right)$ (effectuer un développement asymptotique de $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ ou appliquer l'inégalité des accroissements finis à $x \mapsto x^{1-\alpha}$). La série de terme général $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ est de même nature que la suite $\left(\frac{1}{n^{\alpha-1}}\right)$, d'où le résultat. $\square$

Chapitre XXI

Familles de vecteurs et espaces vectoriels de dimension finie

Sommaire

1	Familles de vecteurs.	316
1.1	Familles génératrices.	316
1.2	Familles libres et liées.	317
1.3	Bases.	320
1.4	Bases canoniques.	321
2	Notion de dimension.	322
2.1	Définition.	322
2.2	Théorème fondamental.	322
2.3	Existence de bases.	323
2.4	Existence de la dimension.	325
2.5	Exemples avancés.	326
3	Sous-espaces vectoriels en dimension finie.	326
3.1	Dimension d'un sous-espace vectoriel.	326
3.2	Existence de supplémentaires.	327
3.3	Dimension d'une somme de sous-espaces vectoriels.	328

Dans tout ce chapitre, sauf mention expresse du contraire, E désigne un espace vectoriel sur un corps $\mathbb{K}$, valant $\mathbb{R}$ ou $\mathbb{C}$.

1 Familles de vecteurs.

Dans cette partie, sauf mention expresse du contraire, I désigne un ensemble et $(x_i)_{i \in I}$ une famille de vecteurs de E indexée par cet ensemble.

Définition 1.0.1.

Étant donné deux familles de vecteurs $(x_i)_{i \in I}$ et $(y_j)_{j \in J}$, on note $(x_i)_{i \in I} \uplus (y_j)_{j \in J}$ leur concaténation.

Remarque 1.0.2.

Ce n'est pas une notation officielle et nous ne définirons pas formellement cette notion. On pourra aussi utiliser le symbole $\biguplus_{i=1}^n$ pour écrire la concaténation de n familles de vecteurs de E .

Exemple 1.0.3.

$(x_1, x_2, x_3) \uplus (y_1, y_2) = (x_1, x_2, x_3, y_1, y_2)$.

1.1 Familles génératrices.

Définition 1.1.1.

On dit que la famille $(x_i)_{i \in I}$ est *génératrice* du $\mathbb{K}$ -espace vectoriel E ou qu'elle *engendre* le $\mathbb{K}$ -espace vectoriel E si $E = \text{Vect}_{\mathbb{K}}((x_i)_{i \in I})$.

Proposition 1.1.2.

Une famille $(x_i)_{i \in I}$ de vecteurs de E est *génératrice* de E si et seulement si tout élément de E peut s'écrire comme une combinaison linéaire des vecteurs de cette famille.

Démonstration.

$\text{Vect}_{\mathbb{K}}((x_i)_{i \in I}) \subset E$ puisque tous les éléments de $(x_i)_{i \in I}$ appartiennent à E . On a donc

$$E = \text{Vect}_{\mathbb{K}}((x_i)_{i \in I}) \iff E \subset \text{Vect}_{\mathbb{K}}((x_i)_{i \in I})$$

Qui est exactement ce que dit la proposition. $\square$

Exemple 1.1.3.

1. Dans $\mathbb{R}^3$,
 $\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right)$ est génératrice car
 $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = xe_1 + ye_2 + ze_3$. Se généralise à $\mathbb{R}^n$
 avec base canonique.

2. Dans $\mathbb{C}$ considéré comme un $\mathbb{R}$ -ev, une famille génératrice est $(1, i)$.
3. Dans $\mathbb{C}$ considéré comme un $\mathbb{C}$ -ev, une famille génératrice est (z) , pour n'importe quel $z \neq 0$. On peut noter $\mathbb{C} = \text{Vect}_{\mathbb{R}}(1, i) = \text{Vect}_{\mathbb{C}}(z)$.
4. Dans le $\mathbb{R}$ -espace vectoriel $\mathbb{R}[X]$, la famille $(X^k)_{k \in \mathbb{N}}$ est une famille génératrice de $\mathbb{R}[X]$. Dans le $\mathbb{C}$ -espace vectoriel $\mathbb{C}[X]$, la famille $(X^k)_{k \in \mathbb{N}}$ est une famille génératrice de $\mathbb{C}[X]$. En revanche, dans le $\mathbb{R}$ -espace vectoriel $\mathbb{C}[X]$, la famille $(X^k)_{k \in \mathbb{N}}$ n'est pas génératrice de $\mathbb{C}[X]$ (car $\text{Vect}_{\mathbb{R}}((X^k)_{k \in \mathbb{N}}) = \mathbb{R}[X] \neq \mathbb{C}[X]$).
5. Dans le $\mathbb{C}$ -espace vectoriel $\mathbb{C}(X)$, d'après le cours sur la décomposition en élément simple, on obtient une famille génératrice de $\mathbb{C}(X)$ en regroupant les familles $(X^k)_{k \in \mathbb{N}}$ et $\left(\frac{1}{(X-\alpha)^k} \right)_{(\alpha, k) \in \mathbb{C} \times \mathbb{N}^*}$.

Exemple 1.1.4.

La famille $((1, 0), (0, 1))$ est génératrice de $\mathbb{R}^2$ et

$$\begin{aligned} \mathbb{R}^2 &= \text{Vect}((1, 0), (0, 1)) \\ &= \text{Vect}((2, 3), (0, 1)) \\ &= \text{Vect}((2, 3), (1, 2)). \end{aligned}$$

La famille $((2, 3), (1, 2))$ est donc une famille génératrice de $\mathbb{R}^2$.

C'est l'autre sens qui est le plus souvent utilisé, et qui fait apparaître un pivot de Gauss (encore et toujours) :

$$\begin{aligned} \text{Vect}((3, 4), (1, 5)) &= \text{Vect}((0, -11), (1, 5)) \\ &= \text{Vect}((0, 1), (1, 5)) \\ &= \text{Vect}((0, 1), (1, 0)) \\ &= \mathbb{R}^2 \end{aligned}$$

La famille $((3, 4), (1, 5))$ est donc une famille génératrice de $\mathbb{R}^2$.

Remarque 1.1.5.

On a aussi la notion de famille génératrice d'un sev F de E .

Remarque 1.1.6.

On appelle *droite vectorielle* tout sev engendré par un seul vecteur non nul, qui est alors *vecteur directeur*. Correspond bien à ce qui se passe dans $\mathbb{R}^2$ et $\mathbb{R}^3$.

Idem avec *plan vectoriel* et deux vecteurs non colinéaires.

Proposition 1.1.7. 1. Une famille génératrice à laquelle on ajoute des vecteurs est toujours génératrice.

2. On peut retirer tout vecteur qui est combinaison linéaire des autres vecteurs de la famille (c'est une condition suffisante mais elle est en fait aussi nécessaire).

Démonstration. 1. Découle du fait que l'inclusion de deux parties implique l'inclusion des sous-espaces engendrés.

2. Découle du fait que pour toutes parties X et Y de E , $X \subset Y \subset \text{Vect}(X)$ implique $\text{Vect}(X) = \text{Vect}(Y)$. $\square$

Exemple 1.1.8. 1. Dans $\mathbb{R}^4$, on considère $\mathcal{P}$ l'ensemble de $\mathbb{R}^4$ défini par

$$\mathcal{P} : \begin{cases} x - y + 2t = 0 \\ x + y - z = 0 \end{cases}$$

où (x, y, z, t) sont les coordonnées dans $\mathbb{R}^4$. On trouve

$$\mathcal{P} = \text{Vect}((1, 0, 1, -1/2), (0, 1, 1, 1/2))$$

donc c'est bien un plan.

2. On considère l'ensemble S des suites réelles vérifiant $u_{n+2} + 2u_{n+1} - 3u_n = 0$. S est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$ (le vérifier). On veut en donner une famille génératrice. On résout comme dans le cours, on trouve deux vecteurs générateurs. Cela fonctionnerait de manière identique pour les solutions d'une équation différentielle.

Théorème 1.1.9.

Soient F et G deux sous-espaces vectoriels de E . Alors toute concaténation d'une famille génératrice de F et d'une famille génératrice de G est une famille génératrice de $F + G$.

Démonstration.

Soit $(x_i)_{i \in I_1}$ une famille génératrice de F et $(x_i)_{i \in I_2}$ une famille génératrice de G . Notons $(x_i)_{i \in I} = (x_i)_{i \in I_1} \uplus (x_i)_{i \in I_2}$.

Toute combinaison linéaire d'éléments de la famille $(x_i)_{i \in I}$ est dans $F + G$.

Réciproquement, tout élément de $F + G$ s'écrit comme somme d'un élément de F et d'un élément de G . Le premier est une combinaison linéaire d'éléments de la famille $(x_i)_{i \in I_1}$ et le second de la famille $(x_i)_{i \in I_2}$. Donc leur somme est une combinaison linéaire d'éléments de la famille $(x_i)_{i \in I}$. $\square$

1.2 Familles libres et liées.

Définition 1.2.1.

On dit que la famille $(x_i)_{i \in I}$ est *libre* si toute combinaison linéaire d'éléments de $(x_i)_{i \in I}$ dont la valeur est 0_E est la combinaison triviale, c'est-à-dire n'a que des coefficients nuls. Formellement, la famille est libre si et seulement si, pour toute famille de scalaires $(\lambda_i)_{i \in I}$ à support fini, on a

$$\sum_{i \in I} \lambda_i x_i = 0_E \Rightarrow \forall i \in I \lambda_i = 0$$

Dans le cas où $I = \llbracket 1, n \rrbracket$, cette condition s'écrit : pour tout n -uplet $(\lambda_1, \dots, \lambda_n)$ de scalaires, on a

$$\sum_{i=1}^n \lambda_i x_i = 0_E \Rightarrow (\lambda_1, \dots, \lambda_n) = (0, \dots, 0)$$

Une famille non libre est dite *liée*.

Remarque 1.2.2. • Une famille est donc liée si et seulement s'il existe une combinaison linéaire de valeur nulle à coefficients non tous nuls.

- Si l'un des x_i est nul, la famille est liée.
- Si la famille comporte deux fois le même vecteur, elle est liée.

Proposition 1.2.3.

La famille $(x_i)_{i \in I}$ est libre si et seulement si tout élément x de E s'écrit d'au plus une façon comme combinaison linéaire d'éléments de $(x_i)_{i \in I}$.

Démonstration. Sens direct Supposons que la famille $(x_i)_{i \in I}$ est libre et montrons que tout élément x de E s'écrit d'au plus une façon comme combinaison linéaire d'éléments de $(x_i)_{i \in I}$.

Soit x un élément de E . Supposons qu'il existe deux familles de scalaires à support fini $(\lambda_i)_{i \in I}$ et $(\mu_i)_{i \in I}$ vérifiant

$$x = \sum_{i \in I} \lambda_i x_i = \sum_{i \in I} \mu_i x_i$$

Alors

$$0_E = x - x = \sum_{i \in I} (\lambda_i - \mu_i) x_i.$$

Or la famille $(x_i)_{i \in I}$ est libre, donc pour tout $i \in I$, on a $\lambda_i - \mu_i = 0$.

Donc tout élément de E s'écrit d'au plus une façon comme combinaison linéaire d'éléments de $(x_i)_{i \in I}$.

Sens indirect Supposons que tout élément de E s'écrit d'au plus une façon comme combinaison linéaire d'éléments de E et montrons que la famille $(x_i)_{i \in I}$ est libre.

Soit $(\lambda_i)_{i \in I}$ une famille de scalaires à support fini vérifiant

$$\sum_{i \in I} \lambda_i x_i = 0_E.$$

Alors en posant $\mu_i = 0$ pour tout $i \in I$, on a aussi

$$\sum_{i \in I} \mu_i x_i = 0_E.$$

Ainsi, 0_E s'écrit de deux façons comme combinaison linéaire de la famille $(x_i)_{i \in I}$: les deux familles $(\lambda_i)_{i \in I}$ et $(\mu_i)_{i \in I}$ sont donc la même famille, donc

$$\forall i \in I \quad \lambda_i = 0$$

La famille $(x_i)_{i \in I}$ est donc libre. $\square$

Proposition 1.2.4.

La famille $(x_i)_{i \in I}$ est *libre* si et seulement si aucun élément de cette famille ne peut s'exprimer comme combinaison linéaire des autres éléments de la famille.

Démonstration.

On fera ici la démonstration dans le cas où $I = \llbracket 1, n \rrbracket$ qui est le cas qu'on rencontrera le plus fréquemment par la suite. La démonstration n'est pas plus compliquée dans le cas général.

Montrons que la famille considérée est liée, c'est-à-dire qu'il existe une combinaison linéaire non triviale valant 0, si et seulement si au moins un élément de la famille s'écrit comme combinaison linéaire des autres éléments de la famille.

Sens indirect Supposons qu'il existe une combinaison linéaire non triviale de $(x_1, \dots, x_n)$ valant 0. Notons $\lambda_1, \dots, \lambda_n$ ses coefficients. L'un d'eux au moins étant non nul, on peut supposer $\lambda_1 \neq 0$, quitte à permuter les vecteurs. Alors a

$$\sum_{k=1}^n \lambda_k x_k = 0_E,$$

donc

$$x_1 = \sum_{k=2}^n \left(-\frac{\lambda_k}{\lambda_1} \right) x_k.$$

Donc x_1 est combinaison linéaire des autres vecteurs de la famille.

Sens direct Supposons que x_1 s'écrit

$$x_1 = \sum_{k=2}^n \lambda_k x_k,$$

où $x_2, \dots, x_n$ sont d'autres éléments de la famille et $\lambda_1, \dots, \lambda_k$ sont des scalaires. Alors, en posant $\lambda_1 = -1$,

$$\sum_{k=1}^n \lambda_k x_k = 0_E.$$

Cette combinaison linéaire n'est pas triviale puisque λ_1 n'est pas nul, donc la famille est liée.

(le cas général fonctionne de même). $\square$

Exemple 1.2.5. 1. Dans $\mathbb{R}^2$: une famille de deux vecteurs est liée si et seulement si les deux vecteurs sont colinéaires.

2. Dans $\mathbb{R}^3$, une famille de 3 vecteurs est liée si et seulement si les 3 vecteurs sont coplanaires.

Remarque 1.2.6.

Dans $\mathbb{R}^n$, si on utilise la définition pour chercher si une famille est libre, on est ramené à la résolution d'un système linéaire (une fois de plus).

Exemple 1.2.7.

- Montrer que $((1, 0), (-1, 2), (2, 4))$ est liée dans $\mathbb{R}^2$.
- Montrer que $((1, 0, 0), (0, -1, 1), (1, 0, 2))$ est libre dans $\mathbb{R}^3$.
- $(x \mapsto \sin x, x \mapsto \sin 2x, x \mapsto \sin 3x)$ est libre.

Définition 1.2.8.

Soit x, y deux vecteurs de E . On dit que

- x est colinéaire à y s'il existe $\lambda \in \mathbb{K}$ tel que $x = \lambda y$;
- x et y sont colinéaires si x est colinéaire à y ou si y est colinéaire à x .

Remarque 1.2.9.

Si x et y sont tous les deux non nuls, x est colinéaire à y si et seulement si x et y sont colinéaires.

Proposition 1.2.10.

La famille vide est toujours libre.

Soit x et y deux vecteurs de E .

1. (x) est libre si et seulement si $x \neq 0_E$.
2. (x, y) est libre si et seulement si x et y ne sont pas colinéaires.

Démonstration.

Élémentaire : à vous de le faire. $\square$



Cet argument n'est valable que pour deux vecteurs, comme nous l'avons vu plus haut.

Définition 1.2.11.

Soit $(x_i)_{i \in I}$ une famille de vecteurs de E . Pour tout $J \subset I$, on dit que $(x_i)_{i \in J}$ est une sous-famille de $(x_i)_{i \in I}$ et que $(x_i)_{i \in I}$ est une sur-famille de $(x_i)_{i \in J}$.

Théorème 1.2.12. 1. Toute sur-famille d'une famille liée est liée.

2. Toute sous-famille d'une famille libre est libre.
3. Si $(x_1, \dots, x_n)$ est une famille libre, alors $(x_1, \dots, x_n, x_{n+1})$ est libre si et seulement si x_{n+1} n'est pas combinaison linéaire des $x_1, \dots, x_n$.

Démonstration. 1. Il existe une combinaison linéaire nulle non triviale de la sous-famille. Il suffit de la compléter par des 0 pour en obtenir une pour la sur-famille.

2. C'est la contraposée du point précédent.

3. Le sens direct est évident. Pour l'autre sens, par contraposée supposons que $(x_1, \dots, x_n, x_{n+1})$ est liée. Alors il existe une combinaison linéaire nulle non triviale de $x_1, \dots, x_n, x_{n+1}$. Si le coefficient de x_{n+1} est nul, il s'agit d'une combinaison linéaire des $x_1, \dots, x_n$. Sinon, on peut exprimer x_{n+1} comme combinaison linéaire de $x_1, \dots, x_n$. $\square$

Exemple 1.2.13.

Dans $\mathbb{R}^2$, toute famille de trois vecteurs ou plus est liée : si les deux premiers vecteurs sont liés, la famille l'est aussi. Sinon, le troisième vecteur est combinaison linéaire des deux premiers, car les deux premiers forment une base.

Idem dans $\mathbb{R}^3$ avec les familles de plus de 4 vecteurs.

Proposition 1.2.14.

Soient F, G deux sev d'un $\mathbb{K}$ -ev E , et $\mathcal{F}, \mathcal{G}$ deux familles libres de F, G respectivement.

Si $F + G$ est directe, alors $\mathcal{F} \uplus \mathcal{G}$ est une famille libre.

Démonstration.

Notons $\mathcal{F} = (f_i)_{i \in I}$ et $\mathcal{G} = (g_j)_{j \in J}$.

Soit $(\lambda_i) \in \mathbb{K}^I, (\mu_j) \in \mathbb{K}^J$ à support fini telles que

$$\underbrace{\sum_{i \in I} \lambda_i f_i}_{\in F} + \underbrace{\sum_{j \in J} \mu_j g_j}_{\in G} = 0_E.$$

Comme $F + G$ est directe, on a

$$\sum_{i \in I} \lambda_i f_i = \sum_{j \in J} \mu_j g_j = 0_E.$$

Comme $\mathcal{F}$ et $\mathcal{G}$ sont libres, tous les λ_i, μ_j sont nuls. Ainsi, $\mathcal{F} \uplus \mathcal{G}$ est libre. $\square$

Enfin, terminons par un résultat bien pratique :

Définition 1.2.15.

Soit $n \in \mathbb{N}^*$ et $E = \mathbb{K}^n$. Soit $p \in \llbracket 1, n \rrbracket$ et $(v_1, \dots, v_p)$ une famille de vecteurs de E . Pour tout $i \in \llbracket 1, p \rrbracket$, notons $(v_{i,j})_{j \in \llbracket 1, n \rrbracket}$ les coordonnées du vecteur v_i . On dit que la famille $(v_1, \dots, v_p)$ est *échelonnée* si :

1. pour tout $i \in \llbracket 1, p \rrbracket$ il existe $r_i \in \llbracket 1, n \rrbracket$ tel que $v_{i,r_i} \neq 0$ et pour tout $j \in \llbracket 1, n \rrbracket$ tel que $j > r_i, v_{i,j} = 0$;
2. la suite des r_i est strictement croissante.

Exemple 1.2.16.

Dans $\mathbb{R}^5$, $\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \\ -5 \end{pmatrix} \right)$ est une famille échelonnée.

La famille $\left(\begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 0 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \\ -5 \end{pmatrix} \right)$ n'en est pas une.

Remarque 1.2.17.

Avec les mêmes notations, si $0 \leq k < i \leq p$, alors $v_{k,r_i} = 0$.

Remarque 1.2.18.

Une famille échelonnée ne peut contenir de vecteur nul.

Proposition 1.2.19.

Toute famille échelonnée est libre.

Démonstration.

Soit $n \in \mathbb{N}^*$ et $E = \mathbb{K}^n$. Soit $p \in \llbracket 1, n \rrbracket$ et $(v_1, \dots, v_p)$ une famille échelonnée de vecteurs de E .

Le résultat est assez intuitif et se voit facilement, par exemple en considérant le système $\sum_{i=1}^p \lambda_i v_i = 0$. En écri-

vant le système, on se rend compte qu'en remontant les lignes, les coefficients λ_i s'annulent les uns après les autres (le faire sur un exemple).

Donnons tout de même une démonstration propre, par récurrence sur le nombre de vecteurs. Pour tout $p \in \llbracket 1, n \rrbracket$, posons (H_p) : toute famille échelonnée de E ayant p vecteurs non nuls est libre.

Un vecteur non nul formant à lui seul une famille libre, (H_1) est immédiate.

Soit $p \in \llbracket 1, n-1 \rrbracket$ tel que (H_p) soit vraie. Soit $(v_1, \dots, v_{p+1})$ une famille échelonnée à vecteurs non nuls. Définissons les r_i comme dans la définition 1.2.15. Soit $\lambda_1, \dots, \lambda_{p+1}$

des scalaires tels que $\sum_{i=1}^{p+1} \lambda_i v_i = 0$. La r_{p+1} -ème ligne de

ce système s'écrit $\lambda_{p+1} v_{p+1, r_{p+1}} = 0$, puisque pour tout $i \leq p$, $v_{i, r_{p+1}} = 0$, par définition d'une famille échelonnée. Mais comme $v_{p+1, r_{p+1}} \neq 0$, alors $\lambda_{p+1} = 0$. Il reste alors

$\sum_{i=1}^p \lambda_i v_i = 0$. Mais $(v_1, \dots, v_p)$ est échelonnée, donc par hypothèse de récurrence elle est libre, ce qui implique que tous les λ_i sont nuls, d'où (H_{p+1}) . $\square$

Remarque 1.2.20.

Par abus, les familles de vecteurs présentant des blocs de zéros dans d'autres « coins » que le « coin inférieur gauche » peuvent aussi être dites échelonnées. En tout cas, avec la même démonstration, elles sont également libres. Par exemple les familles $\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right), \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$ et $\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$ sont libres.

Proposition 1.2.21.

Une famille de polynômes non nuls de degrés distincts deux à deux est libre.

Démonstration.

Par des considérations de degré. $\square$

1.3 Bases.

Définition 1.3.1.

Une famille $((x_i)_{i \in I})$ est une *base* de E si elle est libre et génératrice.

Exemple 1.3.2.

Les bases canoniques des $\mathbb{R}^n$.

Remarque 1.3.3.

On a aussi la notion de base d'un sev de E .

Remarque 1.3.4.

Comme pour les familles libres et génératrices, on peut permuter l'ordre des vecteurs d'une base, et on a toujours une base (mais ce n'est pas la même).

Proposition 1.3.5.

Soit $\mathcal{B} = (x_i)_{i \in I}$ une famille de E . Alors $\mathcal{B}$ est une base si et seulement si pour tout $y \in E$, il existe une unique famille de scalaires $(\lambda_i)_{i \in I}$ à support fini telle que

$$y = \sum_{i \in I} \lambda_i x_i.$$

En particulier dans le cas où $I = \llbracket 1, n \rrbracket$, $\mathcal{B}$ est une base si et seulement si pour tout $y \in E$, il existe un unique n -uplet $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ tel que

$$y = \sum_{k=1}^n \lambda_k x_k.$$

Démonstration.

On a déjà vu que cette famille de scalaires existe si et seulement si $(x_i)_{i \in I}$ est génératrice et est unique sous réserve d'existence si et seulement si $(x_i)_{i \in I}$ est libre. On en déduit le résultat. $\square$

Définition 1.3.6.

Soit $\mathcal{B} = (x_i)_{i \in I}$ une base de E et $y \in E$. Alors l'unique famille de scalaires (à support fini) $(\lambda_i)_{i \in I}$ telle que $y = \sum_{i \in I} \lambda_i x_i$ est appelée *famille des coordonnées* de y dans $\mathcal{B}$.

Dans le cas où $I = \llbracket 1, n \rrbracket$, cette famille est un n -uplet, appelé *n -uplet des coordonnées*.

Exercice 1.3.7 (Classique).

Montrer que $((1, 0, 1), (2, -1, 0), (0, 1, 1))$ est une base de $\mathbb{R}^3$, donner les coordonnées d'un vecteur dans cette base (mais attention, les coordonnées des vecteurs dans cette base et dans la base canonique ne sont pas les mêmes !).

Exemple 1.3.8.

Donner une base de $\mathcal{P} \subset \mathbb{R}^3$ où $\mathcal{P} = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y - z = 0\}$.

$(x, y, z) \in \mathcal{P}$ si et seulement si $z = x + 2y$ si et seulement s'il existe $\alpha, \beta \in \mathbb{R}$ tel que $(x, y, z) = \alpha(1, 0, 1) + \beta(0, 1, 2)$ si et seulement si $(x, y, z) \in \text{Vect}((1, 0, 1), (0, 1, 2))$. Ces deux vecteurs sont non colinéaires, donc forment une famille libre.

Une base de $\mathcal{P}$ est donc $((1, 0, 1), (0, 1, 2))$.

Exemple 1.3.9.

Trouver une base de

$$\mathcal{E} = \{(u_n) \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}, u_{n+2} + u_{n+1} - 2u_n = 0\}.$$

Le polynôme caractéristique est $X^2 + X - 2$ de racine 1 et -2. Donc tout élément de $\mathcal{E}$ est combinaison linéaire de la suite $(v_n) = (1)$ et $(w_n) = ((-2)^n)$. Donc $((v_n), (w_n))$ est génératrice.

On montre qu'elle est aussi libre, c'est donc une base de $\mathcal{E}$.

Remarque 1.3.10.

Une famille libre est toujours une base du sous-espace vectoriel qu'elle engendre.

Théorème 1.3.11.

Soient F, G deux sev d'un $\mathbb{K}$ -ev E , de bases respectifs $\mathcal{B}$ et $\mathcal{C}$.

Si F et G sont en somme directe alors $\mathcal{B} \uplus \mathcal{C}$ est une base de $F + G$.

Notamment, si F et G sont supplémentaires alors $\mathcal{B} \uplus \mathcal{C}$ est une base de E .

Démonstration.

Découle directement de 1.1.9 et 1.2.14. $\square$

1.4 Bases canoniques.

Les espaces vectoriels de référence viennent souvent avec des bases «par construction», que l'on appellera *canoniques*. Elles n'ont pas de propriétés particulières, mais vous pouvez les utiliser sans justifier leur caractère de base.

Proposition 1.4.1 (Base canonique de $\mathbb{K}^n$).

Soit $n \in \mathbb{N}^*$, pour tout $i \in \llbracket 1, n \rrbracket$ posons

$$e_i = (0, \dots, 0, \underbrace{1}_{i^{\text{ème}} \text{ position}}, 0, \dots, 0).$$

Alors $(e_1, \dots, e_n)$ est une base de $\mathbb{K}^n$, appelée *base canonique* de $\mathbb{K}^n$.

Proposition 1.4.2 (Bases canoniques de $\mathbb{K}_n[X]$ et $\mathbb{K}[X]$).

Soit $n \in \mathbb{N}^*$, alors la famille $(1, X, \dots, X^n)$ est une base de $\mathbb{K}_n[X]$, appelée *base canonique* de $\mathbb{K}_n[X]$.

La famille $(X^k)_{k \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$, appelée *base canonique* de $\mathbb{K}[X]$.

Proposition 1.4.3 (Base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$).

Soit $n, p \in \mathbb{N}^*$, pour tout $i \in \llbracket 1, n \rrbracket$ et $j \in \llbracket 1, p \rrbracket$, posons $E_{i,j}$ la matrice dont tous les coefficients sont nuls, sauf celui de la ligne i et la colonne j , qui vaut 1.

Alors $(E_{i,j})_{1 \leq i \leq n, 1 \leq j \leq p}$ est une base de $\mathcal{M}_{n,p}(\mathbb{K})$, appelée *base canonique* de $\mathcal{M}_{n,p}(\mathbb{K})$.

2 Notion de dimension.

2.1 Définition.

Définition 2.1.1.

On dit que E est de *dimension finie* si E admet une famille génératrice finie.

Exemple 2.1.2. 1. $\mathbb{K}^n$ est de dimension finie car engendré notamment par la famille des $(\delta_{ij})_{i \in \llbracket 1, n \rrbracket, j \in \llbracket 1, n \rrbracket}$.

2. $\mathbb{K}[X]$ n'est pas de dimension finie. En effet, considérons une famille finie de polynômes $(P_i)_{i \in \llbracket 1, n \rrbracket}$. Alors toute combinaison linéaire de cette famille a un degré borné par le maximum des degrés des P_i . Or les éléments de $\mathbb{K}[X]$ ont des degrés arbitrairement élevés, donc la famille considérée ne peut être génératrice.

3. Soit A un ensemble. L'espace vectoriel $\mathbb{K}^A$ est de dimension finie si et seulement si A est fini¹.

4. Soit E un $\mathbb{K}$ -espace vectoriel (pas nécessairement de dimension finie). Soit $n \in \mathbb{N}$ et $x_1, \dots, x_n$, n vecteurs de E . Alors le sous-espace vectoriel de E $\text{Vect}(x_1, \dots, x_n)$ est un espace vectoriel de dimension finie.

Remarque 2.1.3.

Cas particulier : l'espace vectoriel $\{0\}$ est de dimension finie. En effet, toute famille en est génératrice (y compris la famille vide).

1. Le «si» est facile à voir, le «seulement si» est beaucoup plus difficile à démontrer ; on pourra utiliser le résultat 2.2.1

2.2 Théorème fondamental.

Dans toute la suite du chapitre, E est un $\mathbb{K}$ -ev de dimension finie.

Théorème 2.2.1.

Soit $n \in \mathbb{N}$ tel que E admette une famille génératrice à n éléments. Alors toute famille de E contenant strictement plus de n vecteurs est liée.

Démonstration.

Remarquons d'abord qu'il suffit de montrer que toute famille de E contenant $n + 1$ vecteurs est liée. En effet, une famille contenant strictement plus de n vecteurs, en contient au moins $n + 1$. Elle contient donc une sous-famille liée, donc est liée elle-même.

Montrons le résultat par récurrence sur n , en posant pour tout $n \in \mathbb{N}$:

(H_n) : pour tout $\mathbb{K}$ -ev E admettant une famille génératrice à n éléments, toute famille de E contenant $n + 1$ vecteurs est liée.

• Le cas $n = 0$ est celui où $E = \{0\}$, et le résultat est alors vrai.

• Soit $n \in \mathbb{N}$. Supposons (H_n) vraie. Soient $(g_1, \dots, g_{n+1})$ une famille génératrice d'un $\mathbb{K}$ -ev E , et $(v_1, \dots, v_{n+2})$ une famille de vecteurs de E .

Pour tout $i \in \llbracket 1, n + 2 \rrbracket$, on note $v_i = \sum_{k=1}^{n+1} \alpha_{i,k} g_k$. Distinguons deux cas :

1er cas : si pour tout i , $\alpha_{i,1} = 0$, alors pour tout i , $v_i \in \text{Vect}(g_2, \dots, g_{n+1})$. Si l'on note $F = \text{Vect}(g_2, \dots, g_{n+1})$, on peut appliquer l'hypothèse de récurrence à F , qui admet une famille génératrice à n éléments, et à $(v_1, \dots, v_{n+1})$: $(v_1, \dots, v_{n+1})$ est liée dans F , donc $(v_1, \dots, v_{n+2})$ est liée dans F , donc aussi dans E , dont F est un sev.

2ème cas : il existe $i \in \llbracket 1, n + 2 \rrbracket$ tel que $\alpha_{i,1} \neq 0$, par exemple $\alpha_{1,1} \neq 0$.

Alors

$$g_1 = \frac{1}{\alpha_{1,1}} \left(v_1 - \sum_{k=2}^{n+1} \alpha_{1,k} g_k \right),$$

d'où

$$v_i = \frac{\alpha_{i,1}}{\alpha_{1,1}} \left(v_1 - \sum_{k=2}^{n+1} \alpha_{1,k} g_k \right) + \sum_{k=2}^{n+1} \alpha_{i,k} g_k.$$

Si l'on pose $w_i = v_i - \frac{\alpha_{i,1}}{\alpha_{1,1}} v_1$, alors pour tout $i \in \llbracket 2, n + 2 \rrbracket$ $w_i \in \text{Vect}(g_2, \dots, g_{n+1})$. Par hypothèse de récurrence, $(w_2, \dots, w_{n+2})$ est liée. Il existe donc une combinaison linéaire nulle en les w_i , à coefficients non tous nuls. Il est facile de voir que cette combinaison linéaire est aussi une combinaison linéaire nulle en les $v_1, \dots, v_{n+2}$, à coefficients non tous nuls. Ainsi (H_{n+1}) est vraie. $\square$

Remarque 2.2.2.

On notera que l'idée de la démonstration précédente est très proche de celle de l'algorithme du pivot de Gauss.

Exemple 2.2.3.

- Dans $\mathbb{R}^2$, toute famille de trois vecteurs est liée. Mais une famille de strictement moins de trois vecteurs n'est pas forcément libre !
- Dans $\mathbb{R}^3$, toute famille de quatre vecteurs est liée.
- Dans $\mathbb{R}_n[X]$, toute famille de $n + 2$ polynômes est liée.
- Dans $\mathbb{C}_n[X]$, vu comme $\mathbb{C}$ -espace vectoriel, toute famille de $n + 2$ polynômes est liée.
- Dans $\mathbb{C}_n[X]$, vu comme $\mathbb{R}$ -espace vectoriel, toute famille de $2n + 3$ polynômes est liée, tandis que la famille de $2n + 2$ polynômes $(1, i, X, iX, \dots, X^n, iX^n)$ est libre.

Nous verrons dans la partie 2.4 que ce résultat (fondamental !) mène directement au corollaire suivant.

Corollaire 2.2.4.

Dans un espace vectoriel de dimension finie, toutes les bases sont finies et de même cardinal.

2.3 Existence de bases.

On peut développer une première idée afin d'obtenir une base dans un espace vectoriel de dimension finie, idée d'ailleurs déjà ébauchée dans le cours sur les espaces vectoriels. On part d'une famille génératrice finie de E :

- si cette famille est libre, c'est une base ;
- sinon, un de ses vecteurs est « redondant », soit combinaison linéaire des autres, et on peut l'enlever pour obtenir une famille génératrice strictement plus petite.

En itérant, on obtient une suite de familles génératrices strictement décroissante (en taille) : on s'arrête donc et l'on obtient une base.

Nous allons voir un résultat plus fin qui nous permet de retrouver ceci : le théorème de la base incomplète.

Lemme 2.3.1.

Soit $p \in \mathbb{N}$ et $(x_i)_{i \in \llbracket 1, p \rrbracket}$ une famille de vecteurs de E .

La famille $(x_i)_{i \in \llbracket 1, p \rrbracket}$ est liée si et seulement s'il existe $k \in \llbracket 1, p \rrbracket$ vérifiant

$$x_k \in \text{Vect}(x_1, \dots, x_{k-1}).$$

Autrement dit si et seulement si l'un des vecteurs de la famille est combinaison linéaire des précédents.

Démonstration.

Supposons que la famille est liée. Alors il existe une combinaison linéaire $\sum_{i=1}^p \lambda_i x_i$ non triviale de valeur 0. On note k le plus grand entier i tel que $\lambda_i \neq 0$. Alors on a successivement :

$$\begin{aligned} \sum_{i=1}^k \lambda_i x_i &= 0, \\ x_k &= -\frac{1}{\lambda_k} \sum_{i=1}^{k-1} \lambda_i x_i, \\ x_k &\in \text{Vect}(x_1, \dots, x_{k-1}). \end{aligned}$$

L'implication réciproque est évidente. $\square$

Corollaire 2.3.2.

Soit

- $p \in \mathbb{N}$,
- $(x_1, \dots, x_p)$ une famille libre de vecteurs de E ,
- x un vecteur de E .

Alors

$$(x_1, \dots, x_p, x) \text{ est liée} \iff x \in \text{Vect}(x_1, \dots, x_p).$$

Démonstration.

Supposons $(x_1, \dots, x_p, x)$ liée, et posons $x_{p+1} = x$. D'après le lemme, il existe $k \in \llbracket 1, p+1 \rrbracket$ vérifiant $x_k \in \text{Vect}(x_1, \dots, x_{k-1})$. On ne peut avoir $k \leq p$ puisque la famille $(x_1, \dots, x_p)$ est libre. Donc $k = p+1$ et on a $x \in \text{Vect}(x_1, \dots, x_p)$. $\square$

Théorème 2.3.3 (de la base incomplète).

Soient E un $\mathbb{K}$ -espace vectoriel engendré par une famille $\mathcal{G}$ finie, et $\mathcal{L}$ une famille libre de E . Alors on peut compléter $\mathcal{L}$ en une base de E en lui rajoutant des vecteurs de $\mathcal{G}$.

Remarque 2.3.4.

Ce théorème est vrai pour tout espace vectoriel E et non seulement pour ceux de dimension finie. La démonstration est relativement délicate dans le cas général (on utilise en général le lemme de Zorn, équivalent à l'axiome du choix), nous nous contenterons de la donner dans le cas de la dimension finie.

Démonstration.

Une démonstration possible est de considérer l'algorithme suivant :

```

 $\mathcal{B} \leftarrow \mathcal{L}$ 
# Invariant de boucle :  $\mathcal{B}$  est libre et  $\mathcal{L} \subset \mathcal{B}$ 
# Variant :  $\text{Card } \mathcal{G} - \text{Card } \mathcal{B}$ 
TantQue  $\mathcal{G} \not\subset \text{Vect } \mathcal{B}$  Faire
    Choisir  $v \in (\mathcal{G} \setminus \text{Vect } \mathcal{B})$ 
     $\mathcal{B} \leftarrow \mathcal{B} \cup \{v\}$ 
FinTantQue
    
```

$\mathcal{L}$ est libre et l'invariant est clairement vérifié avant l'entrée dans la boucle.

Si l'invariant est vérifié, au début d'un tour de boucle, $\mathcal{B}$ est libre et $\mathcal{G} \setminus \text{Vect } \mathcal{B} \neq \emptyset$, donc on peut effectivement choisir v dans $\mathcal{G} \setminus \text{Vect } \mathcal{B}$.

Alors puisque $\mathcal{B}$ est libre, d'après le lemme 2.3.1, $\mathcal{B} \cup \{v\}$ est libre également.

À la fin du tour de boucle, $\mathcal{B}$ est donc toujours libre, est toujours un sur-ensemble de $\mathcal{L}$ et un sous-ensemble de $\mathcal{G}$, l'invariant est donc encore vérifié.

Par ailleurs, $\mathcal{B}$ est libre et $\mathcal{G}$ est génératrice, donc, avec le lemme fondamental, $\text{Card } \mathcal{B} \leq \text{Card } \mathcal{G}$. Ainsi $\text{Card } \mathcal{G} - \text{Card } \mathcal{B}$ est un entier naturel. De plus, à chaque étape de la boucle, on ajoute à $\mathcal{B}$ un élément de $\mathcal{G}$ qui n'est pas déjà dans $\text{Vect } \mathcal{B}$, donc pas déjà dans $\mathcal{B}$, donc le cardinal de $\mathcal{B}$ augmente strictement. Donc à chaque tour de boucle $\text{Card } \mathcal{G} - \text{Card } \mathcal{B}$ décroît strictement, donc l'algorithme termine.

À la fin de l'exécution de l'algorithme, $\mathcal{B}$ est une famille libre, et $\mathcal{G} \subset \text{Vect } \mathcal{B}$. Donc $\mathcal{B}$ est une base de E . De plus, on a $\mathcal{L} \subset \mathcal{B}$ donc on a bien construit $\mathcal{B}$ en rajoutant à $\mathcal{L}$ des vecteurs de $\mathcal{G}$. $\square$

Exemple 2.3.5.

Compléter $((1, 2, 0, 0), (1, 0, 1, 0))$ en une base de $\mathbb{R}^4$.

Le théorème de la base incomplète a deux corollaires. Le premier est fondamental.

Corollaire 2.3.6.

Tout espace vectoriel de dimension finie admet une base finie.

Démonstration.

Il suffit d'appliquer le théorème de la base incomplète avec la famille vide et une famille génératrice finie. $\square$

Remarque 2.3.7.

Cas particulier : l'espace vectoriel $\{0\}$ a pour base la famille vide. C'est la seule famille libre (donc la seule base) de cet espace vectoriel, puisque toute famille d'au moins un élément contient le vecteur nul et est donc liée.

Il peut sembler étonnant (au premier abord) que le résultat qui suit soit un corollaire du théorème de la base incomplète.

Corollaire 2.3.8.

De toute famille génératrice finie on peut extraire une base.

Démonstration.

Lorsque la famille génératrice considérée est finie, il suffit là encore d'appliquer le théorème de la base incomplète avec la famille vide et une famille génératrice finie : en complétant la famille vide avec des vecteurs de la famille génératrice considérée, on obtient bien une base extraite de la famille génératrice de départ.

Lorsque la famille génératrice considérée est infinie, on peut montrer le résultat en utilisant l'algorithme donné pour la démonstration du théorème de la base incomplète mais un problème se pose, celui de la terminaison. Celle-ci peut être justifiée par le théorème fondamental 2.2.1 : dans un espace de dimension finie, le nombre d'éléments d'une famille libre est majoré par un entier p , où p est par exemple le cardinal d'une famille génératrice finie de E . Or le nombre d'éléments de la famille $\mathcal{B}$ croît strictement à chaque tour de boucle, p moins ce nombre d'éléments est donc un variant de l'algorithme, donc celui-ci termine. $\square$

2.4 Existence de la dimension.

Théorème 2.4.1 (de la dimension).

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Alors toutes les bases ont même nombre d'éléments.

Démonstration.

E étant de dimension finie, il admet une base $\mathcal{B}_1$ finie. Soit $\mathcal{B}_2$ une seconde base de E . Étant libre, elle a moins d'éléments que $\mathcal{B}_1$. Mais réciproquement, $\mathcal{B}_2$ est génératrice et $\mathcal{B}_1$ est libre, donc $\mathcal{B}_1$ a moins d'éléments que $\mathcal{B}_2$, ce qui montre que toutes les bases de E ont le même nombre d'éléments que $\mathcal{B}_1$. D'où le résultat. $\square$

Définition 2.4.2.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. On appelle *dimension du $\mathbb{K}$ -espace vectoriel E* et on note $\dim_{\mathbb{K}} E$ (voire $\dim E$ si le contexte permet de savoir clairement ce qu'est $\mathbb{K}$) le nombre d'éléments commun à toutes les bases de E .

On notera parfois $\dim_{\mathbb{K}} E < +\infty$ l'assertion «le $\mathbb{K}$ -espace vectoriel E est de dimension finie».

Remarque 2.4.3.

Pour que cette définition ait un sens il est nécessaire et suffisant d'être assuré :

- d'une part que toutes les bases d'un espace vectoriel de dimension finie ont toutes le même nombre d'éléments
- d'autre part que tout espace vectoriel de dimension finie possède bien au moins une base.

Ce qu'on a bien vérifié plus haut.

Remarque 2.4.4.

Cas particulier : $\dim\{0\} = 0$.

Exemple 2.4.5.

Soit $n, p \in \mathbb{N}$.

- $\dim_{\mathbb{K}} \mathbb{K}^n = n$
- $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$
- $\dim_{\mathbb{K}} \mathbb{K}_n[X] = n + 1$
- $\dim_{\mathbb{R}} \mathbb{C}_n[X] = 2(n + 1)$
- $\dim_{\mathbb{K}} \mathcal{M}_{n,p}(\mathbb{K}) = np$
- $\dim_{\mathbb{R}} \mathcal{M}_{n,p}(\mathbb{C}) = 2np$

Proposition 2.4.6.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie.

- Toute famille libre de E a au plus $\dim_{\mathbb{K}} E$ éléments.
- Toute famille génératrice de E a au moins $\dim_{\mathbb{K}} E$ éléments.

Démonstration.

C'est une conséquence directe du théorème fondamental 2.2.1. $\square$

Proposition 2.4.7 (Caractérisation des bases).

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. et soit $\mathcal{F}$ une famille constituée d'exactly $\dim_{\mathbb{K}} E$ vecteurs de E .

Alors les trois propositions suivantes sont équivalentes.

1. $\mathcal{F}$ est une base de E .
2. $\mathcal{F}$ est une famille génératrice de E .
3. $\mathcal{F}$ est une famille libre de E .

Démonstration.

Il est clair que si $\mathcal{F}$ est une base alors elle est libre et génératrice.

Supposons que $\mathcal{F}$ est génératrice. Par le théorème de la base incomplète, on peut extraire de $\mathcal{F}$ une base $\mathcal{B}$, qui possède $\dim_{\mathbb{K}}(E)$ vecteurs, c'est-à-dire autant que $\mathcal{F}$. On a donc $\mathcal{B} = \mathcal{F}$, donc $\mathcal{F}$ est une base de E .

De même, supposons que $\mathcal{F}$ est libre. On pourrait raisonner comme précédemment en complétant $\mathcal{F}$ en une base de E . Voici un autre raisonnement. Si $x \in E$, alors $\mathcal{F} \cup \{x\}$ contient strictement plus de $\dim_{\mathbb{K}}(E)$ donc est liée. Par le corollaire 2.3.2, $x \in \text{Vect}(\mathcal{F})$. Ainsi, $\text{Vect}(\mathcal{F}) = E$, donc $\mathcal{F}$ engendre E , donc est une base de E . $\square$

Exercice 2.4.8.

Soient $a, b, c, d \in \mathbb{K}$ deux à deux distincts et

$$\begin{aligned} A &= (X - b)(X - c)(X - d), \\ B &= (X - a)(X - c)(X - d), \\ C &= (X - a)(X - b)(X - d), \\ D &= (X - a)(X - b)(X - c). \end{aligned}$$

Montrer que (A, B, C, D) est une base de $\mathbb{K}_3[X]$.

Enfin, terminons par un outil bien pratique.

Définition 2.4.9.

Une famille de polynômes $(P_0, \dots, P_n)$ est dite échelonnée en degrés si $\forall k \in \llbracket 0, n \rrbracket$, $\deg P_k = k$.

Une famille de polynômes $(P_k)_{k \in \mathbb{N}}$ est dite échelonnée en degrés si $\forall k \in \mathbb{N}$, $\deg P_k = k$.

Proposition 2.4.10.

Toute famille de polynômes $(P_0, \dots, P_n)$ échelonnée en degrés est une base de $\mathbb{K}_n[X]$.

Toute famille de polynômes $(P_k)_{k \in \mathbb{N}}$ échelonnée en degrés est une base de $\mathbb{K}[X]$.

Démonstration.

Si pour tout $k \in \llbracket 0, n \rrbracket$, $\deg P_k = k$, alors $(P_0, \dots, P_n)$ est une famille de $n + 1$ polynômes de $\mathbb{K}_n[X]$, et est libre d'après la proposition 1.2.21. Comme $\dim_{\mathbb{K}} \mathbb{K}_n[X] = n + 1$, la proposition 2.4.7 permet d'affirmer que $(P_0, \dots, P_n)$ est une base de $\mathbb{K}_n[X]$.

De même, si pour tout $k \in \mathbb{N}$, $\deg P_k = k$, alors la famille $(P_k)_{k \in \mathbb{N}}$ est libre, et tout polynôme appartient à $\mathbb{K}_n[X]$ pour un certain n et est donc combinaison linéaire de la famille $(P_k)_{k \in \mathbb{N}}$. $\square$

2.5 Exemples avancés.**Exemple 2.5.1.**

- Les solutions d'une équation différentielle linéaire homogène du premier ordre forment un espace vectoriel de dimension 1.
- Les solutions d'une équation différentielle linéaire homogène du second ordre à coefficients constants forment un espace vectoriel de dimension 2.

Proposition 2.5.2.

Soit E et F deux $\mathbb{K}$ -espaces vectoriels de dimensions finies.

Alors $E \times F$ est de dimension finie et

$$\dim_{\mathbb{K}}(E \times F) = \dim_{\mathbb{K}} E + \dim_{\mathbb{K}} F.$$

Plus précisément, posons $n = \dim E$ et $p = \dim F$ et choisissons $(e_1, \dots, e_n)$ une base de E et $(f_1, \dots, f_p)$ une base de F . Alors $(b_i)_{i \in \llbracket 1, n+p \rrbracket}$ est une base de $E \times F$, où

$$\begin{cases} b_i = (e_i, 0_F) & \text{pour } i \in \llbracket 1, n \rrbracket, \\ b_{n+i} = (0_E, f_i) & \text{pour } i \in \llbracket 1, p \rrbracket. \end{cases}$$

Démonstration.

Un vecteur $z \in E \times F$ s'écrit de manière unique $(x, y) = (x, 0_F) + (0_E, y)$. De plus, x (resp. y) s'écrit de manière unique comme combinaison linéaire des e_i (resp. f_i).

L'existence assure l'aspect générateur de la famille. L'unicité assure la liberté. $\square$

Remarque 2.5.3.

Ce résultat se généralise à n $\mathbb{K}$ -ev de dimension finie et à leur produit $E_1 \times \dots \times E_n$.

3 Sous-espaces vectoriels en dimension finie.**3.1 Dimension d'un sous-espace vectoriel.**

Pour démontrer qu'un sous-espace vectoriel d'un espace de dimension finie est de dimension finie, nous utiliserons le résultat suivant :

Proposition 3.1.1.

Soit E un $\mathbb{K}$ -espace vectoriel. Notons L l'ensemble des entiers n tels qu'il existe au moins une famille libre de E à n éléments. Alors

- ou bien E est de dimension finie et alors $L = \llbracket 0, \dim E \rrbracket$.
- ou bien E n'est pas de dimension finie et alors $L = \mathbb{N}$.

En particulier, E est de dimension finie si et seulement si L est majoré.

Démonstration.

Si E est de dimension finie, on a nécessairement $L \subset \llbracket 0, \dim E \rrbracket$. Notons alors $\mathcal{B}$ une base de E . $\mathcal{B}$ est une famille libre à $\dim E$ éléments et toute sous-famille de $\mathcal{B}$ est encore libre. Donc $\llbracket 0, \dim E \rrbracket \subset L$. D'où l'égalité.

Supposons désormais que E n'est pas de dimension finie. Montrons qu'alors L n'est pas majoré.

Par l'absurde supposons que L possède un majorant. Comme L est un ensemble d'entiers non vide (il contient 0), il admet alors un maximum M . Soit alors $\mathcal{F}$ une famille libre à M éléments. Si on rajoute un élément à $\mathcal{F}$ on obtient une famille à $M + 1$ éléments, or $M + 1 \notin L$ donc cette sur-famille ne peut être libre. Par le corollaire 2.3.2, cet élément est dans $\text{Vect}(\mathcal{F})$, donc $\mathcal{F}$ engendre E , donc c'est une base de E , donc E est de dimension finie ce qui est absurde.

L n'est donc pas majoré, donc pour tout entier n il existe $p \in L$ vérifiant $p \geq n$. On peut donc trouver une famille libre à p éléments. Toute sous-famille de cette famille en est

libre, en prenant une sous-famille arbitraire à n éléments, on voit donc qu'on a $n \in L$.

Donc $L \supset \mathbb{N}$, donc $L = \mathbb{N}$. $\square$

Proposition 3.1.2.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie et F un sous-espace vectoriel de E .

Alors F est de dimension finie et $\dim F \leq \dim E$.

De plus $\dim F = \dim E$ si et seulement si $F = E$.

Démonstration.

Toute famille libre de F est une famille libre d'éléments de E et a donc un nombre d'élément majoré par $\dim E$. Donc d'après la proposition 3.1.1, F est de dimension finie, et $\dim F \leq \dim E$.

En outre on a trivialement $F = E \Rightarrow \dim F = \dim E$.

Réciproquement, supposons $\dim F = \dim E$ et montrons $F = E$. Alors on peut trouver une base $\mathcal{B}$ de F comportant $\dim E$ éléments. On a $\text{Vect}(\mathcal{B}) = F$. En outre, $\mathcal{B}$ est une famille libre de F donc de E or elle comporte $\dim E$ éléments, donc d'après 2.4.7, c'est une famille génératrice de E , donc $\text{Vect}(\mathcal{B}) = E$. On a donc $F = E$. $\square$

Définition 3.1.3.

Soit E un $\mathbb{K}$ -espace vectoriel (non nécessairement de dimension finie). Soit $n \in \mathbb{N}$ et $(x_1, \dots, x_n)$ une famille de n vecteurs. On appelle *rang de la famille* $(x_1, \dots, x_n)$ et on note $\text{rg}(x_1, \dots, x_n)$ la dimension de l'espace vectoriel qu'ils engendrent :

$$\text{rg}(x_1, \dots, x_n) = \dim \text{Vect}(x_1, \dots, x_n).$$

Remarque 3.1.4.

$\text{Vect}(x_1, \dots, x_n)$ étant engendré par la famille de n vecteurs $(x_i)_{i \in [1, n]}$, il s'agit d'un espace vectoriel de dimension finie, et sa dimension est au plus n .

Donc le rang de $(x_i)_{i \in [1, n]}$ est bien défini et $\text{rg}(x_1, \dots, x_n) \leq n$.

De manière directe, ce rang vaut n si et seulement si la famille est libre.

De plus, $(x_i)_{i \in [1, n]}$ est génératrice si et seulement si E est de dimension finie et $(x_i)_{i \in [1, n]}$ est de rang $\dim E$.

De plus, si E est de dimension finie p , alors $\text{rg}(x_1, \dots, x_n) \leq p$.

Proposition 3.1.5.

Soit E un $\mathbb{K}$ -espace vectoriel (non nécessairement de dimension finie). Soit $n \in \mathbb{N}$ et $(x_1, \dots, x_n)$ une famille de n vecteurs.

Alors $(x_1, \dots, x_n)$ est libre si et seulement si $\text{rg}(x_1, \dots, x_n) = n$.

Démonstration.

$(x_1, \dots, x_n)$ étant génératrice de $\text{Vect}(x_1, \dots, x_n)$, elle est libre si et seulement si c'est une base de $\text{Vect}(x_1, \dots, x_n)$, i.e si et seulement si $\dim \text{Vect}(x_1, \dots, x_n) = n$. $\square$

3.2 Existence de supplémentaires.

Théorème 3.2.1 (Existence de supplémentaires).

Soit E un $\mathbb{K}$ -espace vectoriel et F un sous-espace vectoriel de E .

Alors F admet un supplémentaire S dans E .

Remarque 3.2.2.

Ce théorème est vrai pour tout espace vectoriel E et non seulement pour ceux de dimension finie. Nous nous contenterons de donner la démonstration dans le cas de la dimension finie, mais la généralisation au cas infini est relativement immédiate.

Démonstration.

Supposons que E soit de dimension finie. Alors, on peut choisir une base $(b_1, \dots, b_p)$ de F où $p = \dim F$.

Cette base de F est une famille libre de vecteurs de E , donc de E . On peut donc la compléter en une base $(b_1, \dots, b_n)$ de E , avec $n = \dim E \geq p$.

Posons alors $S = \text{Vect}(b_{p+1}, \dots, b_n)$. La famille $(b_{p+1}, \dots, b_n)$, sous-famille d'une base de E , est une famille libre. De plus, elle est génératrice de S , donc c'est une base de S .

On a donc trouvé une base de F et une base de S dont la réunion est une base de E . F et S sont donc supplémentaires. $\square$



Ne parlez jamais **du** supplémentaire : en effet tout sev admet en fait une infinité de supplémentaires ! Regardez l'exercice suivant pour vous convaincre que dans la démonstration précédente, il existe une infinité de choix pour compléter une famille libre en une base, ce qui mène à une infinité de supplémentaires à un sev, sans rien supposer sur l'espace vectoriel de départ.

Exercice 3.2.3.

Soit F et G deux sous-espaces supplémentaires d'un $\mathbb{K}$ -ev E , tous les trois non nuls. Soit x un vecteur non nul de F et $(y_1, y_2, \dots, y_p)$ une base de G .

1. Montrer que les vecteurs $x + y_1, x + y_2, \dots, x + y_p$ engendrent un sous-espace supplémentaire de F , noté G_x .
2. Montrer que si $x, x' \in F$ tel que $x \neq x'$ alors $G_x \neq G_{x'}$. En déduire que F admet une infinité de sous-espaces supplémentaires distincts (sauf dans des cas triviaux : lesquels ?)

Exemple 3.2.4.

Déterminer un supplémentaire dans $\mathbb{R}^4$ de

$$F = \text{Vect}((1, 2, 0, 0), (1, 0, 0, -3)).$$

3.3 Dimension d'une somme de sous-espaces vectoriels.

Proposition 3.3.1 (Formule de Grassmann).

Soit E un $\mathbb{K}$ -espace vectoriel. Soit F et G deux sous-espaces de dimensions finies de E . Alors $F + G$ est de dimension finie et

$$\dim(F + G) = \dim F + \dim G - \dim(F \cap G).$$

En particulier

$$\dim(F + G) \leq \dim F + \dim G$$

et l'égalité a lieu si et seulement si F et G sont en somme directe.

Démonstration. 1. Montrons tout d'abord le résultat dans le cas où la somme $F + G$ est directe : On peut alors choisir une base de F et une base de G , elles ont respectivement $\dim F$ et $\dim G$ éléments. Leur réunion possède donc $\dim F + \dim G$ éléments et est une base de $F \oplus G$. Donc $F \oplus G$ est de dimension finie et

$$\dim(F \oplus G) = \dim F + \dim G$$

(c'est bien un cas particulier car alors $\dim(F \cap G) = \dim\{0\} = 0$).

2. Montrons maintenant le résultat dans le cas général. Remarquons tout d'abord que $F \cap G$ est un sous-espace vectoriel de F qui est de dimension finie. Donc

$F \cap G$ possède un supplémentaire S dans F et $\dim F = \dim(F \cap G) + \dim S$, d'où

$$\dim S = \dim F - \dim(F \cap G)$$

De plus

$$\begin{aligned} S \cap G &= (S \cap F) \cap G \\ &= S \cap (F \cap G) \\ &= \{0\}. \end{aligned}$$

Comme $F \cap G \subset G$, on a $F + G = (S + (F \cap G)) + G = S + G$, donc S et G sont supplémentaires dans $F + G$.

Donc $F + G$ est de dimension finie et

$$\dim(F + G) = \dim S + \dim G,$$

$$\dim(F + G) = \dim F - \dim(F \cap G) + \dim G.$$

□

Exercice 3.3.2.

Soit $\mathcal{P}_1$ et $\mathcal{P}_2$ deux plans distincts de $\mathbb{R}^3$ (sev de dimension 2). Montrer que $\mathcal{P}_1 + \mathcal{P}_2 = \mathbb{R}^3$. Que peut-on dire de $\mathcal{P}_1 \cap \mathcal{P}_2$?

Proposition 3.3.3.

Soit E un $\mathbb{K}$ -espace vectoriel et F et G deux sous-espaces vectoriels de dimensions finies.

Alors si F et G sont supplémentaires, les trois propositions suivantes sont vraies :

1. $F \cap G = \{0\}$,
2. $F + G = E$,
3. $\dim E < +\infty$ et $\dim F + \dim G = \dim E$.

Réciproquement il suffit que deux de ces propositions soient vraies pour que F et G soient supplémentaires.

Démonstration.

Pour le sens direct, les deux premières propositions sont des conséquences connues, la troisième est la conséquence de la formule de Grassmann.

Pour le sens réciproque, étudions les différentes possibilités :

1. Supposons 1 et 2. Alors F et G sont supplémentaires dans E .
2. Supposons 1 et 3. Alors

$$\begin{aligned} \dim(F + G) &= \dim F + \dim G - \dim(F \cap G) \\ &= \dim F + \dim G \\ &= \dim E. \end{aligned}$$

Or $F + G$ est un sous-espace vectoriel de E donc $F + G = E$. Donc F et G sont supplémentaires.

3. Supposons 2 et 3. Alors

$$\dim E = \dim F + \dim G - \dim (F \cap G)$$

et $\dim E = \dim F + \dim G$.

Ainsi, $\dim (F \cap G) = 0$, et donc $F \cap G = \{0\}$. F et G sont donc supplémentaires.

□

Corollaire 3.3.4.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie et F un sous-espace vectoriel de E . Alors tous les supplémentaires de F ont même dimension : $\dim E - \dim F$.

Démonstration.

E est de dimension finie donc F et tous ses supplémentaires également. D'après ce qui précède tout supplémentaire S de F vérifie $\dim F + \dim S = \dim E$, donc $\dim S = \dim E - \dim F$.

□

Chapitre XXII

Intégration

Sommaire

1	Continuité uniforme.	332
2	Construction de l'intégrale.	333
2.1	Fonctions en escalier sur un segment. .	333
2.2	Fonctions continues par morceaux sur un segment.	334
2.3	Extension au cas où $b \leq a$	338
3	Le théorème fondamental du calcul différentiel.	338
3.1	Primitives.	338
3.2	Existence de primitives.	338
4	Méthodes de calcul.	339
5	Formules de Taylor.	340
6	Cas des fonctions à valeurs complexes.	341
7	Approximation d'intégrales.	341
7.1	Sommes de Riemann.	342
7.2	La méthode des trapèzes.	343
8	Comparaison série-intégrale.	344
9	Annexes.	345
9.1	Fonctions dont la variable intervient dans les bornes d'une intégrale (cas par- ticulier d'intégrales dépendant d'un pa- ramètre).	345

Dans tout ce chapitre, a et b sont deux réels tels que $a \leq b$.

1 Continuité uniforme.

Définition 1.0.1.

On dit que f est *uniformément continue* sur I si :

$$\forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall (x, y) \in I^2 \quad |x - y| \leq \alpha \Rightarrow |f(x) - f(y)| < \varepsilon$$

Remarque 1.0.2. 1. C'est une notion qui n'a de sens que sur un intervalle, jamais en un point.

2. Comparer cette expression avec celle de f continue sur I :

$$\forall x \in I \quad \forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall y \in I \\ |x - y| \leq \alpha \Rightarrow |f(x) - f(y)| < \varepsilon.$$

La différence essentielle est l'inversion d'un $\forall$ avec un $\exists$.

Exemple 1.0.3.

La fonction $f : \mathbb{R}_+^* \rightarrow \mathbb{R}_+^*$ n'est pas uniformément continue. Montrons la négation d'uniforme continuité :

$$\exists \varepsilon > 0 \quad \forall \alpha > 0 \quad \exists (x, y) \in I^2 \quad |x - y| \leq \alpha \text{ et } |f(x) - f(y)| > \varepsilon.$$

Posons $\varepsilon = \frac{1}{2}$. Soit $\alpha > 0$. Posons $x = \min(\alpha, 1)$ et $y = \frac{x}{2}$. On a $|x - y| = \frac{x}{2} \leq \alpha/2 < \alpha$. De plus $|1/x - 1/y| = |1/x - 2/x| = 1/x \geq 1 > \varepsilon$.

Théorème 1.0.4. 1. Toute fonction uniformément continue sur I est continue sur I .

2. Toute application lipschitzienne sur I est uniformément continue sur I .

Démonstration. 1. Facile : on réécrit f uniformément continue en fixant $y = a$, et on trouve f continue en a .

2. On fixe ε , on pose $\alpha = \frac{\varepsilon}{K}$. Et on déroule les définitions. □

Remarque 1.0.5.

Nous avons déjà vu que la fonction $f : [1, +\infty[\rightarrow \mathbb{R}$ est 1-lipschitzienne. Ce théorème n'est-il pas contradictoire avec ce dernier point et avec 1.0.3 ?

Théorème 1.0.6 (de Heine).

Toute fonction continue sur un segment est uniformément continue sur ce segment.

Démonstration.

(non exigible). On pose $I = [a, b]$. Soit f continue sur I .

Par l'absurde, supposons que f n'est pas uniformément continue. Alors il existe $\varepsilon > 0$ vérifiant

$$\forall \alpha > 0 \quad \exists (x, y) \in I^2 \quad |x - y| \leq \alpha \text{ et } |f(x) - f(y)| > \varepsilon. \quad (\text{XXII.1})$$

Soit alors $n \in \mathbb{N}$. D'après la propriété (XXII.1), il existe $(x_n, y_n) \in I^2$ vérifiant

$$|x_n - y_n| < \frac{1}{n+1}, \quad (\text{XXII.2})$$

$$|f(x_n) - f(y_n)| > \varepsilon. \quad (\text{XXII.3})$$

Or, $(x_n)_{n \in \mathbb{N}}$ est une suite à valeurs dans le segment $[a, b]$, donc est bornée. Par le théorème de Bolzano-Weierstrass, on peut extraire de $(x_n)_{n \in \mathbb{N}}$ une suite $(x_{\varphi(n)})_{n \in \mathbb{N}}$ qui converge vers une limite $\ell \in [a, b]$.

Posons alors, pour $n \in \mathbb{N}$, $u_n = x_{\varphi(n)}$, $v_n = y_{\varphi(n)}$.

On a alors

$$u_n - v_n \xrightarrow{n \rightarrow +\infty} 0$$

$$\text{et } u_n \xrightarrow{n \rightarrow +\infty} \ell.$$

Donc, par somme de limites :

$$v_n \xrightarrow{n \rightarrow +\infty} \ell.$$

Or f est continue sur $[a, b]$ donc en ℓ , on a donc

$$f(u_n) \xrightarrow{n \rightarrow +\infty} f(\ell),$$

$$f(v_n) \xrightarrow{n \rightarrow +\infty} f(\ell).$$

Ainsi,

$$|f(u_n) - f(v_n)| \xrightarrow{n \rightarrow +\infty} 0.$$

Donc il existe $n \in \mathbb{N}$ vérifiant

$$|f(u_n) - f(v_n)| < \varepsilon/2,$$

ce qui est contradictoire avec (XXII.3). C'est donc absurde. □

Remarque 1.0.7.

Attention : ce résultat est faux si l'ensemble de départ considéré pour f n'est pas un segment. Ainsi $]0, 1] \rightarrow \mathbb{R}$ est continue mais pas uniformément continue.

2 Construction de l'intégrale.

2.1 Fonctions en escalier sur un segment.

Définition 2.1.1.

On appelle *fonction en escalier* sur $[a, b]$ toute fonction $f : [a, b] \rightarrow \mathbb{R}$ telle qu'il existe $n \in \mathbb{N}$ et $n + 1$ réels $x_0 \dots x_n$ tels que :

- (i) $a = x_0 < x_1 < x_2 < \dots < x_n = b$;
- (ii) pour tout $i \in \llbracket 0, n - 1 \rrbracket$, $f|_{]x_i, x_{i+1}[}$ est constante.

L'ensemble $\{x_0, \dots, x_n\}$ est appelé une *subdivision* de $[a, b]$ adaptée à f . On note $\mathcal{E}([a, b])$ l'ensemble des fonctions en escalier sur $[a, b]$. Alors $\mathcal{E}([a, b])$ est un sev et un sous-anneau de $\mathbb{R}^{[a, b]}$.

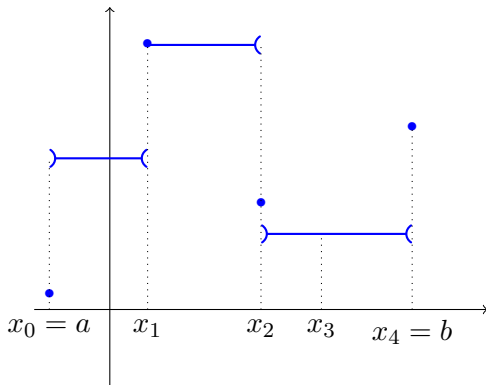


FIGURE XXII.1 – Illustration de la définition d'une fonction en escalier.

Remarque 2.1.2.

Attention aux valeurs prises aux points de la subdivision : elles peuvent valoir n'importe quoi. Si on rajoute des points à une subdivision adaptée, elle est toujours adaptée. Pas si on en ôte.

Remarque 2.1.3.

Si S et T sont deux subdivisions de $[a, b]$, alors :

1. Si S est adaptée à une application en escalier f et $S \subset T$, alors T est adaptée à f .
2. Si S et T sont des subdivisions adaptées à des applications en escalier respectivement f et g , alors $S \cup T$ est adaptée à la fois à f et à g .

Définition 2.1.4 (Intégrale d'une fonction en escalier).

Soit $f \in \mathcal{E}([a, b])$ et $\{x_i\}_{i \in \llbracket 0, n \rrbracket}$ une subdivision adaptée à f . Alors on appelle *intégrale de f sur $[a, b]$* et on note

$$\int_{[a, b]} f \text{ ou } \int_a^b f \text{ ou } \int_{[a, b]} f(t) dt \text{ ou } \int_a^b f(t) dt \text{ le réel}$$

$$\sum_{i=0}^{n-1} v_i \times (x_{i+1} - x_i)$$

où, pour $i \in \llbracket 0, n - 1 \rrbracket$, v_i est la valeur (constante) prise par f sur $]x_i, x_{i+1}[$ (on a en particulier $v_i = f\left(\frac{x_i + x_{i+1}}{2}\right)$).

Ce réel ne dépend pas de la subdivision choisie.

Démonstration.

La démonstration consiste à remarquer :

1. Que la valeur définie ci-dessus pour une subdivision S adaptée à f ne change pas si on ajoute un point à cette subdivision.
2. Que, par une récurrence immédiate, elle ne change pas si on rajoute un nombre fini de point et qu'en particulier, si on a deux subdivisions S et T avec $S \subset T$ et S adaptée à f , alors la valeur calculée pour S est la même que pour T .
3. Qu'enfin, si S et T sont deux subdivisions adaptées à f , alors la valeur calculée pour S est la même que pour $S \cup T$ et que celle calculée pour T est la même que pour $S \cup T$.

On se contentera de donner la démonstration du premier point : étant donné une subdivision $S = \{x_0, \dots, x_n\}$ adaptée à f en escalier sur $[a, b]$, et un point supplémentaire x' , comparons la valeur calculée pour la subdivision S et pour la subdivision $S \cup \{x'\}$. En notant i l'entier tel que $x_i < x' < x_{i+1}$ le terme $v_i(x_{i+1} - x_i)$ dans la somme pour la subdivision S est remplacée par la somme des deux termes $v_i(x' - x_i) + v_i(x_{i+1} - x')$ dans la somme obtenue pour la subdivision $S \cup \{x'\}$. Or ces deux valeurs sont les mêmes. $\square$

- Remarque 2.1.5.** 1. L'intégrale d'une fonction en escalier est bien la somme des aires algébriques des rectangles délimités par les subdivisions.
2. L'intégrale de f ne dépend pas de la valeur de f aux points de la subdivision choisie.
3. Changer la valeur de $f \in \mathcal{E}([a, b])$ en un point seulement ne change pas la valeur de l'intégrale : il suffit de rajouter ce point dans la subdivision.
4. L'intégrale de la fonction constante λ sur $[a, b]$ vaut $\lambda(b-a)$, en utilisant la subdivision adaptée $\{a, b\}$.

4. Soit S une subdivision adaptée à f . Ajoutons le point c et notons $\{z_i \mid i \in \llbracket 0, q \rrbracket\}$ la subdivision obtenue. Soit $s \in \llbracket 1, q-1 \rrbracket$ tel que $z_s = c$. Alors :

$$\begin{aligned} \int_a^b f &= \sum_{i=0}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\ &= \sum_{i=0}^{s-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\ &\quad + \sum_{i=s}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\ &= \int_a^c f + \int_c^b f. \end{aligned}$$

□

Proposition 2.1.6 (Propriétés de l'intégrale).

Soient $f, g \in \mathcal{E}([a, b])$, $\lambda \in \mathbb{R}$.

1. Linéarité : $\int_a^b (f + \lambda g) = \int_a^b f + \lambda \int_a^b g$.
2. Positivité : $f \geq 0 \Rightarrow \int_a^b f \geq 0$.
3. Croissance : $f \geq g \Rightarrow \int_a^b f \geq \int_a^b g$.
4. Relation de Chasles : si $c \in]a, b[$, $\int_a^b f = \int_a^c f + \int_c^b f$.

Démonstration. 1. Soit S une subdivision adaptée à f , T une subdivision adaptée à g , alors $S \cup T$ est adaptée à f et g . Notons $\{z_i \mid i \in \llbracket 0, q \rrbracket\}$ cette subdivision et exprimons $\int_a^b f$ et $\int_a^b g$:

$$\begin{aligned} \int_a^b (f + \lambda g) &= \sum_{i=0}^{q-1} (f + \lambda g)\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\ &= \sum_{i=0}^{q-1} f\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) + \lambda \sum_{i=0}^{q-1} g\left(\frac{z_{i+1} + z_i}{2}\right) \times (z_{i+1} - z_i) \\ &= \int_a^b f + \lambda \int_a^b g. \end{aligned}$$

2. On exprime $\int_a^b f$ avec une subdivision adaptée à f : tous les termes sont positifs.
3. Appliquer le point précédent à $(f - g)$.

2.2 Fonctions continues par morceaux sur un segment.

Définition 2.2.1.

Soit $f : [a, b] \rightarrow \mathbb{R}$. On dit que f est continue par morceaux s'il existe une subdivision $\{x_0, \dots, x_n\}$ de $[a, b]$ telle que

1. $a = x_0 < x_1 < \dots < x_n = b$;
2. pour tout $i \in \llbracket 0, n-1 \rrbracket$, $f|_{]x_i, x_{i+1}[}$ est continue et prolongeable par continuité en x_i et en x_{i+1} .

L'ensemble $\{x_0, \dots, x_n\}$ est appelé une *subdivision* de $[a, b]$ adaptée à f . On note $\mathcal{E}_m([a, b])$ l'ensemble des fonctions continues par morceaux sur $[a, b]$. Alors $\mathcal{E}_m([a, b])$ est un sev et un sous-anneau de $\mathbb{R}^{[a, b]}$.

Remarque 2.2.2.

Attention aux valeurs prises aux points de la subdivision : elles peuvent valoir n'importe quoi.

Exemple 2.2.3. 1. Dessiner des exemples de fonctions continues par morceaux.

2. La fonction tangente, prolongée en $\mathbb{R}$ en lui donnant la valeur 0 là où elle n'est pas définie, n'est pas continue par morceaux car elle n'est pas prolongeable par continuité en les points de discontinuité.

3. Idem pour $\mathbb{R}^* \rightarrow \mathbb{R}$:

$$x \mapsto \sin 1/x$$

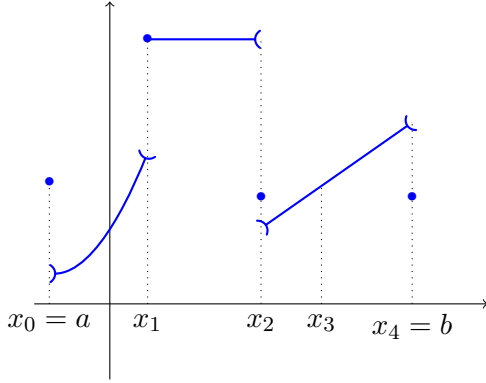


FIGURE XXII.2 – Illustration de la définition d'une fonction continue par morceaux.

On construit l'intégrale d'une fonction continue par morceaux en approchant celle-ci par des fonctions en escaliers.

Théorème 2.2.4.

Soit $f \in \mathcal{C}_m([a, b])$. Soit $\varepsilon > 0$. Alors il existe φ_ε^+ et $\varphi_\varepsilon^- \in \mathcal{E}([a, b])$ telles que $\varphi_\varepsilon^- \leq f \leq \varphi_\varepsilon^+$ et $0 \leq \varphi_\varepsilon^+ - \varphi_\varepsilon^- \leq \varepsilon$.

Démonstration. Première étape On suppose que f est continue sur $]a, b[$ et prolongeable par continuité en a et en b . On appelle $\tilde{f}$ ce prolongement. Alors f et $\tilde{f}$ coïncident sur $]a, b[$, mais pas forcément en a ni en b . On utilise le théorème de Heine : $\tilde{f}$ est uniformément continue sur $[a, b]$, donc il existe $\alpha > 0$ vérifiant

$$\forall x, y \in [a, b] \quad |x - y| \leq \alpha \Rightarrow |\tilde{f}(x) - \tilde{f}(y)| \leq \varepsilon.$$

On choisit n tel que $h = \frac{b-a}{n} \leq \alpha$ et l'on pose pour $0 \leq k \leq n$:

$$x_k = a + kh.$$

Ainsi, $\{x_0, \dots, x_n\}$ est une subdivision régulière de $[a, b]$, et

$$\forall i \in \llbracket 0, n-1 \rrbracket, \forall x, y \in [x_i, x_{i+1}], |\tilde{f}(x) - \tilde{f}(y)| \leq \varepsilon$$

Soit $i \in \llbracket 0, n-1 \rrbracket$, $\tilde{f}$ est continue sur le segment $[a, b]$, donc est bornée et atteint ses bornes sur $[x_i, x_{i+1}]$.

On pose

$$\varphi_i^+ = \max_{[x_i, x_{i+1}]} \tilde{f}$$

$$\varphi_i^- = \min_{[x_i, x_{i+1}]} \tilde{f}$$

$$\varphi_\varepsilon^+ : [a, b] \rightarrow \mathbb{R} \quad x \mapsto \begin{cases} \varphi_i^+ & \text{si } x \in [x_i, x_{i+1}[\\ \varphi_{n-1}^+ & \text{si } x = b \end{cases}$$

$$\varphi_\varepsilon^- : [a, b] \rightarrow \mathbb{R} \quad x \mapsto \begin{cases} \varphi_i^- & \text{si } x \in [x_i, x_{i+1}[\\ \varphi_{n-1}^- & \text{si } x = b \end{cases}.$$

On a bien $\varphi_\varepsilon^- \leq \tilde{f} \leq \varphi_\varepsilon^+$.

Puisque ces maximums et minimums sont atteints, pour chaque $i \in \llbracket 0, n-1 \rrbracket$, il existe $y_i, z_i \in [x_i, x_{i+1}]$ tels que $\varphi_i^+ = \tilde{f}(y_i)$ et $\varphi_i^- = \tilde{f}(z_i)$. Ainsi, comme on a toujours $|y_i - z_i| \leq \alpha$,

$$\forall i \in \llbracket 0, n-1 \rrbracket, 0 \leq \varphi_i^+ - \varphi_i^- = \tilde{f}(y_i) - \tilde{f}(z_i) \leq \varepsilon$$

donc nécessairement

$$0 \leq \varphi_\varepsilon^+ - \varphi_\varepsilon^- \leq \varepsilon.$$



φ_ε^+ et φ_ε^- conviennent pour $\tilde{f}$ et non f : il suffit alors de changer leurs valeurs en a et b , en posant $\varphi_\varepsilon^+(a) = \varphi_\varepsilon^-(a) = f(a)$ et $\varphi_\varepsilon^+(b) = \varphi_\varepsilon^-(b) = f(b)$.

Deuxième étape On traite le cas général.

Soit $f \in \mathcal{C}_m([a, b])$ et $\{x_0, \dots, x_n\}$ une subdivision adaptée. Alors on définit des φ_ε^+ et φ_ε^- sur chaque morceau de la subdivision, et on recolle en définissant φ_ε^+ et φ_ε^- comme valant $f(x_i)$ en chaque x_i . $\square$

Définition 2.2.5 (Intégrale d'une fonction continue par morceaux).

Soit $f \in \mathcal{C}_m([a, b])$. On note :

- $\mathcal{E}^+(f) = \{h \in \mathcal{E}([a, b]) \mid h \geq f\}$,
- $\mathcal{E}^-(f) = \{h \in \mathcal{E}([a, b]) \mid h \leq f\}$,
- $I^+(f) = \left\{ \int_a^b h \mid h \in \mathcal{E}^+(f) \right\}$,
- $I^-(f) = \left\{ \int_a^b h \mid h \in \mathcal{E}^-(f) \right\}$.

Alors $\sup I^-(f)$ et $\inf I^+(f)$ existent et sont égales. On appelle alors cette constante l'intégrale de f sur $[a, b]$, notée $\int_{[a, b]} f$ ou $\int_a^b f$ ou $\int_{[a, b]} f(t) dt$ ou $\int_a^b f(t) dt$.

Démonstration.

D'après le théorème d'approximation, il existe $\varphi^+ \in \mathcal{E}^+(f)$ et $\varphi^- \in \mathcal{E}^-(f)$, donc $\mathcal{E}^+(f)$ et $\mathcal{E}^-(f)$ ne sont pas vides, donc $I^\pm(f)$ non plus. De plus $I^+(f)$ est minorée par $\int_a^b \varphi^-$ et $I^-(f)$ est majorée par $\int_a^b \varphi^+$. Ainsi, avec le théorème de la borne sup, $\sup I^-(f)$ et $\inf I^+(f)$ existent, et $\sup I^-(f) \leq \int_a^b \varphi^+$.

Mais cette inégalité est valable pour tout $\varphi^+ \in \mathcal{E}^+(f)$, donc $\sup I^-(f) \leq \inf I^+(f)$.

Pour conclure, montrons l'inégalité inverse : soit $\varepsilon > 0$, alors il existe $\varphi_\varepsilon^+ \in \mathcal{E}^+(f)$ et $\varphi_\varepsilon^- \in \mathcal{E}^-(f)$ telles que $\varphi_\varepsilon^+ - \varphi_\varepsilon^- \leq \varepsilon$. Ainsi

$$\begin{aligned} \int_a^b \varphi_\varepsilon^+ &\leq \int_a^b \varphi_\varepsilon^- + \int_a^b \varepsilon \\ &\leq \int_a^b \varphi_\varepsilon^- + (b-a)\varepsilon. \end{aligned}$$

On obtient donc $\inf I^+(f) \leq \sup I^-(f) + (b-a)\varepsilon$ pour tout $\varepsilon > 0$, donc par passage à la limite, on a : $\inf I^+(f) \leq \sup I^-(f)$. $\square$

Remarque 2.2.6.

Cette intégrale représente bien la notion « d'aire sous la courbe », même si la construction s'éloigne quelque peu d'une définition géométrique.

Remarque 2.2.7.

La notion d'intégrale de fonction continue par morceaux prolonge celle de fonction en escalier. En effet, si $f \in \mathcal{C}([a, b])$, alors $f \in \mathcal{E}^+(f) \cap \mathcal{E}^-(f)$, et l'on voit directement que $\int_a^b f \in I^+(f) \cap I^-(f)$.

Remarque 2.2.8.

Changer la valeur de $h \in \mathcal{E}([a, b])$ en un point seulement ne change pas la valeur de son intégrale : il suffit de rajouter ce point dans la subdivision. On peut en déduire que changer la valeur de $f \in \mathcal{C}_m([a, b])$ en un point seulement ne change pas la valeur de son intégrale.

Exercice 2.2.9.

Le démontrer.

Proposition 2.2.10.

Soient $f, g \in \mathcal{C}_m([a, b])$, $\lambda \in \mathbb{R}$.

1. Linéarité : $\int_a^b (f + \lambda g) = \int_a^b f + \lambda \int_a^b g$.
2. Positivité : $f \geq 0 \Rightarrow \int_a^b f \geq 0$.
3. Croissance : $f \geq g \Rightarrow \int_a^b f \geq \int_a^b g$.
4. Continuité (ou inégalité triangulaire) : $\left| \int_a^b f \right| \leq \int_a^b |f|$.
5. Relation de Chasles :
si $c \in]a, b[$, $\int_a^b f = \int_a^c f + \int_c^b f$.

Démonstration. 1. (a) Montrons d'abord que pour tout $\lambda \in \mathbb{R}_+$, $\int_a^b \lambda f = \lambda \int_a^b f$.

Il suffit pour cela de montrer que pour tout $\varepsilon > 0$, on a

$$\left| \int_a^b \lambda f - \lambda \int_a^b f \right| \leq \lambda(b-a)\varepsilon$$

et d'en déduire le résultat par passage à la limite.

Considérons donc $\varepsilon > 0$. Choisissons φ^- et φ^+ des applications en escaliers encadrant f vérifiant $0 \leq \varphi^+ - \varphi^- \leq \varepsilon$. Alors λf est encadrée par $\lambda\varphi^-$ et $\lambda\varphi^+$. On en déduit

$$\begin{aligned} \int_a^b \lambda f - \lambda \int_a^b f &\leq \int_a^b \lambda\varphi^+ - \lambda \int_a^b \varphi^- \\ &\leq \lambda \int_a^b (\varphi^+ - \varphi^-) \quad (\text{car } \varphi^+ \\ &\quad \text{et } \varphi^- \text{ sont en escalier}) \\ &\leq \lambda(b-a)\varepsilon \quad (\text{car } \varphi^+ - \varphi^- \leq \varepsilon). \end{aligned}$$

De même, on a

$$\int_a^b \lambda f - \lambda \int_a^b f \geq -\lambda(b-a)\varepsilon.$$

D'où le résultat.

(b) On procède de la même manière pour le cas $\lambda \in \mathbb{R}_-$, en faisant attention aux changements de sens dans les inégalités dus au signe de λ .

(c) Montrons ensuite que $\int_a^b (f + g) = \int_a^b f + \int_a^b g$.

Il suffit de montrer que pour tout $\varepsilon > 0$, on a

$$\left| \int_a^b (f + g) - \left(\int_a^b f + \int_a^b g \right) \right| \leq 2\varepsilon(b-a)$$

Soit donc $\varepsilon > 0$. Choisissons φ_f^- et φ_f^+ encadrant f et φ_g^- et φ_g^+ encadrant g et vérifiant $\varphi_f^+ - \varphi_f^- \leq \varepsilon$ et $\varphi_g^+ - \varphi_g^- \leq \varepsilon$.

Alors a :

$$\begin{aligned} \int_a^b f &\geq \int_a^b \varphi_f^- \quad \text{et} \quad \int_a^b g \geq \int_a^b \varphi_g^- \\ \int_a^b (f + g) &\leq \int_a^b (\varphi_f^+ + \varphi_g^+) \\ &\quad (\text{car } \varphi_f^+ + \varphi_g^+ \in \mathcal{E}^+(f + g)) \\ \int_a^b (f + g) &\leq \int_a^b \varphi_f^+ + \int_a^b \varphi_g^+ \\ &\quad (\text{car } (\varphi_f^+, \varphi_g^+) \in \mathcal{E}([a, b])^2) \end{aligned}$$

et finalement

$$\begin{aligned} \int_a^b (f + g) - \left(\int_a^b f + \int_a^b g \right) &\leq \int_a^b \varphi_f^+ - \int_a^b \varphi_f^- + \int_a^b \varphi_g^+ - \int_a^b \varphi_g^- \\ &\leq 2\varepsilon(b-a). \end{aligned}$$

On montre de même

$$\int_a^b (f+g) - \left(\int_a^b f + \int_a^b g \right) \geq -2\varepsilon(b-a)$$

D'où le résultat. $\square$

2. Si $f \geq 0$, la fonction nulle est un élément de $\mathcal{E}^-(f)$ et donc $\int_a^b f \geq \int_a^b 0 = 0$.
3. La croissance découle directement de la positivité, appliquée à $f-g$.
4. Si f est continue par morceaux, alors $-f$, $|f|$ et $-|f|$ le sont aussi. Or $-|f| \leq f \leq |f|$, donc par croissance et linéarité de l'intégrale :

$$-\int_a^b |f| \leq \int_a^b f \leq \int_a^b |f|,$$

$$\text{d'où } \left| \int_a^b f \right| \leq \int_a^b |f|.$$

5. Soit $c \in]a, b[$.

Il suffit de montrer que pour tout $\varepsilon > 0$, on a

$$\left| \int_a^c f + \int_c^b f - \int_a^b f \right| \leq \varepsilon(b-a).$$

Soit donc $\varepsilon > 0$. Notons $I_1 = [a, c]$ et $I_2 = [c, b]$.

Alors pour $i = 1, 2$, il existe φ_i^- et φ_i^+ des applications en escalier sur I_i encadrant la restriction de f à I_i vérifiant

$$\varphi_i^+ - \varphi_i^- \leq \varepsilon.$$

Posons alors

$$\begin{aligned} \varphi^- : [a, b] &\rightarrow \mathbb{R} \\ x &\mapsto \begin{cases} \varphi_1^-(x) & \text{si } x < c \\ \varphi_2^-(x) & \text{si } x \geq c \end{cases} \end{aligned}$$

$$\begin{aligned} \text{et } \varphi^+ : [a, b] &\rightarrow \mathbb{R} \\ x &\mapsto \begin{cases} \varphi_1^+(x) & \text{si } x < c \\ \varphi_2^+(x) & \text{si } x \geq c \end{cases} \end{aligned}$$

φ^- et φ^+ sont en escalier et :

$$\begin{aligned} \int_a^c f + \int_c^b f &\leq \int_a^c \varphi_1^+ + \int_c^b \varphi_2^+ \\ &\leq \int_a^c \varphi^+ + \int_c^b \varphi^+ \quad (\varphi_1^+ \text{ et } \varphi_2^+ \text{ diffèrent de } f \text{ au plus de } \varepsilon) \\ &\leq \int_a^b \varphi^+ \end{aligned}$$

$$\text{Or } \int_a^b f \geq \int_a^b \varphi^- \text{ car } (\varphi^- \in \mathcal{E}^-(f))$$

Donc

$$\begin{aligned} \int_a^c f + \int_c^b f - \int_a^b f &\leq \int_a^b \varphi^+ - \int_a^b \varphi^- \quad (\text{par différence des inégalités précédentes}) \\ &\leq \int_a^b (\varphi^+ - \varphi^-) \\ &\leq (b-a)\varepsilon \end{aligned}$$

De la même façon on montre

$$\int_a^c f + \int_c^b f - \int_a^b f \geq -(b-a)\varepsilon$$

On en déduit le résultat. $\square$

Remarque 2.2.11.

On appelle *moyenne* de f sur $[a, b]$ la quantité

$$m = \frac{1}{b-a} \int_a^b f.$$

L'inégalité triangulaire permet de démontrer

$$\text{que } \left| \int_a^b f \right| \leq (b-a) \sup_{[a,b]} |f| \text{ et donc que } m \leq \sup_{[a,b]} |f|.$$

Théorème 2.2.12.

Soit $f \in \mathcal{C}^0([a, b])$, vérifiant $f \geq 0$. Alors :

- (i) s'il existe $x_0 \in [a, b]$ tel que $f(x_0) > 0$, alors

$$\int_a^b f > 0 ;$$

- (ii) si $\int_a^b f = 0$, alors $f = 0$.

Remarque 2.2.13.

Toutes les hypothèses sont indispensables : cherchez des contre-exemples !

Démonstration.

- (ii) n'est que la contraposée de (i). Il suffit donc de montrer (i).

Si $f(x_0) > 0$ et f continue, alors il existe $\alpha > 0$ tel que $f > f(x_0)/2$ sur $[x_0 - \alpha, x_0 + \alpha] \cap [a, b]$. On note alors φ l'application prenant la valeur $f(x_0)/2$ sur $[x_0 - \alpha, x_0 + \alpha] \cap [a, b]$ et 0 ailleurs. φ est une fonction inférieure à f , donc $\int_a^b \varphi \leq \int_a^b f$. De plus φ est en escalier, elle est nulle sauf sur l'intervalle $[x_0 - \alpha, x_0 + \alpha] \cap [a, b]$ où elle a pour valeur $f(x_0)/2$. Soit ℓ la longueur de cet intervalle. Or celle-ci est non nulle (regarder les différents cas suivant que x_0 est intérieur à $[a, b]$ ou non), donc $\int_a^b \varphi > 0$, d'où le résultat. $\square$

Exercice 2.2.14.

1. Soit $P \in \mathbb{R}[X]$ vérifiant $\int_0^1 P = 0$. Montrer que $P = 0$.

2. Soit $n \in \mathbb{N}$. Quels sont les polynômes $P \in \mathbb{R}_n[X]$ tels que $\int_0^1 P(t)t^k dt = 0$?

2.3 Extension au cas où $b \leq a$.

Soit I un intervalle on dit qu'une application f est continue par morceaux sur I si elle est continue par morceaux sur tout segment non trivial de I .

Soit donc $f : I \rightarrow \mathbb{R}$ continue par morceaux.

Soit a et b deux réels quelconques de I . Si $a < b$, on a vu comment définir $\int_a^b f$.

Si $b < a$, alors on définit $\int_a^b f$ comme étant le réel $-\int_b^a f$.

Si $a = b$, on pose $\int_a^b f = 0$.

L'intérêt principal de cette définition est de généraliser la relation de Chasles aux cas où les points a , b et c sont dans un ordre quelconque.

Proposition 2.3.1 (Relation de Chasles).

Soit I un intervalle et f continue par morceaux sur I . Alors, pour tout $(a, b, c) \in I^3$, on a

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

Démonstration.

Remarquons tout d'abord que nous avons déjà démontré ce résultat proposition 2.2.10 dans le cas où $a < c < b$.

Notons que ce résultat est trivial si $a = c$ ou $c = b$. On a donc le résultat pour $a \leq c \leq b$.

Remarquons ensuite que pour tout m , x , y appartenant à I , avec $m \leq x$ et $m \leq y$, on a

$$\int_x^y f = \int_m^y f - \int_m^x f.$$

En effet, si $x \leq y$, il suffit de remarquer que

$$\int_m^y f = \int_m^x f + \int_x^y f$$

et, si $x \geq y$, de remarquer que

$$\int_m^x f = \int_m^y f + \int_y^x f = \int_m^y f - \int_x^y f.$$

En posant $m = \min(a, b, c)$ on a alors successivement :

$$\begin{aligned} \int_a^c f + \int_c^b f &= \int_m^c f - \int_m^a f + \int_m^b f - \int_m^c f \\ &= \int_m^b f - \int_m^a f \\ &= \int_a^b f. \end{aligned}$$

□

Exercice 2.3.2.

Que deviennent les résultats de la proposition 2.2.10 si on remplace les hypothèses $a < b$ et $f, g \in \mathcal{C}_m([a, b])$ par I est un intervalle, $f, g \in \mathcal{C}_m(I)$ et a et b sont des éléments quelconques de I ?

3 Le théorème fondamental du calcul différentiel.

Dans toute la suite, I est un intervalle de $\mathbb{R}$.

3.1 Primitives.

Définition 3.1.1.

Soit f une application de I dans $\mathbb{R}$. On appelle primitive de f sur I toute application $F \in \mathcal{D}(I, \mathbb{R})$ telle que $F' = f$.

Théorème 3.1.2.

Si $f : I \rightarrow \mathbb{R}$ a une primitive F , alors l'ensemble des primitives de f est $\{ F + \lambda \mid \lambda \in \mathbb{R} \}$.

Démonstration.

Déjà fait dans le chapitre sur les équations différentielles. □

Remarque 3.1.3.

Il ne faut donc JAMAIS parler de LA primitive de f , sous peine de se faire lourdement châtier.

3.2 Existence de primitives.

Remarque 3.2.1.

Commençons par une première remarque : toutes les fonctions n'ont pas de primitive.

Exemple 3.2.2.

Posons

$$f : [-1, 1] \rightarrow \mathbb{R} \quad x \mapsto \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{sinon} \end{cases}.$$

Par l'absurde supposons que f admet une primitive F . Alors $F' = 0$ sur $[-1, 0[$ et $]0, 1]$, donc

$F = a$ sur $[-1, 0[$ et b sur $]0, 1]$. Mais F est dérivable donc continue, donc les limites à gauche et à droite en 0 doivent être égales, i.e. $a = b$. Mais alors F est constante sur $[-1, 1]$, donc F' est nulle partout, et ainsi $F' \neq f$.

Remarque 3.2.3.

En revanche, la fonction f de l'exemple 3.2.2 a une **intégrale**, et l'application

$$\begin{aligned} F : [-1, 1] &\rightarrow \mathbb{R} \\ x &\mapsto \int_{-1}^x f(t) dt \end{aligned}$$

est bien définie.



Il ne faut donc pas confondre primitive et intégrale.

Remarque 3.2.4.

De manière plus générale, le théorème de Darboux (HP, mais c'est une conséquence simple du théorème de Rolle) montre qu'une fonction dérivée vérifie toujours la propriété des valeurs intermédiaires. Une fonction ne vérifiant pas cette propriété (comme celle de l'exemple 3.2.2) ne peut donc admettre de primitive.

Théorème 3.2.5 (Théorème fondamental du calcul différentiel).

Soit $f \in \mathcal{C}^0(I, \mathbb{R})$, et $a \in I$.

1. f a une primitive, par exemple la fonction

$$\begin{aligned} F : I &\rightarrow \mathbb{R} \\ x &\mapsto \int_a^x f(t) dt \end{aligned}$$

2. Soit $A \in \mathbb{R}$. Alors f admet une unique primitive valant A en a . Il s'agit de la fonction

$$\begin{aligned} F : I &\rightarrow \mathbb{R} \\ x &\mapsto \int_a^x f(t) dt + A \end{aligned}$$

3. Soient $a, b \in I$ et $\tilde{F}$ une primitive de f sur I . Alors $\int_a^b f = \tilde{F}(b) - \tilde{F}(a)$. Cette quantité est aussi notée $[\tilde{F}]_a^b$, ou $[\tilde{F}(t)]_{t=a}^b$.

Remarque 3.2.6.

C'est souvent le deuxième ou le troisième point

que l'on appelle théorème fondamental du calcul différentiel, mais en fait le point le plus important est le premier, les deux autres en découlent facilement.

Démonstration. 1. Montrons que F est dérivable et $F' = f$.

Soit $x_0 \in I$, montrons que F est dérivable en x_0 , de dérivée $f(x_0)$.

Soit alors $\varepsilon > 0$. Puisque f est continue en x_0 , alors on peut trouver $\alpha > 0$ tel que

$$\forall y \in I, |x_0 - y| \leq \alpha \Rightarrow |f(x_0) - f(y)| \leq \varepsilon$$

$|f - f(x_0)|$ est alors majorée par ε sur $[x_0 - \alpha, x_0 + \alpha]$.

Soit $x \in [x_0 - \alpha, x_0 + \alpha] \cap I \setminus \{x_0\}$.

$$\begin{aligned} \left| \frac{F(x) - F(x_0)}{x - x_0} - f(x_0) \right| &= \left| \frac{\int_a^x f - \int_a^{x_0} f}{x - x_0} - f(x_0) \right| \\ &= \left| \frac{\int_{x_0}^x f}{x - x_0} - \frac{\int_{x_0}^{x_0} f(x_0)}{x - x_0} \right| \\ &= \left| \frac{\int_{x_0}^x (f - f(x_0))}{x - x_0} \right| \\ &\leq \frac{|x - x_0| \varepsilon}{|x - x_0|} \\ &\leq \varepsilon. \end{aligned}$$

On a montré que pour ε fixé, il existe $\alpha > 0$ tel que

$$\forall x \in I \quad |x - x_0| \leq \alpha \Rightarrow \left| \frac{F(x) - F(x_0)}{x - x_0} - f(x_0) \right| \leq \varepsilon,$$

donc $\frac{F(x) - F(x_0)}{x - x_0} \xrightarrow[x \neq x_0]{x \rightarrow x_0} f(x_0)$, d'où le résultat.

2. Facile.

3. Il existe K tel que $\tilde{F}(x) = \int_a^x f + K$, la suite est laissée en exercice. □

Exemple 3.2.7. 1. Calculer l'intégrale

$$\int_1^2 \frac{1}{(x+1)^n} dx.$$

2. Calculer $\lim_{n \rightarrow +\infty} \int_0^1 \frac{t^n}{(2+t)^n} dt$.

4 Méthodes de calcul.

Se référer au chapitre sur les équations différentielles.

5 Formules de Taylor.

Nous allons maintenant voir deux nouvelles formules de Taylor, mais qui sont cette fois des résultats *globaux*, alors que la formule de Taylor-Young est un résultat *local*.

Théorème 5.0.1 (Formule de Taylor avec reste intégral).

Soient $n \in \mathbb{N}$ et $f \in \mathcal{C}^{n+1}(I, \mathbb{R})$ et $(a, b) \in I^2$. Alors :

$$f(b) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (b-a)^k + \int_a^b \frac{f^{(n+1)}(t)}{n!} (b-t)^n dt. \quad (\star)$$

Remarque 5.0.2.

Si f est un polynôme de degré n , alors pour tout $k > n$, $f^{(k)} = 0$, et ainsi, en appliquant Taylor à un ordre supérieur à n , on retrouve la formule de Taylor pour les polynômes.

Démonstration.

Soit f une application de I dans $\mathbb{R}$ et $(a, b) \in I^2$. Pour $n \in \mathbb{N}$, on note $P(n)$ l'assertion « si $f \in \mathcal{C}^{n+1}(I, \mathbb{R})$, alors on a $(\star)$ ».

Alors :

- Montrons $P(0)$, c'est-à-dire si $f \in \mathcal{C}^1(I, \mathbb{R})$, alors $f(b) = f(a) + \int_a^b f'(t) dt$. C'est tout simplement le théorème fondamental de l'analyse.
- Montrons $\forall n \in \mathbb{N} (P(n) \Rightarrow P(n+1))$.

Soit $n \in \mathbb{N}$. Supposons $P(n)$. Montrons $P(n+1)$. Pour cela, supposons $f \in \mathcal{C}^{n+2}(I, \mathbb{R})$. Alors $f \in \mathcal{C}^{n+1}(I, \mathbb{R})$ donc, puisqu'on a $P(n)$, on a

$$f(b) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (b-a)^k + \int_a^b \frac{f^{(n+1)}(t)}{n!} (b-t)^n dt.$$

Calculons alors $\int_a^b \frac{f^{(n+1)}(t)}{n!} (b-t)^n dt$ grâce à une intégration par parties. On dérive $f^{(n+1)}$ (qui est bien $\mathcal{C}^1$) et on intègre $t \mapsto \frac{(b-t)^n}{n!}$, qui est bien continue. On obtient :

$$\begin{aligned} & \int_a^b \frac{f^{(n+1)}(t)}{n!} (b-t)^n dt \\ &= \left[f^{(n+1)}(t) \left(-\frac{(b-t)^{n+1}}{(n+1)!} \right) \right]_a^b - \int_a^b f^{(n+2)}(t) \left(-\frac{(b-t)^{n+1}}{(n+1)!} \right) dt \\ &= 0 + \frac{f^{(n+1)}(a)}{(n+1)!} (b-a)^{n+1} + \int_a^b f^{(n+2)}(t) \frac{(b-t)^{n+1}}{(n+1)!} dt. \end{aligned}$$

On a donc bien $\forall n \in \mathbb{N} P(n) \Rightarrow P(n+1)$.

On a donc $P(0)$ et $\forall n \in \mathbb{N} P(n) \Rightarrow P(n+1)$, donc on a $\forall n \in \mathbb{N} P(n)$. On a donc le résultat cherché. $\square$

Corollaire 5.0.3 (Inégalité de Taylor-Lagrange).
Avec les mêmes notations et hypothèses,

$$\left| f(b) - \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (b-a)^k \right| \leq \frac{|b-a|^{n+1}}{(n+1)!} \sup_{[a,b] \cup [b,a]} |f^{(n+1)}|.$$

Démonstration.

Faisons la démonstration dans le cas $a < b$ (le cas $a > b$ se traite de la même manière, en faisant attention au signe). On a alors $[a, b] \cup [b, a] = [a, b]$.

La formule de Taylor donne :

$$\begin{aligned} \underbrace{\left| f(b) - \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (b-a)^k \right|}_A &= \left| \int_a^b \frac{f^{(n+1)}(t)}{n!} (b-t)^n dt \right| \\ &\leq \int_a^b |f^{(n+1)}(t)| \frac{|b-t|^n}{n!} dt. \end{aligned}$$

$f^{(n+1)}$ est continue sur le segment $[a, b]$, donc bornée, donc on a :

$$\begin{aligned} A &\leq \int_a^b \sup_{[a,b]} |f^{(n+1)}| \frac{|b-t|^n}{n!} dt \\ &\leq \sup_{[a,b]} |f^{(n+1)}| \int_a^b \frac{|b-t|^n}{n!} dt \\ &\leq \sup_{[a,b]} |f^{(n+1)}| \left[\frac{-(b-t)^{n+1}}{(n+1)!} \right]_a^b \\ &\leq \sup_{[a,b]} |f^{(n+1)}| \frac{(b-a)^{n+1}}{(n+1)!}. \end{aligned}$$

$\square$

Exercice 5.0.4.

En appliquant l'inégalité de Taylor-Lagrange à la fonction exponentielle en zéro, montrer que pour tout $x \in \mathbb{R}$, $\sum_{k=0}^n \frac{x^k}{k!} \xrightarrow{n \rightarrow +\infty} e^x$.

Exercice 5.0.5.

Déterminer une valeur approchée rationnelle de $\frac{1}{e}$ à 10^{-3} près de $\frac{1}{e}$. En déduire un encadrement décimal de e , le plus précis possible.

6 Cas des fonctions à valeurs complexes.

Définition 6.0.1.

Soit $f : I \rightarrow \mathbb{C}$ telle que $g = \operatorname{Re}(f)$ et $h = \operatorname{Im}(f)$. Donc $g, h : I \rightarrow \mathbb{R}$ et $f = g + ih$. On suppose g et h de classe $\mathcal{C}_m$. Soient $a, b \in I$. On appelle *intégrale de f de a à b* , notée $\int_{[a,b]} f$ ou $\int_a^b f$ ou $\int_{[a,b]} f(t) dt$ ou $\int_a^b f(t) dt$, le **complexe** $\int_a^b f = \int_a^b g + i \int_a^b h$.

Remarque 6.0.2.

- On a donc $\operatorname{Re} \left(\int_a^b f \right) = \int_a^b \operatorname{Re}(f)$ et $\operatorname{Im} \left(\int_a^b f \right) = \int_a^b \operatorname{Im}(f)$.
- « L'aire sous la courbe » n'a plus aucun sens dans le cas d'une fonction à valeurs dans $\mathbb{C}$, et ne peut donc pas servir à interpréter l'intégrale d'une fonction à valeurs dans $\mathbb{C}$.

Théorème 6.0.3.

Soit $f \in \mathcal{C}^0(I, \mathbb{C})$ et $(a, b) \in I^2$ avec $a < b$.

1. La linéarité et la relation de Chasles sont toujours valables pour les fonctions à valeurs complexes.
2. Continuité : $\left| \int_a^b f \right| \leq \int_a^b |f|$.
3. Inégalité de la moyenne : $\left| \int_a^b (fg) \right| \leq (\sup_{[a,b]} |f|) \times \int_a^b |g|$.

Démonstration. 1. Se démontre comme pour les fonctions réelles.

2. On note $\theta = \arg \left(\int_a^b f \right)$, i.e. $e^{-i\theta} \int_a^b f = \left| \int_a^b f \right|$.
On pose pour $a, x \in I$:

$$F(x) = \int_a^x f(t) dt \text{ et } G(x) = \operatorname{Re} (e^{-i\theta} F(x)).$$

Alors

$$\begin{aligned} G(b) &= \operatorname{Re}(e^{-i\theta} F(b)) \\ &= \operatorname{Re} \left(e^{-i\theta} \int_a^b f(t) dt \right) \\ &= \operatorname{Re} \left| \int_a^b f(t) dt \right| \\ &= \left| \int_a^b f(t) dt \right|. \end{aligned}$$

On a aussi

$$\begin{aligned} G(b) &= \operatorname{Re} \left(\int_a^b e^{-i\theta} f(t) dt \right) \\ &= \int_a^b \operatorname{Re}(e^{-i\theta} f(t)) dt \\ &\leq \int_a^b |\operatorname{Re}(e^{-i\theta} f(t))| dt. \end{aligned}$$

On peut alors utiliser l'inégalité classique :

$$|\operatorname{Re}(e^{-i\theta} f(t))| \leq |e^{-i\theta} f(t)|,$$

donc

$$\begin{aligned} \left| \int_a^b f(t) dt \right| &= G(b) \\ &\leq \int_a^b |e^{-i\theta} f(t)| dt \\ &\leq \int_a^b |f(t)| dt. \end{aligned}$$

3. D'après ce qui précède, $\left| \int_a^b fg \right| \leq \int_a^b (|f| \times |g|)$. Il suffit alors d'utiliser les résultats sur les applications à valeurs réelles. $\square$

Exemple 6.0.4.

$$\begin{aligned} \int \frac{dt}{1+it} &= \int \frac{1-it}{1+t^2} dt \\ &= \int \frac{1}{1+t^2} dt - i \int \frac{t}{1+t^2} dt \\ &= \operatorname{Arctan} t - \frac{i}{2} \ln(1+t^2) + K, \quad K \in \mathbb{C}. \end{aligned}$$

7 Approximation d'intégrales.

On cherche maintenant à approcher des intégrales par des formes géométriques simples : rectangles à bases régulières d'abord, trapèzes ensuite.

7.1 Sommes de Riemann.

Théorème 7.1.1 (Sommes de Riemann).

Soient $a, b \in \mathbb{R}$ tels que $a < b$, $f \in \mathcal{C}_m([a, b], \mathbb{R})$ et $n \in \mathbb{N}^*$. On note alors, pour tout $k \in \llbracket 0, n \rrbracket$, $x_k = a + k \frac{b-a}{n}$. Les $\{x_k\}_{k \in \llbracket 0, n \rrbracket}$ forment alors une subdivision régulière de $[a, b]$ (i.e. tous les sous-intervalles sont de la même longueur). En posant

$$S_n = \frac{b-a}{n} \sum_{k=0}^{n-1} f(x_k) \text{ et } S'_n = \frac{b-a}{n} \sum_{k=1}^n f(x_k),$$

$(S_n)_{n \in \mathbb{N}^*}$ et $(S'_n)_{n \in \mathbb{N}^*}$ convergent toutes deux vers $\int_a^b f$.

Si de plus f est lipschitzienne sur $[a, b]$, alors

$$\left| S_n - \int_a^b f \right| = O\left(\frac{1}{n}\right),$$

$$\left| S'_n - \int_a^b f \right| = O\left(\frac{1}{n}\right),$$

c'est-à-dire que dans les deux cas l'erreur de l'approximation est un $O(1/n)$.

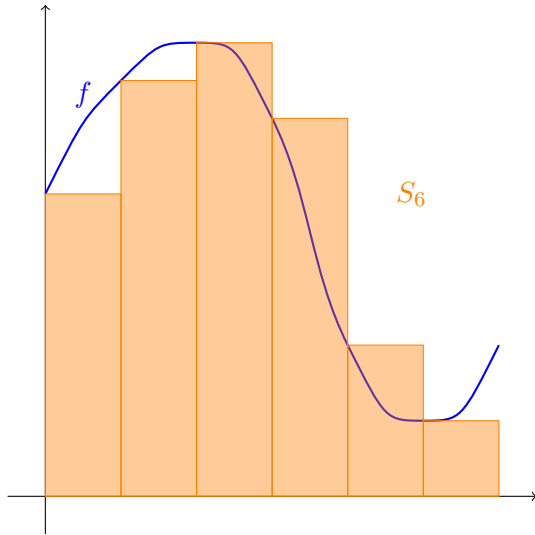


FIGURE XXII.3 – Exemple de somme de Riemann pour une fonction f , pour S_6 .

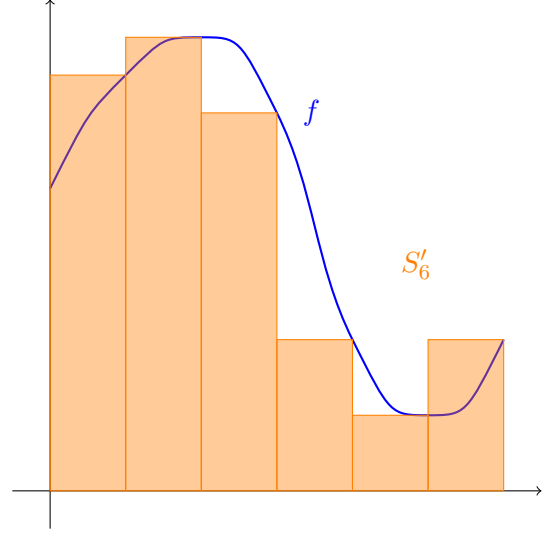


FIGURE XXII.4 – Exemple de somme de Riemann pour une fonction f , pour S'_6 .

Démonstration.

On se contentera de démontrer le résultat dans le cas où f est continue sur $[a, b]$.

Traitons le cas de S'_n . Comme $S_n = S'_n - \frac{(b-a)}{n}(f(b) - f(a))$, les choses se passent exactement de la même manière pour S_n .

On a par la relation de Chasles :

$$\begin{aligned} \int_a^b f(t) dt &= \int_{x_0}^{x_n} f(t) dt \\ &= \sum_{k=1}^n \int_{x_{k-1}}^{x_k} f(t) dt. \end{aligned}$$

Or pour chaque $k \in \llbracket 1, n \rrbracket$,

$$\begin{aligned} \int_{x_{k-1}}^{x_k} f(x_k) dt &= f(x_k) \int_{x_{k-1}}^{x_k} 1 dt \\ &= f(x_k)(x_k - x_{k-1}) \\ &= \frac{b-a}{n} f(x_k). \end{aligned}$$

On obtient donc

$$\left| \frac{b-a}{n} \sum_{k=1}^n f(x_k) - \int_a^b f(t) dt \right| = \left| \sum_{k=1}^n \int_{x_{k-1}}^{x_k} (f(x_k) - f(t)) dt \right|.$$

Ainsi, par l'inégalité triangulaire,

$$\left| S'_n - \int_a^b f(t) dt \right| \leq \sum_{k=1}^n \int_{x_{k-1}}^{x_k} |f(x_k) - f(t)| dt. \quad (\heartsuit)$$

Mais f est continue sur le segment $[a, b]$, donc d'après le théorème de Heine, elle y est uniformément continue. Si l'on considère $\varepsilon > 0$, alors il existe $\alpha > 0$ tel que

$$\forall x, y \in [a, b], \quad |x - y| < \alpha \Rightarrow |f(x) - f(y)| < \varepsilon.$$

Choisissons $N \in \mathbb{N}$ tel que $\frac{b-a}{N} < \alpha$. Pour tout $n \geq N$, on a donc $\frac{b-a}{n} < \alpha$.

Par conséquent, si $n \geq N$ et si l'on note encore $\{x_k\}$ la subdivision de l'énoncé associée à ce n , on a, pour tout $t \in [x_{k-1}, x_k]$,

$$|t - x_k| \leq |x_k - x_{k-1}| = \frac{b-a}{n} < \alpha.$$

Dans ce cas, on obtient de (♡) :

$$\begin{aligned} \left| S'_n - \int_a^b f(t) dt \right| &\leq \sum_{k=1}^n \int_{x_{k-1}}^{x_k} \varepsilon dt \\ &\leq \varepsilon \sum_{k=1}^n (x_k - x_{k-1}) \\ &\leq \varepsilon \sum_{k=1}^n \frac{b-a}{n} \\ &\leq \varepsilon (b-a). \end{aligned}$$

Ainsi, par définition,

$$\left| S'_n - \int_a^b f(t) dt \right| \xrightarrow{n \rightarrow +\infty} 0.$$

Soit $K > 0$ tel que f est K -lipschitzienne sur $[a, b]$. On obtient alors de (♡) :

$$\begin{aligned} \left| S'_n - \int_a^b f(t) dt \right| &\leq \sum_{k=1}^n \int_{x_{k-1}}^{x_k} K|x_k - t| dt \\ &\leq K \sum_{k=1}^n \int_{x_{k-1}}^{x_k} (x_k - t) dt \\ &\leq K \sum_{k=1}^n \left[-\frac{1}{2}(x_k - t)^2 \right]_{x_{k-1}}^{x_k} \\ &\leq \frac{K}{2} \sum_{k=1}^n (x_k - x_{k-1})^2 \\ &\leq \frac{K}{2} \sum_{k=1}^n \left(\frac{b-a}{n} \right)^2 \\ &\leq \frac{K}{2} n \left(\frac{b-a}{n} \right)^2 \\ &\leq \frac{K(b-a)^2}{2} \times \frac{1}{n}, \end{aligned}$$

donc par définition

$$\left| S'_n - \int_a^b f(t) dt \right| = O\left(\frac{1}{n}\right).$$

□

Remarque 7.1.2.

Si f est de classe $\mathcal{C}^1$ sur $[a, b]$, alors f est lipschitzienne sur $[a, b]$ (on peut prendre comme constante de Lipschitz $K = \sup_{[a, b]} |f'|$).

Alors, l'erreur d'approximation obtenue en approchant $\int_a^b$ par S_n ou S'_n est un $O\left(\frac{1}{n}\right)$.

Remarque 7.1.3.

Quand f est continue, on peut toujours écrire

$$\begin{aligned} S_n &= \frac{b-a}{n} \sum_{k=1}^n f\left(a + k \frac{b-a}{n}\right) \\ &= (b-a) \times \frac{1}{n} \sum_{k=1}^n g\left(\frac{k}{n}\right) \\ &\xrightarrow{n \rightarrow +\infty} (b-a) \int_0^1 g, \end{aligned}$$

avec $g : [0, 1] \rightarrow \mathbb{R}$, $t \mapsto f(a + t(b-a))$.

Exercice 7.1.4.

Faire apparaître une somme de Riemann dans

$$S_n = \sum_{k=1}^n \frac{n}{k^2 + 3n^2}$$

puis étudier la convergence de (S_n) .

Exercice 7.1.5.

Déterminer pour tout $p \in \mathbb{N}$ un équivalent lorsque n tend vers $+\infty$ de

$$S_n^p = \sum_{k=1}^n k^p.$$

7.2 La méthode des trapèzes.

La méthode d'approximation des sommes de Riemann est couramment appelée *méthode des rectangles*. Sa convergence n'est pas très rapide car elle est seulement en $O(1/n)$. Une amélioration possible est la méthode qui suit : la *méthode des trapèzes*.

Théorème 7.2.1.

On reprend les mêmes notations que dans le théorème 7.1.1, mais cette fois f est de classe $\mathcal{C}^2$. Alors :

$$\begin{aligned} \left| \frac{b-a}{n} \left(\frac{f(a) + f(b)}{2} + \sum_{k=1}^{n-1} f(x_k) \right) - \int_a^b f(t) dt \right| \\ = O(1/n^2). \end{aligned}$$

Remarque 7.2.2.

Ce résultat est admis, mais remarquons tout de même les choses suivantes :

- la somme des aires des trapèzes obtenus avec la subdivision $\{x_k\}$ vaut

$$\begin{aligned}
 T_n &= \sum_{k=0}^{n-1} \underbrace{\frac{b-a}{n}}_{\text{base}} \times \underbrace{\frac{f(x_{k+1}) + f(x_k)}{2}}_{\text{moyenne des deux hauteurs}} \\
 &= \frac{b-a}{2n} \left(\sum_{k=0}^{n-1} f(x_{k+1}) + \sum_{k=0}^{n-1} f(x_k) \right) \\
 &= \frac{b-a}{2n} \left(\sum_{k=1}^n f(x_k) + \sum_{k=0}^{n-1} f(x_k) \right) \\
 &= \frac{b-a}{2n} \left(f(x_0) + f(x_n) + 2 \sum_{k=1}^{n-1} f(x_k) \right) \\
 &= \frac{b-a}{2n} \left(f(a) + f(b) + 2 \sum_{k=1}^{n-1} f(x_k) \right).
 \end{aligned}$$

- il est aisé de voir que $(T_n)_{n \in \mathbb{N}^*}$ converge vers l'intégrale, et que la différence entre T_n et sa limite est un $O(1/n)$. En effet, pour tout $n \in \mathbb{N}^*$, $T_n = \frac{1}{2}(S_n + S'_n)$.

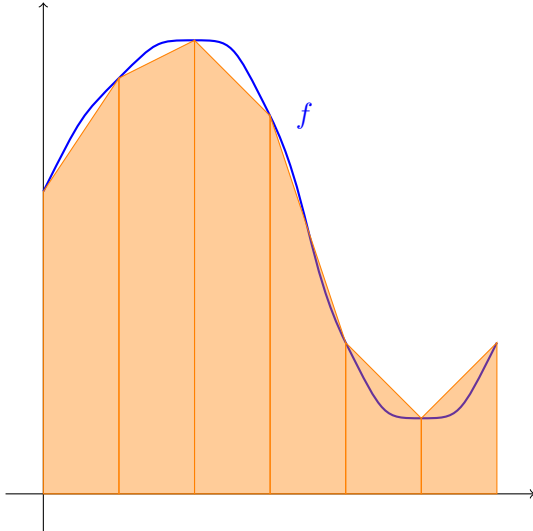


FIGURE XXII.5 – Exemple de la méthode des trapèzes pour une fonction f , avec 6 subdivision.

$$0 \leq \sum_{k=0}^5 f(k) - \int_0^6 f(t) dt \leq f(0)$$

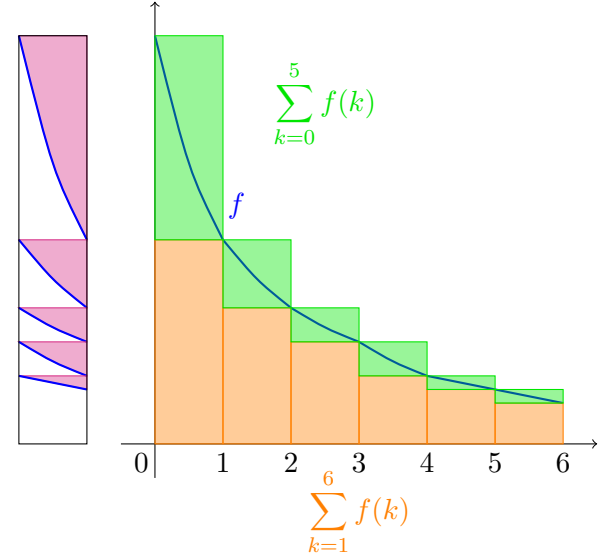


FIGURE XXII.6 – Exemple de comparaison série-intégrale pour une fonction f décroissante, positive.

8 Comparaison série-intégrale.

Proposition 8.0.1.

Soit $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ une fonction continue par morceaux et décroissante.

Alors la suite $\left(\sum_{k=0}^n f(k) \right)_{n \in \mathbb{N}}$ converge si et seulement si la suite $\left(\int_0^n f(t) dt \right)_{n \in \mathbb{N}}$ est convergente.

De plus la suite définie par $u_n = \sum_{k=0}^n f(k) - \int_0^n f(t) dt$ converge.

Démonstration.

Soit $k \in \mathbb{N}$. Par décroissance de f , on a :

$$\forall t \in [k, k+1], 0 \leq f(k+1) \leq f(t) \leq f(k).$$

Puis, par intégration de cet encadrement sur $[k, k+1]$,

$$0 \leq f(k+1) \leq \int_k^{k+1} f(t) dt \leq f(k) \quad (\text{XXII.4})$$

et, par sommation, pour $n \geq 1$,

$$0 \leq \sum_{k=0}^{n-1} f(k+1) \leq \int_0^n f(t) dt \leq \sum_{k=0}^{n-1} f(k),$$

ou encore

$$0 \leq \sum_{k=0}^n f(k) - f(0) \leq \int_0^n f(t) dt \leq \sum_{k=0}^n f(k) - f(n).$$

Les suites croissantes $\left(\sum_{k=0}^n f(k) \right)_{n \in \mathbb{N}}$ et $\left(\int_0^n f(t) dt \right)_{n \in \mathbb{N}}$ ont donc la même nature. De plus, il vient

$$0 \leq f(n) \leq \sum_{k=0}^n f(k) - \int_0^n f(t) dt$$

soit $0 \leq u_n$. Ainsi (u_n) est minorée. Enfin, on a

$$u_{n+1} - u_n = f(n+1) - \int_n^{n+1} f(t) dt \leq 0.$$

La suite (u_n) est donc décroissante et minorée et converge donc. $\square$

Remarque 8.0.2.

L'encadrement XXVIII.1 est à rapprocher de la méthode des rectangles.

Exercice 8.0.3.

Retrouver la nature de la suite $\left(\sum_{n=1}^N \frac{1}{n^\alpha} \right)_{N \in \mathbb{N}}$, pour $\alpha > 0$.

Exemple 8.0.4.

On pose $f : x \mapsto \frac{1}{1+x}$. On sait alors que la suite de terme général $u_n = \sum_{k=0}^n f(k) - \int_0^n f(t) dt = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \ln n$ converge, vers une limite notée γ et nommée *constante d'Euler*.

9 Annexes.

9.1 Fonctions dont la variable intervient dans les bornes d'une intégrale (cas particulier d'intégrales dépendant d'un paramètre).

Théorème 9.1.1.

Soit $\varphi, \psi \in \mathcal{C}^1(I, J)$ où I et J sont deux intervalles de $\mathbb{R}$, et soit $f \in \mathcal{C}^0(J, \mathbb{R})$. Alors la fonction

$$\Gamma : \begin{cases} I & \rightarrow \mathbb{R} \\ x & \mapsto \int_{\varphi(x)}^{\psi(x)} f(t) dt \end{cases}$$

est de classe $\mathcal{C}^1$, et sa dérivée est

$$\gamma : \begin{cases} I & \rightarrow \mathbb{R} \\ x & \mapsto \psi'(x) \times (f \circ \psi)(x) - \varphi'(x) \times (f \circ \varphi)(x) \end{cases}.$$

Démonstration.

f étant continue, elle admet une primitive F . On a alors, pour tout $x \in I$:

$$\begin{aligned} \Gamma(x) &= \int_{\varphi(x)}^{\psi(x)} f(t) dt = F(\psi(x)) - F(\varphi(x)) \\ &= F \circ \psi(x) - F \circ \varphi(x). \end{aligned}$$

Mais F , ψ et φ étant de classe $\mathcal{C}^1$, Γ l'est aussi et on a

$$\begin{aligned} \Gamma' &= (F \circ \psi - F \circ \varphi)' \\ &= \psi' \times (F' \circ \psi) - \varphi' \times (F' \circ \varphi) \\ &= \psi' \times (f \circ \psi) - \varphi' \times (f \circ \varphi) \\ &= \gamma. \end{aligned}$$

$\square$

Chapitre XXIII

Dénombrement

Sommaire

1	Cardinal d'un ensemble fini.	348
2	Dénombrement.	350
2.1	Réunion, intersection et complémentaire.	350
2.2	Produit cartésien.	350
2.3	Applications entre ensembles finis. . .	351
2.4	Parties d'un ensemble fini.	351

Soient E , F et G trois ensembles.

Définition 0.0.1.

On dit que E et F sont *équipotents* s'il existe une bijection de E dans F . Dans ce cas, on notera $E \cong F$ (notation non officielle), et si φ est une bijection de E dans F , on notera $\varphi : E \xrightarrow{\sim} F$.

Proposition 0.0.2.

La relation d'équipotence est une relation d'équivalence.

1 Cardinal d'un ensemble fini.

Le programme stipule que parmi les propriétés de la partie 1, les plus intuitives seront admises sans démonstration ; il stipule également que l'utilisation systématique de bijections dans les problèmes de dénombrement n'est pas un attendu du programme.

Définition 1.0.1.

On dit que E est *fini* s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel que $E \cong \llbracket 1, n \rrbracket$.
Dans le cas contraire, E est dit *infini*.

Le résultat qui donne un sens à ce que l'on appelle intuitivement *le nombre d'éléments d'un ensemble fini* est alors le suivant.

Théorème 1.0.2. (i) Soient n, m deux entiers naturels non nuls. Si $\llbracket 1, n \rrbracket \cong \llbracket 1, m \rrbracket$, alors $n = m$.

(ii) Cela assure que si un ensemble est fini et équipotent à $\llbracket 1, n \rrbracket$ pour un certain $n \in \mathbb{N}^*$, alors ce n est unique et est appelé le *cardinal* de E , et est noté $\text{Card } E$ ou $|E|$.

Par convention, $\text{Card } \emptyset = 0$.

Démonstration.

La démonstration du premier point se fait par récurrence sur n en posant l'hypothèse (P_n) : pour tout $m \in \mathbb{N}^*$, si $\llbracket 1, m \rrbracket \cong \llbracket 1, n \rrbracket$, alors $m = n$.
La démonstration est tout à fait du même style que les démonstrations des résultats 1.0.6 et 1.0.7, et est laissée en exercice. $\square$

Remarque 1.0.3.

On trouvera parfois la notation $\#E$.

Exemple 1.0.4. 1. Pour tout $n \in \mathbb{N}$, $\llbracket 1, n \rrbracket$ est évidemment fini et de cardinal n .

2. Soient $n, m \in \mathbb{N}$, $n < m$.

Alors $\text{Card} \llbracket n, m \rrbracket = m - n + 1$. En effet, l'application $\llbracket 1, m - n + 1 \rrbracket \rightarrow \llbracket n, m \rrbracket$, $a \mapsto a + n - 1$ est une bijection.

Dans toute la suite on supposera que E est fini de cardinal n .

Théorème 1.0.5.

E est équipotent à F si et seulement si (F est aussi fini et $\text{Card } E = \text{Card } F$).

Démonstration.

Si E est vide, F aussi.

Sinon, soit $\varphi : \llbracket 1, n \rrbracket \xrightarrow{\sim} E$, et $\psi : E \xrightarrow{\sim} F$. Alors $\psi \circ \varphi : \llbracket 1, n \rrbracket \xrightarrow{\sim} F$. $\square$

Lemme 1.0.6.

Supposons E non vide, et $a \in E$. Alors $E \setminus \{a\}$ est fini de cardinal $n - 1$.

Démonstration.

Le cas où $E = \{a\}$ est évident. Supposons donc que $E \setminus \{a\}$ est non vide.

Soit $\varphi : \llbracket 1, n \rrbracket \xrightarrow{\sim} E$.

- Si $\varphi(n) = a$, posons $\psi = \varphi$.
- Si $\varphi(n) = b$ pour b un élément de E différent de a , notons p l'antécédent de a . Donc $p < n$. Posons alors $\psi = \varphi \circ \tau_{p,n}$, où $\tau_{p,n}$ est la transposition de S_n échangeant p et n .

Alors, dans tous les cas, $\psi : \llbracket 1, n \rrbracket \xrightarrow{\sim} E$, et $\psi(n) = a$.
Ainsi, $\psi|_{\llbracket 1, n-1 \rrbracket} : \llbracket 1, n-1 \rrbracket \xrightarrow{\sim} E \setminus \{a\}$, d'où le résultat. $\square$

Théorème 1.0.7.

Soit $A \subset E$. Alors A est fini et $\text{Card } A \leq \text{Card } E$.
De plus, $\text{Card } A = \text{Card } E$ si et seulement si $A = E$.

Démonstration.

On le montre par récurrence sur $n = \text{Card } E$.

Si $n = 0$, $E = A = \emptyset$, et le résultat est évident.

Soit $n \in \mathbb{N}$ tel que pour tout ensemble E de cardinal n , et pour tout $A \subset E$, A est fini et $\text{Card } A \leq \text{Card } E$.

Soit E de cardinal $n + 1$, et $A \subset E$. Si $A = E$, alors A est fini et $\text{Card } A = \text{Card } E$.

Sinon, soit $a \in E \setminus A$. Posons $\tilde{E} = E \setminus \{a\}$. Alors $\text{Card } \tilde{E} = n$ d'après le lemme précédent, et $A \subset \tilde{E}$. Par hypothèse de récurrence, A est fini, et $\text{Card } A \leq n$. En particulier, $\text{Card } A < \text{Card } E$, donc $A \neq E$, ce qui prouve au passage que $\text{Card } A = \text{Card } E$ si et seulement si $A = E$. $\square$

Remarque 1.0.8.

Grâce à ce résultat, pour montrer l'égalité de deux ensembles finis, on peut montrer la double inclusion, mais aussi se contenter d'une inclusion et montrer l'égalité des cardinaux.

Ce résultat est à rapprocher du résultat assurant que deux espaces vectoriels de dimension finie sont égaux si et seulement si l'un est inclus dans l'autre et ils ont même dimension.

Lemme 1.0.9.

Soit f une application surjective de F dans G . Alors il existe une injection de G dans F .

Démonstration.

Soit $y \in G$. Alors y a un (ou plusieurs) antécédent(s) par f . Choisissons un de ces antécédents, et notons-le $g(y)$. On définit ainsi une application $g : G \rightarrow F$, tel que pour tout $y \in G$, $f(g(y)) = y$. Ainsi, $f \circ g$ est injective, et on sait alors que g est injective de G dans F . $\square$

Exercice 1.0.10.

Montrer que s'il existe une injection $f : F \rightarrow G$, alors il existe une surjection $g : G \rightarrow F$.

Théorème 1.0.11.

Soit f une application de F dans G .

- (i) Si G est fini et f est injective, alors F est fini également, et $\text{Card } F \leq \text{Card } G$.
- (ii) Si F est fini et f est surjective, alors G est fini également, et $\text{Card } F \geq \text{Card } G$.
- (iii) Si F et G sont finis et $\text{Card } F = \text{Card } G$, alors :

f est injective $\Leftrightarrow f$ est surjective $\Leftrightarrow f$ est bijective.

Remarque 1.0.12.

La relation « F a moins d'éléments que G » correspond donc à « F s'injecte dans G » (au moins pour des ensembles finis).

De même, la relation « F a plus d'éléments que G » correspond donc à « F se surjecte sur G » (au moins pour des ensembles finis).

Concernant des ensembles quelconques, le lecteur intéressé pourra étudier le théorème de Cantor-Bernstein.

Remarque 1.0.13.

Une fois encore, ce résultat est à rapprocher des résultats sur les espaces vectoriels et les applications linéaires en dimension finie.

Démonstration. (i) f étant injective, elle établit une bijection de F dans $f(F)$. Or $f(F) \subset G$, donc $f(F)$ est fini et $\text{Card } f(F) \leq \text{Card } G$. Ainsi, puisque $F \cong f(F)$, F est fini et $\text{Card } F \leq \text{Card } G$.

(ii) En utilisant 1.0.9, soit g injective de G dans F . En appliquant le premier point, G est donc fini et $\text{Card } G \leq \text{Card } F$.

(iii) Il suffit de démontrer : f est injective $\Leftrightarrow f$ est surjective, le reste étant alors facile.

Pour le sens direct, si f est injective, f est une bijection de F dans $f(F)$, donc $\text{Card } F = \text{Card } f(F)$. Mais $\text{Card } G = \text{Card } F$, donc $\text{Card } f(F) = \text{Card } G$, et comme $f(F) \subset G$, nous avons $f(F) = G$, ce qui signifie bien que f est surjective.

Pour le sens indirect, soient $x, y \in F$ tels que $f(x) = f(y)$ et $x \neq y$. Alors $f(y) \in f(F \setminus \{x\})$, et donc $f(F \setminus \{x\}) = G$. Par conséquent, $f|_{F \setminus \{x\}}$ est surjective à valeurs dans G , donc avec le point (ii), $\text{Card } F \setminus \{x\} \geq \text{Card } G$. Mais $\text{Card } F \setminus \{x\} = \text{Card } F - 1 = \text{Card } G - 1$, ce qui est absurde. Par conséquent, f est aussi injective. $\square$

Exercice 1.0.14.

Soient $(G, \star)$ un groupe et A une partie *finie* non vide de G stable par $\star$. Soit $x \in A$.

1. Soit $\varphi : \mathbb{N}^* \rightarrow G$ l'application définie par $\varphi(n) = x^n$. Montrer que φ n'est pas injective.
2. En déduire que $x^{-1} \in A$, puis que A est un sous-groupe de $(G, \star)$.

Corollaire 1.0.15 (Principe des tiroirs, ou *Pigeonhole Principle* en anglais).

Si $m < n$, il est impossible de ranger n paires de chaussettes dans m tiroirs sans en mettre au moins deux dans le même tiroir.

Exercice 1.0.16.

Soit $n \in \mathbb{N}^*$ et $a_0, \dots, a_n \in \mathbb{Z}$. Montrer qu'il existe $0 \leq i \neq j \leq n$ tels que $n \mid (a_i - a_j)$.

Exercice 1.0.17. 1. On prend un Rubik's Cube fini sur lequel on effectue la même manipulation encore et toujours. Démontrer que l'on finit par se retrouver avec ce Rubik's Cube de nouveau terminé.¹

2. Les membres d'une société internationale sont originaires de six pays différents. La liste des membres contient 1978 noms numérotés de 1 à 1978. Montrer qu'il y a un membre dont le numéro vaut la somme des numéros de deux autres membres venant du même pays ou le double du numéro d'un compatriote.²

2 Dénombrement.

2.1 Réunion, intersection et complémentaire.

Définition 2.1.1.

Lorsque deux ensembles A et B sont disjoints, la réunion de A et B est appelée *union disjointe* de A et B , et est notée $A \sqcup B$.

Théorème 2.1.2.

Soient A et B deux parties de E .

- (i) Si A et B sont disjoints, alors $\text{Card}(A \sqcup B) = \text{Card } A + \text{Card } B$;
- (ii) $\text{Card}(A \setminus B) = \text{Card } A - \text{Card}(A \cap B)$;
- (iii) $\text{Card}(A \cup B) = \text{Card } A + \text{Card } B - \text{Card}(A \cap B)$.
- (iv) $\text{Card}(\mathcal{C}_E^A) = \text{Card } E - \text{Card } A$.

Démonstration. (i) Soient m, p les cardinaux de A et B , et $\varphi : [1, m] \xrightarrow{\sim} A$ et $\psi : [1, p] \xrightarrow{\sim} B$.

Soit $\chi : [1, m+p] \rightarrow A \sqcup B$

$$x \mapsto \begin{cases} \varphi(x) & \text{si } x \leq m \\ \psi(x-m) & \text{si } x > m \end{cases}.$$

Cette application est bien définie et il est facile de voir qu'elle est surjective. De plus, A et B étant disjoints, elle est injective, donc $A \sqcup B \cong [1, m+p]$, donc $\text{Card}(A \sqcup B) = m+p = \text{Card } A + \text{Card } B$.

(ii) Il suffit d'écrire que $A = (A \cap B) \sqcup (A \setminus B)$ et d'utiliser le premier point.

(iii) Là encore, on remarque que $A \cup B = B \sqcup (A \setminus B)$ et on utilise les deux premiers points.

(iv) Remarquer que $\mathcal{C}_E^A = E \setminus A$. □

Remarque 2.1.3.

Il existe une formule qui généralise le résultat précédent à la réunion d'une famille finie d'ensembles finis : c'est la *formule de Poincaré*, aussi appelée *formule du crible*. Elle est hors-programme et sera vue en TD.

2.2 Produit cartésien.

Théorème 2.2.1.

Soient E et F deux ensembles finis. Alors $E \times F$ est fini et

$$\text{Card}(E \times F) = (\text{Card } E) \times (\text{Card } F).$$



Il existe beaucoup d'analogies entre la dimension d'un espace vectoriel et le cardinal d'un ensemble, mais $\dim(E \times F) = \dim E + \dim F$.

Démonstration.

On note :

$$n = \text{Card } E, p = \text{Card } F, \\ E = \{e_1, \dots, e_n\}, F = \{f_1, \dots, f_p\}.$$

Donc $E \times F = \{(e_i, f_j), i \in [1, n], j \in [1, p]\}$.

Donc en notant $A_i = \{e_i\} \times F$ pour $i \in [1, n]$, on a :

$$E \times F = \bigsqcup_{i=1}^n A_i,$$

ainsi

$$\begin{aligned} \text{Card } E \times F &= \sum_{i=1}^n \text{Card } A_i \\ &= \sum_{i=1}^n \text{Card } F \\ &= n \text{Card } F \\ &= \text{Card } E \times \text{Card } F. \end{aligned}$$

□

Remarque 2.2.2.

Ce résultat se généralise facilement par récurrence à un produit de q ensembles finis, $q \in \mathbb{N}^*$:

$$\text{Card} \left(\prod_{i=1}^q E_i \right) = \prod_{i=1}^q \text{Card } E_i.$$

Exercice 2.2.3.

Combien y a-t-il de possibilités de tirer neuf cartes avec remise dans un jeu de 32 cartes ?

2.3 Applications entre ensembles finis.**Théorème 2.3.1.**

Soient E et F deux ensembles finis. Alors F^E est fini et

$$\text{Card} (F^E) = (\text{Card } F)^{\text{Card } E}.$$

Démonstration.

On pose $\varphi : \llbracket 1, n \rrbracket \xrightarrow{\sim} E$, et :

$$\begin{aligned} \mu : F^E &\rightarrow F^n \\ f &\mapsto (f \circ \varphi(1), \dots, f \circ \varphi(n)) = (f \circ \varphi(i))_{i \in \llbracket 1, n \rrbracket} \\ \nu : F^n &\rightarrow F^E \\ (f_1, \dots, f_n) = (f_i)_{i \in \llbracket 1, n \rrbracket} &\mapsto \begin{cases} E &\rightarrow F \\ x &\mapsto f_{\varphi^{-1}(x)} \end{cases} \end{aligned}$$

On vérifie que $\nu \circ \mu = \text{Id}_{F^E}$ et $\mu \circ \nu = \text{Id}_{F^n}$, donc ce sont des bijections. Ainsi $F^E \cong F^n$ et l'on peut conclure avec 1.0.5. $\square$

Définition 2.3.2.

Soit $p \in \llbracket 1, n \rrbracket$. On appelle *p -arrangement de E* toute injection de $\llbracket 1, p \rrbracket$ dans E . Autrement dit, un p -arrangement est une manière de choisir p éléments deux à deux distincts de E **en tenant compte de l'ordre dans lequel on choisit ces éléments** ; c'est donc aussi un p -uplet de E , ou encore une liste de p éléments de E .

Exemple 2.3.3.

Si $E = \llbracket 1, 5 \rrbracket$ et $p = 2$, les applications φ et ψ de $\llbracket 1, 2 \rrbracket$ dans E telles que $\varphi(1) = 3$, $\varphi(2) = 5$, $\psi(1) = 5$ et $\psi(2) = 3$, sont deux p -arrangements **différents** de E .

On peut aussi les identifier aux couples $(3, 5)$ et $(5, 3)$.

Théorème 2.3.4.

Si $\text{Card } E = n$, il y a exactement $\frac{n!}{(n-p)!}$ p -arrangements de E .

Démonstration.

Pour construire une injection f de $\llbracket 1, p \rrbracket$ dans E , il y a n choix possibles pour $f(1)$. Il reste alors $n-1$ choix possibles pour $f(2)$ et ainsi de suite, jusqu'aux $n-p+1$ choix possibles pour $f(p)$: il y a donc $n \times (n-1) \times \dots \times (n-p+1)$ injections possibles. $\square$

Remarque 2.3.5.

Les arrangements sont utilisés pour modéliser des tirages **successifs** et **sans remise**.

Exercice 2.3.6.

Vous jouez « au hasard » au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans l'ordre ?

Corollaire 2.3.7.

Le groupe S_n des permutations sur n éléments est fini de cardinal $n!$.

Démonstration.

S_n correspond à l'ensemble des n -arrangements de $\llbracket 1, n \rrbracket$. $\square$

2.4 Parties d'un ensemble fini.**Définition 2.4.1.**

Soit $p \in \llbracket 0, n \rrbracket$. On appelle *p -combinaison de E* toute partie de E de cardinal p . Autrement dit, une p -combinaison est une manière de choisir p éléments distincts de E **sans tenir compte de l'ordre dans lequel on choisit ces éléments**.

On note alors $\binom{n}{p}$ le nombre de p -combinaisons de E ; ce nombre se lit « p parmi n ».

Remarque 2.4.2.

Les combinaisons sont utilisées pour modéliser des tirages **simultanés**.

Remarque 2.4.3.

On étend cette définition à $p \in \mathbb{Z}$ par $\binom{n}{p} = 0$ lorsque $p \notin \llbracket 0, n \rrbracket$.

Théorème 2.4.4.

Si $n \in \mathbb{N}$ et $p \in \llbracket 0, n \rrbracket$, alors $\binom{n}{p} = \frac{n!}{(n-p)!p!}$.

Remarque 2.4.5.

Nous venons donc de donner une nouvelle définition du coefficient binomial $\binom{n}{p}$, défini en début d'année, et que nous avons interprété comme le nombre de chemins réalisant p succès lors de n répétitions d'une même expérience aléatoire. Remarquons à nouveau qu'il s'agit d'un entier, ce qui n'est absolument pas évident avec la formule du théorème 2.4.4.

Démonstration.

Commençons par remarquer qu'ordonner (totalement) un ensemble à n éléments revient à numéroté ses éléments de 1 à n . Par conséquent, un ordre sur E peut être vu comme une bijection de $\llbracket 1, n \rrbracket$ dans E , ou encore comme une permutation de E . Il y a donc $n!$ façons d'ordonner un ensemble à n éléments.

Ainsi, pour chaque choix de p éléments parmi n , il existe $p!$ p -arrangements contenant ces p -éléments : il y a donc exactement $p!$ fois plus de p -arrangements que de p -combinaisons. Ainsi, $\binom{n}{p} = \frac{1}{p!} \times \frac{n!}{(n-p)!}$. $\square$

Exercice 2.4.6.

Vous jouez au hasard au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans le désordre ?

Proposition 2.4.7 (Formule du triangle de Pascal).

Si $n \in \mathbb{N}^*$ et si $p \in \mathbb{N}$, $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$.

Démonstration.

On donne ici une preuve combinatoire. Le cas où $p \notin \llbracket 1, n-1 \rrbracket$ est évident. Sinon, soit E de cardinal n et $a \in E$. Notons F_p l'ensemble des parties de E à p éléments, A_p l'ensemble de ces parties qui contiennent a et B_p l'ensemble de ces parties qui ne contiennent pas a , i.e

$$F_p = \{A \subset E \mid |A| = p\}$$

$$A_p = \{A \in F_p \mid a \in A\}; B_p = \{A \in F_p \mid a \notin A\}.$$

Alors $F_p = A_p \sqcup B_p$.

De plus, A_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant $p-1$ éléments (par $A \mapsto A \setminus \{a\}$) et possède donc $\binom{n-1}{p-1}$ éléments. De même,

B_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant p éléments (par $A \mapsto A$) et possède donc $\binom{n-1}{p}$ éléments. Cela permet donc de conclure, car $|F_p| = |A_p| + |B_p|$. $\square$

Proposition 2.4.8 (Formule du binôme de Newton).

Soit x et y deux éléments d'un anneau $(A, +, \cdot)$ commutant l'un avec l'autre ($xy = yx$), soit $n \in \mathbb{N}$. Alors

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

Démonstration.

En voici une preuve combinatoire. On montre d'abord aisément par récurrence que toutes les puissances de x et de y commutent. Ensuite, lorsque l'on développe le produit

$$(x+y)^n = \underbrace{(x+y) \cdots (x+y)}_{n \text{ fois}}$$

on obtient des termes qui sont des produits de k facteurs valant x , et de $n-k$ facteurs valant y , pour k allant de 0 à n . Or, pour chacun de ces k , il y a k parmi n possibilités d'obtenir un produit de k facteurs valant x , et de $n-k$ facteurs valant y , d'où le résultat. $\square$

Théorème 2.4.9.

Si E est fini, l'ensemble $\mathcal{P}(E)$ des parties l'est aussi et

$$\text{Card } \mathcal{P}(E) = 2^{\text{Card } E}.$$

Démonstration.

Pour tout $i \in \llbracket 0, n \rrbracket$, notons P_i l'ensemble des parties de E ayant i éléments. Nous avons alors $\mathcal{P}(E) = \bigsqcup_{i=0}^n P_i$. Or chaque P_i est de cardinal $\binom{n}{i}$, donc $\mathcal{P}(E)$ est fini et :

$$\begin{aligned} \text{Card } \mathcal{P}(E) &= \sum_{i=0}^n \binom{n}{i} \\ &= (1+1)^n \quad (\text{binôme de Newton}) \\ &= 2^n. \end{aligned}$$

On peut aussi voir qu'il y a une correspondance bijective entre les parties de E et les applications à variables dans E et à valeurs dans $\{0, 1\}$, par $\mathcal{P}(E) \rightarrow \{0, 1\}^E$, $A \mapsto 1_A$. $\square$

Exercice 2.4.10.

Dans une urne, on place quatre boules rouges (numérotées 1 à 4) et trois boules vertes (numérotées

5 à 7). On réalise trois tirages avec remise, un résultat est le triplet des boules tirées.

Combien y a-t-il de résultats contenant exactement une boule rouge ? Au moins une boule rouge ? Au plus deux boules rouges ? Dont les deux dernières boules sont de couleurs différentes ?

Et si les tirages se font sans remise ?

Notes

¹Pour mémoire, il y a plus de 43.10^{12} combinaisons possibles sur un Rubik's Cube classique.

²L'idée est d'utiliser des différences.

On remarque que $6 \times 329 = 1974$ donc au moins 330 membres viennent d'un même pays. Appelons ce pays P_1 . Notons $a_1 < a_2 < \dots < a_{330}$ les numéros des membres de ce pays. Considérons maintenant les 329 différences $a_2 - a_1, a_3 - a_1, \dots, a_{330} - a_1$. Si l'un de ces nombres est dans P_1 , nous avons fini.

Sinon, ils sont tous dans l'un des 5 pays restants. On réitère le procédé : au moins 66 de ces nouveaux nombres doivent venir d'un même pays noté P_2 . On les note $b_1, \dots, b_{66}$ et on regarde les différences $b_2 - b_1, \dots, b_{66} - b_1$. Si l'un de ces nombres est le numéro d'un membre de P_2 , c'est terminé. Mais ces nombres sont de la forme $(a_i - a_1) - (a_j - a_1) = a_i - a_j$, donc si l'un d'eux est dans P_1 , c'est terminé aussi.

Sinon, au moins 17 viennent de l'un des quatre pays restants, noté P_3 . On les note $c_1, \dots, c_{17}$. Si l'un des $c_i - c_1$ est dans P_1, P_2 ou P_3 , c'est fini.

Sinon, au moins 6 viennent de l'un des trois pays restants, noté P_4 . On les note $d_1, \dots, d_6$. Si l'un des 5 $d_i - d_1$ est dans P_1, P_2, P_3 ou P_4 , c'est fini.

Sinon, au moins 3 viennent de l'un des deux pays restants, noté P_5 . On les note $e_1, \dots, e_3$. Si l'un des 2 $e_i - e_1$ est dans P_1, P_2, P_3, P_4 ou P_5 , c'est fini.

Sinon, les deux sont dans le dernier pays, P_6 . Et donc leur différence est obligatoirement dans l'un des pays, et voilà.

NOTES

Chapitre XXIV

Applications linéaires

Sommaire

1	Généralités.	356
1.1	Définitions.	356
1.2	Opérations sur les applications linéaires.	357
1.3	Noyau et image.	358
1.4	Isomorphismes.	360
1.5	Image d'une base par une application linéaire.	360
1.6	Classification en dimension finie.	361
2	Applications linéaires en dimension finie.362	
2.1	Dimension de $\mathcal{L}(E, F)$	362
2.2	Rang d'une application linéaire	362
2.3	Le théorème du rang.	363
3	Endomorphismes particuliers.	365
3.1	Homothéties.	365
3.2	Projecteurs.	365
3.3	Symétries.	366
4	Formes linéaires et hyperplans.	367

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'important est que $\mathbb{K}$ soit un corps, mais le programme se limite à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 Généralités.

Soient E_1 et E_2 deux $\mathbb{K}$ -ev ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).

1.1 Définitions.

Définition 1.1.1.

On appelle *application linéaire* (ou *morphisme d'espaces vectoriels*) de E_1 dans E_2 toute application $\varphi : E_1 \rightarrow E_2$ vérifiant

$$\forall (x, y) \in E_1^2, \forall (\lambda, \mu) \in \mathbb{K}^2 \\ \varphi(\lambda x + \mu y) = \lambda \varphi(x) + \mu \varphi(y). \quad (\text{XXIV.1})$$

Autrement dit, l'image d'une combinaison linéaire est la combinaison linéaire des images : une application linéaire préserve les combinaisons linéaires.

- L'ensemble des applications linéaires de E_1 dans E_2 est noté $\mathcal{L}(E_1, E_2)$.
- Une application linéaire de E_1 dans E_1 est appelé *endomorphisme*. On note $\mathcal{L}(E_1, E_1) = \mathcal{L}(E_1)$.
- Une application linéaire bijective est appelée *isomorphisme*. L'ensemble des isomorphismes de E_1 dans E_2 est noté $\mathcal{GL}(E_1, E_2)$.
- Un *automorphisme* est un endomorphisme qui est aussi un isomorphisme, on note $\mathcal{GL}(E_1) = \mathcal{GL}(E_1, E_1)$ l'ensemble des automorphismes de E_1 , appelé *groupe linéaire*.
- Une application linéaire de E_1 dans $\mathbb{K}$ est une *forme linéaire*.

Remarque 1.1.2.

Une application linéaire φ de E_1 dans E_2 est un morphisme *de groupes* de $(E_1, +)$ dans $(E_2, +)$, avec une propriété supplémentaire vis-à-vis de la loi externe.

Remarque 1.1.3.

La propriété fondamentale des applications

linéaires se généralise aux combinaisons linéaires d'un nombre quelconque de vecteurs : si $x_1, \dots, x_n \in E$ et $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ et $f \in \mathcal{L}(E, F)$, alors $f\left(\sum_{k=1}^n \lambda_k x_k\right) = \sum_{k=1}^n \lambda_k f(x_k)$.

De manière plus générale, pour toute famille $(x_i)_{i \in I}$ et toute famille à support fini $(\lambda_i)_{i \in I}$, on a

$$f\left(\sum_{i \in I} \lambda_i x_i\right) = \sum_{i \in I} \lambda_i f(x_i)$$

Remarque 1.1.4 (Très utile en pratique).

La propriété fondamentale des applications linéaires (XXIV.1) est équivalente à

$$\forall (x, y) \in E_1^2, \forall \lambda \in \mathbb{K} \\ \varphi(\lambda x + y) = \lambda \varphi(x) + \varphi(y) \quad (\text{XXIV.2})$$

ainsi qu'à

$$\forall (x, y) \in E_1^2, \varphi(x + y) = \varphi(x) + \varphi(y) \\ \text{et } \forall (\lambda, x) \in \mathbb{K} \times E_1, \varphi(\lambda x) = \lambda \varphi(x).$$

La démonstration est analogue à celle pour les sev.

Exemple 1.1.5.

- Soit $u \in \mathbb{R}^3$. Alors $\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}$ est une

$$v \mapsto u \cdot v$$

forme linéaire (on dit que le produit scalaire est linéaire à droite).

- Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors $\varphi : \mathcal{M}_{q,n}(\mathbb{K}) \rightarrow \mathcal{M}_{q,p}(\mathbb{K})$ est linéaire (on

$$B \mapsto BA$$

dit que le produit matriciel est linéaire à gauche).

Exemple 1.1.6.

$$\varphi : \mathbb{R}^3 \rightarrow \mathbb{R}^3 \quad \text{est} \\ (x, y, z) \mapsto (3x + y, 2z, x - y + z)$$

un endomorphisme.

Remarque 1.1.7.

Toute application polynomiale (en plusieurs variables) faisant intervenir des termes de degrés différents de 1 n'est pas linéaire.

Exemple 1.1.8.

$$\varphi : \mathbb{R}^2 \rightarrow \mathbb{R} \quad \text{n'est pas une application} \\ (x, y) \mapsto xy$$

linéaire, idem avec x^2 et $3x + 2y + 2$.

Exemple 1.1.9.

On note $\ell_{\mathbb{N}}(\mathbb{R})$ l'ensemble des suites réelles convergentes, c'est un sev de $\mathbb{R}^{\mathbb{N}}$, et l'application φ :

$$\begin{aligned} \ell_{\mathbb{N}}(\mathbb{R}) &\rightarrow \mathbb{R} && \text{est une forme linéaire.} \\ (u_n) &\mapsto \lim_{n \rightarrow +\infty} u_n \end{aligned}$$

Exemple 1.1.10.

La dérivation, l'intégration sur un segment sont des opérations linéaires (en fonction de la fonction dérivée, de l'intégrande).

Exemple 1.1.11.

Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ et $a \in \mathbb{R}$.

L'application $\text{ev}_a : E \rightarrow \mathbb{R}$ est une forme linéaire appelée *évaluation en a*.

Remarque 1.1.12 (Notations multiplicatives).

Dans le cas des endomorphismes, on notera souvent uv pour signifier $u \circ v$.

De même, on notera souvent

$$u^k = \underbrace{u \circ \cdots \circ u}_{k \text{ fois}}$$

où $k \in \mathbb{N}$, avec la convention $u^0 = \text{Id}_E$.

Proposition 1.1.13.

Si $\varphi \in \mathcal{L}(E_1, E_2)$, alors $\varphi(0_{E_1}) = 0_{E_2}$.

Démonstration.

Comme pour les morphismes de groupes : $\varphi(0_{E_1}) = \varphi(0_{E_1} + 0_{E_1}) = \varphi(0_{E_1}) + \varphi(0_{E_1})$. $\square$

Montrons enfin un théorème central, qui permet de caractériser bon nombre d'applications linéaires.

Théorème 1.1.14.

Soit E, F deux $\mathbb{K}$ -ev, soit E_1, E_2 deux sev supplémentaires de E (i.e. $E = E_1 \oplus E_2$).

Soit $f_1 \in \mathcal{L}(E_1, F)$ et $f_2 \in \mathcal{L}(E_2, F)$.

Alors, il existe une unique $f \in \mathcal{L}(E, F)$ telle que $f|_{E_1} = f_1$ et $f|_{E_2} = f_2$.

Démonstration.

On raisonne par analyse-synthèse.

Analyse. Soit $f \in \mathcal{L}(E, F)$ telle que $f|_{E_1} = f_1$ et $f|_{E_2} = f_2$, soit $x \in E$, $x_1 \in E_1$ et $x_2 \in E_2$ vérifiant $x = x_1 + x_2$. Alors

$$f(x) = f(x_1) + f(x_2) = f_1(x_1) + f_2(x_2).$$

Synthèse. Soit $x \in E$, soit $x_1 \in E_1$ et $x_2 \in E_2$ vérifiant $x = x_1 + x_2$. On pose $f(x) = f_1(x_1) + f_2(x_2)$. Tout d'abord, par définition et par linéarité de f_2 ,

$$f(x_1) = f(x_1 + 0_E) = f_1(x_1) + f_2(0_E) = f_1(x_1).$$

Ainsi, $f|_{E_1} = f_1$. De même, $f|_{E_2} = f_2$.

Vérifions donc la linéarité de f . Soit $x, y \in E$, $x_1, y_1 \in E_1$ et $x_2, y_2 \in E_2$ vérifiant $x = x_1 + x_2$ et $y = y_1 + y_2$. Soit $\lambda, \mu \in \mathbb{K}$. Alors

$$\lambda x + \mu y = \underbrace{\lambda x_1 + \mu y_1}_{\in E_1} + \underbrace{\lambda x_2 + \mu y_2}_{\in E_2},$$

donc par définition

$$f(\lambda x + \mu y) = f_1(\lambda x_1 + \mu y_1) + f_2(\lambda x_2 + \mu y_2).$$

Par linéarité de f_1 et de f_2 , on a donc

$$\begin{aligned} f(\lambda x + \mu y) &= \lambda f_1(x_1) + \mu f_1(y_1) + \lambda f_2(x_2) + \mu f_2(y_2) \\ &= \lambda f(x) + \mu f(y). \end{aligned}$$

Ainsi, f est linéaire. $\square$

Exemple 1.1.15.

Avec $E = F = \mathbb{R}^3$, considérons le plan $\mathcal{P}$ d'équation $x + y + z = 0$ et la droite $\mathcal{D} = \text{Vect} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. On

montre aisément que $\mathbb{R}^3 = \mathcal{P} \oplus \mathcal{D}$.

On peut donc considérer l'endomorphisme f de E caractérisé par

- $\forall u \in \mathcal{P}, f(u) = u$;
- $\forall u \in \mathcal{D}, f(u) = -u$.

1.2 Opérations sur les applications linéaires.

Dans toute la suite, E_1, E_2 et E_3 sont des $\mathbb{K}$ -ev.

Théorème 1.2.1. 1. $\mathcal{L}(E_1, E_2)$ est un sev de $(\mathcal{F}(E_1, E_2), +, \cdot)$.

2. Si $f \in \mathcal{L}(E_1, E_2)$ et $g \in \mathcal{L}(E_2, E_3)$, alors $g \circ f \in \mathcal{L}(E_1, E_3)$.

3. Soit $f \in \mathcal{L}(E_1, E_2)$. Alors les applications

$$\varphi : \begin{cases} \mathcal{L}(E_2, E_3) &\longrightarrow \mathcal{L}(E_1, E_3) \\ g &\longmapsto g \circ f \end{cases}$$

et

$$\psi : \begin{cases} \mathcal{L}(E_3, E_1) &\longrightarrow \mathcal{L}(E_3, E_2) \\ g &\longmapsto f \circ g \end{cases}$$

sont linéaires.

Démonstration.

 Élémentaire. $\square$
Remarque 1.2.2.

 Ces résultats montrent, avec $E_1 = E_2 = E_3$, que $(\mathcal{L}(E_1), +, \circ)$ est un anneau.


En général, cet anneau n'est pas commutatif.

Exemple 1.2.3.

 On pose $E_1 = \mathcal{C}^{+\infty}(\mathbb{R}, \mathbb{R})$: c'est un sev de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ (le montrer). On note

$$\begin{aligned} \varphi : E_1 &\rightarrow E_1 \text{ et } \psi : E_1 \rightarrow E_1 \\ f &\mapsto f' \qquad \qquad f \mapsto \begin{cases} \mathbb{R} \rightarrow \mathbb{R} \\ x \mapsto xf(x) \end{cases} \end{aligned}$$

 On constate alors que $\psi \circ \varphi \neq \varphi \circ \psi$.

1.3 Noyau et image.

Théorème 1.3.1.

 Soit $\varphi \in \mathcal{L}(E_1, E_2)$, A un sev de E_1 et B un sev de E_2 .

1. L'image directe de A par φ est un sev de E_2 .
2. L'image réciproque de B par φ est un sev de E_1 .

Démonstration. 1. On a bien $\varphi(A) \subset E_2$ ainsi que $0_{E_2} \in \varphi(A)$, car $\varphi(0_{E_1}) = 0_{E_2}$ et $0_{E_1} \in A$.

 Soit $(y_1, y_2) \in \varphi(A)^2$, soit $\lambda \in \mathbb{K}$ et soit $(x_1, x_2) \in A^2$ vérifiant $y_1 = \varphi(x_1)$ et $y_2 = \varphi(x_2)$. Alors, comme A est un sev de E_1 , on a $x_1 + \lambda x_2 \in A$ et donc, par linéarité de φ , on a $y_1 + \lambda y_2 = \varphi(x_1) + \lambda \varphi(x_2) = \varphi(x_1 + \lambda x_2) \in \varphi(A)$. Ainsi, $\varphi(A)$ est un sev de E_2 .

2. On a bien $\varphi^{-1}(B) \subset E_1$ ainsi que $0_{E_1} \in \varphi^{-1}(B)$, car $\varphi(0_{E_1}) = 0_{E_2}$ et $0_{E_2} \in B$.

 Soit $(x_1, x_2) \in \varphi^{-1}(B)^2$, $\lambda \in \mathbb{K}$. Alors, $\varphi(x_1) \in B$ et $\varphi(x_2) \in B$ et, par linéarité de φ , $\varphi(x_1 + \lambda x_2) = \varphi(x_1) + \lambda \varphi(x_2) \in B$, car B est un sev de E_2 . Ainsi, $x_1 + \lambda x_2 \in \varphi^{-1}(B)$ et donc $\varphi^{-1}(B)$ est un sev de E_1 . $\square$
Proposition 1.3.2.

 Soit E, F deux $\mathbb{K}$ -espaces-vectoriels, soit V un sev de E , $f \in \mathcal{L}(E, F)$, soit $(x_i)_{i \in I}$ une famille

 génératrice de V . Alors, $(f(x_i))_{i \in I}$ est une famille génératrice de $f(V)$:

$$f(\text{Vect}((x_i)_{i \in I})) = \text{Vect}((f(x_i))_{i \in I})$$

Démonstration.
 $f(V)$ est un sous-espace vectoriel de F . Comme V contient tous les x_i pour $i \in I$, $f(V)$ contient tous les $f(x_i)$ pour $i \in I$. Donc il contient le sous-espace engendré par les $f(x_i) : \text{Vect}((f(x_i))_{i \in I}) \subset f(V)$.

 Réciproquement, soit y un élément de $f(V)$. y est l'image d'un élément x de V . Alors x est une combinaison linéaire $\sum_{i \in I} \lambda_i x_i$ (où la famille $(\lambda_i)_{i \in I}$ est à support fini), donc on a

$$\begin{aligned} y &= f(x) \\ &= f\left(\sum_{i \in I} \lambda_i x_i\right) \\ &= \sum_{i \in I} \lambda_i f(x_i) \\ &\in \text{Vect}((f(x_i))_{i \in I}) \end{aligned}$$

 Donc $f(V) \subset \text{Vect}((f(x_i))_{i \in I})$. $\square$
Exercice 1.3.3.

Soit

$$f : \begin{matrix} \mathbb{R}^3 & \rightarrow & \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} & \mapsto & \begin{pmatrix} x + 3y + 2z \\ x + 4y + z \\ y - z \end{pmatrix} \end{matrix}.$$

Déterminer une famille génératrice (la plus petite possible) de

$$f\left(\text{Vect}\left(\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -3 \\ -1 \\ -1 \end{pmatrix}\right)\right).$$

Définition 1.3.4.

 Soit $\varphi \in \mathcal{L}(E_1, E_2)$.

1. On appelle *noyau* de φ noté $\text{Ker } \varphi$, l'ensemble $\{x \in E_1 \mid \varphi(x) = 0_{E_2}\}$
2. On appelle *image* de φ et on note $\text{Im } \varphi$, l'ensemble $\{\varphi(x) \mid x \in E_1\}$.

Remarque 1.3.5.

 Le théorème 1.3.1 assure ainsi que $\text{Ker } \varphi$ et $\text{Im } \varphi$ sont des sev.

Remarque 1.3.6.

Pour montrer qu'un ensemble est muni d'une structure d'ev, on essaiera TOUJOURS de l'identifier comme noyau ou image d'une application linéaire. Sinon, on essaiera de l'identifier directement comme sev. d'un ev. de référence.

Rappel : on ne revient JAMAIS à la définition générale d'un ev.

Théorème 1.3.7.

Soit $\varphi \in \mathcal{L}(E_1, E_2)$.

1. φ est injective si et seulement si $\text{Ker } \varphi = \{0\}$.
2. φ est surjective si et seulement si $\text{Im } \varphi = E_2$.

Démonstration. 1. Deux méthodes : refaire comme la démo analogue pour les morphismes de groupes, ou utiliser directement ce théorème : on choisit la deuxième méthode. Il suffit alors remarquer que $\text{Ker } \varphi$ est le même que l'on adopte le point de vue «groupe» ou le point de vue «espace vectoriel».

On peut aussi refaire la première méthode pour s'entraîner.

2. Immédiat. □

Remarque 1.3.8.

Les calculs de noyaux et d'images se ramènent souvent à des résolutions de systèmes linéaires.

Corollaire 1.3.9.

Soit E et F deux $\mathbb{K}$ -espaces vectoriels, $f \in \mathcal{L}(E, F)$ et $(x_i)_{i \in I}$ une famille **génératrice** de E . Alors l'image de cette famille par f est une famille génératrice de $\text{Im } f$.

Notamment, f est surjective si et seulement si $(f(x_i))_{i \in I}$ est une famille génératrice de F

Démonstration.

C'est une conséquence directe de la proposition 1.3.2 :

$$\begin{aligned} \text{Im } f &= f(E) && \text{par définition} \\ &= f(\text{Vect}((x_i)_{i \in I})) && \text{car } (x_i)_{i \in I} \text{ génératrice} \\ &= \text{Vect}((f(x_i))_{i \in I}) && \text{par prop. 1.3.2} \end{aligned}$$

□

Exemple 1.3.10.

Soit

$$f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 3x & - & y \\ 2x & + & y & + & z \\ x & + & 3y & + & 2z \end{pmatrix}.$$

Alors,

$$\begin{aligned} \text{Im}(f) &= \text{Vect}(f(1, 0, 0), f(0, 1, 0), f(0, 0, 1)) \\ &= \text{Vect}((3, 2, 1), (-1, 1, 3), (0, 1, 2)) \\ &= \text{Vect}((0, 5, 10), (-1, 1, 3), (0, 1, 2)) \\ &= \text{Vect}((-1, 1, 3), (0, 1, 2)). \end{aligned}$$

Exemple 1.3.11.

Déterminer $\text{Ker } \varphi$ et $\text{Im } \varphi$, avec

$$\varphi : \begin{cases} \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x & + & 2y & + & 5z \\ & - & y & - & z \\ -x & + & y & - & 2z \end{pmatrix} \end{cases}.$$

Exemple 1.3.12.

Soit $\varphi : \mathbb{R}_3[X] \rightarrow \mathbb{R}_2[X]$. Donner $\text{Im } \varphi$.

$$P \mapsto P' - XP''$$
Exemple 1.3.13.

Soit $\varphi : \mathbb{R}^{\mathbb{R}} \rightarrow \mathbb{R}^{\mathbb{R}}$. On montre que φ est

$$f \mapsto f \times \sin$$

linéaire, puis que φ n'est pas injective, en trouvant une fonction f non nulle dans $\text{Ker } \varphi$. Par exemple $f(x) = 0$ si $x \neq 0$ et $f(0) = 1$.

On montre enfin que $\psi = \varphi|_{\mathcal{C}^0(\mathbb{R})}$ est injective, en montrant que son noyau est réduit à $\{0\}$.

On peut maintenant unifier les résultats sur les structures des solutions de nombreux problèmes linéaires étudiés auparavant (systèmes linéaires, équations différentielles linéaires).

Proposition 1.3.14.

Soit $f \in \mathcal{L}(E_1, E_2)$ et $a \in E_2$. Alors $f^{-1}(\{a\})$ est soit vide, soit un sea de E_1 de direction $\text{Ker } f$.

Remarque 1.3.15.

$f^{-1}(\{a\})$ est l'ensemble des solutions de l'équation $f(x) = a$, avec $x \in E_1$.

Démonstration.

Reprendre chaque preuve effectuée lorsque l'on a rencontré ce type de structure de solution. $\square$

Exemple 1.3.16.

L'ensemble des suites réelles $(u_n)_{n \in \mathbb{N}}$ vérifiant pour tout $n \in \mathbb{N}$, $u_{n+2} = 3u_{n+1} - 2u_n - 4$ est le sea de direction $\text{Vect}((2^n)_{n \in \mathbb{N}}, 1)$ et passant par $(4n)_{n \in \mathbb{N}}$.

Remarque 1.3.17.

On retrouve ainsi que l'ensemble des solutions d'un système linéaire est soit vide soit un sea.

1.4 Isomorphismes.

Un isomorphisme transporte la structure d'ev, comme pour les groupes.



Dire que E_1 et E_2 sont isomorphes ne signifie pas que toute application linéaire de E_1 dans E_2 est un isomorphisme. On peut donner un exemple : $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2, (x, y) \mapsto (x, 0)$.

Théorème 1.4.1.

Soit $\varphi \in \mathcal{L}(E_1, E_2)$.

1. Si φ est un isomorphisme, alors φ^{-1} aussi.
2. Une composée d'isomorphismes est un isomorphisme : si $\varphi \in \mathcal{GL}(E_1, E_2)$ et $\psi \in \mathcal{GL}(E_2, E_3)$, alors $\psi \circ \varphi \in \mathcal{GL}(E_1, E_3)$.
3. $(\mathcal{GL}(E_1), \circ)$ est un groupe appelé *groupe linéaire* (groupe des automorphismes).

Démonstration. 1. Soit $(y_1, y_2) \in E_2^2$, soit $\lambda \in \mathbb{K}$ et soit $(x_1, x_2) \in E_1^2$ vérifiant $x_1 = \varphi^{-1}(y_1)$ et $x_2 = \varphi^{-1}(y_2)$. On a alors, par linéarité de φ , $\varphi(x_1 + \lambda x_2) = \varphi(x_1) + \lambda \varphi(x_2) = y_1 + \lambda y_2$, donc $\varphi^{-1}(y_1 + \lambda y_2) = \varphi^{-1}(y_1) + \lambda \varphi^{-1}(y_2)$. Ainsi, φ^{-1} est linéaire.

2. On a déjà vu que $\psi \circ \varphi$ est bijective et linéaire : c'est fini !

3. Montrons que c'est un sous-groupe du groupe des permutations de $E_1 : (S_{E_1}, \circ)$. L'application identité est bijective et linéaire, donc $\text{Id}_{E_1} \in \mathcal{GL}(E_1)$. Les deux résultats précédents montrent que $\mathcal{GL}(E_1)$ est stable par passage à l'inverse et composition, ce qui permet de conclure. $\square$

Remarque 1.4.2.

Notation : Si $n \in \mathbb{N}^*$, $\mathcal{GL}(\mathbb{K}^n)$ est noté $\mathcal{GL}_n(\mathbb{K})$.

Exemple 1.4.3.

$$\begin{aligned} \varphi : \mathbb{R}^2 &\rightarrow \mathbb{R}^2 && \in \mathcal{GL}_2(\mathbb{R}) \\ (x, y) &\mapsto (x - y, x + 2y) \end{aligned}$$

On résout le système $\varphi(x, y) = (a, b)$, et cela montre que φ est bijective, et donne l'expression de φ^{-1} .

Remarque 1.4.4.

$\mathcal{GL}(E)$ ayant une structure de groupe, on utilise les notations multiplicatives usuelles.

Notamment, si u est un automorphisme de E et si $k \in \mathbb{N}$, on note

$$u^{-k} = (u^k)^{-1} = (u^{-1})^k = \underbrace{u^{-1} \circ \dots \circ u^{-1}}_{k \text{ fois}}.$$

1.5 Image d'une base par une application linéaire.

Théorème 1.5.1.

Soit E_1 et E_2 deux $\mathbb{K}$ -ev, et soit $(f_i)_{i \in I}$ une base de E_1 et $(g_i)_{i \in I}$ une famille **quelconque** de E_2 . Alors il existe une **unique** application linéaire $\varphi : E_1 \rightarrow E_2$ telle que pour tout $i \in I$, $\varphi(f_i) = g_i$.

Démonstration. Analyse Soit φ une telle application. Soit $x \in E$. Alors x s'écrit $\sum_{i \in I} \lambda_i f_i$, donc

$$\begin{aligned} \varphi(x) &= \sum_{i \in I} \lambda_i \varphi(f_i) \\ &= \sum_{i \in I} \lambda_i g_i \end{aligned}$$

où $(\lambda_i)_{i \in I}$ est la famille des coordonnées de x dans la base $(f_i)_{i \in I}$.

$\varphi(x)$ est donc déterminé de façon unique.

Donc φ est déterminée de façon unique.

Synthèse Considérons l'application qui à tout élément x de E associe $\sum_{i \in I} \lambda_i g_i$, où $(\lambda_i)_{i \in I}$ est la famille des coordonnées de x dans la base $(f_i)_{i \in I}$.

On montre que φ est une application linéaire. De plus on peut montrer qu'elle vérifie les conditions demandées : $\forall i \in I \varphi(f_i) = g_i$.

Conclusion Il existe bien une unique application répondant à la question posée. $\square$

Proposition 1.5.2.

Soit E et F deux $\mathbb{K}$ -espaces vectoriels, $f \in \mathcal{L}(E, F)$ avec f **injective** et $(x_i)_{i \in I}$ une famille **libre** de E . Alors l'image de cette famille par f est libre.

Démonstration.

Soit $(\lambda_i)_{i \in I}$ une famille de scalaires à support fini telle que $\sum_{i \in I} \lambda_i f(x_i) = 0$

Alors $f\left(\sum_{i \in I} \lambda_i x_i\right) = 0$. par linéarité de f .

Or f est injective donc $\sum_{i \in I} \lambda_i x_i = 0$

Or $(x_i)_{i \in I}$ est libre, donc pour tout $i \in I$, $\lambda_i = 0$. $\square$

Remarque 1.5.3.

Autrement dit, l'image d'une famille libre par une application linéaire injective est une famille libre.

Or nous avons vu que l'image d'une famille génératrice par une application linéaire est une famille génératrice de l'image ; on en déduit que l'image d'une base par une application linéaire injective est une base de l'image.

Par ailleurs, l'image d'une famille génératrice par une application linéaire surjective étant une famille génératrice de l'espace d'arrivée, on en déduit que l'image d'une base par un isomorphisme est une base de l'espace d'arrivée.

Proposition 1.5.4.

Soit E_1 et E_2 deux $\mathbb{K}$ -ev, et soit $(f_i)_{i \in I}$ une base de E_1 . Soit $\varphi \in \mathcal{L}(E_1, E_2)$.

1. φ est injective si et seulement si $(\varphi(f_i))_{i \in I}$ est une famille libre.
2. φ est surjective si et seulement si $(\varphi(f_i))_{i \in I}$ est une famille génératrice de E_2 .
3. φ est un isomorphisme si et seulement si $(\varphi(f_i))_{i \in I}$ est une base de E_2 .

Démonstration.

On traite le cas où $I = [1, n]$.

1. Si φ est injective, par la proposition 1.5.2 la famille $(\varphi(f_i))_{i \in I}$ est libre.

Réciproquement, si $(\varphi(f_i))_{i \in I}$ est libre, soit $x \in$

$\text{Ker } \varphi$. Il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tel que $x = \sum_{k=1}^n \lambda_k f_k$.

Par linéarité de φ , $\varphi(x) = \sum_{k=1}^n \lambda_k \varphi(f_k) = 0_{E_2}$. Par liberté de la famille $(\varphi(f_i))_{i \in I}$, $\lambda_1 = \dots = \lambda_n = 0$, donc $x = 0_{E_1}$. Ainsi, $\text{Ker } \varphi = \{0_{E_1}\}$, donc φ est injective.

2. Si φ est surjective, par le corollaire 1.3.9 la famille $(\varphi(f_i))_{i \in I}$ engendre E_2 .

Réciproquement, si $(\varphi(f_i))_{i \in I}$ engendre E_2 , $\varphi(E_1) = \varphi(\text{Vect}(f_1, \dots, f_n)) = \text{Vect}(\varphi(f_1), \dots, \varphi(f_n)) = E_2$, donc φ est surjective $\square$

Exemple 1.5.5.

Montrer qu'il existe une unique application linéaire $\varphi : \mathbb{R}_2[X] \rightarrow \mathbb{R}^2$ vérifiant les conditions suivantes :

$$\begin{aligned}\varphi(1) &= (1, 2) \\ \varphi(X + 1) &= (2, 3) \\ \varphi(X^2 + 1) &= (0, 1)\end{aligned}$$

Cette application linéaire est-elle injective ? Surjective ? Un isomorphisme ?

1.6 Classification en dimension finie.

Proposition 1.6.1.

Soit $n \in \mathbb{N}$ et E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Alors E est isomorphe à $\mathbb{K}^n$.

Démonstration.

On a $\dim E = n$, donc on peut trouver une base $(e_1, \dots, e_n)$ de E .

Posons alors

$$\begin{aligned}\varphi : \quad \mathbb{K}^n &\rightarrow E \\ (\lambda_1, \dots, \lambda_n) &\mapsto \sum_{k=1}^n \lambda_k e_k\end{aligned}$$

On peut alors remarquer que

1. φ est une application linéaire,
2. φ est injective (car la famille $(e_1, \dots, e_n)$ est libre),
3. φ est surjective (car la famille $(e_1, \dots, e_n)$ est génératrice de E).

La fonction φ est donc un isomorphisme de $\mathbb{K}^n$ sur E . E et $\mathbb{K}^n$ sont donc isomorphes. $\square$

Proposition 1.6.2.

Si E est un $\mathbb{K}$ -ev de dimension finie n et si $\mathcal{B}$ est une base de E , alors l'application qui à un vecteur de E associe le n -uplet de ses coordonnées dans la base $\mathcal{B}$ est un isomorphisme de E dans $\mathbb{K}^n$.

Démonstration.

Il suffit de considérer la réciproque de l'isomorphisme φ de la démonstration précédente. $\square$

Proposition 1.6.3.

Soit E et F deux $\mathbb{K}$ -espaces vectoriels. Supposons que E est de dimension finie.

Alors E et F sont isomorphes si et seulement si F est aussi de dimension finie et $\dim E = \dim F$.

Démonstration.

Notons tout d'abord n la dimension de E et choisissons $(e_1, \dots, e_n)$ une base de E .

Supposons E et F isomorphes. On peut alors trouver un isomorphisme φ de E sur F . $(\varphi(e_1), \dots, \varphi(e_n))$ est alors une base de F . Donc F est de dimension finie et $\dim F = n = \dim E$.

Réciproquement, supposons que F soit de dimension finie, égale à celle de E . Alors d'après la proposition 1.6.1 E et F sont tous les deux isomorphes à $\mathbb{K}^n$, donc sont isomorphes. $\square$

Corollaire 1.6.4.

En particulier, tout espace vectoriel E est de dimension finie n si et seulement si E est isomorphe à $\mathbb{K}^n$.

2 Applications linéaires en dimension finie.

2.1 Dimension de $\mathcal{L}(E, F)$

Proposition 2.1.1.

Soient E et F deux $\mathbb{K}$ -ev de dimension finie. Alors $\mathcal{L}(E, F)$ est un $\mathbb{K}$ -ev de dimension finie, et $\dim \mathcal{L}(E, F) = \dim E \times \dim F$.

Démonstration.

Soit $n \in \mathbb{N}$ et $(e_1, \dots, e_n)$ une base de E .

On considère $\varphi : \mathcal{L}(E, F) \rightarrow F^n$.
 $u \mapsto (u(e_k))_{1 \leq k \leq n}$.

Il est aisé de vérifier que φ est linéaire.

En se souvenant que pour toute famille $f_1, \dots, f_n$ de F il existe une unique application linéaire $u \in \mathcal{L}(E, F)$ tel que pour tout $k \in \llbracket 1, n \rrbracket$, $u(e_k) = f_k$, on constate que φ est bijective.

Par conséquent $\mathcal{L}(E, F)$ et F^n sont isomorphes, ils ont donc même dimension. Or F^n a pour dimension $n \dim F = \dim E \times \dim F$, d'où le résultat. $\square$

2.2 Rang d'une application linéaire

Définition 2.2.1.

Soit E, F deux $\mathbb{K}$ -ev, soit $u \in \mathcal{L}(E, F)$.

Si $\text{Im}(u)$ est de dimension finie, on appelle *rang* de u sa dimension :

$$\text{rg}(u) = \dim(\text{Im}(u)).$$

Lemme 2.2.2.

Soit E, F deux $\mathbb{K}$ -ev, soit $u \in \mathcal{L}(E, F)$, soit H un sev de E de dimension finie. Alors, $u(H)$ est de dimension finie et

$$\dim(u(H)) \leq \dim(H).$$

Démonstration.

Il suffit de prendre une base de H : son image par u engendre $u(H)$. $\square$

Proposition 2.2.3.

Soient E et F deux $\mathbb{K}$ -ev de dimension finie, et $u \in \mathcal{L}(E, F)$. Alors $\text{rg } u \leq \min(\dim E, \dim F)$.

Démonstration.

Il suffit de voir que $\text{Im}(u)$ est un sev de F et $\text{Im}(u) = u(E)$. $\square$

Proposition 2.2.4.

Soit E, F, G trois $\mathbb{K}$ -ev de dimension finie, soit $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$. Alors,

$$\text{rg}(v \circ u) \leq \min(\text{rg}(v), \text{rg}(u)).$$

Démonstration.

On a

$$\operatorname{Im}(v \circ u) \subset \operatorname{Im}(v),$$

donc $\operatorname{rg}(v \circ u) \leq \operatorname{rg}(v)$.

De plus,

$$\operatorname{Im}(v \circ u) = v(\operatorname{Im}(u)),$$

donc comme $\dim(\operatorname{Im}(u)) = \operatorname{rg}(u)$, on a $\operatorname{rg}(v \circ u) \leq \operatorname{rg}(u)$. $\square$

Corollaire 2.2.5.

Soit E un $\mathbb{K}$ -espace vectoriel et $u \in \mathcal{GL}(E)$. Alors, pour tout sous-espace vectoriel F de E , si F est de dimension finie, $u(F)$ l'est également et $\dim u(F) = \dim F$.

Démonstration.

Soit n la dimension de F et $(f_1, \dots, f_n)$ une base de F . Alors $(u(f_1), \dots, u(f_n))$ engendre $u(F)$ et est libre car u est injective, donc la dimension de $u(F)$ est aussi n . $\square$

Théorème 2.2.6 (d'invariance du rang).

Soit E et F deux espaces vectoriels avec E de dimension finie. Soit $u \in \mathcal{L}(E, F)$. Alors :

- (i) soit $v \in \mathcal{GL}(F)$, alors $\operatorname{rg}(v \circ u) = \operatorname{rg} u$;
- (ii) soit $w \in \mathcal{GL}(E)$, alors $\operatorname{rg}(u \circ w) = \operatorname{rg} u$.

Démonstration. (i) Il suffit de remarquer $\operatorname{Im}(v \circ u) = v(\operatorname{Im} u)$. E étant de dimension finie, $\operatorname{Im} u$ aussi. Or $v \in \mathcal{GL}(F)$, donc $v(\operatorname{Im} u)$ est de dimension finie égale à celle de $\operatorname{Im} u$, donc à $\operatorname{rg} u$.

(ii) Il suffit de remarquer $\operatorname{Im}(u \circ w) = u(w(E)) = u(E) = \operatorname{Im} u$. $\square$

Remarque 2.2.7.

Pour le point (i) l'injectivité de v suffit, tandis que pour le point (ii), la surjectivité de w suffit.

2.3 Le théorème du rang.**Proposition 2.3.1.**

Soit E et F deux $\mathbb{K}$ -espaces vectoriels et $u \in \mathcal{L}(E, F)$.

Supposons qu'il existe un supplémentaire S de $\operatorname{Ker} u$ dans E .

Alors u réalise un isomorphisme de S sur $\operatorname{Im} u$ (ou, si l'on préfère, $u|_S^{\operatorname{Im} u} : S \rightarrow \operatorname{Im} u$ est un isomorphisme).

Démonstration.

Notons φ la restriction de u à S au départ et à $\operatorname{Im} u$ à l'arrivée. Il est clair que φ est bien définie et que c'est une application linéaire de S dans $\operatorname{Im} u$.

- Montrons que φ est surjective. Soit $y \in \operatorname{Im} u$. Montrons qu'il existe $s \in S$ vérifiant $\varphi(s) = y$.

Pour cela, remarquons tout d'abord qu'il existe $x \in E$ vérifiant $u(x) = y$. Comme S et $\operatorname{Ker} u$ sont supplémentaires dans E , il existe $s \in S$ et $k \in \operatorname{Ker} u$ vérifiant $x = s + k$. On a alors $u(x) = u(s) + u(k) = u(s) + 0$. Donc $\varphi(s) = u(s) = y$.

φ est donc surjective.

- Montrons que φ est injective. Pour cela, il suffit de montrer $\operatorname{Ker} \varphi \subset \{0\}$.

Soit $k \in \operatorname{Ker} \varphi$. On a $\varphi(k) = 0$, donc $u(k) = 0$, donc $k \in \operatorname{Ker} u$. Or $k \in S$, donc $k \in \operatorname{Ker} u \cap S$. Or $\operatorname{Ker} u$ et S sont supplémentaires, donc $k = 0$.

Ainsi, φ est injective.

Finalement, φ est donc bijective. $\square$

Remarque 2.3.2.

Ce théorème est fondamental pour comprendre comment «fonctionne» une application linéaire. De nombreuses questions (dont des exercices) se résolvent aisément grâce à lui ou grâce aux idées contenues dans sa démonstration.

Théorème 2.3.3 (Théorème du rang).

Soit E et F deux $\mathbb{K}$ -espaces vectoriels, avec E de dimension finie et $u \in \mathcal{L}(E, F)$.

Alors $\operatorname{Im} u$ est de dimension finie et

$$\dim \operatorname{Im} u = \dim E - \dim \operatorname{Ker} u.$$

Démonstration.

On sait que $\operatorname{Ker} u$ possède un supplémentaire S dans E . On a donc $\dim S + \dim \operatorname{Ker} u = \dim E$. De plus S et $\operatorname{Im} u$ sont isomorphes d'après 2.3.1, donc $\dim S = \dim \operatorname{Im} u$. On en déduit immédiatement le résultat. $\square$

Exemple 2.3.4.

- Le rang d'une forme linéaire non nulle vaut 1, celui d'une forme linéaire nulle vaut 0.
- Calculer de deux manières le rang de l'application

$$u : \mathbb{R}^4 \rightarrow \mathbb{R}^3$$

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \mapsto \begin{pmatrix} 2x & -y & & -t \\ x & & +z & +t \\ x & -y & -z & -2t \end{pmatrix}$$

□

Corollaire 2.3.5.

Soient E et F deux $\mathbb{K}$ -ev de dimension finie, et $u \in \mathcal{L}(E, F)$. Alors,

- (i) u est surjective si et seulement si $\operatorname{rg} u = \dim F$;
- (ii) u est injective si et seulement si $\operatorname{rg} u = \dim E$.

Corollaire 2.3.6.

Soient E et F deux $\mathbb{K}$ -ev de dimension finie, et $u \in \mathcal{L}(E, F)$. Alors,

1. si $\dim E < \dim F$, u ne peut être surjective,
2. si $\dim E > \dim F$, u ne peut être injective.

Proposition 2.3.7 (Caractérisation des isomorphismes).

Soit E et F deux $\mathbb{K}$ -espaces vectoriels de dimension finie. Soit $\varphi \in \mathcal{L}(E, F)$.

Alors si φ est un isomorphisme, on a les trois propriétés suivantes :

1. φ est injective,
2. φ est surjective,
3. $\dim E = \dim F$.

Réciproquement, il suffit que deux de ces trois propositions soient vraies pour que φ soit un isomorphisme.

Démonstration.

On a déjà montré que si φ était un isomorphisme les trois propositions étaient vraies. Montrons que si deux sont vraies, alors l'autre l'est aussi.

D'après le théorème du rang, $\dim \operatorname{Im} \varphi = \dim E - \dim \operatorname{Ker} \varphi$.

Par ailleurs, on sait que φ est injective si et seulement si son noyau est de dimension 0 et que φ est surjective si et seulement si $\operatorname{Im} \varphi$ est de dimension $\dim F$.

On peut alors remarquer :

- que si les deux premières propriétés sont vraies, alors φ est un isomorphisme ;
- que si φ est injective et $\dim E = \dim F$, alors $\dim \operatorname{Im} \varphi = \dim E = \dim F$, donc φ est surjective donc bijective.
- que si φ est surjective et $\dim E = \dim F$, alors $\dim \operatorname{Ker} \varphi = \dim E - \dim \operatorname{Im} \varphi = \dim E - \dim F = 0$, donc φ est injective donc bijective.

Exemple 2.3.8.

Soit $n \in \mathbb{N}^*$, $x_0, \dots, x_n \in \mathbb{K}$ des scalaires tous distincts et $\varphi : \mathbb{K}_n[X] \rightarrow \mathbb{K}^{n+1}$.

$$P \mapsto (P(x_0), \dots, P(x_n))$$

Alors φ est un isomorphisme.

φ est aisément linéaire, et l'égalité $\dim \mathbb{K}_n[X] = n + 1 = \dim \mathbb{K}^{n+1}$ assure qu'il suffit de montrer l'injectivité OU la surjectivité de φ , mais pas les deux.

Il s'agit de faire le bon choix : l'injectivité se démontre sans peine en utilisant qu'un polynôme de degré au plus n ayant $(n + 1)$ racines distinctes ne peut être que le polynôme nul. La surjectivité quant à elle peut se démontrer en utilisant les polynômes de Lagrange, ce qui est nettement moins immédiat.

Le résultat précédent s'exprime simplement dans le cas des endomorphismes.

Corollaire 2.3.9 (Éléments inversibles de $\mathcal{L}(E)$).

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit $\varphi \in \mathcal{L}(E)$.

Alors les trois propositions suivantes sont équivalentes :

1. φ est injective,
2. φ est surjective,
3. φ est bijective.

Exercice 2.3.10.

Soit $\alpha \in \mathbb{K} \setminus \{\pm i\}$, soit

$$E = \{ \mathbb{R} \rightarrow \mathbb{K}, x \mapsto (a \cos(x) + b \sin(x))e^{\alpha x} \mid a, b \in \mathbb{K} \}.$$

Montrer que $d : f \mapsto f'$ est un automorphisme de E .

Sous quelle forme peut-on donc chercher une primitive de $x \mapsto \cos(x)e^{3x}$?

Corollaire 2.3.11.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie. Soit φ un élément de l'anneau $(\mathcal{L}(E), +, \circ)$. Alors les trois propositions suivantes sont équivalentes :

1. φ est inversible à gauche,
2. φ est inversible à droite,
3. φ est inversible.



L'hypothèse de dimension finie est indispensable.

Considérer par exemple les applications

$$\begin{aligned}\varphi : \mathbb{R}^{\mathbb{N}} &\rightarrow \mathbb{R}^{\mathbb{N}} \\ (u_n)_{n \in \mathbb{N}} &\mapsto (u_{n+1})_{n \in \mathbb{N}} \\ \psi : \mathbb{R}^{\mathbb{N}} &\rightarrow \mathbb{R}^{\mathbb{N}} \\ (u_n)_{n \in \mathbb{N}} &\mapsto (u_{p(n)})_{n \in \mathbb{N}}\end{aligned}$$

$$\begin{aligned}\text{où } p : \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto \begin{cases} 0 & \text{si } n = 0, \\ n-1 & \text{si } n \neq 0. \end{cases}\end{aligned}$$

Remarque 2.3.12.

De la même manière que le corollaire 2.3.11, on peut montrer que si E et F sont deux $\mathbb{K}$ -espaces vectoriels de dimension finie tels que $\dim E = \dim F$, et si φ est un élément de $\mathcal{L}(E, F)$, alors les trois propositions suivantes sont équivalentes :

1. il existe $\psi \in \mathcal{L}(F, E)$ telle que $\psi \circ \varphi = \text{Id}_E$,
2. il existe $\chi \in \mathcal{L}(F, E)$ telle que $\varphi \circ \chi = \text{Id}_F$,
3. φ est bijective.

3 Endomorphismes particuliers.

3.1 Homothéties.

Définition 3.1.1.

Soit E un $\mathbb{K}$ -ev. Soit $\lambda \in \mathbb{K}^*$. On appelle *homothétie de rapport λ* l'application

$$\begin{aligned}h_\lambda = \lambda \text{Id}_E : E &\rightarrow E \\ x &\mapsto \lambda x\end{aligned}$$

Remarque 3.1.2.

Cas particuliers : $\lambda = 1$: identité ; $\lambda = -1$, symétrie de centre 0.

Théorème 3.1.3.

Toute homothétie est un automorphisme de E , et $(h_\lambda)^{-1} = h_{\lambda^{-1}} = h_{1/\lambda}$.

Démonstration.

- Linéarité : simple.
- Bijectivité et réciproque : calculer $h_\lambda \circ h_{\lambda^{-1}}$ et $h_{\lambda^{-1}} \circ h_\lambda$. $\square$

Proposition 3.1.4.

Soit $\mathcal{H}(E)$ l'ensemble des homothéties de E . Alors $(\mathcal{H}(E), \circ)$ est un sous-groupe de $\mathcal{GL}(E)$.

Démonstration.

- $\mathcal{H}(E) \subset \mathcal{GL}(E)$ d'après le théorème précédent.
- $\text{Id} \in \mathcal{H}(E)$.
- Stable par passage à l'inverse d'après le théorème précédent.
- et on remarque que pour tout $\lambda, \mu \in \mathbb{K}^*$, $h_\mu \circ h_\lambda = h_{\mu\lambda}$, donc on a la stabilité par produit. $\square$

Remarque 3.1.5.

$\mathcal{GL}(E)$ n'est pas un sous-groupe commutatif, mais $\mathcal{H}(E)$ l'est. En fait il est isomorphe à $\mathbb{K}^*$ via $\lambda \mapsto h_\lambda$.

3.2 Projecteurs.

Dans toute la suite, on suppose que F et G sont deux sev supplémentaires, i.e. $E = F \oplus G$.

Définition 3.2.1.

On appelle *projection* sur F parallèlement à G l'endomorphisme $p_{F\parallel G}$ de $\mathcal{L}(E)$ défini par :

$$\forall y \in F, \forall z \in G \quad p_{F\parallel G}(y + z) = y. \quad (\text{XXIV.3})$$

Remarque 3.2.2.

Voir le dessin sur la figure XXIV.1. Exemple dans $\mathbb{R}^3$ avec $F = \{x = 0\}$ et $G = \{x + y = 0, y + z = 0\}$.

Démonstration.

Il convient de montrer que cette définition est correcte, c'est-à-dire qu'il existe une unique application vérifiant les conditions demandées.

Analyse Soit $p_{F\|G}$ un endomorphisme vérifiant les conditions demandées. Alors pour tout $x \in E$, $p_{F\|G}(x) = y$ où (y, z) est l'unique couple¹ de $F \times G$ tel que $x = y + z$. $p_{F\|G}$ est donc déterminé.

Synthèse Soit $p_{F\|G}$ l'application associant à tout $x \in E$ l'unique valeur² y telle que x s'écrive $y + z$ avec $y \in F$ et $z \in G$.

La proposition (XXIV.3) est manifestement vérifiée. On peut par ailleurs montrer que $p_{F\|G}$ est une application linéaire.

Conclusion Il existe une unique application vérifiant les conditions demandées

□

Remarque 3.2.3.

$p_{F\|G}$ est en fait l'unique endomorphisme de E dont la restriction à F est l'identité et dont la restriction à G est nulle (voir théorème 1.1.14).

Théorème 3.2.4.

$p_{F\|G} \in \mathcal{L}(E)$, $\text{Ker } p_{F\|G} = G$, $\text{Im}(p_{F\|G}) = F$.

Démonstration.

- Linéarité : élémentaire.
- Soit $x = y + z \in E$, $y \in F$, $z \in G$, donc $x \in \text{Ker } p_{F\|G}$ si et seulement si $y = 0$ si et seulement si $x = z$ si et seulement si $x \in G$.
- $x \in \text{Im } p_{F\|G}$ si et seulement si il existe $x' = y' + z'$ tel que $x = y'$ si et seulement si $x \in F$.

□

Remarque 3.2.5.

- Cas particuliers : $F = \{0_E\}$ et $G = E$: $p_{F\|G} = 0_{\mathcal{L}(E)}$.
- $G = \{0_E\}$ et $F = E$: $p_{F\|G} = \text{Id}$. Hormis ce dernier cas, une projection n'est jamais injective, ni surjective.
- $p_{F\|G} + p_{G\|F} = \text{Id}$, $p_{F\|G}|_G = 0$, $p_{F\|G}|_F = \text{Id}|_F$.
- Si E est de dimension finie, $\text{rg } p_{F\|G} = \dim F$.

Définition 3.2.6.

On appelle *projecteur* tout endomorphisme f tel que $f \circ f = f$.

Théorème 3.2.7.

Toute projection est un projecteur.

Démonstration.

Il s'agit essentiellement d'utiliser que si $x = y + z$, alors $p_{F\|G}(p_{F\|G}(x)) = p_{F\|G}(y) = p_{F\|G}(y + 0_E) = y$. □

Théorème 3.2.8 (Réciproque).

Soit f un projecteur. Alors $\text{Ker } f \oplus \text{Im } f = E$, et f est la projection sur $\text{Im } f$ parallèlement à $\text{Ker } f$.

Démonstration.

Soit $x \in \text{Ker } f \cap \text{Im } f$. Alors il existe y tel que $x = f(y)$. Or $f(x) = 0$ mais $f(x) = f(f(y)) = f(y) = x$, donc $x = 0$. $\text{Ker } f$ et $\text{Im } f$ sont donc en somme directe.

Montrons que $E = \text{Ker } f + \text{Im } f$.

Analyse : soient $y \in \text{Im } f$ et $z \in \text{Ker } f$ tels que $x = y + z$. Alors il existe u tel que $y = f(u)$. Donc $f(x) = f(f(u)) + f(z) = f(f(u)) = f(u) = y$. Donc on a $y = f(x)$ et donc $z = x - f(x)$.

Synthèse : on pose $y = f(x)$ et $z = x - f(x)$. Alors on a bien $x = y + z$. de plus $f(x) = y$, donc $y \in \text{Im } f$, et $f(z) = f(x - f(x)) = f(x) - f(f(x)) = f(x) - f(x) = 0$, et ainsi $z \in \text{Ker } f$. On a bien le résultat voulu.

Mais pour tout $x \in E$, si l'on note $x = y + z$ la décomposition associée à $\text{Im } f \oplus \text{Ker } f = E$, alors $f(x) = y$, donc f est bien la projection sur $\text{Im } f$ parallèlement à $\text{Ker } f$. □

Remarque 3.2.9. 1. Si f est un projecteur, alors $\text{Im } f = \text{Ker}(f - \text{Id})$: on utilise que $x \in \text{Im } f$ si et seulement si $f(x) = x$ si et seulement si $f(x) - x = 0_E$ si et seulement si $(f - \text{Id})(x) = 0_E$.

2. Si $E = F \oplus G$, alors $p_{F\|G} + p_{G\|F} = \text{Id}$, et $p_{F\|G} \circ p_{G\|F} = p_{G\|F} \circ p_{F\|G} = 0_{\mathcal{L}(E)}$. En effet, si $x = y + z$, alors $p_{F\|G}(x) = y$ et $p_{G\|F}(x) = z$. Et $p_{F\|G}(z) = p_{G\|F}(y) = 0_E$.

Exercice 3.2.10.

Montrer que l'ensemble des fonctions paires et celui des fonctions impaires sont supplémentaires dans $\mathbb{R}^{\mathbb{R}}$. Donner l'expression des projections sur l'un de ces deux ensembles parallèlement au second.

3.3 Symétries.

Définition 3.3.1.

On appelle *symétrie par rapport à F et parallèlement à G* l'endomorphisme $s_{F\|G}$ de $\mathcal{L}(E)$ défini par :

$$\forall y \in F, \forall z \in G \quad s_{F\|G}(y + z) = y - z. \quad (\text{XXIV.4})$$

1. Il existe et est unique puisque $E = F \oplus G$.

2. Voir remarque précédente.

Démonstration.

Comme pour une projection, on montre que ceci définit bien une fonction, qui est linéaire. $\square$

Remarque 3.3.2.

Voir le dessin sur la figure XXIV.1. Même exemple que pour la projection.

Théorème 3.3.3.

$s_{F\parallel G} \in \mathcal{GL}(E)$, et $s_{F\parallel G}^2 = \text{Id}_E$, i.e. $s_{F\parallel G} = s_{F\parallel G}^{-1}$.

Remarque 3.3.4.

On dit que $s_{F\parallel G}$ est une *involution linéaire*.

Démonstration.

On a déjà observé la linéarité.

Soit $x \in E$, soit $y \in F$ et $z \in G$ vérifiant $x = y + z$. Alors

$$s_{F\parallel G}(s_{F\parallel G}(x)) = s_{F\parallel G}(y - z) = y + z = x.$$

$\square$

Théorème 3.3.5 (Réciproque).

Toute involution linéaire est une symétrie, plus précisément, si f est une involution linéaire, on a :

1. $\text{Ker}(f - \text{Id}) \oplus \text{Ker}(f + \text{Id}) = E$.
2. f est la symétrie par rapport à $\text{Ker}(f - \text{Id})$ parallèlement à $\text{Ker}(f + \text{Id})$.

Démonstration. 1. • Analyse : si $x = y + z$ avec $y \in \text{Ker}(f - \text{Id})$ et $z \in \text{Ker}(f + \text{Id})$, alors $f(y) = y$ et $f(z) = -z$. Donc $f(x) = y - z$. D'où : $f(x) + x = 2y$ et $x - f(x) = 2z$. Donc $y = \frac{1}{2}(f(x) + x)$ et $z = \frac{1}{2}(x - f(x))$.
• Synthèse.
2. On vient de voir que si la décomposition de x dans $\text{Ker}(f - \text{Id}) \oplus \text{Ker}(f + \text{Id})$ est $x = y + z$, alors $f(x) = y - z$. CQFD. $\square$

Remarque 3.3.6.

On peut aussi montrer que $\text{Ker}(s_{F\parallel G} - \text{Id}) = \text{Im}(s_{F\parallel G} + \text{Id})$ et $\text{Ker}(s_{F\parallel G} + \text{Id}) = \text{Im}(s_{F\parallel G} - \text{Id})$. Montrons la première égalité :

- Soit $x \in \text{Im}(s_{F\parallel G} + \text{Id})$ alors il existe $x' \in E$ tel que $x = s_{F\parallel G}(x') + x'$. Donc $s_{F\parallel G}(x) = s_{F\parallel G}(s_{F\parallel G}(x') + x') = x' + s_{F\parallel G}(x') = x$.
- Soit $x \in \text{Ker}(s_{F\parallel G} - \text{Id})$ alors $s_{F\parallel G}(x) = x$, donc

$$x = \frac{1}{2}(x + x) = \frac{1}{2}(s_{F\parallel G}(x) + x) \in \text{Im}(s_{F\parallel G} + \text{Id}).$$

Remarque 3.3.7.

On peut enfin montrer que $s_{G\parallel F} + s_{F\parallel G} = 0_{\mathcal{L}(E)}$, $s_{F\parallel G} \circ s_{G\parallel F} = -\text{Id} = s_{G\parallel F} \circ s_{F\parallel G}$, et $p_{F\parallel G} = \frac{1}{2}(s_{F\parallel G} + \text{Id})$. Faire un dessin.

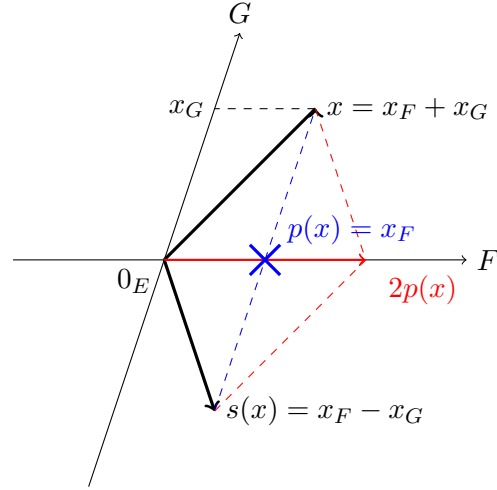


FIGURE XXIV.1 – Représentation de la projection et de la symétrie sur F , parallèlement à G .

4 Formes linéaires et hyperplans.

Proposition 4.0.1 (Expression d'une forme linéaire en dimension finie.).

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n et soit φ une forme linéaire sur E .

Soit alors $\mathcal{E} = (e_1, \dots, e_n)$ une base de E .

Pour $j \in \llbracket 1, n \rrbracket$, notons $a_j = \varphi(e_j)$.

Soit $u \in E$. Notons $x_1, \dots, x_n$ ses coordonnées dans la base $\mathcal{E}$.

Alors on a

$$\varphi(u) = \sum_{j=1}^n a_j x_j.$$

Démonstration.

$$u = \sum_{j=1}^p x_j e_j, \text{ donc par linéarité de } \varphi, \varphi(u) = \sum_{j=1}^p x_j \varphi(e_j) = \sum_{j=1}^p x_j a_j. \quad \square$$

Définition 4.0.2.

Soit E un $\mathbb{K}$ -espace vectoriel. On appelle *hyperplan* de E tout sev qui est le noyau d'une forme linéaire non nulle sur E .

Remarque 4.0.3.

Une forme linéaire non nulle est nécessairement de rang 1. Ainsi, dans un ev E de dimension finie n , un hyperplan est un sev de dimension $n - 1$. Nous allons voir plus loin que la réciproque est vraie.

Proposition 4.0.4.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n . Soit $(e_1, \dots, e_n)$ une base de E .

Soit H un hyperplan de E . Alors les éléments de H sont les points dont les coordonnées $(x_1, \dots, x_n)$ sont les solutions d'une équation de la forme $a_1 x_1 + \dots + a_n x_n = 0$, où $a_1, \dots, a_n$ sont des scalaires fixés non tous nuls.

Réciproquement, toute équation de cette forme est celle d'un hyperplan.

Démonstration.

Soit H un hyperplan de E . Alors par définition il existe une forme linéaire φ dont H est le noyau. Or d'après 4.0.1, pour tout élément $x \in E$, la valeur de $\varphi(x)$ (qui est la coordonnée de $\varphi(x)$ dans la base canonique de $\mathbb{K}$) s'exprime sous la forme $a_1 x_1 + \dots + a_n x_n$. $\text{Ker } \varphi$ est donc l'ensemble des points dont les coordonnées vérifient $a_1 x_1 + \dots + a_n x_n = 0$.

Réciproquement, pour tout n -uplet de scalaires $(a_1, \dots, a_n)$ non tous nuls, l'application φ qui à tout vecteur de E de coordonnées $(x_1, \dots, x_n)$ associe $a_1 x_1 + \dots + a_n x_n$ est une forme linéaire, à l'évidence non nulle (considérer le vecteur de E dont toutes les coordonnées sont nulles, exceptées la i^{e} , où $i \in \llbracket 1, n \rrbracket$ est tel que $a_i \neq 0$), les points dont les coordonnées sont solutions de l'équation $a_1 x_1 + \dots + a_n x_n = 0$ sont donc les éléments du noyau de $\text{Ker } \varphi$, qui est un hyperplan. $\square$

Définition 4.0.5.

Soit E un $\mathbb{K}$ -espace vectoriel. On appelle *droite vectorielle* de E tout sous-espace vectoriel de dimension 1.

Proposition 4.0.6.

Soit E un $\mathbb{K}$ -espace vectoriel et H un hyperplan de E . Alors toute droite vectorielle D non contenue dans H est supplémentaire de H dans E .

Démonstration.

Soit D une droite vectorielle non contenue dans H , et φ une forme linéaire non nulle dont le noyau est H .

Alors $D \cap H$ est strictement inclus dans D , donc $\dim D \cap H < \dim D = 1$, donc $D \cap H = \{0\}$, et ainsi D et H sont en somme directe.

Enfin, soit $x \in E$. Notons $\mathfrak{l} = \varphi(x)$. Soit également e un vecteur directeur de D , et $\alpha = \varphi(e)$. Alors $\alpha \neq 0$ car $e \notin H$. Posons alors $h = x - \frac{\mathfrak{l}}{\alpha} e$. Alors $x = h + \frac{\mathfrak{l}}{\alpha} e$, $\frac{\mathfrak{l}}{\alpha} e \in D$, et $\varphi(h) = \mathfrak{l} - \frac{\mathfrak{l}}{\alpha} \cdot \alpha = 0$, donc $h \in H$. Ceci assure que $E = H + D$, et donc avec le premier point, H et D sont supplémentaires. $\square$

Étudions la réciproque :

Proposition 4.0.7.

Soit E un $\mathbb{K}$ -ev et H un sev admettant une droite D comme supplémentaire. Alors H est un hyperplan de E .

Démonstration.

Soit e un vecteur directeur de D . Tout élément de x de E s'écrit donc de façon unique sous la forme $h + \lambda e$, où $h \in H$ et $\lambda \in \mathbb{K}$.

Notons $\varphi(x)$ ce scalaire λ . Alors nous pouvons montrer que φ est une application linéaire de E dans $\mathbb{K}$. Elle est non nulle car $\varphi(e) \neq 0$.

De plus, pour tout $x \in E$, on a $x \in \text{Ker } \varphi$ si et seulement si x s'écrit sous la forme $h + 0 \cdot e$, où $h \in H$. Donc $\text{Ker } \varphi = H$. $\square$

Remarque 4.0.8.

Ce dernier résultat assure donc la réciproque de 4.0.3 : dans un ev de dimension finie n , les hyperplans sont exactement les sev de dimension $n - 1$.

Exemple 4.0.9.

• Les droites vectorielles sont les hyperplans de

$\mathbb{R}^2$.

- Les plans vectoriels sont les hyperplans de $\mathbb{R}^3$.
- L'espace est un hyperplan de l'espace-temps.
- $\mathbb{K}_n[X]$ est un hyperplan de $\mathbb{K}_{n+1}[X]$.
- $\mathbb{K}^n$ peut être vu comme un hyperplan de $\mathbb{K}^{n+1}$, si l'on considère que $\mathbb{K}^n$ est isomorphe à $\mathbb{K}^n \times \{0\}$, qui est un hyperplan de $\mathbb{K}^{n+1}$.

Lemme 4.0.10.

Soit H un hyperplan d'un espace vectoriel E et soit e un vecteur non nul n'appartenant pas à H . Alors pour toute forme linéaire u de noyau H , on a $u = \lambda\varphi$, où $\lambda = u(e)$ et φ est l'application associant α à tout vecteur de la forme $h + \alpha e$.

Démonstration.

Posons $D = \text{Vect}(e)$. L'application φ est bien définie car $E = H \oplus D$ et elle est linéaire. Soit $u \in \mathcal{L}(E, \mathbb{K})$ vérifiant $\text{Ker } u = H$. Alors soit $x \in E$. x s'écrit sous la forme $h + \alpha e$ et on a $u(x) = u(h) + \alpha u(e) = 0 + \alpha\lambda = \lambda\varphi(x)$.

Donc $\forall x \in E, u(x) = \lambda\varphi(x)$. Donc $u = \lambda\varphi$. De plus, $\lambda \neq 0$ (sinon $\text{ker } u = E \neq H$). $\square$

Proposition 4.0.11.

Deux formes linéaires de même noyau sont proportionnelles.

Démonstration.

Direct d'après le lemme précédent. $\square$

Ce résultat implique le suivant :

Proposition 4.0.12. • Soit H un hyperplan, noyau d'une forme linéaire non nulle u . Alors les formes linéaires de noyau H sont exactement les $\lambda u, \lambda \in \mathbb{K}^*$.

- Soit H un hyperplan en dimension finie, d'équation $a_1x_1 + \dots + a_nx_n = 0$. Alors les équations de H sont exactement les équations de la forme $\lambda a_1x_1 + \dots + \lambda a_nx_n = 0, \lambda \in \mathbb{K}^*$.

Lemme 4.0.13.

Soit H un hyperplan d'un espace vectoriel E . Soit F un sous-espace vectoriel de E de dimension finie p . Alors $H \cap F$ est de dimension $p - 1$ ou p .

Démonstration.

Soit φ une forme linéaire non nulle dont le noyau est H . Alors $H \cap F = \{x \in F \mid \varphi(x) = 0\} = \text{Ker } \varphi|_F$.

Si $\varphi|_F$ est nulle, alors $H \cap F = F$ et le résultat est évident.

Sinon, $\text{Ker } \varphi|_F$ est un hyperplan de F , donc $\dim H \cap F = p - 1$. $\square$

Proposition 4.0.14.

Soit $H_1, \dots, H_m$ m hyperplans d'un espace vectoriel E de dimension finie n . Alors $\bigcap_{k=1}^m H_k$ est de dimension au moins $n - m$.

Réciproquement soit F un sous-espace vectoriel de dimension $n - m$ d'un espace vectoriel E de dimension finie n , où $m \in \mathbb{N}$. Alors F est l'intersection de m hyperplans.

Démonstration.

Le premier point se démontre par une récurrence immédiate en utilisant le lemme 4.0.13.

Pour la réciproque, considérons un supplémentaire S de F dans E . Alors $\dim S = m$. Choisissons une base $(e_1, \dots, e_m)$ de S . Notons p la projection sur S parallèlement à F . Pour tout $k \in \llbracket 1, m \rrbracket$, notons f_k la forme linéaire qui à $x \in E$ associe la k^{e} coordonnée de $p(x)$.

Soit $x \in E$. On a $x \in F$ si et seulement si $x \in \text{Ker } p$ si et seulement si pour tout $k \in \llbracket 1, m \rrbracket$, $f_k(x) = 0$ si et seulement si $x \in \bigcap_{k=1}^m \text{Ker } f_k$. Donc on a

$$F = \bigcap_{k=1}^m \text{Ker } f_k$$

Donc F est l'intersection de m hyperplans. $\square$

Chapitre XXV

Probabilités sur un univers fini

Sommaire

1	Événements, probabilités.	372
1.1	Expérience aléatoire et univers.	372
a	Introduction.	372
b	Univers, événements.	372
c	Variables aléatoires	373
d	Système complet d'événements . .	374
1.2	Espaces probabilisés finis	374
a	Définition	374
b	Probabilité uniforme	375
c	Propriétés élémentaires.	376
d	Détermination par les images des événements élémentaires.	377
1.3	Probabilités conditionnelles.	378
a	Définition.	378
b	Probabilités composées, probabili- tés totales.	378
c	Formule de Bayes.	379
1.4	Événements indépendants.	380
a	Couple d'événements indépendants.	380
b	Famille finie d'événements mutuel- lement indépendants.	381
2	Variables aléatoires.	382
2.1	Définitions.	382
2.2	Loi d'une variable aléatoire.	382
2.3	Lois usuelles	384
a	Loi uniforme	384
b	Loi de Bernoulli.	384
c	Loi binomiale.	385
2.4	Couples de variables aléatoires.	385
2.5	Variables aléatoires indépendantes. . .	386
2.6	Espérance.	391
2.7	Variance, écart type et covariance. . .	393

La théorie des probabilités cherche à modéliser des phénomènes faisant intervenir le hasard. Puisqu'il s'agit d'une modélisation, il conviendra, pour chaque définition que nous allons donner, d'une part d'apprendre sa définition mathématique et d'autre part de comprendre en quoi cette définition modélise un phénomène aléatoire.

1 Événements, probabilités.

1.1 Expérience aléatoire et univers.

a Introduction.

On parlera d'expérience aléatoire pour modéliser un processus dont le résultat est incertain. Exemple : tirage au sort d'une boule dans une urne, tirage à pile ou face avec une pièce de monnaie, lancer d'un ou plusieurs dés, choix au hasard d'une personne dans la population française, tirage de trois cartes à jouer au hasard dans un paquet, etc.

On appellera généralement *univers des possibles* ou *univers*, l'ensemble des résultats possibles d'une expérience aléatoire. Cet univers dépend bien évidemment de la modélisation choisie : par exemple pour un tirage à pile ou face, on peut modéliser l'univers comme étant l'ensemble { pile, face } ou comme { pile, face, tranche }.

Il arrive parfois qu'on s'intéresse à une expérience aléatoire donnant plusieurs résultats. Par exemple, si on tire une carte à jouer dans un jeu, on peut s'intéresser à la couleur de la carte, auquel cas on considérera l'univers $\Omega_1 = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$ ou à sa valeur, auquel cas on s'intéressera à l'univers $\Omega_2 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \text{Valet}, \text{Dame}, \text{Roi}\}$. Si on s'intéresse aux deux simultanément, on prendra plutôt comme univers $\Omega = \Omega_1 \times \Omega_2$.

De manière générale, on prendra pour univers un ensemble nous permettant de représenter simultanément tous les résultats qui nous intéresseront.

Sur l'exemple précédent, on peut s'intéresser à l'événement qui consiste à tirer une carte rouge et de valeurs trois ou quatre. Cet événement est modélisé comme une partie de Ω , en l'espèce la partie $\{(\heartsuit, 3), (\heartsuit, 4), (\diamondsuit, 3), (\diamondsuit, 4)\}$.

Dans toute la suite de ce chapitre, on utilisera

souvent des expériences imaginées : tirages de dés, de boules dans une urne *etc.* On adoptera les conventions suivantes, sauf mention du contraire :

- les dés sont équilibrés, à six faces ;
- les urnes sont opaques, les boules sont indiscernables au toucher et, si une urne contient n boules, ces dernières sont numérotées de 1 à n ;
- les jeux de cartes sont parfaitement mélangés.

b Univers, événements.

Définition 1.1.1 (Univers).

On appelle *univers* un ensemble non vide Ω , et *issues* les éléments de Ω .

Cette année, on se limitera au cas où Ω est fini.

Dans ce cas¹, on appelle *événement* toute partie de l'univers, c'est-à-dire tout élément de $\mathcal{P}(\Omega)$ et on appelle *événement élémentaire* ou *éventualité* les événements singletons, c'est-à-dire de la forme $\{\omega\}$, pour $\omega \in \Omega$ (selon le contexte, le terme événement élémentaire peut parfois désigner les éléments de Ω et non les singletons).

Un événement est dit *impossible* s'il désigne la partie vide ($\emptyset$) et *certain* s'il désigne la partie pleine (Ω).

Étant donnés deux événements A et B , on définit

- l'événement *contraire* de A : $\Omega \setminus A$, noté $\bar{A}$.
- l'événement « A et B » (conjonction de A et B) : $A \cap B$.
- l'événement « A ou B » (disjonction de A et B) : $A \cup B$.

On dit que A et B sont incompatibles si $A \cap B = \emptyset$, autrement dit si leur conjonction est impossible.

On dit que des événements $A_1, \dots, A_n$ sont *mutuellement incompatibles* si leur conjonction est impossible. On dit qu'ils sont *deux à deux incompatibles* si pour tout i et j , $i \neq j$ implique A_i et A_j incompatibles. Dans ce dernier cas, on dit que leur union $A_1 \cup \dots \cup A_n$ est une *union disjointe*.

Remarque 1.1.2.

L'incompatibilité deux à deux de n événements (avec $n \geq 2$) implique l'incompatibilité mutuelle mais la réciproque est fausse. Considérons par exemple $\Omega = \{1, 2, 3, 4, 5, 6\}$ l'univers des résultats d'un tirage d'un dé à six faces. Alors les trois événements «le résultat est pair», «le résultat est divisible par 3» et «le résultat est un nombre premier» ne sont pas deux à deux incompatibles mais sont mutuellement incompatibles.

Remarque 1.1.3.

Dans le cas où Ω n'est pas fini ni dénombrable, modéliser les événements par les éléments de $\mathcal{P}(\Omega)$ pose des problèmes techniques. Pour les résoudre, on impose aux événements d'être des éléments d'un sous-ensemble $\mathcal{T}$ de $\mathcal{P}(\Omega)$, cet ensemble $\mathcal{T}$ devant former ce qu'on appelle une *tribu*. Dans le cas fini ou dénombrable, $\mathcal{P}(\Omega)$ est une tribu.

Exemple 1.1.4.

Pour modéliser les tirages successifs, sans remise, de deux boules dans une urne contenant n boules numérotées de 1 à n , on peut utiliser l'univers $\llbracket 1, n \rrbracket^2$.

Ici, l'événement $\{(i, k)\}$ modélise «on tire d'abord la boule i , puis la boule k ». Les événements du type $\{(i, i)\}$ n'ont pas d'interprétation dans notre modèle. Ce n'est pas grave : on leur attribuera plus tard une probabilité nulle.

c Variables aléatoires**Définition 1.1.5.**

Une *variable aléatoire* (v.a.) X est une application définie sur l'univers Ω à valeurs dans un ensemble E . Lorsque $E \subset \mathbb{R}$, la variable aléatoire est dite *réelle*. On appelle parfois *univers image* l'image directe de Ω par X .

Exemple 1.1.6.

Intuitivement, X représente une valeur associée à une expérience aléatoire : si l'on prend l'exemple du cas d'une personne jouant au loto, la valeur X , exprimée en euros, de son gain au loto lors

du tirage qui aura lieu à une certaine date peut être modélisée par une variable aléatoire à valeurs réelles (l'univers Ω étant l'ensemble des tirages de loto possible).

Remarque 1.1.7.

Une variable aléatoire modélise donc un «objet aléatoire». Si l'on considère une matrice aléatoire, on manipulera donc des variables aléatoires à valeurs matricielles, tandis que si l'on considère des triangles aléatoires on manipulera des variables aléatoires à valeurs dans l'ensemble des triangles du plan.

Par exemple, si $X_1, \dots, X_n$ sont des variables aléatoires à valeurs dans un ensemble A , alors en posant pour tout $B \subset A$, $P_n(B) = \frac{1}{n} \sum_{k=1}^n 1_B(X_k)$,

P_n est une variable aléatoire à valeurs dans l'ensemble des (mesures de) probabilités sur A , appelée (mesure de) probabilité empirique par rapport à $X_1, \dots, X_n$.

Remarque 1.1.8.

En toute généralité, la définition de variable aléatoire est plus subtile. On se place ici dans un cadre très simplifié (univers fini).

Définition 1.1.9.

Soit X une variable aléatoire à valeurs dans un ensemble E .

Pour toute partie A de E , on note $\{X \in A\}$ ou $(X \in A)$, (voire $[X \in A]$) l'événement $X^{-1}(A)$.

Si $E \subset \mathbb{R}$, et $x \in \mathbb{R}$, X est dite *réelle* et on note $(X = x)$, $(X \leq x)$, $(X < x)$, $(X \geq x)$, $(X > x)$ respectivement les événements $X^{-1}(\{x\})$, $X^{-1}([-\infty, x])$, $\dots$

On note $P(X \in A)$, $P(X = x)$, $P(X \leq x)$, $\dots$ les probabilités de ces événements.

Exemple 1.1.10.

Pour reprendre l'exemple précédent, $(X \geq 1000)$ représente l'événement «le gain du joueur au loto est supérieur ou égal à mille euros» et $P(X \geq 1000)$ représente la probabilité de cet événement.

1. Dans le cas infini, la définition est un peu plus subtile. Le cas dénombrable sera traité en seconde année.

d Système complet d'événements

Définition 1.1.11.

On dit qu'une famille $(A_i)_{i \in I}$ d'événements dans un univers Ω est un *système complet d'événements* si ces événements sont deux à deux incompatibles et que leur union (disjointe) est certaine : $\Omega = \bigsqcup_{i \in I} A_i$.

Proposition 1.1.12.

Si A est un événement, $(A, \overline{A})$ est un système complet d'événements, appelé *système complet d'événements associé à A* .

Démonstration.

Immédiat en revenant à la définition. $\square$

Proposition 1.1.13.

Soit X une variable aléatoire à valeurs dans un ensemble fini E . Alors $([X = x])_{x \in E}$ est un système complet d'événements, appelé *système complet d'événements associé à X* .

Démonstration.

Soit $\omega \in \Omega$, alors $\omega \in [X = X(\omega)]$ donc $\cup_{x \in E} [X = x] = \Omega$. Soit $(x, y) \in E^2$, avec $x \neq y$. Si $\omega \in [X = x] \cap [X = y]$, alors $X(\omega) = x = y$, ce qui est impossible, donc $[X = x] \cap [X = y] = \emptyset$. $\square$

Remarque 1.1.14.

On utilisera presque tout le temps un de ces deux types de systèmes complets d'événements.

Exercice 1.1.15.

On lance un dé à 6 faces, on note X le numéro obtenu. Montrer que les événements $[X = 1]$, $[X = 2]$ et $[X \geq 3]$ forment un système complet.

Remarque 1.1.16.

La notion de système complet d'événements est très proche de celle de partition. Les différences sont les suivantes :

1. un système complet d'événements est une famille de parties de Ω alors qu'une partition est un ensemble de parties de Ω ;
2. la notion de système complet d'événements ne s'utilise qu'en probabilités ;

3. rien dans la définition de système complet d'événements n'impose aux A_i d'être non vides.

Proposition 1.1.17.

Soit $(A_i)_{i \in I}$ un système complet d'événements sur un univers Ω , soit B un événement. Alors, B peut s'écrire comme l'union disjointe suivante :

$$B = \bigsqcup_{i \in I} B \cap A_i.$$

Démonstration.

Montrons tout d'abord que B est inclus dans cette réunion. Soit $b \in B$. On a $b \in \Omega$ et la réunion des A_i pour $i \in I$ est égale à Ω , donc il existe un $i_0 \in I$ vérifiant $b \in A_{i_0}$. On a alors $b \in B \cap A_{i_0}$. On a donc

$$b \in \bigcup_{i \in I} B \cap A_i$$

Ce qui montre cette première inclusion.

L'inclusion réciproque est immédiate : pour tout $i \in I$, on a $B \cap A_i \subset B$, donc

$$\bigcup_{i \in I} B \cap A_i \subset B$$

On a donc l'égalité voulue.

On peut aussi montrer cela par calcul sur les ensembles :

$$B = B \cap \Omega = B \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} B \cap A_i.$$

Le fait que l'union soit disjointe est immédiat : soit $(i, j) \in \llbracket 1, n \rrbracket^2$ vérifiant $i \neq j$. Alors $(B \cap A_i) \cap (B \cap A_j) \subset A_i \cap A_j = \emptyset$. $\square$

Remarque 1.1.18.

Cette écriture est typique des énoncés en probabilités. Il faut bien voir qu'elle dissimule deux résultats : l'égalité ensembliste et le fait que l'union écrite est disjointe.

1.2 Espaces probabilisés finis

a Définition

À tout événement, on veut associer sa *probabilité*, qui modélise la « probabilité de réalisation » de cet événement lors de la réalisation de cette expérience aléatoire. Mais que veut dire cette phrase ? On peut le voir comme la fréquence de la réalisation de cet événement au bout d'un

« grand » nombre de répétitions « indépendantes » de cette expérience. La loi des grands nombres (sa version faible dans le cas dénombrable sera vue en seconde année) justifie la consistance de la définition suivante avec son interprétation concrète.

Définition 1.2.1.

Une *probabilité* (ou *mesure de probabilité*) sur un univers fini Ω est une application P de $\mathcal{P}(\Omega)$ dans $\mathbb{R}$ vérifiant les trois propriétés suivantes :

1. Pour tout événement A , $0 \leq P(A) \leq 1$.
2. $P(\Omega) = 1$.
3. Pour tout couple (A, B) d'événements, si A et B sont incompatibles alors $P(A \sqcup B) = P(A) + P(B)$.

Un *espace probabilisé fini* est un couple (Ω, P) , où Ω est un univers fini et P une probabilité.

Pour tout événement A d'un espace probabilisé (Ω, P) , la valeur $P(A)$ est appelée probabilité de l'événement A .

On dit qu'un événement A est *presque sûr* (ou *quasi certain*) si $P(A) = 1$ et est *négligeable* (ou *quasi impossible*) si $P(A) = 0$.

Remarque 1.2.2. 1. Dans le cas où l'univers est infini, il faut adapter un peu la définition : l'ensemble de départ de P est alors la tribu des événements et on donne au troisième axiome une forme plus générale. Comme on ne verra cette année que le cas fini, on s'autorisera à omettre la précision « fini » quand on parlera d'espaces probabilisés.

2. L'intérêt de la notion de quasi certitude ou quasi impossibilité n'est pas évidente quand il s'agit de probabilités sur un univers fini. Donnons un exemple intuitif dans le cas d'un univers infini : si on tire un réel au hasard dans $[0, 1]$, il n'est pas impossible d'obtenir exactement le réel $1/3$ mais la probabilité de cet événement est nulle (la probabilité d'obtenir un réel situé dans un intervalle donné est proportionnelle au diamètre de cet intervalle). C'est donc un événement quasi-impossible mais non impossible.

3. Il est important de retenir que la notion de quasi impossibilité ne veut pas dire « probabilité faible ». Un physicien dirait qu'un événement de probabilité 10^{-100} est impossible (le nombre d'atomes dans l'univers est de l'ordre de 10^{80}) mais pour un mathématicien, un tel événement n'est même pas un événement quasi impossible.

Définition 1.2.3.

Un prédicat défini sur Ω vrai sur un événement de probabilité 1 sera dit « presque-sûr ».

Exemple 1.2.4.

Reprenons l'exemple 1.1.4 : on tire successivement, sans remise, deux boules dans une urne contenant $n \geq 2$ boules numérotées de 1 à n . Il est pratique de considérer comme univers $\Omega = \llbracket 1, n \rrbracket^2$. On prend alors une probabilité P telle que l'événement $\{(i, i) \mid 1 \leq i \leq n\}$ est négligeable.

Sur cet univers, presque-sûrement on aura « $i \neq k$ » pour $1 \leq i, k \leq n$.

b Probabilité uniforme
Définition 1.2.5 (probabilité uniforme).

Soit Ω un univers fini. L'application

$$\begin{aligned} P : \mathcal{P}(\Omega) &\rightarrow \mathbb{R} \\ A &\mapsto \frac{\text{Card } A}{\text{Card } \Omega} \end{aligned}$$

est une probabilité, appelée *probabilité uniforme*.

Démonstration.

Remarquons que Ω est un ensemble fini, donc ses parties sont finies également donc ont des cardinaux entiers. Comme de plus $\Omega \neq \emptyset$, son cardinal est non nul, donc on peut diviser par $\text{Card } \Omega$. P est donc bien définie sur $\mathcal{P}(\Omega)$.

Pour montrer que P est une probabilité, il suffit de vérifier les trois propriétés de la définition :

1. Soit $A \in \mathcal{P}(\Omega)$, alors $0 \leq \text{Card } A \leq \text{Card}(\Omega)$ donc $0 \leq P(A) \leq 1$.
2. On a bien $P(\Omega) = 1$.
3. Soit (A, B) deux événements incompatibles. Alors $A \cap B = \emptyset$ donc $\text{Card}(A \cup B) = \text{Card } A + \text{Card } B$, donc $P(A \cup B) = P(A) + P(B)$.

□

Remarque 1.2.6.

Cette probabilité modélise souvent l'expression « au hasard », prise dans son acception courante (tirer une boule au hasard dans une urne, etc.).

Exercice 1.2.7.

On modélise le tirage d'une boule dans une urne (qui en contient n). On pose $\Omega = \llbracket 1, n \rrbracket$, si $1 \leq k \leq n$, l'événement $\{k\}$ modélise « le numéro k a été tiré ». Si $A \subset \llbracket 1, n \rrbracket$, on définit

$$P(A) = \begin{cases} 1 & \text{si } 1 \in A \\ 0 & \text{sinon} \end{cases}.$$

Vérifier que P définit bien une probabilité sur Ω . Quelle est la situation modélisée ?

Exemple 1.2.8.

Continuons l'exemple 1.2.4 : la probabilité que l'on considérera sur Ω n'est pas uniforme, mais sa restriction à $\{(i, k) \mid 1 \leq i, k \leq n \text{ et } i \neq k\}$ le sera.

c Propriétés élémentaires.
Proposition 1.2.9.

Soit (Ω, P) un espace probabilisé. Soit A et B deux événements. Alors on a

1. $P(\emptyset) = 0$;
2. $A \subset B \Rightarrow P(A) \leq P(B)$;
3. $P(A \setminus B) = P(A) - P(A \cap B)$;
4. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;
5. $P(A) = 1 - P(\bar{A})$.

Démonstration. 1. $\emptyset = \emptyset \sqcup \emptyset$ donc $P(\emptyset) = P(\emptyset) + P(\emptyset) = 0$, d'où le résultat.

2. Supposons $A \subset B$. Alors $B = A \cup (B \setminus A)$. De plus, A et $B \setminus A$ sont incompatibles, donc $P(B) = P(A) + P(B \setminus A) \geq P(A)$.

3. Il suffit de remarquer que $A = (A \setminus B) \sqcup (A \cap B)$.

4. On a $A \cup B = A \sqcup (B \setminus A)$, donc $P(A \cup B) = P(A) + P(B \setminus A) = P(A) + P(B) - P(A \cap B)$.

5. $\Omega = A \sqcup \bar{A}$, donc $1 = P(\Omega) = P(A) + P(\bar{A})$ d'où le résultat. $\square$

Remarque 1.2.10 (hors-programme).

La formule donnée en 4 se généralise en la formule

du *crible de Poincaré*, comme pour le cardinal : pour des événements $A_1, \dots, A_n$:

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} P(A_{i_1} \cap \dots \cap A_{i_k}).$$

Proposition 1.2.11.

Soit (Ω, P) un espace probabilisé. Soit $n \in \mathbb{N}$ et $A_1, \dots, A_n$ des événements deux à deux incompatibles. Alors la probabilité de leur union (appelée union disjointe) est la somme de leurs probabilités :

$$P\left(\bigsqcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i).$$

Démonstration.

Pour $k \in \llbracket 0, n \rrbracket$, notons $E(k)$ la proposition

$$P\left(\bigsqcup_{i=1}^k A_i\right) = \sum_{i=1}^k P(A_i)$$

Montrons $\forall k \in \llbracket 0, n \rrbracket \quad E(k)$ par récurrence :

- On a $P\left(\bigsqcup_{i=1}^0 A_i\right) = P(\emptyset) = 0 = \sum_{i=1}^0 P(A_i)$.
- Montrons $\forall k \in \llbracket 0, n-1 \rrbracket \quad E(k) \Rightarrow E(k+1)$. Soit $k \in \llbracket 0, n-1 \rrbracket$ vérifiant $P(k)$. Alors, comme les événements A_i pour $i \in \llbracket 1, n \rrbracket$ sont deux à deux incompatibles, on a $\forall i \in \llbracket 1, k \rrbracket \quad A_i \cap A_{k+1} = \emptyset$. Donc

$$\left(\bigsqcup_{i=1}^k A_i\right) \cap A_{k+1} = \emptyset$$

On a donc

$$P\left(\left(\bigsqcup_{i=1}^k A_i\right) \sqcup A_{k+1}\right) = P\left(\bigsqcup_{i=1}^k A_i\right) + P(A_{k+1})$$

Or on a $E(k)$, donc

$$P\left(\bigsqcup_{i=1}^{k+1} A_i\right) = \left(\sum_{i=1}^k P(A_i)\right) + P(A_{k+1})$$

On a donc $E(k+1)$.

Enfin : $\forall k \in \llbracket 0, n \rrbracket, E(k)$. $\square$

Proposition 1.2.12 (Formule des probabilités totales, première forme).

Soit (Ω, P) un espace probabilisé, $n \in \mathbb{N}^*$, $(A_i)_{i \in \llbracket 1, n \rrbracket}$ un système complet d'événements et B un événement. Alors

$$P(B) = \sum_{i=1}^n P(A_i \cap B).$$

Démonstration.

D'après la proposition 1.1.17, on a

$$B = \bigcup_{i=1}^n A_i \cap B.$$

et cette union est une union disjointe. Donc d'après la proposition 1.2.11, on a le résultat. $\square$

d Détermination par les images des événements élémentaires.

Dans cette partie, on considère un univers fini $\Omega = \{\omega_1, \dots, \omega_n\}$ de cardinal $n \in \mathbb{N}^*$.

Proposition 1.2.13.

Soit P une probabilité sur Ω . Alors pour tout événement A , on a

$$P(A) = \sum_{\omega \in A} P(\{\omega\}). \quad (\text{XXV.1})$$

Démonstration.

Il suffit de remarquer que pour tout événement A , A est l'union disjointe des $\{\omega\}$ pour $\omega \in A$ et d'utiliser la proposition 1.2.11. $\square$

Corollaire 1.2.14.

En particulier, des réels $p_1, \dots, p_n$ étant donnés, il existe au plus une probabilité sur Ω vérifiant $\forall i \in \llbracket 1, n \rrbracket \quad P(\{\omega_i\}) = p_i$.

Démonstration.

En effet, considérons deux probabilités P_1 et P_2 vérifiant cette condition. Alors, d'après la proposition, pour tout événement A , $P_1(A) = P_2(A)$. $\square$

Remarque 1.2.15.

Remarquons que pour qu'une probabilité vérifiant cette condition existe, il est nécessaire que les p_i soit tous positifs ou nuls (car ce sont des probabilités) et que leur somme soit égale à 1 (car d'après l'égalité (XXV.1) c'est la probabilité de Ω). La proposition suivante montre que ces deux conditions sont suffisantes.

Proposition 1.2.16.

Soit $p_1, \dots, p_n$, n réels positifs ou nuls de somme égale à 1. Alors il existe une (unique) fonction P de probabilité sur Ω telle que pour tout $i \in \llbracket 1, n \rrbracket$, on a $P(\{\omega_i\}) = p_i$.

Démonstration.

On a déjà vu l'unicité sous réserve d'existence. Montrons l'existence. Notons P l'application de $\mathcal{P}(\Omega)$ dans $\mathbb{R}$ qui à tout événement A associe

$$P(A) = \sum_{i \in \llbracket 1, n \rrbracket, \omega_i \in A} p_i$$

Il est clair que pour tout $i \in \llbracket 1, n \rrbracket$, on a $P(\{\omega_i\}) = p_i$. Montrons que P est une probabilité sur Ω .

1. Soit A un événement. Les p_i pour $i \in \llbracket 1, n \rrbracket$ étant positifs ou nuls, on a pour tout A , $P(A) \geq 0$. De plus, $P(A)$ est inférieur ou égal à la somme des p_i , qui vaut 1, donc $0 \leq P(A) \leq 1$.
2. On a $P(\Omega) = \sum_{i=1}^n p_i = 1$.
3. Pour tout couple (A, B) d'événements incompatibles, comme $\{i \in \llbracket 1, n \rrbracket \mid \omega_i \in A \cup B\}$ est la réunion disjointe de $\{i \in \llbracket 1, n \rrbracket \mid \omega_i \in A\}$ et $\{i \in \llbracket 1, n \rrbracket \mid \omega_i \in B\}$, on a

$$\begin{aligned} P(A \cup B) &= \sum_{i \in \llbracket 1, n \rrbracket, \omega_i \in A \cup B} p_i \\ &= \sum_{i \in \llbracket 1, n \rrbracket, \omega_i \in A} p_i + \sum_{i \in \llbracket 1, n \rrbracket, \omega_i \in B} p_i \\ &= P(A) + P(B). \end{aligned}$$

Ainsi, P est donc bien une probabilité. $\square$

Exemple 1.2.17.

Nous pouvons maintenant définir des mesures de probabilités de la manière suivante : « la probabilité P est définie sur $\llbracket 0, 5 \rrbracket$ par

k	0	1	2	3	4	5
$P(\{k\})$	1/4	0	1/2	1/12	1/12	1/12

».

Exemple 1.2.18.

Étant donné des points $A_1, \dots, A_n$ dans un ensemble (fini) Ω , on définit la (mesure de) probabilité empirique par rapport à $A_1, \dots, A_n$ par

$$\forall x \in \Omega, P_n(\{x\}) = \frac{1}{n} \text{Card} \{i \in \llbracket 1, n \rrbracket \mid A_i = x\}.$$

1.3 Probabilités conditionnelles.

a Définition.

Le résultat d'une expérience aléatoire dépend parfois du résultat d'une autre. Par exemple, en prenant pour univers l'ensemble des jours de l'année 2026 muni de la probabilité uniforme P , si on appelle A l'événement «j'attrape un rhume aujourd'hui» et B l'événement «il fait un temps froid et humide aujourd'hui», on aimerait pouvoir exprimer que lorsque B est réalisé, A a une plus grande probabilité d'être réalisé.

Pour cela, on peut restreindre notre univers Ω à l'ensemble des jours où B est réalisé et regarder quelle est la probabilité de l'événement «attraper un rhume» dans cet univers restreint. On appellera cette probabilité la probabilité de A sachant B .

Dans l'univers Ω , l'événement A est l'ensemble des jours où j'attrape un rhume, B est l'ensemble des jours froids et humides. Notre univers restreint est B et l'événement «j'attrape un rhume» dans cet univers est l'ensemble $A \cap B$. Sa probabilité, si on le munit de la probabilité uniforme est $\text{Card}(A \cap B) / \text{Card } B = P(A \cap B) / P(B)$.

Cet exemple nous conduit à la définition suivante.

Définition 1.3.1 (Probabilité conditionnelle). Soit (Ω, P) un espace probabilisé et A et B deux événements, avec B de probabilité non nulle. On appelle probabilité de A sachant B , et on note $P_B(A)$ le réel $\frac{P(A \cap B)}{P(B)}$.

Remarque 1.3.2.

La notation donnée est la notation officielle. Vous retrouverez parfois la notation usuelle $P(A|B)$, que nous vous déconseillons fortement.

Remarque 1.3.3.

Même si l'exemple donné concernait une probabilité uniforme, la définition donnée s'applique à toute probabilité.

Proposition 1.3.4.

Sous les hypothèses de la définition ci-dessus, l'application $P_B : \mathcal{P}(\Omega) \rightarrow \mathbb{R}$ est une probabilité sur Ω .

Démonstration.

En effet, elle est bien définie car $P(B) > 0$. Elle est à valeurs positives ou nulles et pour tout $A \in \mathcal{P}(\Omega)$, on a $A \cap B \subset B$ donc $P(A \cap B) \leq P(B)$ donc $P_B(A) \leq 1$. De plus $P_B(\Omega) = P(B)/P(B) = 1$. Enfin, pour tout couple (A, C) d'événements incompatibles, $A \cap B$ et $C \cap B$ sont incompatibles, donc

$$\begin{aligned} P_B(A \cup C) &= \frac{P((A \cap B) \cup (C \cap B))}{P(B)} \\ &= \frac{P(A \cap B) + P(C \cap B)}{P(B)} \\ &= P_B(A) + P_B(C) \end{aligned}$$

□

Remarque 1.3.5.

Dans les exercices de probabilités, l'un des points délicats (et donc intéressant) est souvent de traduire correctement l'énoncé en termes de probabilités conditionnelles. En effet, les énoncés ne sont pas toujours donnés de manière mathématisée et vous avez alors un (petit) travail de modélisation à effectuer. On pourra commencer par s'entraîner sur les exercices 1.3.11 et 1.3.12.

Exercice 1.3.6.

Dans une urne, on place deux boules blanches et une boule noire. On effectue un premier tirage dans l'urne, dans laquelle on remet la boule tirée en y rajoutant une boule de même couleur. On effectue un second tirage dans l'urne.

Modéliser (*i.e.* traduire l'énoncé mathématiquement, ici en termes de probabilités conditionnelles).

b Probabilités composées, probabilités totales.

Proposition 1.3.7 (Formule des probabilités composées).

Soit A et B deux événements, avec $P(A) > 0$. Alors

$$P(A \cap B) = P(A) \times P_B(B|A).$$

Dans le cas où $P(A) = 0$, on utilise la convention $P(A) \times P_A(B) = 0$.

Démonstration.

C'est une simple réécriture de la définition. $\square$

Remarque 1.3.8.

On généralise cela au cas de plusieurs événements. Soit par exemple A, B, C et D quatre événements tels que $P(A \cap B \cap C \cap D) \neq 0$. Alors

$$P(A \cap B \cap C \cap D) = P(A) \times P_A(B) \\ \times P_{A \cap B}(C) \times P_{A \cap B \cap C}(D).$$

Exercice 1.3.9.

Soit $(A_1, \dots, A_n)$ des événements dont la probabilité de l'intersection est non nulle. Exprimer $P\left(\bigcap_{i=1}^n A_i\right)$ à l'aide de la formule des probabilités composées.

Proposition 1.3.10 (Formule des probabilités totales, deuxième forme).

Soit $n \in \mathbb{N}^*$, $(A_i)_{i \in [1, n]}$ un système complet d'événements et B un événement. Alors

$$P(B) = \sum_{i=1}^n P_{A_i}(B) \times P(A_i).$$

Démonstration.

C'est une conséquence immédiate de la première forme (proposition 1.2.12) et de la formule des probabilités composées. $\square$

Exercice 1.3.11.

On considère une urne contenant quatre boules blanches et trois boules noires. On tire successivement et sans remise trois boules.

Calculer la probabilité de tirer exactement deux boules noires.

Note : il peut être intéressant de dessiner un arbre des possibilités pour raisonner. Mais un tel arbre n'est en *aucun cas* une justification.

Exercice 1.3.12.

On effectue $N \geq 2$ tirages successifs dans une urne, contenant initialement une boule blanche et une boule noire.

Chaque fois que l'on tire une boule blanche, on la remet et on rajoute une boule blanche supplémentaire dans l'urne.

Chaque fois que l'on tire une boule noire, on la remet dans l'urne.

On suppose que cette expérience est modélisée par un espace probabilisé fini (Ω, P) . Quelle est la probabilité p_N d'obtenir la première boule noire au N^{e} tirage ?

Remarque 1.3.13. • Un des points attendus est de justifier rigoureusement l'utilisation d'une certaine formule ...

- L'exercice précédent est souvent modifié en « si l'on tire une boule noire, on s'arrête ». Cela change-t-il la modélisation ?
- L'année prochaine, vous pourrez modéliser cela en considérant une suite infinie de tirages. Comme nous ne considérons que des espaces probabilisés finis, nous nous limitons à N tirages successifs ... avec N quelconque.
- Que vaut $\sum_{n=1}^{+\infty} p_n$? Pouvez-vous l'interpréter, au moins intuitivement ?

c Formule de Bayes.

Exercice 1.3.14 (fondamental).

On effectue un test de dépistage d'une maladie. Le test rend un résultat binaire : positif ou négatif. La probabilité que le test rende un résultat positif pour une personne si cette personne a contracté la maladie est appelé *sensibilité* du test et est notée p_1 . La probabilité que le test rende un résultat négatif pour une personne qui n'a pas contracté cette maladie est appelée *spécificité* et est notée p_2 .

Une personne prise au hasard dans la population française effectue le test et celui-ci rend un résultat positif. Quelle est la probabilité que cette personne soit malade ?

On donne : $p_1 = 0,99$, $p_2 = 0,98$, population française : $N = 6 \times 10^7$ personnes, nombre de personnes ayant contracté la maladie dans la population française : $m = 10^3$.

Proposition 1.3.15 (Formule de Bayes, cas particulier).

Démonstration.

Il suffit de remplacer $P_B(A)$ et $P_A(B)$ par leurs définitions pour constater le résultat. $\square$

Remarque 1.3.16.

Le théorème de Bayes dit, que pour deux événements A et B de probabilité non nulle, la probabilité d'avoir l'événement A , sachant qu'on a observé B (appelée probabilité *a posteriori*) est la probabilité d'avoir B sachant A multipliée par le rapport de la probabilité d'avoir A (probabilité *a priori*) et de la probabilité d'avoir B .

Proposition 1.3.17 (Formule de Bayes, cas général).

Soit $(A_i)_{i \in \llbracket 1, n \rrbracket}$ un système complet d'événements de probabilités toutes non nulles et B un événement de probabilité non nulle. Alors pour tout $j \in \llbracket 1, n \rrbracket$, on a

$$P_B(A_j) = \frac{P_{A_j}(B)P(A_j)}{\sum_{i=1}^n P_{A_i}(B)P(A_i)}.$$

Démonstration.

Soit $j \in \llbracket 1, n \rrbracket$. Alors en utilisant la version précédente du théorème de Bayes, on obtient

$$P_B(A_j) = \frac{P_{A_j}(B)P(A_j)}{P(B)}.$$

Or d'après le théorème des probabilités totales, on a

$$P(B) = \sum_{i=1}^n P_{A_i}(B)P(A_i).$$

$\square$

Remarque 1.3.18.

Il est essentiel d'avoir compris ce que dit cette formule et d'être capable de la redémontrer rapidement.

Exercice 1.3.19.

Monsieur C. vient au lycée à pied, à cheval ou en voiture avec des probabilités respectives $9/100$, $9/10$ et $1/100$. Quand il vient à pied, il met des chaussures de sport avec probabilité $9/10$; à cheval, avec probabilité $5/10$ et en voiture avec probabilité $1/10$. Aujourd'hui, vous constatez qu'il a mis des chaussures de sport. Quelle est la probabilité qu'il soit venu à cheval ?

Remarque 1.3.20.

Remarquez l'abus de langage de l'exercice ci-dessus : en réalité, si on se place aujourd'hui et que Monsieur C. est déjà au lycée, ou bien il est venu à cheval ou bien il est venu par un autre moyen et parler de probabilité n'a plus de sens. En réalité, ce que signifie la formulation, c'est : « si on se place dans l'univers de tous les jours possibles, quelle est la probabilité que M. C. soit venu à cheval sachant qu'il a mis des chaussures de sport ». Cet abus de langage est typique de nombreux problèmes de probabilités et modéliser correctement le problème n'est pas toujours chose facile (voir le problème des trois portes).

1.4 Événements indépendants.**a Couple d'événements indépendants.****Définition 1.4.1.**

Soit A et B deux événements. On dit que A et B sont indépendants si et seulement si $P(A \cap B) = P(A) \times P(B)$.

- Remarque 1.4.2.** 1. Si $P(B) > 0$, alors cette condition est équivalente à $P_B(A) = P(A)$. Autrement dit, de façon informelle, savoir B ne modifie pas la probabilité de A .
2. Si $P(B) > 0$ et $P(\bar{B}) > 0$, elle est également équivalente à $P_B(A) = P_{\bar{B}}(A)$.
3. Il arrive que l'on démontre l'indépendance de deux événements mais le plus souvent, il s'agit d'une hypothèse de modélisation du problème considéré.
4. Dans tout exercice de probabilités, il est primordial de bien repérer dans l'énoncé les hypothèses d'indépendance.

Exercice 1.4.3.

Quels sont les événements indépendants d'eux-mêmes ?

Exemple 1.4.4.

Si on lance deux fois un dé à six faces et qu'on note A et B les événements «obtenir un 6» respectivement au premier et deuxième tirage, on aura tendance à modéliser le problème en disant que les deux événements sont indépendants ce qui correspond à l'intuition physique : le fait qu'on obtienne un 6 au deuxième tirage ne dépend pas du fait qu'on a obtenu un 6 au tirage précédent, le dé n'ayant pas de «mémoire» de ce qui s'est passé. Attention : même si le dé est pipé, il est raisonnable de considérer que les deux événements sont indépendants.

Si au lieu de considérer deux lancers d'un même dé, on considère plutôt le lancer simultané d'un dé rouge et d'un dé vert, il est encore raisonnable de penser que les deux événements sont indépendants, même si les dés sont pipés et même s'ils sont pipés de deux façons différentes. À moins par exemple que les dés soient aimantés, auquel cas les résultats des deux dés pourraient être reliés.

Exercice 1.4.5.

On considère une urne contenant 10 boules noires et 10 boules blanches. On tire successivement deux boules, sans remise. On note A (resp. B) l'événement «la première (resp. seconde) est blanche».

Modéliser ce problème.

A et B sont-elles indépendantes ? Calculer $P(A)$ et $P(B)$. Que vaut $P_B(A)$? Que vaut $P_A(B)$?

Mêmes questions si on tire maintenant simultanément deux boules, l'une de la main gauche, l'autre de la main droite et qu'on note A (resp. B) l'événement «la boule tirée par la main gauche (resp. droite) est blanche».

b Famille finie d'événements mutuellement indépendants.

Définition 1.4.6.

Soit n un entier. On dit que des événements $A_1, \dots, A_n$ sont *mutuellement indépendants* si pour

toute partie I de $\llbracket 1, n \rrbracket$, on a

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

On dit qu'ils sont *deux à deux indépendants* si et seulement si pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$, avec $i \neq j$, A_i et A_j sont indépendants.

Remarque 1.4.7. 1. L'ordre des éléments n'a aucune importance.

2. L'indépendance mutuelle entraîne l'indépendance deux à deux (prendre pour I une paire d'indices).
3. La réciproque est fautive. Considérer par exemple deux tirages d'un dé et les événements «le premier tirage donne un nombre pair», «le second tirage donne un nombre pair» et «la somme des deux nombres obtenus est paire».
4. Si $(A_1, \dots, A_n)$ sont mutuellement indépendants et si $J \subset \llbracket 1, n \rrbracket$, alors $(A_j)_{j \in J}$ est une famille d'événements mutuellement indépendants.

Remarque 1.4.8. 1. Il ne suffit pas de vérifier que la probabilité de l'intersection des A_i est égale au produit des $P(A_i)$ pour l'ensemble de tous les indices mais bien de le vérifier pour tous les ensembles d'indices possibles. Considérer par exemple l'univers $\Omega = \llbracket 1, 8 \rrbracket$ des résultats possibles d'un dé équilibré à 8 faces, et les événements $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{1, 2, 3, 4\}$ et $A_3 = \{1, 5, 6, 7\}$.

2. Le plus souvent, l'indépendance mutuelle est une hypothèse faite lors de la modélisation du problème. Le problème, c'est que dans de nombreux énoncés, cette hypothèse n'est écrite nulle part : c'est le mathématicien qui analyse le problème² qui doit se poser la question de l'indépendance des événements.
3. Lorsqu'il s'agit de montrer l'indépendance mutuelle de plusieurs événements, il faut vérifier autant de conditions que de sous-ensembles de $\llbracket 1, n \rrbracket$, soit 2^n , dont $n + 1$ sont

2. Donc vous en particulier !

trivialement vérifiées (celles pour lesquelles I possède 0 ou 1 élément).

Proposition 1.4.9.

Remplacer, dans une famille d'événements mutuellement indépendants, certains événements par leurs contraires donne une nouvelle famille d'événements mutuellement indépendants. En d'autres termes, soit n un entier et $A_1, \dots, A_n$ n événements indépendants. On se donne n événements $B_1, \dots, B_n$ tels que pour tout $i \in \llbracket 1, n \rrbracket$, B_i est égal à A_i ou à $\bar{A}_i$. Alors la famille $B_1, \dots, B_n$ est une famille d'événements indépendants.

Démonstration.

Il suffit de montrer le cas où $B_i = A_i$ pour $i = 1, \dots, n-1$ et où $B_n = \bar{A}_n$. En effet, on peut alors en déduire que si, dans une famille d'événements mutuellement indépendants, on change l'un des événements en son contraire, on obtient de nouveau une famille d'événements mutuellement indépendants. Par une récurrence immédiate, il vient alors que si on change p événements en leurs contraires, on obtient de nouveau une famille d'événements mutuellement indépendants.

Posons donc $B_i = A_i$ pour $i \in \llbracket 1, n-1 \rrbracket$ et $B_n = \bar{A}_n$.

Soit alors I une partie de $\llbracket 1, n \rrbracket$, montrons qu'on a

$$P\left(\bigcap_{i \in I} B_i\right) = \prod_{i \in I} P(B_i)$$

Si I ne contient pas n , c'est évident.

Si I contient n , alors posons $J = I \setminus \{n\}$. On a successivement :

$$\begin{aligned} P\left(\bigcap_{i \in I} B_i\right) &= P\left(\bar{A}_n \cap \bigcap_{i \in J} A_i\right) \\ &= P\left(\left(\bigcap_{i \in J} A_i\right) \setminus A_n\right) \\ &= P\left(\bigcap_{i \in J} A_i\right) - P\left(\left(\bigcap_{i \in J} A_i\right) \cap A_n\right) \\ &= P\left(\bigcap_{i \in J} A_i\right) - P\left(\bigcap_{i \in I} A_i\right) \\ &= \prod_{i \in J} P(A_i) - \prod_{i \in I} P(A_i) \\ &= (1 - P(A_n)) \prod_{i \in J} P(A_i) \\ &= P(B_n) \prod_{i \in J} P(B_i) \\ &= \prod_{i \in I} P(B_i). \end{aligned}$$

□

2 Variables aléatoires.

2.1 Définitions.

Toutes les définitions ont été données dans la partie c.

2.2 Loi d'une variable aléatoire.

Définition 2.2.1.

Soit X une variable aléatoire définie sur un espace probabilisé fini (Ω, P) à valeurs dans un ensemble E . Alors $X(\Omega)$ est fini.

On appelle *loi de la variable aléatoire* X la loi de probabilité sur $X(\Omega)$ $P_X : \mathcal{P}(X(\Omega)) \rightarrow \mathbb{R}$ telle que

$$\forall x \in X(\Omega) \quad P_X(\{x\}) = P(X = x).$$

Remarque 2.2.2.

Cette propriété définit bien une et une seule probabilité sur $X(\Omega)$, par la caractérisation d'une loi par l'image de ses singletons. Il suffit de vérifier que

$$\sum_{x \in X(\Omega)} P(X = x) = 1.$$

Notation 2.2.3.

Si X et Y sont deux variables aléatoires à valeurs dans un même ensemble, $X \sim Y$ signifie que X et Y ont la même loi.

Proposition 2.2.4.

Si $A \subset X(\Omega)$, $P_X(A) = P(X \in A)$.

Remarque 2.2.5.

On peut donc définir la loi d'une variable aléatoire en précisant la probabilité que cette v.a. soit égale à chaque élément de son image. Par exemple, on peut dire « la v.a. X à valeurs dans $\llbracket 0, 5 \rrbracket$ dont la loi est déterminée par

k	0	1	2	3	4	5
$P(X = k)$	1/4	0	1/2	1/12	1/12	1/12

».

Remarque 2.2.6.

Pour déterminer la loi d'une variable aléatoire X , on procédera *systématiquement* de la manière suivante :

- on détermine l'image de X ;
- pour chaque $k \in X(\Omega)$, on calcule $P(X = k)$;
- si on obtient une loi connue, on la nomme.

Exercice 2.2.7.

Soit X à valeurs dans $\{-1; 0; 1\}$ dont la loi est déterminée par

$$P(X = -1) = P(X = 0) = P(X = 1) = \frac{1}{3}.$$

Comment s'appelle la loi de X ? Quelle est la loi de $-X$? A-t-on $X = -X$?

Remarque 2.2.8.

La définition ci-dessus pose problème dans le cas où X est une variable aléatoire réelle continue (hors-programme) : la probabilité d'avoir $P(X = x)$ ne donne aucune information puisque pour tout x fixé, $P(X = x) = 0$.

C'est pourquoi on trouve parfois une autre définition de P_X : P_X est alors l'application de $\mathcal{P}(E)$ dans $\mathbb{R}$ qui, à une partie A de E , associe $P(X \in A)$. Dans ce cas, P_X a la propriété d'être une probabilité sur E (lorsque E est fini) et est déterminée de façon unique par les valeurs des $P(X = x)$ pour $x \in E$ puisqu'on a $P(X \in A) = \sum_{x \in A} P(X = x)$.

Cette deuxième définition pose également des problèmes dans le cas des variables continues mais ils sont plus facilement réparables (on ne peut plus définir P_X sur $\mathcal{P}(E)$ mais seulement sur une partie).

Définition 2.2.9.

Soit E et F deux ensembles. Soit X une variable aléatoire à valeurs dans un ensemble E . Soit $f : E \rightarrow F$. L'application $f \circ X : \Omega \rightarrow F$ est une variable aléatoire à valeurs dans F appelée *image de X par f* et parfois notée $f(X)$.

Remarque 2.2.10.

Le terme «image d'une variable aléatoire» vient du fait que pour tout $\omega \in \Omega$, $f(X)(\omega)$ est l'image de $X(\omega)$ par f .

Exemple 2.2.11.

Si X est une v.a. réelle, on pourra considérer les v.a. réelles X^2 , $|X|$ etc.

Proposition 2.2.12.

La loi associée à la variable aléatoire $f(X)$ introduite ci-dessus est

$$P_{f(X)} : \mathcal{P}(f(X(\Omega))) \rightarrow \mathbb{R}$$

telle que pour tout $y \in f(X(\Omega))$, $P_{f(X)}(\{y\}) = P(X \in f^{-1}(\{y\}))$.

Par conséquent, pour tout $y \in f(X(\Omega))$,

$$P(f(X) = y) = \sum_{\substack{x \in X(\Omega) \\ f(x) = y}} P(X = x)$$

Démonstration.

Il suffit de remarquer

$$\begin{aligned} (X \in f^{-1}(\{y\})) &= \{ \omega \in \Omega \mid X(\omega) \in f^{-1}(\{y\}) \} \\ &= \{ \omega \in \Omega \mid f(X(\omega)) \in \{y\} \} \\ &= \{ \omega \in \Omega \mid f(X)(\omega) \in \{y\} \} \\ &= \{ \omega \in \Omega \mid \omega \in (f(X))^{-1}(\{y\}) \} \\ &= (f(X) = y). \end{aligned}$$

et que $(X \in f^{-1}(\{y\})) = \bigsqcup_{x \in f^{-1}(\{y\})} (X = x)$. $\square$

Remarque 2.2.13.

La loi de $f(X)$ dépend donc uniquement de celle de X (et de f , bien entendu).

Corollaire 2.2.14.

Soit X, Y deux variables aléatoires à valeurs dans un ensemble E , soit $f : E \rightarrow F$.

Si $X \sim Y$, alors $f(X) \sim f(Y)$.

Démonstration.

Immédiat. $\square$

Exemple 2.2.15.

Soit X un v.a. à valeurs dans $\{-1, 0, 1\}$ telle que $P(X = -1) = P(X = 0) = P(X = 1) = \frac{1}{3}$. Déterminer les lois de X^2 et de X^3 .

Définition 2.2.16 (Loi conditionnelle).

Soit X une variable aléatoire à valeurs dans un ensemble E . Soit A un événement vérifiant $P(A) \neq 0$.

Alors, on appelle *loi conditionnelle de X sachant A* la loi de la variable X sur l'univers Ω muni de la probabilité P_A .

C'est donc la fonction $P_{X|A} : \mathcal{P}(X(\Omega)) \rightarrow \mathbb{R}$ vérifiant :

$$\forall x \in X(\Omega), P_{X|A}(x) = P_A(X = x).$$

C'est aussi la donnée des $P_A(X = x)$ pour chaque x dans l'image de X .

2.3 Lois usuelles

Dans cette partie, on étendra automatiquement les définitions données en commettant l'abus de notation suivant. Soit X une variable aléatoire X à valeurs dans E , $A \subset E$ tel que $\forall x \in E \setminus A, P(X = x) = 0$ et $\forall a \in A, P(X = a) > 0$ (on dit que A est le support de la loi de X). Formellement, $X(\Omega) = E$, mais on étendra les définitions suivantes comme si $X(\Omega) = A$.

Exemple 2.3.1.

Si $X : \Omega \rightarrow \{1, 2, 3, 4\}$, avec $P(X = 1) = P(X = 2) = P(X = 3) = \frac{1}{3}$ et $P(X = 4) = 0$, on s'autorisera à dire que X suit la loi uniforme sur $\{1, 2, 3\}$.

a Loi uniforme**Définition 2.3.2.**

Soit E un ensemble fini, non vide. On dit qu'une variable aléatoire réelle X suit la *loi uniforme* sur E et on note $X \sim \mathcal{U}(E)$ (voire $X \equiv \mathcal{U}(E)$) si $X(\Omega) = E$ et P_X est la probabilité uniforme sur E (autrement dit, pour tout $x \in E$, $P(X = x) = 1/\text{Card } E$).

En particulier pour tout couple (a, b) d'entiers relatifs avec $a \leq b$, on a $X \sim \mathcal{U}([a, b])$ si et seulement si

$$\forall x \in [a, b] \quad P(X = x) = \frac{1}{b - a + 1}.$$

Exemple 2.3.3. • La variable aléatoire modélisant le nombre obtenu par tirage d'un dé équilibré à 6 faces suit la loi uniforme sur $[1, 6]$.

- Pour modéliser le numéro d'une boule tirée dans une urne contenant n boules numérotées de 1 à n on prendra une variable aléatoire suivant la loi uniforme sur $[1, n]$.

Exercice 2.3.4.

On tire deux boules *sans remise* dans une urne. Montrer que le couple des numéros tirés (dans l'ordre) suit une loi uniforme dans l'ensemble des 2-arrangements de $[1, n]$.

Exercice 2.3.5.

Un joueur possède quatre dés : le dé n° 1 a 4 faces, le n° 2 en a 6, le n° 3 8 et le n° 4 12. Il lance un dé à 4 faces, obtient i , lance le dé n° i et note X le résultat obtenu.

Quelle est la loi de X ?

b Loi de Bernoulli.**Définition 2.3.6.**

Soit $p \in [0, 1]$. On dit qu'une variable aléatoire X est une variable de Bernoulli (ou suit la loi de Bernoulli) de paramètre p et on note $X \sim \mathcal{B}(p)$ si X est à valeurs dans $\{0, 1\}$ et $P(X = 1) = p$.

Exemple 2.3.7. • Modélisons le tirage d'une pièce à pile ou face par la variable X valant 0 si l'on obtient pile et 1 si l'on obtient face. Si la pièce est supposée équilibrée, on supposera que X suit la loi uniforme sur $\{0, 1\}$; que ce soit le cas ou non, il s'agit d'une variable de Bernoulli de paramètre la probabilité d'obtenir face.

- Si X est à valeurs dans $\{0, 1\}$, alors $X \sim \mathcal{B}(P(X = 1))$.
- De manière générale, notons A un événement sur un espace probablisé Ω . Alors $\mathbb{1}_A$,

la fonction indicatrice de A , définie par

$$\mathbb{1}_A : \begin{cases} \Omega & \longrightarrow \{0, 1\} \\ \omega & \longmapsto \begin{cases} 1 & \text{si } \omega \in A, \\ 0 & \text{si } \omega \notin A. \end{cases} \end{cases}$$

est une variable de Bernoulli de paramètre $P(A)$.

Très souvent, on s'intéressera à un événement A lors d'une expérience aléatoire et on dira que l'expérience est un succès si A est réalisé et un échec si A ne l'est pas. $\mathbb{1}_A$ est alors la variable de Bernoulli prenant la valeur 1 en cas de succès et 0 en cas d'échec.

Exercice 2.3.8.

Montrer que toute variable aléatoire réelle définie sur un espace probabilisé fini peut s'écrire comme une combinaison linéaire de variables aléatoires suivant des lois de Bernoulli.

c Loi binomiale.

Définition 2.3.9.

Soit $n \in \mathbb{N}$ et $p \in [0, 1]$. On dit qu'une variable aléatoire X suit la loi binomiale de paramètres n et p et on note $X \sim \mathcal{B}(n, p)$ si X est à valeurs dans $\llbracket 0, n \rrbracket$ et pour tout $k \in \llbracket 0, n \rrbracket$, on a

$$P(X = k) = \binom{n}{k} p^k (1 - p)^{n-k}.$$

Exemple 2.3.10. • Considérons n expériences aléatoires mutuellement indépendantes toutes de probabilité de succès p . On modélisera le nombre de succès par une variable binomiale de paramètres n et p . On verra dans la proposition 2.5.21 une justification mathématique à cette modélisation.

- En particulier considérons une urne opaque contenant B boules blanches et N boules noires indiscernables au toucher ($B \in \mathbb{N}^*$, $N \in \mathbb{N}^*$), dans laquelle on tire n fois une boule, avec remise. Alors on modélisera le nombre de fois où l'on tire une boule noire

par une variable aléatoire suivant la loi binomiale de paramètres n et $N/(B + N)$.

Exercice 2.3.11.

On considère un joueur jouant au jeu suivant :

- Il mise un euro. Cette mise est définitivement perdue.
- Il lance quatre pièces de monnaie.
- Si exactement trois des pièces tombent sur pile, il perçoit un euro. Si les quatre pièces tombent sur pile, il perçoit dix euros.

On note X le gain du joueur (mise incluse, le gain peut donc être négatif). Donner la loi de X .

2.4 Couples de variables aléatoires.

Dans cette partie, on considère Ω un espace probabilisé fini et deux variables aléatoires X et Y .

On écrira $X(\Omega)$ sous la forme $\{x_1, \dots, x_N\}$ et $Y(\Omega)$ sous la forme $\{y_1, \dots, y_P\}$ où N et P sont des entiers.

Remarque 2.4.1.

On peut considérer, en commettant un léger abus de notation, que (X, Y) est une variable aléatoire, à valeurs dans $\{x_1, \dots, x_N\} \times \{y_1, \dots, y_P\}$.

Proposition 2.4.2.

La famille $((X = x_i) \cap (Y = y_j))_{(i,j) \in \llbracket 1, N \rrbracket \times \llbracket 1, P \rrbracket}$ est un système complet d'événements.

Démonstration.

Soit $(i, j) \in \llbracket 1, N \rrbracket \times \llbracket 1, P \rrbracket$, il suffit de remarquer que $[(X, Y) = (x_i, y_j)] = [X = x_i] \cap [Y = y_j]$ et d'utiliser la proposition 1.1.13. $\square$

Remarque 2.4.3.

On notera souvent l'événement $[X = x] \cap [Y = y]$ par $[X = x, Y = y]$.

Définition 2.4.4 (Loi conjointe).

On appelle *loi conjointe* de X et Y la loi du couple (X, Y) , soit la loi $P_{X,Y} : \mathcal{P}(X(\Omega) \times Y(\Omega)) \rightarrow \mathbb{R}$ vérifiant $\forall (x, y) \in X(\Omega) \times Y(\Omega)$, $P_{X,Y}(\{(x, y)\}) = P((X = x) \cap (Y = y)) = P(X = x, Y = y)$.

Exercice 2.4.5.

On tire un dé équilibré à six faces et on lance une pièce de monnaie équilibrée. On note X la variable de Bernoulli associée à l'événement «obtenir pile» et Y la valeur tirée sur le dé.

Donner la loi conjointe de X et Y .

Exercice 2.4.6.

On tire deux dés équilibrés à quatre faces, un vert et un rouge. On appelle X la valeur obtenue sur le dé vert, Y la valeur obtenue sur le dé rouge et Z la somme des deux. Donner la loi conjointe de X et Y puis de X et Z .

Définition 2.4.7.

On appelle *première (resp. seconde) loi marginale du couple* (X, Y) la loi de X (resp. de Y).

Proposition 2.4.8.

Les lois marginales du couple (X, Y) sont déterminées de façon unique par la loi du couple $P_{X,Y}$. Plus précisément, on a pour tout $x \in X(\Omega)$

$$\begin{aligned} P(X = x) &= P_X(\{x\}) = \sum_{y \in Y(\Omega)} P_{X,Y}(\{(x, y)\}) \\ &= \sum_{y \in Y(\Omega)} P(X = x, Y = y). \end{aligned}$$

Symétriquement, pour tout $y \in Y(\Omega)$, on a

$$\begin{aligned} P(Y = y) &= P_Y(\{y\}) = \sum_{x \in X(\Omega)} P_{X,Y}(\{(x, y)\}) \\ &= \sum_{x \in X(\Omega)} P(X = x, Y = y). \end{aligned}$$

En revanche, les lois marginales ne suffisent pas à déterminer la loi du couple.

Démonstration.

Pour le premier point, considérons $x \in X(\Omega)$ et remarquons alors qu'on a

$$(X = x) = \bigcup_{y \in Y(\Omega)} (X = x) \cap (Y = y).$$

Or cette union est une union disjointe, d'où l'égalité

$$P(X = x) = \sum_{y \in Y(\Omega)} P((X = x) \cap (Y = y)).$$

D'où le premier point. Autrement dit : la famille des $(Y = y)$ pour $y \in Y(\Omega)$ constitue un système complet d'événements et le résultat se déduit immédiatement de la formule des probabilités totales.

Pour le second point, il suffit de montrer que deux couples peuvent avoir des lois différentes bien qu'ayant les mêmes lois marginales. On peut par exemple considérer, sur l'univers $\Omega = \{1, 2\}$ muni de la probabilité uniforme, les variables de Bernoulli X et Y définies par $X(1) = 1$, $X(2) = 0$, $Y(1) = 0$ et $Y(2) = 1$. Alors les variables X et Y ont même loi, les deux couples de variables aléatoires (X, X) et (X, Y) ont donc mêmes lois marginales. Cependant, ils ont des lois conjointes différentes puisque $P_{X,X}(1, 1) = \frac{1}{2}$ et $P_{X,Y}(1, 1) = 0$. $\square$

Exemple 2.4.9.

On lance deux dés à 6 faces et l'on note X et Y le résultat de chacun. Alors (après avoir modélisé cela), les lois jointes de (X, X) et de (X, Y) sont différentes alors que (X, X) et (X, Y) ont les mêmes lois marginales.

Remarque 2.4.10.

La loi de Y conditionnellement à $X = x$ ne dépend que de la loi jointe de X et de Y :

$$P_{(X=x)}(Y = y) = \frac{P(X = x, Y = y)}{\sum_{z \in Y(\Omega)} P(X = x, Y = z)}.$$

On peut généraliser de la même manière ces notions sur les couples de variables aléatoires et définir la loi conjointe d'un n -uplet de variables aléatoires, les n lois marginales de ce n -uplet ainsi que la loi conditionnelle d'une variable, par exemple X_n , sachant $X_1 = x_1, \dots$ et $X_{n-1} = x_{n-1}$.

2.5 Variables aléatoires indépendantes.

Dans ces parties, sauf mention expresse du contraire, X et Y sont des variables aléatoires à valeurs respectivement dans des ensembles E et F .

Définition 2.5.1.

On dit que X et Y sont indépendantes si pour tout $x \in E$ et tout $y \in F$ on a

$$P([X = x] \cap [Y = y]) = P(X = x)P(Y = y). \quad (\text{XXV.2})$$

On dira que deux variables aléatoires sont *indépendantes et identiquement distribuées* (i.i.d.) si elles sont indépendantes et de même loi.

Notation 2.5.2.

On note $X \perp\!\!\!\perp Y$ pour signifier que X et Y sont indépendantes.

Remarque 2.5.3.

On écrira souvent cela comme

$$P(X = x, Y = y) = P(X = x)P(Y = y).$$

Deux v.a. sont donc indépendantes si et seulement si leur loi jointe se factorise en le produit de leurs lois.

Exemple 2.5.4.

Si l'on tire deux dés ou si l'on effectue deux tirages avec remise dans une urne, on modélisera les deux résultats comme des v.a. indépendantes.

Exercice 2.5.5.

On effectue deux tirages sans remise dans une urne contenant n boules. Modéliser. Les numéros tirés sont-ils indépendants ?

Proposition 2.5.6.

X et Y sont indépendantes si et seulement si pour tout $A \subset E$ et tout $B \subset F$, on a

$$P((X, Y) \in A \times B) = P(X \in A)P(Y \in B). \quad (\text{XXV.3})$$

Démonstration.

Pour le sens indirect, c'est-à-dire pour montrer l'égalité (XXV.2), sous l'hypothèse que l'égalité (XXV.3) est vérifiée pour tout A et tout B , il suffit de choisir $A = \{x\}$ et $B = \{y\}$.

Montrons le sens direct : supposons donc qu'on a (XXV.2) pour tout $(x, y) \in E \times F$ et montrons que pour tout $(A, B) \in \mathcal{P}(E) \times \mathcal{P}(F)$, on a (XXV.3). Quitte à remplacer A par $A \cap X(\Omega)$ et B par $B \cap Y(\Omega)$, on peut supposer que A et B sont des ensembles finis. On a alors

$$\begin{aligned} [X \in A] &= \bigcup_{x \in A} [X = x] \\ [Y \in B] &= \bigcup_{y \in B} [Y = y] \\ [(X, Y) \in A \times B] &= \bigcup_{(x, y) \in A \times B} [X = x] \cap [Y = y] \end{aligned}$$

Or ces trois unions sont des unions disjointes, donc :

$$\begin{aligned} P((X, Y) \in A \times B) &= P\left(\bigcup_{(x, y) \in A \times B} [X = x] \cap [Y = y]\right) \\ &= \sum_{(x, y) \in A \times B} P([X = x] \cap [Y = y]) \\ &= \sum_{(x, y) \in A \times B} P(X = x) \times P(Y = y) \\ &= \left(\sum_{x \in A} P(X = x)\right) \times \left(\sum_{y \in B} P(Y = y)\right) \\ &= P\left(\bigcup_{x \in A} [X = x]\right) \times P\left(\bigcup_{y \in B} [Y = y]\right) \\ &= P(X \in A) \times P(Y \in B). \end{aligned}$$

□

Exercice 2.5.7.

Soit X, Y indépendantes de loi uniforme sur $\llbracket 1, n \rrbracket$. Calculer $P(X \leq Y)$.

Proposition 2.5.8.

Soit E, E', F et F' quatre ensembles. Soit $f : E \rightarrow E'$ et $g : F \rightarrow F'$. Soit alors X et Y deux variables aléatoires indépendantes. Alors $f(X)$ et $g(Y)$ sont des variables aléatoires indépendantes.

Démonstration.

Soit $A' \subset E'$ et $B' \subset F'$. D'après la proposition qui précède, il suffit de montrer

$$P((f(X), g(Y)) \in A' \times B') = P(f(X) \in A') \times P(g(Y) \in B').$$

Or on a

$$[(f(X), g(Y)) \in A' \times B'] = [f(X) \in A'] \cap [g(Y) \in B'].$$

Et d'autre part, on a

$$\begin{aligned} [f(X) \in A'] &= \{\omega \in \Omega \mid f(X(\omega)) \in A'\} \\ &= \{\omega \in \Omega \mid X(\omega) \in f^{-1}(A')\} \\ &= [X \in f^{-1}(A')] \end{aligned}$$

et de la même façon, on obtient :

$$[g(Y) \in B'] = [Y \in g^{-1}(B')].$$

On en déduit

$$\begin{aligned} &[(f(X), g(Y)) \in A' \times B'] \\ &= [f(X) \in A'] \cap [g(Y) \in B'] \\ &= [X \in f^{-1}(A')] \cap [Y \in g^{-1}(B')] \\ &= [(X, Y) \in f^{-1}(A') \times g^{-1}(B')]. \end{aligned}$$

Puis :

$$\begin{aligned} & P((f(X), g(Y)) \in A' \times B') \\ &= P((X, Y) \in f^{-1}(A') \times g^{-1}(B')) \\ &= P(X \in f^{-1}(A')) \times P(Y \in g^{-1}(B')) \\ &= P(f(X) \in A') \times P(g(Y) \in B'), \end{aligned}$$

qui est ce qu'on voulait démontrer. $\square$

Définition 2.5.9.

Soit n un entier et $X_1, \dots, X_n$ des variables aléatoires à valeurs dans des ensembles respectifs $E_1, \dots, E_n$. On dit que les variables $X_1, \dots, X_n$ sont mutuellement indépendantes si pour tous $x_1, \dots, x_n$ appartenant respectivement à $X_1(\Omega), \dots, X_n(\Omega)$, on a

$$P\left(\bigcap_{i=1}^n (X_i = x_i)\right) = \prod_{i=1}^n P(X_i = x_i). \quad (\text{XXV.4})$$

On dira que des variables aléatoires sont *indépendantes et identiquement distribuées* (i.i.d.) si elles sont mutuellement indépendantes et de même loi.

Remarque 2.5.10.

On montrera bientôt que des variables aléatoires mutuellement indépendantes le sont deux à deux.



Comme le montre l'exemple 2.5.11, des v.a. indépendantes deux à deux ne le sont pas forcément mutuellement.

Exemple 2.5.11.

Soit X, Y i.i.d. de loi de Rademacher : $P(X = 1) = P(X = -1) = \frac{1}{2}$, soit $Z = XY$. Montrer que X, Y et Z sont indépendantes deux à deux, mais pas mutuellement.

Proposition 2.5.12.

Les variables aléatoires $X_1, \dots, X_n$ à valeurs dans des ensembles respectifs $E_1, \dots, E_n$ sont mutuellement indépendantes si et seulement pour tous sous ensembles respectifs $A_1, \dots, A_n$ de $E_1, \dots, E_n$, on a

$$P\left(\bigcap_{i=1}^n (X_i \in A_i)\right) = \prod_{i=1}^n P(X_i \in A_i). \quad (\text{XXV.5})$$

Démonstration.

La démonstration est similaire à celle du cas de deux variables.

Pour le sens indirect, c'est-à-dire pour montrer l'égalité (XXV.4), sous l'hypothèse que l'égalité (XXV.5) est vérifiée pour tous ensembles $A_1, \dots, A_n$, il suffit de choisir $A_i = \{x_i\}$ pour $i = 1, \dots, n$.

Montrons le sens direct : supposons donc qu'on a (XXV.4) pour tous $x_1, \dots, x_n$ appartenant respectivement à $E_1, \dots, E_n$ et montrons que pour tous sous ensembles respectifs $A_1, \dots, A_n$ de $E_1, \dots, E_n$, on a (XXV.5). Quitte à remplacer chaque A_i par $A_i \cap X_i(\Omega)$, on peut supposer que les A_i sont des ensembles finis. On a alors, si $1 \leq i \leq n$,

$$(X_i \in A_i) = \bigcup_{x_i \in A_i} (X_i = x_i).$$

Ainsi,

$$\begin{aligned} P\left(\bigcap_{i=1}^n (X_i \in A_i)\right) &= P\left(\bigcap_{i=1}^n \bigcup_{x_i \in A_i} (X_i = x_i)\right) \\ &= P\left(\bigcup_{(x_1, \dots, x_n) \in A_1 \times \dots \times A_n} \bigcap_{i=1}^n (X_i = x_i)\right). \end{aligned}$$

Or, cette réunion est disjointe, donc

$$P\left(\bigcap_{i=1}^n (X_i \in A_i)\right) = \sum_{(x_1, \dots, x_n) \in A_1 \times \dots \times A_n} P\left(\bigcap_{i=1}^n (X_i = x_i)\right).$$

Par indépendance mutuelle,

$$\begin{aligned} P\left(\bigcap_{i=1}^n (X_i \in A_i)\right) &= \sum_{(x_1, \dots, x_n) \in A_1 \times \dots \times A_n} \prod_{i=1}^n P(X_i = x_i) \\ &= \prod_{i=1}^n \sum_{x_i \in A_i} P(X_i = x_i) \\ &= \prod_{i=1}^n P(X_i \in A_i), \end{aligned}$$

d'où le résultat. $\square$

Remarque 2.5.13.

Notez la différence entre la définition d'événements mutuellement indépendants et celle de variables mutuellement indépendantes : dans ce dernier cas, la définition ne demande pas de regarder pour tous les sous-ensembles de $\llbracket 1, n \rrbracket$, pour une bonne raison : le résultat suivant assure que si l'égalité (XXV.4) est vérifiée, alors elle est vraie aussi si l'on effectue le produit et l'intersection seulement pour un sous-ensemble de $\llbracket 1, n \rrbracket$.

Proposition 2.5.14.

Toute sous-famille d'une famille de variables aléatoires mutuellement indépendantes est constituée de variables mutuellement indépendantes : soit $X_1, \dots, X_n$ des variables aléatoires mutuellement indépendantes et $I \subset \llbracket 1, n \rrbracket$; alors les X_i pour $i \in I$ sont mutuellement indépendantes.

Démonstration.

D'après la proposition 2.5.12, il suffit de montrer que pour toute famille d'événements A_i pour $i \in I$, on a

$$P\left(\bigcap_{i \in I} (X_i \in A_i)\right) = \prod_{i \in I} P(X_i \in A_i).$$

Considérons donc une telle famille quelconque, et posons $A_i = E_i$ pour $i \in \llbracket 1, n \rrbracket \setminus I$. Alors, pour tout $i \in \llbracket 1, n \rrbracket \setminus I$, l'événement $X_i \in A_i$ est certain, c'est-à-dire est égal à Ω . Donc

$$\begin{aligned} P\left(\bigcap_{i \in I} (X_i \in A_i)\right) &= P\left(\bigcap_{i=1}^n (X_i \in A_i)\right) \\ &= \prod_{i=1}^n P(X_i \in A_i) \\ &= \prod_{i \in I} P(X_i \in A_i). \end{aligned}$$

□

Corollaire 2.5.15 (Lemme des coalitions).

Soit $(X_1, \dots, X_n)$ des variables aléatoires mutuellement indépendantes, I et J deux sous-ensembles disjoints de $\{1, \dots, n\}$.

Alors les variables aléatoires $(X_i)_{i \in I}$ et $(X_j)_{j \in J}$ sont indépendantes.

Démonstration.

Direct, par indépendance mutuelle de la famille $(X_k)_{k \in I \cup J}$.

□

Remarque 2.5.16.

Ce lemme se généralise directement à l'indépendance mutuelle de m « paquets » de variables aléatoires pris sur m sous-ensembles disjoints deux à deux de $\{1, \dots, n\}$.

Proposition 2.5.17.

Si $X_1, \dots, X_n$ sont des variables aléatoires mutuellement indépendantes et $f_1, \dots, f_n$ sont des fonctions définies sur $X_1(\Omega), \dots, X_n(\Omega)$, alors $f_1(X_1), \dots, f_n(X_n)$ sont mutuellement indépendantes.

Démonstration.

Exactement comme pour deux v.a. □

Exemple 2.5.18.

Si X, Y, Z, T sont quatre v.a. réelles mutuellement indépendantes, alors $(X, Y), Z, T$ sont aussi mutuellement indépendantes, tout comme $X + Y, e^Z$ et T^2 .

Proposition 2.5.19.

Soit $n \in \mathbb{N}$, $A_1, \dots, A_n$ n événements et $X_1, \dots, X_n$ les variables de Bernoulli respectivement associées à ces événements. Alors les événements $A_1, \dots, A_n$ sont mutuellement indépendants si et seulement si les variables aléatoires $X_1, \dots, X_n$ sont mutuellement indépendantes.

Démonstration.

Supposons que les événements $A_1, \dots, A_n$ sont indépendants. Soit alors $x_1, \dots, x_n$ n éléments de $\{0, 1\}$. Notons B_i l'événement $X_i = x_i$ pour $i \in \llbracket 1, n \rrbracket$. Alors pour tout i , on a $B_i = A_i$ ou $B_i = \bar{A}_i$. Donc les événements $B_1, \dots, B_n$ sont mutuellement indépendants. On en déduit successivement :

$$\begin{aligned} P\left(\bigcap_{i=1}^n (X_i = x_i)\right) &= P\left(\bigcap_{i=1}^n B_i\right) \\ &= \prod_{i=1}^n P(B_i) \\ &= \prod_{i=1}^n P(X_i = x_i). \end{aligned}$$

Ainsi, les variables aléatoires $X_1, \dots, X_n$ sont mutuellement indépendantes.

Réciproquement, supposons que les variables aléatoires $X_1, \dots, X_n$ sont mutuellement indépendantes et montrons que les événements $A_1, \dots, A_n$ le sont aussi. Soit $I \subset \llbracket 1, n \rrbracket$. Alors les X_i pour $i \in I$ sont mutuellement indépendantes, en particulier, on a

$$P\left(\bigcap_{i \in I} (X_i = 1)\right) = \prod_{i \in I} P(X_i = 1)$$

Or pour tout $i \in I$, l'événement $(X_i = 1)$ n'est autre que A_i . On en déduit donc le résultat. □

Remarque 2.5.20.

Si $X_1, \dots, X_n$ sont des variables aléatoires suivant des lois de Bernoulli, alors

$$\sum_{i=1}^n X_i = \text{Card} \{ i \in \llbracket 1, n \rrbracket \mid X_i = 1 \}.$$

On remarquera, sans s'émouvoir, que $\{ i \in \llbracket 1, n \rrbracket \mid X_i = 1 \}$ est une variable aléatoire à valeurs dans $\mathcal{P}(\llbracket 1, n \rrbracket)$.

Proposition 2.5.21.

Soit $p \in [0, 1]$ et $n \in \mathbb{N}$. Soit $X_1, \dots, X_n$ n variables aléatoires suivant toutes la loi de Bernoulli de paramètre p et mutuellement indépendantes. Alors la variable X à valeurs dans $\llbracket 0, n \rrbracket$ définie par

$$X = X_1 + \dots + X_n$$

suit la loi binomiale de paramètres n et p .

Démonstration.

On a, pour tout $i \in \llbracket 1, n \rrbracket$, $X_i(\Omega) = \{0, 1\}$, donc $X(\Omega) \subset \llbracket 0, n \rrbracket$.

Posons $E = \{0, 1\}^n$, et pour tout élément $(x_1, \dots, x_n)$ de E , on note $A_{(x_1, \dots, x_n)}$ l'événement $\bigcap_{i=1}^n (X_i = x_i)$. La famille $(A_x)_{x \in E}$ est un système complet d'événements. Donc on a, pour tout $k \in \llbracket 0, n \rrbracket$

$$\begin{aligned} (X = k) &= \bigcup_{x \in E} (X = k) \cap A_x \\ &= \bigcup_{\substack{(x_1, \dots, x_n) \in E \\ x_1 + \dots + x_n = k}} A_{(x_1, \dots, x_n)}. \end{aligned}$$

Or les A_x forment un système complet d'événements. On a donc

$$\begin{aligned} P(X = k) &= \sum_{(x_1, \dots, x_n) \in E} P(A_{(x_1, \dots, x_n)} \cap [X = k]) \\ &= \sum_{\substack{(x_1, \dots, x_n) \in E \\ x_1 + \dots + x_n = k}} P(A_{(x_1, \dots, x_n)}). \end{aligned}$$

Or, les X_i étant mutuellement indépendantes, pour tout $(x_1, \dots, x_n) \in E$, on a

$$P(A_{(x_1, \dots, x_n)}) = \prod_{i=1}^n P(X_i = x_i).$$

Or pour tout $i \in \llbracket 1, n \rrbracket$, X_i est une variable de Bernoulli de paramètre p , donc si $x_i = 1$, $P(X_i = x_i)$ vaut p et si $x_i = 0$, $P(X_i = x_i)$ vaut $(1 - p)$. Donc si k est le nombre de membres du n -uplet $(x_1, \dots, x_n)$ valant 1, on a

$$P(A_{(x_1, \dots, x_n)}) = p^k (1 - p)^{n-k}$$

D'où

$$\begin{aligned} P(X = k) &= \sum_{\substack{(x_1, \dots, x_n) \in E \\ x_1 + \dots + x_n = k}} p^k (1 - p)^{n-k} \\ &= \binom{n}{k} p^k (1 - p)^{n-k}. \end{aligned}$$

On peut aussi le montrer par récurrence sur n . En notant $S_n = \sum_{k=1}^n X_k$, alors naturellement $S_1 \sim \mathcal{B}(1, p)$.

Supposons que $S_{n-1} \sim \mathcal{B}(n-1, p)$. Alors X_n est indépendante de $(X_1, \dots, X_{n-1})$ donc de S_{n-1} . Il ne reste plus qu'à montrer que si $Y \sim \mathcal{B}(n-1, p)$ est indépendante de X_n , alors $S = X_n + Y \sim \mathcal{B}(n, p)$.

Comme $X_1(\Omega) = \{0, 1\}$ et $Y(\Omega) = \llbracket 0, n-1 \rrbracket$, alors $S(\Omega) \subset \llbracket 0, n \rrbracket$. Soit $k \in \llbracket 0, n \rrbracket$, calculons $P(S = k)$.

- Si $k = 0$, $P(S = 0) = P([X_n = 0] \cap [Y = 0])$ et donc par indépendance de X_n et de Y , $P(S = 0) = P(X_n = 0)P(Y = 0) = (1-p) \cdot (1-p)^{n-1} = (1-p)^n$.
- De même, si $k = n$, $P(S = n) = P([X_n = 1] \cap [Y = n-1])$ et donc $P(S = n) = P(X_n = 1)P(Y = n-1) = p \cdot p^{n-1} = p^n$.
- Si $0 < k < n$, alors $([X_n = 0], [X_n = 1])$ est un système complet d'événements, donc par la formule des probabilités totales

$$\begin{aligned} P(S = k) &= P([S = k] \cap [X_n = 0]) \\ &\quad + P([S = k-1] \cap [X_n = 1]) \\ &= P([Y = k] \cap [X_n = 0]) \\ &\quad + P([Y = k-1] \cap [X_n = 1]) \\ &\stackrel{\text{ind.}}{=} P(Y = k)P(X_n = 0) \\ &\quad + P(Y = k-1)P(X_n = 1) \\ &= \binom{n-1}{k} p^k (1-p)^{n-1-k} \cdot (1-p) \\ &\quad + \binom{n-1}{k-1} p^{k-1} (1-p)^{n-1-(k-1)} \cdot p \\ &= p^k (1-p)^{n-k} \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] \\ &= p^k (1-p)^{n-k} \binom{n}{k} \end{aligned}$$

par la formule du triangle de Pascal, ce qui permet de conclure. $\square$

Remarque 2.5.22.

Dans le dernier calcul, on pouvait aussi écrire

$$\begin{aligned} P(S = k) &= P_{[X=0]}(S = k)P(X = 0) \\ &\quad + P_{[X=1]}(S = k)P(X = 1) \\ &= P_{[X=0]}(Y = k)P(X = 0) \\ &\quad + P_{[X=1]}(Y = k-1)P(X = 1) \end{aligned}$$

puis de voir, par indépendance de X et de Y , que $P_{[X=0]}(Y = k) = P(Y = k)$ ainsi que $P_{[X=1]}(Y = k - 1) = P(Y = k - 1)$.

Nous n'avons fait que détailler ceci.

2.6 Espérance.

Définition 2.6.1.

Soit X une variable aléatoire réelle. On appelle espérance de X et on note $E(X)$ la somme

$$\sum_{x \in X(\Omega)} P(X = x)x.$$

On dit qu'une variable aléatoire X est *centrée* si son espérance est nulle.

Remarque 2.6.2. 1. L'espérance est la moyenne des valeurs prises par X , pondérées par leurs probabilités.

2. L'espérance de X ne dépend que de la loi de X , donc deux variables ayant même loi ont même espérance.

Exercice 2.6.3.

On lance deux dés et on note X la somme des deux résultats. Calculer l'espérance de X .

Proposition 2.6.4.

Soit X une variable aléatoire réelle. Alors on a

$$E(X) = \sum_{\omega \in \Omega} P(\{\omega\})X(\omega).$$

Démonstration.

Il suffit de remarquer que pour tout $x \in X(\Omega)$, on a $\{X = x\} = \{\omega \in \Omega \mid X(\omega) = x\}$, donc

$$P(X = x) = \sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\})$$

On a alors successivement :

$$\begin{aligned} E(X) &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\}) \right) x \\ &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\})X(\omega) \right) \\ &= \sum_{\omega \in \Omega} P(\{\omega\})X(\omega) \end{aligned}$$

□

Proposition 2.6.5.

L'espérance est linéaire et positive, donc croissante. Plus précisément, soit X et Y deux variables aléatoires réelles et α et β deux réels.

Alors

$$E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y)$$

De plus si X est presque sûrement à valeurs positives ($P(X \geq 0) = 1$) alors $E(X) \geq 0$.

Enfin, si l'événement $X \leq Y$ est presque sûr, alors $E(X) \leq E(Y)$.

Démonstration.

Les deux premiers points se déduisent immédiatement de la proposition 2.6.4 (pour le second on utilise que pour $x < 0$, on a $P(X = x) \leq P(X < 0) = 1 - P(X \geq 0) = 0$).

Le troisième se déduit du fait que $E(Y) = E(Y - X) + E(X)$ et que $P(Y - X \geq 0) = P(X \leq Y) = 1$. □

Remarque 2.6.6.

La propriété précédente s'étend naturellement, par récurrence, à toute combinaison linéaire (finie !) de variables aléatoires.

Remarque 2.6.7.

Si X est une v.a. réelle, alors $X - E(X)$ est centrée.

Proposition 2.6.8.

Une variable aléatoire positive d'espérance nulle est nulle presque-sûrement.

Démonstration.

On a une somme de termes positifs qui est nulle. □

Proposition 2.6.9 (Espérance des lois usuelles.).
Soit $C \in \mathbb{R}$, $p \in [0, 1]$, $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

1. L'espérance d'une variable aléatoire constante de valeur C est égale à C .
2. L'espérance d'une variable aléatoire suivant la loi de Bernoulli de paramètre p est p .
3. L'espérance d'une variable aléatoire suivant la loi binomiale de paramètres n et p vaut np .
4. L'espérance d'une variable aléatoire suivant la loi uniforme sur $\llbracket a, b \rrbracket$, avec $a < b$, vaut $\frac{a+b}{2}$.

Démonstration.

Les deux premiers points se déduisent directement de la définition. Pour le troisième, on sait que l'espérance d'une variable aléatoire ne dépend que de sa loi. Étant donné une variable X sur un espace probabilisé Ω suivant la loi binomiale de paramètres n et p où $n \in \mathbb{N}$ et $p \in [0, 1]$, on construit une variable aléatoire Y , sur un autre espace de probabilité Ω' , de façon à ce que d'une part Y suive la loi binomiale de paramètres n et p et d'autre part Y s'écrive comme somme de variables $Y_1, \dots, Y_n$ de Bernoulli indépendantes, toutes de paramètre p . On a alors

$$\begin{aligned} E(X) &= E(Y) \\ &= E\left(\sum_{i=1}^n Y_i\right) \\ &= \sum_{i=1}^n E(Y_i) \\ &= \sum_{i=1}^n p \\ &= np. \end{aligned}$$

Voici comment construire Ω' et Y . On pose $\Omega' = \{0, 1\}^n$ et pour tout $\omega = (\omega_1, \dots, \omega_n) \in \Omega'$, on pose $p_\omega = \prod_{i=1}^n \alpha(\omega_i)$, où $\alpha(0) = 1 - p$ et $\alpha(1) = p$.

On a

$$\begin{aligned} \sum_{\omega \in \Omega'} p_\omega &= \sum_{(\omega_1, \dots, \omega_n) \in \{0, 1\}^n} \prod_{i=1}^n \alpha(\omega_i) \\ &= \prod_{i=1}^n \sum_{\omega_i \in \{0, 1\}} \alpha(\omega_i) \\ &= \prod_{i=1}^n (1 - p + p). \end{aligned}$$

Ainsi, il existe une probabilité sur Ω' vérifiant pour tout $\omega \in \Omega'$, $P(\{\omega\}) = p_\omega$.

On définit alors, pour $i \in I$, Y_i la variable aléatoire de Bernoulli vérifiant $Y_i(\omega_1, \dots, \omega_n) = \omega_i$. Alors les Y_i , pour $i = 1, \dots, n$ sont des variables aléatoires mutuellement indépendantes. En effet, soit x_i pour $i = 1, \dots, n$ des éléments de $\{0, 1\}$.

Soit $i \in \llbracket 1, n \rrbracket$, on a alors

$$\begin{aligned} P(Y_i = x_i) &= \sum_{\substack{(\omega_1, \dots, \omega_n) \in \{0, 1\}^n \\ \omega_i = x_i}} \prod_{j=1}^n \alpha(\omega_j) \\ &= \alpha(x_i) \prod_{\substack{j=1 \\ j \neq i}}^n \sum_{\omega_j \in \{0, 1\}} \alpha(\omega_j) \\ &= \alpha(x_i) \prod_{\substack{j=1 \\ j \neq i}}^n (1 - p + p) \\ &= \alpha(x_i). \end{aligned}$$

Par ailleurs, on a

$$\begin{aligned} P\left(\bigcap_{i=1}^n \{Y_i = x_i\}\right) &= P(\{(x_1, \dots, x_n)\}) \\ &= \prod_{i=1}^n \alpha(x_i), \end{aligned}$$

donc

$$P\left(\bigcap_{i=1}^n \{Y_i = x_i\}\right) = \prod_{i=1}^n P(Y_i = x_i).$$

Concernant le dernier point, il suffit de voir que si $X \sim \mathcal{U}(\llbracket a, b \rrbracket)$, alors $X - a \sim \mathcal{U}(\llbracket 0, b - a \rrbracket)$. Soit donc $n \in \mathbb{N}$ et $Y \sim \mathcal{U}(\llbracket 0, n \rrbracket)$, alors

$$E(Y) = \sum_{k=0}^n k P(Y = k) = \frac{1}{n+1} \sum_{k=0}^n k = \frac{n}{2},$$

ce qui permet de conclure par $E(X) = E[X - a] + a = \frac{b-a}{2} + a = \frac{a+b}{2}$. $\square$

Remarque 2.6.10 (très utile).

Si A est un événement, comme $\mathbf{1}_A \sim \mathcal{B}(P(A))$, alors $E[\mathbf{1}_A] = P(A)$.

Proposition 2.6.11 (Formule de transfert).

Soit X une variable aléatoire à valeurs dans E et $f : X(\Omega) \rightarrow \mathbb{R}$. Alors

$$E[f(X)] = \sum_{x \in X(\Omega)} P(X = x) f(x)$$

Démonstration.

On a déjà noté que pour tout $x \in X(\Omega)$, on a

$$P(X = x) = \sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\}).$$

En posant $s = \sum_{x \in X(\Omega)} P(X = x)f(x)$, on a alors successivement :

$$\begin{aligned} s &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\}) \right) f(x) \\ &= \sum_{x \in X(\Omega)} \left(\sum_{\substack{\omega \in \Omega \\ X(\omega) = x}} P(\{\omega\}) f(X(\omega)) \right) \\ &= \sum_{\omega \in \Omega} P(\{\omega\}) f(X(\omega)) \\ &= E[f(X)]. \end{aligned}$$

□

Remarque 2.6.12.

La formule de transfert montre que $E[f(X)]$ dépend juste de la loi de X et de f . Pour calculer cette espérance, nul besoin d'obtenir la loi de $f(X)$!

Exercice 2.6.13.

Si $X \sim \mathcal{U}([0, n])$, calculer $E[X^2]$.

Proposition 2.6.14 (Espérance de variables indépendantes).

Soit X et Y deux variables à valeurs réelles indépendantes. Alors $E(XY) = E(X)E(Y)$.

Démonstration.

On a, par la formule de transfert (appliquée à (X, Y) et à $(x, y) \mapsto xy$),

$$\begin{aligned} E(XY) &= \sum_{(x,y) \in X(\Omega) \times Y(\Omega)} P((X, Y) = (x, y)) xy \\ &= \sum_{(x,y) \in X(\Omega) \times Y(\Omega)} P(X = x) P(Y = y) xy \\ &= \sum_{x \in X(\Omega)} P(X = x) x \times \sum_{y \in Y(\Omega)} P(Y = y) y \\ &= E(X)E(Y) \end{aligned}$$

□

Remarque 2.6.15.

La réciproque est bien entendu fausse. Considérez par exemple la variable $X \sim \mathcal{U}(\{-1, 0, 1\})$ et $Y = X^2$.

Remarque 2.6.16.

Cela se généralise : si $X_1, \dots, X_n$ sont des v.a. réelles mutuellement indépendantes, alors $E[X_1 \dots X_n] = E[X_1] \dots E[X_n]$.

Proposition 2.6.17 (Inégalité de Markov).

Soit X une variable aléatoire réelle à valeurs positives presque-sûrement. Soit $t \in \mathbb{R}_+^*$. On a :

$$P(X \geq t) \leq \frac{E(X)}{t}.$$

Démonstration.

On a

$$\begin{aligned} E(X) &= \sum_{\omega \in \Omega} P(\{\omega\}) X(\omega) \\ &= \sum_{\substack{\omega \in \Omega \\ X(\omega) \geq t}} P(\{\omega\}) X(\omega) + \sum_{\substack{\omega \in \Omega \\ 0 \leq X(\omega) < t}} P(\{\omega\}) X(\omega) \\ &\quad + \sum_{\substack{\omega \in \Omega \\ X(\omega) < 0}} P(\{\omega\}) X(\omega) \\ &\geq \sum_{\substack{\omega \in \Omega \\ X(\omega) \geq t}} P(\{\omega\}) X(\omega) \\ &\geq \sum_{\substack{\omega \in \Omega \\ X(\omega) \geq t}} P(\{\omega\}) t \\ &\geq tP(\{\omega \in \Omega \mid X(\omega) \geq t\}) \\ &\geq tP(X \geq t) \end{aligned}$$

Sinon, il suffit de voir que $Y = t\mathbf{1}_{X \geq t}$ est une variable aléatoire inférieure à X p.s., puis de considérer son espérance. En effet, $\mathbf{1}_{X \geq t}$ suit la loi de Bernoulli de paramètre $P(X \geq t)$, donc

$$E[Y] = tE[\mathbf{1}_{X \geq t}] = tP(X \geq t) \leq E[X].$$

□

Remarque 2.6.18.

C'est une inégalité fondamentale en probabilité, vous la retrouverez de nombreuses fois : retenez la bien !

Exemple 2.6.19.

n étudiants ont travaillé au mois de juillet dernier. En moyenne, leur travail leur a rapporté 750 euros chacun. Donner un majorant de la proportion d'étudiants ayant gagné au moins 1000 euros.

2.7 Variance, écart type et covariance.

Définition 2.7.1.

Soit X une variable aléatoire réelle.

On appelle *variance de X* , notée $V(X)$ (ou parfois $\sigma^2(X)$), la quantité

$$V(X) = E((X - E(X))^2).$$

On appelle *écart-type de X* et on note $\sigma(X)$ la racine carrée de la variance :

$$\sigma(X) = \sqrt{V(X)}.$$

On dit que X est une variable aléatoire *réduite* si sa variance est 1.

Remarque 2.7.2. 1. La variance et l'écart-type ne dépendent que de la loi de X .

2. Intuitivement la variance mesure la « moyenne » du carré des écarts à la « moyenne ». C'est donc une mesure de la dispersion des valeurs autour de la valeur moyenne prise par la variable aléatoire X . Si la variable X est exprimée dans une unité u , la variance sera exprimée dans l'unité u^2 (et l'écart-type dans l'unité u).

Proposition 2.7.3 (Formule de König-Huygens). Soit X une variable aléatoire réelle. Alors la variance est la différence entre l'espérance de son carré et le carré de son espérance :

$$V(X) = E(X^2) - E(X)^2.$$

Démonstration.

Il suffit d'utiliser la définition, la linéarité de l'espérance et le résultat sur l'espérance d'une variable constante pour obtenir successivement :

$$\begin{aligned} V(X) &= E((X - E(X))^2) \\ &= E(X^2 - 2E(X)X + E(X)^2) \\ &= E(X^2) - 2E(X)E(X) + E(X)^2 \\ &= E(X^2) - E(X)^2. \end{aligned}$$

□

Proposition 2.7.4.

Soit X une variable aléatoire réelle, et a et b deux réels.

Alors

$$E(aX + b) = aE(X) + b,$$

$$V(aX + b) = a^2V(X),$$

$$\sigma(aX + b) = |a|\sigma(X).$$

En particulier, si $\sigma(X) \neq 0$, la variable Y définie par

$$Y = \frac{X - E(X)}{\sigma(X)}$$

est une variable centrée réduite.

Démonstration.

On connaît déjà le premier point. Il suffit de remplacer par les définitions et de calculer pour conclure pour les autres. □

Proposition 2.7.5 (Variance des lois usuelles).

Soit $p \in [0, 1]$ et $n \in \mathbb{N}^*$.

1. Toute variable aléatoire constante p.s. est de variance nulle.
2. Toute variable aléatoire réelle suivant la loi de Bernoulli de paramètre p a pour variance $p(1 - p)$.
3. Toute variable aléatoire réelle suivant la loi binomiale de paramètres p et n a pour variance $np(1 - p)$.
4. Toute variable aléatoire réelle suivant la loi uniforme sur $\llbracket 1, n \rrbracket$, a pour variance $\frac{n^2 - 1}{12}$.

Démonstration. 1. Direct.

2. Considérons X une variable aléatoire réelle suivant la loi de Bernoulli de paramètre p . Alors $V(X) = E(X^2) - E(X)^2$. Or $P(X^2 = 1) = P(X = 1) = p$ et donc $E(X^2) = p$. Donc $V(X) = p - p^2 = p(1 - p)$.
3. Soit X une variable aléatoire réelle suivant la loi binomiale de paramètres p et n . Alors on peut construire une variable aléatoire réelle Y de même loi que X , donc de même variance, de façon que Y soit la somme de n variables de Bernoulli $Y_1, \dots, Y_n$ de paramètre p mutuellement indépendantes.

On verra plus loin que *dans le cas particulier de variables deux à deux indépendantes*, la variance de la somme est égale à la somme des variances. On a donc ici :

$$V(Y) = \sum_{i=1}^n V(Y_i) = np(1 - p)$$

4. Faisons le calcul dans le cas général $X \sim \mathcal{U}(\llbracket a, b \rrbracket)$, avec $a < b$. $X - a \sim \mathcal{U}(\llbracket 0, b - a \rrbracket)$ et $V(X - a) = V(X)$. Soit $Y \sim \mathcal{U}(\llbracket 0, n \rrbracket)$, avec $n \in \mathbb{N}$, calculons $V(Y)$. Par la formule de König-Huygens, $V(Y) = E[Y^2] - E[Y]^2 = E[Y^2] - \frac{n^2}{4}$. De plus, par la formule de transfert,

$$\begin{aligned} E[Y^2] &= \sum_{k=0}^n k^2 P(Y = k) \\ &= \frac{1}{n+1} \sum_{k=0}^n k^2 \\ &= \frac{n(2n+1)}{6}. \end{aligned}$$

Ainsi,

$$V(Y) = \frac{2n(2n+1)}{12} - \frac{3n^2}{12} = \frac{n(n+2)}{12}.$$

Donc $V(X) = \frac{(b-a)(b-a+2)}{12}$ et l'on retrouve bien l'énoncé avec $b = n$ et $a = 1$. $\square$

Théorème 2.7.6 (Inégalité de Bienaymé-Tchebychev).

Soit X une variable aléatoire réelle, $V(X)$ sa variance, soit $\varepsilon > 0$. Alors

$$P(|X - E(X)| \geq \varepsilon) \leq \frac{V(X)}{\varepsilon^2}.$$

Démonstration.

Il suffit de constater que $(X - E(X))^2$ est une v.a. positive, donc d'après l'inégalité de Markov :

$$\begin{aligned} P(|X - E(X)| \geq \varepsilon) &= P((X - E(X))^2 \geq \varepsilon^2) \\ &\leq \frac{E[(X - E(X))^2]}{\varepsilon^2} \\ &\leq \frac{V(X)}{\varepsilon^2}. \end{aligned}$$

$\square$

Remarque 2.7.7.

Cette inégalité contrôle la déviation d'une variable aléatoire par rapport à sa moyenne. C'est un résultat fondamental !

Corollaire 2.7.8.

Une variable aléatoire de variance nulle est constante presque-sûrement.

Démonstration.

Remarquons que $(X - E[X])^2$ est positive, donc si $V(X) = 0$ alors p.s. $(X - E[X])^2 = 0$, en utilisant le résultat 2.6.8. Ainsi p.s. $X = E[X]$. $\square$

Définition 2.7.9 (Covariance).

Soit X et Y deux variables aléatoires réelles. On appelle covariance de X et Y et on note $\text{Cov}(X, Y)$ le réel

$$\text{Cov}(X, Y) = E((X - E(X))(Y - E(Y))).$$

Si $\text{Cov}(X, Y) = 0$, on dit que X et Y sont décorrélées.

Remarque 2.7.10.

$\text{Cov}(X, X)$ n'est autre que $V(X)$ et $\text{Cov}(X, Y) = \text{Cov}(Y, X)$.

Remarque 2.7.11.

Si $\sigma(X) = 0$, nous avons vu que $X = E[X]$ p.s, donc $\text{Cov}(X, Y) = 0$.

Si $\sigma(X)$ et $\sigma(Y)$ ne sont pas nuls, on définit le *coefficient de corrélation* de X et de Y par

$$\rho(X, Y) = \frac{\text{Cov}(X, Y)}{\sigma(X)\sigma(Y)}.$$

L'inégalité de Cauchy-Schwarz (que nous verrons bientôt) permet de montrer deux résultats intéressants :

- $\rho(X, Y) \in [-1, 1]$;
- si $|\rho(X, Y)| = 1$, alors il existe $a, b, c \in \mathbb{R}$ tels que $aX + bY = c$ p.s, i.e. X et Y sont p.s. en relation affine.

On montre aussi facilement que, si l'on résout le *problème de régression affine de Y sur X par moindres carrés*, i.e. si l'on minimise en $a, b \in \mathbb{R}$ la quantité :

$$E[(Y - aX - b)^2],$$

alors le coefficient a optimal (c'est la pente de la droite de régression de Y sur X) est

$$a = \frac{\text{Cov}(X, Y)}{V(X)} = \rho(X, Y) \times \frac{\sigma(Y)}{\sigma(X)}.$$

Remarquons que, dans ce cas, effectuer la régression de Y sur X n'est pas la même chose que d'effectuer la régression de X sur Y !

Si X et Y sont centrées-réduites (en pratique, il convient souvent de centrer-réduire ses données avant d'effectuer un traitement statistique dessus), on s'aperçoit que

$$a = \rho(X, Y).$$

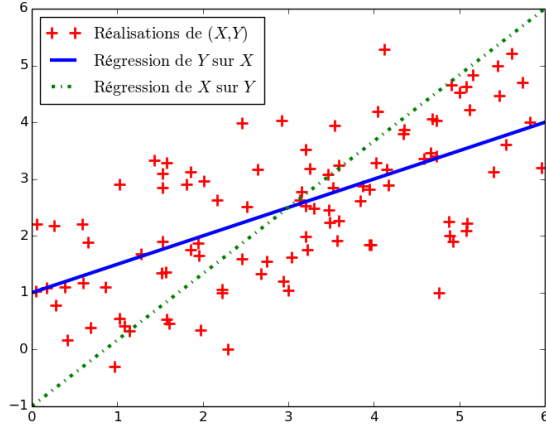


FIGURE XXV.1 – Exemple de régression affine par moindres carrés, ici $\rho(X, Y) = \sqrt{\frac{3}{7}} \approx 0,65$.

Exercice 2.7.12.

Soit (Ω, P) un espace probabilisé fini, X une variable aléatoire réelle définie sur Ω et f une fonction réelle croissante.

Montrer que $\text{Cov}(X, f(X)) \geq 0$.

Proposition 2.7.13.

Soit X et Y deux variables aléatoires réelles. Alors on a

$$\text{Cov}(X, Y) = E(XY) - E(X)E(Y).$$

Démonstration.

Comme pour la formule de König-Huygens :

$$\begin{aligned} \text{Cov}(X, Y) &= E(X - E(X))(Y - E(Y)) \\ &= E(XY - XE(Y) - YE(X) + E(X)E(Y)) \\ &= E(XY) - E(X)E(Y) - E(X)E(Y) + E(X)E(Y) \\ &= E(XY) - E(X)E(Y). \end{aligned}$$

□

Remarque 2.7.14.

Par la formule de transfert,

$$E[XY] = \sum_{x \in X(\Omega), y \in Y(\Omega)} xyP(X = x, Y = y).$$

Corollaire 2.7.15.

Deux variables aléatoires indépendantes ont une covariance nulle.

Remarque 2.7.16.

Comme montré par l'exemple $X \sim \mathcal{U}(-1, 0, 1)$ et $Y = X^2$, deux variables peuvent être non corrélées mais sans être indépendantes.

Proposition 2.7.17.

Soit $n \in \mathbb{N}$ et $X_1, \dots, X_n$ n variables aléatoires réelles. Alors on a

$$V\left(\sum_{i=1}^n X_i\right) = \sum_{i=1}^n V(X_i) + 2 \sum_{1 \leq i < j \leq n} \text{Cov}(X_i, X_j).$$

Démonstration.

Posons, pour $i = 1, \dots, n$, $Y_i = X_i - E(X_i)$ et $X = \sum_{i=1}^n X_i$.

On a :

$$\begin{aligned} V(X) &= E\left(\left(\sum_{i=1}^n Y_i\right)^2\right) \\ &= E\left(\sum_{i=1}^n Y_i^2 + 2 \sum_{1 \leq i < j \leq n} Y_i Y_j\right) \\ &= \sum_{i=1}^n E(Y_i^2) + 2 \sum_{1 \leq i < j \leq n} E(Y_i Y_j) \\ &= \sum_{i=1}^n V(X_i) + 2 \sum_{1 \leq i < j \leq n} \text{Cov}(X_i, X_j). \end{aligned}$$

□

Corollaire 2.7.18.

Dans le cas particulier où les variables $X_1, \dots, X_n$ sont deux à deux décorréées, la variance de leur somme est égale à la somme de leurs variances.

Remarque 2.7.19.

On déduit de ce résultat la variance de la loi binomiale, comme on l'a vu plus haut.

Chapitre XXVI

Matrices et algèbre linéaire

Sommaire

1	Structure de $\mathcal{M}_{n,p}(\mathbb{K})$.	398	e	Trace d'un endomorphisme en dimension finie.	416
1.1	Structure d'espace vectoriel.	398	f	Propriétés.	417
1.2	Remarques sur le produit.	398	g	Trace d'un projecteur.	417
a	Colonnes d'un produit.	398	7	Matrices par blocs (HP).	417
b	Application canoniquement associée.	398			
c	Produit d'éléments des bases canoniques.	399			
2	Matrices, familles de vecteurs et applications linéaires.	399			
2.1	Matrice d'une famille de vecteurs relativement à une base.	399			
2.2	Matrice associée à une application linéaire relativement à deux bases.	400			
2.3	Inversibilité.	403			
2.4	Matrices de passage.	404			
3	Matrices remarquables.	407			
3.1	Matrices triangulaires.	407			
3.2	Matrices diagonales.	408			
3.3	Matrices symétriques et antisymétriques.	408			
4	Rang d'une matrice.	409			
4.1	Définitions.	409			
4.2	Opérations laissant le rang invariant.	411			
4.3	Calculs pratiques.	412			
4.4	Matrices extraites.	412			
5	Systèmes d'équations linéaires.	413			
5.1	Généralités.	413			
5.2	Solutions.	413			
6	Matrices semblables et trace.	414			
6.1	Matrices semblables.	414			
a	Changement de base pour un endomorphisme.	414			
6.2	Trace d'une matrice carrée.	415			
a	Définition.	415			
b	Linéarité.	415			
c	Propriété fondamentale de la trace.	415			
d	Invariance par similitude.	416			

Dans tout ce chapitre et sauf mention expresse du contraire, n, m, p, q, r et t désignent des entiers naturels non nuls, et $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Structure de $\mathcal{M}_{n,p}(\mathbb{K})$.

On reviendra avec profit sur le cours sur les matrices du premier semestre.

1.1 Structure d'espace vectoriel.

Théorème 1.1.1.

$(\mathcal{M}_{n,p}(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$ -espace vectoriel de base $(E_{i,j})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$, avec $E_{i,j} = (\delta_{ki} \times \delta_{\ell j})_{(k,\ell)}$. En particulier

$$\dim_{\mathbb{K}} \mathcal{M}_{n,p}(\mathbb{K}) = np.$$

La base $(E_{i,j})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$ est la *base canonique* de $\mathcal{M}_{n,p}(\mathbb{K})$.

Démonstration.

On a déjà vu qu'il s'agissait d'un $\mathbb{K}$ -ev puisque :

1. $(\mathcal{M}_{n,p}(\mathbb{K}), +)$ est un groupe abélien (+ est une loi de composition interne, associative, commutative, admettant un élément neutre — la matrice nulle — et pour laquelle tout élément admet un opposé — la matrice de coefficients opposés).
2. Pour toute $M \in \mathcal{M}_{n,p}(\mathbb{K})$, $1 \cdot M = M$.
3. Le produit externe est distributif à droite par rapport à l'addition.
4. Le produit externe est distributif à gauche par rapport à l'addition.
5. On a la propriété d'associativité mixte.

Il reste à montrer que la famille des $(E_{i,j})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$ en est une base.

Pour cela, il suffit de remarquer que pour toute matrice M , de coefficients $(m_{ij})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$, on a

$$M = \sum_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket} m_{ij} E_{i,j}.$$

On en déduit donc :

- d'une part que toute matrice M s'écrit d'au moins une façon comme combinaison linéaire des $E_{i,j}$ pour $(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket$ et que la famille $(E_{i,j})$ est génératrice ;
- d'autre part que toute combinaison linéaire des $(E_{i,j})$ est égale à une matrice dont les coefficients sont ceux de la combinaison linéaire, qu'en conséquence toute combinaison linéaire $\sum_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket} \lambda_{ij} E_{i,j}$

de valeur nulle est aussi égale à la matrice des $(\lambda_{ij})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$ qui ne peut donc avoir que des coefficients tous nuls et que la famille des $(E_{i,j})$ est donc libre. $\square$

1.2 Remarques sur le produit.

a Colonnes d'un produit.

Proposition 1.2.1.

Soient $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$. Soit $\alpha \in \llbracket 1, q \rrbracket$. Notons C_α la α^{e} colonne de B . Alors la α^{e} colonne de AB est la matrice AC_α .

Démonstration.

Le produit AB est la matrice de coefficients

$$\left(\sum_{k=1}^p a_{ik} b_{kj} \right)_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,q \rrbracket},$$

qui possède q colonnes, comme B . La α^{e} colonne de cette matrice existe donc et a pour coefficients

$$\left(\sum_{k=1}^p a_{ik} b_{k\alpha} \right)_{i \in \llbracket 1,n \rrbracket}.$$

Notons $c_1, \dots, c_p$ les coefficients de C_α . La matrice AC_α est la matrice colonne de coefficients

$$\left(\sum_{k=1}^p a_{ik} c_k \right)_{i \in \llbracket 1,n \rrbracket}.$$

Or C_α est la α^{e} colonne de B , donc pour tout $k \in \llbracket 1, p \rrbracket$ $c_k = b_{k\alpha}$.

AC_α a donc même coefficients que la α^{e} colonne de AB , elle lui est donc égale. $\square$

b Application canoniquement associée.

Définition 1.2.2.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. On appelle *application linéaire canoniquement associée à M* l'application

$$u : \begin{cases} \mathcal{M}_{p,1}(\mathbb{K}) & \longrightarrow \mathcal{M}_{n,1}(\mathbb{K}) \\ X & \longmapsto MX \end{cases}$$

ou, en identifiant $\mathbb{K}^p$ avec $\mathcal{M}_{p,1}(\mathbb{K})$ et $\mathbb{K}^n$ avec $\mathcal{M}_{n,1}(\mathbb{K})$:

$$u : \begin{cases} \mathbb{K}^p & \longrightarrow \mathbb{K}^n \\ (x_1, \dots, x_p) & \longmapsto M \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}. \end{cases}$$

Proposition 1.2.3.

Cette application est bien une application linéaire.

Démonstration.

Pour tout $(X, Y) \in \mathcal{M}_{p,1}(\mathbb{K})$ et tout $\lambda \in \mathbb{K}$, on a

$$\begin{aligned} u(\lambda X + Y) &= M(\lambda X + Y) \\ &= \lambda(MX) + MY \\ &= \lambda u(X) + u(Y). \end{aligned}$$

□

Définition 1.2.4.

On appelle noyau (resp. image) de M et on note $\text{Ker } M$ (resp. $\text{Im } M$) le noyau (resp. l'image) de l'application linéaire canoniquement associée à M .

Remarque 1.2.5.

Si $M \in \mathcal{M}_{n,p}(\mathbb{K})$, le noyau de M est l'ensemble des solutions du système linéaire homogène $MX = 0$.

c Produit d'éléments des bases canoniques.

On étend les résultats vus au premier semestre au cas des matrices non carrées.

Proposition 1.2.6.

Notons

- $(E_{ij})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$ la base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$;
- $(E'_{ij})_{(i,j) \in \llbracket 1,p \rrbracket \times \llbracket 1,q \rrbracket}$ celle de $\mathcal{M}_{p,q}(\mathbb{K})$.
- $(E''_{ij})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,q \rrbracket}$ celle de $\mathcal{M}_{n,q}(\mathbb{K})$.

Soit

- $(i, j) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket$;
- $(k, h) \in \llbracket 1, p \rrbracket \times \llbracket 1, q \rrbracket$.

Alors

$$\begin{aligned} E_{ij} \times E'_{kh} &= \delta_{jk} E''_{ih} \\ &= \begin{cases} E''_{ih} & \text{si } j = k, \\ 0_{nq} & \text{sinon.} \end{cases} \end{aligned}$$

Remarque 1.2.7.

Dessiner les matrices pour voir de quoi il retourne. La démonstration suivante n'est que la description du dessin.

Démonstration.

Soit $\alpha \in \llbracket 1, q \rrbracket$. La α^{e} colonne de $E_{ij} \times E'_{kh}$ est $E_{ij} C_\alpha$ où C_α est la α^{e} colonne de E'_{kh} . Si $\alpha \neq h$, $C_\alpha = 0_{p1}$, donc toutes les colonnes de $E_{ij} \times E'_{kh}$ sont nulles sauf peut-être la h^{e} .

Cette h^{e} colonne de E_{kh} est égale à $E_{ij} C_h$. C_h étant le k^{e} vecteur de la base canonique de $\mathcal{M}_{p,1}(\mathbb{K})$, $E_{ij} C_h$ est la k^{e} colonne de E_{ij} . Celle-ci est nulle si $j \neq k$. Sinon, il s'agit du i^{e} vecteur de la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$.

On en déduit le résultat.

On peut également adopter une démonstration purement calculatoire. Notons $(m_{ab})_{(a,b) \in \llbracket 1,n \rrbracket \times \llbracket 1,q \rrbracket}$ les coefficients du produit $E_{ij} E'_{kh}$. Alors, soit $(a, b) \in \llbracket 1, n \rrbracket \times \llbracket 1, q \rrbracket$. On a

$$\begin{aligned} m_{ab} &= \sum_{c=1}^p (\delta_{ai} \delta_{cj}) (\delta_{ck} \delta_{bh}) \\ &= (\delta_{ai} \delta_{jj}) (\delta_{jk} \delta_{bh}) \\ &= \delta_{jk} (\delta_{ai} \delta_{bh}) \end{aligned}$$

m_{ab} est donc le coefficient de la ligne a , colonne b de $\delta_{jk} E''_{ih}$. □

2 Matrices, familles de vecteurs et applications linéaires.

2.1 Matrice d'une famille de vecteurs relativement à une base.

Définition 2.1.1.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base d'un $\mathbb{K}$ -ev E de dimension finie n . Soient $v_1, \dots, v_p$ p vecteurs de E . On note a_{ij} la i^{e} coordonnées de v_j dans $\mathcal{B}$, i.e. $v_j = \sum_{i=1}^n a_{ij} e_i$.

Alors, la matrice $A = (a_{ij}) \in \mathcal{M}_{n,p}(\mathbb{K})$ est appelée *matrice de la famille $(v_1, \dots, v_p)$ dans la base $\mathcal{B}$ (ou relativement à la base $\mathcal{B}$)*, et elle est notée $\text{Mat}_{\mathcal{B}}(v_1, \dots, v_p)$ (parfois $\mathcal{M}_{\mathcal{B}}(v_1, \dots, v_p)$).

Exemple 2.1.2. 1. Dans $\mathbb{R}^2$, notons $\mathcal{B}$ la base canonique et $\mathcal{B}'$ la base $((0, 1); (1, 1))$. Avec

$\mathcal{F} = ((1, 2); (0, 3); (-1, 1))$, on a

$$\begin{aligned}\text{Mat}_{\mathcal{B}}(\mathcal{F}) &= \begin{pmatrix} 1 & 0 & -1 \\ 2 & 3 & 1 \end{pmatrix}, \\ \text{Mat}_{\mathcal{B}'}(\mathcal{F}) &= \begin{pmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \end{pmatrix}.\end{aligned}$$

2. Dans $\mathbb{R}_3[X]$ muni de la base canonique $\mathcal{B}$, avec la famille $\mathcal{F} = (1 + X^2; 1 + X + X^2 + X^3; X^3 - 2)$, on a

$$\text{Mat}_{\mathcal{B}}(\mathcal{F}) = \begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

3. Matrice d'une famille de vecteurs de $\mathbb{K}^n$ dans la base canonique.
4. La matrice d'une famille de vecteurs colonnes $C_1, \dots, C_p$ éléments de $\mathcal{M}_{n,1}(\mathbb{K})$ dans la base canonique est la matrice dont les colonnes sont $C_1, \dots, C_p$.

Théorème 2.1.3.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base d'un $\mathbb{K}$ -ev E de dimension finie n . Alors l'application

$$\varphi : \begin{cases} (E, +, \cdot) & \rightarrow (\mathcal{M}_{n,1}(\mathbb{K}), +, \cdot) \\ x & \mapsto \text{Mat}_{\mathcal{B}}(x) \end{cases}$$

est un isomorphisme d'espaces vectoriels.

Démonstration.

Soient $x, y \in E$ tels que $x = \sum_{k=1}^n x_k e_k$ et $y = \sum_{k=1}^n y_k e_k$. Soit $\lambda \in \mathbb{K}$. Alors $\varphi(x + \lambda y) = (x_i + \lambda y_i)_{1 \leq i \leq n} = (x_i)_{1 \leq i \leq n} + \lambda (y_i)_{1 \leq i \leq n} = \varphi(x) + \lambda \varphi(y)$. D'où la linéarité de φ . De plus, soit $M = (m_i)_{1 \leq i \leq n} \in \mathcal{M}_{n,1}(\mathbb{K})$. Alors $\varphi(x) = M$ si et seulement si pour tout i , $m_i = x_i$, d'où la bijectivité de φ . $\square$

2.2 Matrice associée à une application linéaire relativement à deux bases.

Définition 2.2.1.

Soient E un $\mathbb{K}$ -ev de dimension finie p et F un $\mathbb{K}$ -ev de dimension finie n . Soient $\mathcal{B} = (e_1, \dots, e_p)$ et

$\mathcal{C} = (f_1, \dots, f_n)$ des bases de E et F respectivement. Soit $u \in \mathcal{L}(E, F)$. On appelle *matrice de u relativement à $\mathcal{B}$ et $\mathcal{C}$* , notée $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$ (parfois $\mathcal{M}_{\mathcal{B}, \mathcal{C}}(u)$), la matrice $\text{Mat}_{\mathcal{C}}(u(e_1), \dots, u(e_p)) \in \mathcal{M}_{n,p}(\mathbb{K})$.

Autrement dit, cette matrice contient les coordonnées des images des vecteurs de la base de départ décomposés dans la base d'arrivée.

Remarque 2.2.2.

Si $\mathcal{B} = \mathcal{C}$, on note $\text{Mat}_{\mathcal{B}}(u) = \text{Mat}_{\mathcal{B}, \mathcal{B}}(u)$.

Remarque 2.2.3.

On pourra représenter f et sa matrice dans un schéma comme représenté dans la figure XXVI.1.

$$E, \mathcal{B} \xrightarrow[\text{Mat}_{\mathcal{B}, \mathcal{C}}(f)]{f} F, \mathcal{C}$$

FIGURE XXVI.1 – Représentation schématique de la matrice d'une application linéaire.

Exemple 2.2.4.

Soit $u : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $(x, y) \mapsto (x - y, 3x + 2y)$, $\mathcal{B} = (e_1, e_2)$ la base canonique $\mathcal{B}$ de $\mathbb{R}^2$. On a $u(e_1) = (1, 3) = e_1 + 3e_2$ et $u(e_2) = (-1, 2) = -e_1 + 2e_2$. Ainsi, la matrice associée à u relativement à $\mathcal{B}$ est

$$\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix}.$$

Avec $\mathcal{C}$ la base $(f_1, f_2) = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}; \begin{pmatrix} 0 \\ -1 \end{pmatrix} \right)$, on a $u(e_1) = f_1 - 2f_2$ et $u(e_2) = -f_1 - 3f_2$. Ainsi,

$$\text{Mat}_{\mathcal{B}, \mathcal{C}}(u) = \begin{pmatrix} 1 & -1 \\ -2 & -3 \end{pmatrix}.$$

Exercice 2.2.5. 1. Avec les mêmes u , $\mathcal{B}$ et $\mathcal{C}$, calculer $\text{Mat}_{\mathcal{C}, \mathcal{B}}(u)$.

2. Réciproquement, trouver l'application linéaire associée à $M = \begin{pmatrix} 0 & 3 \\ -1 & 2 \end{pmatrix}$ relativement aux bases canoniques de $\mathbb{R}^2$.

3. Notons $\varphi : \mathbb{R}_3[X] \rightarrow \mathbb{R}_4[X]$, $P \mapsto P' + 3XP$, $\mathcal{B} = (1, X, X^2, X^3)$ et $\mathcal{C} = (X^3, X, X^2, 1, X^4)$ Trouver la matrice de φ relativement aux bases $\mathcal{B}$ et $\mathcal{C}$.
4. Réciproquement, avec les mêmes bases, notons φ l'unique application linéaire telle que

$$\text{Mat}_{\mathcal{B}, \mathcal{C}}(\varphi) = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

retrouver l'expression de φ .

5. Donner la matrice de $\mathbb{R}_3[X] \rightarrow \mathbb{R}_3[X]$
 $P \mapsto P'$
 dans les bases canoniques.
6. Donner la matrice de $\mathbb{R}_3[X] \rightarrow \mathbb{R}$
 $P \mapsto P(\pi)$
 dans les bases canoniques.

Exercice 2.2.6.

Soit $a, b \in \mathbb{R}$. Dans $\mathbb{R}$ -espace vectoriel $\mathbb{C}$, exprimer la matrice de $z \mapsto (a+ib)z$ dans la base canonique $(1, i)$.

Théorème 2.2.7.

Soient E un $\mathbb{K}$ -ev de dimension finie p et F un $\mathbb{K}$ -ev de dimension finie n . Soient $\mathcal{B} = (e_1, \dots, e_p)$ et $\mathcal{C} = (f_1, \dots, f_n)$ des bases de E et F respectivement. Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. Il existe une unique application $u \in \mathcal{L}(E, F)$ telle que $M = \text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$: c'est l'unique application linéaire associant, pour tout $j \in \llbracket 1, p \rrbracket$, au j^{e} vecteur de la base $\mathcal{B}$ le vecteur dont la colonne des coordonnées dans la base $\mathcal{C}$ est la j^{e} colonne de M .

Démonstration.

Notons $(m_{ij})_{(i,j) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket}$ les coefficients de M et $C_1, \dots, C_p$ les colonnes de M . Pour $j \in \llbracket 1, p \rrbracket$, on note v_j l'unique vecteur de E tel que $\text{Mat}_{\mathcal{C}}(v_j) = C_j$ (il s'agit du vecteur $m_{1j}f_1 + \dots + m_{nj}f_n$).

Soit alors $u \in \mathcal{L}(E, F)$. On a $M = \text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$ si et seulement si

$$\text{Mat}_{\mathcal{C}}(v_1, \dots, v_p) = \text{Mat}_{\mathcal{C}}(u(e_1), \dots, u(e_p)),$$

c'est-à-dire si et seulement si $\forall i \in \llbracket 1, p \rrbracket v_i = u(e_i)$, or on sait qu'il existe une unique application linéaire u vérifiant cette dernière condition.

Il existe donc une unique application linéaire u vérifiant $M = \text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$. $\square$

Remarque 2.2.8.

Dans le cas où les espaces vectoriels de départ et d'arrivée sont le même, la matrice de l'identité est I_n si on considère **la même base** au départ et à l'arrivée.



dans des bases différentes, la matrice de l'identité n'est pas l'identité ! Exemple : calculer $\text{Mat}_{\mathcal{B}, \mathcal{C}}(\text{Id}_{\mathbb{R}^2})$ où $\mathcal{C} = (\vec{i}, \vec{j})$ est la base canonique de $\mathbb{R}^2$ et $\mathcal{B} = (\vec{i} + \vec{j}, \vec{i} - \vec{j})$.

Proposition 2.2.9.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. La matrice de l'application linéaire canoniquement associée à M dans les bases canoniques de $\mathcal{M}_{n,1}(\mathbb{K})$ et $\mathcal{M}_{p,1}(\mathbb{K})$ est M .

Démonstration.

Notons u l'application canoniquement associée à M . Pour tout $k \in \llbracket 1, p \rrbracket$, l'image par u du k^{e} vecteur de la base canonique est la k^{e} colonne de M . Donc la matrice de u est la matrice des vecteurs colonnes de M dans la base canonique : c'est donc M . $\square$

Théorème 2.2.10.

On garde les mêmes notations. On considère l'application

$$\varphi : \begin{cases} (\mathcal{L}(E, F), +, \cdot) & \longrightarrow & (\mathcal{M}_{n,p}(\mathbb{K}), +, \cdot) \\ u & \longmapsto & \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) \end{cases}.$$

Alors, φ est un isomorphisme d'espaces vectoriels.

Démonstration.

On a déjà vu que cette application était bijective. Voir pourquoi elle est linéaire est laissé en exercice au lecteur.

Remarquons que, puisqu'on sait que les deux espaces vectoriels considérés sont de dimension finie et de même dimension, on aurait pu se dispenser de montrer précédemment qu'elle était injective ou se dispenser de montrer qu'elle était surjective. $\square$

Remarque 2.2.11. 1. Ceci justifie l'identification forme linéaire sur $\mathbb{K}^p$ / matrice ligne à p colonnes. Exemple.

2. Ce résultat permet au passage de dire que si $M \in \mathcal{M}_{p,n}(\mathbb{K})$ et $\forall X \in \mathcal{M}_{n,1}(\mathbb{K})$, $MX = 0$, alors $M = 0$. En effet, les applications $X \mapsto MX$ et $X \mapsto 0_n X$ sont alors égales, donc les matrices M et 0_n le sont.

Le résultat suivant est le résultat fondamental liant l'algèbre linéaire au calcul matriciel.

Proposition 2.2.12.

Avec les mêmes notations qu'en 2.2.1, on a

$$\forall x \in E \quad \text{Mat}_{\mathcal{C}}(u(x)) = \text{Mat}_{\mathcal{B},\mathcal{C}}(u) \times \text{Mat}_{\mathcal{B}}(x).$$

Démonstration.

Soit $x \in E$. Posons $M = \text{Mat}_{\mathcal{B},\mathcal{C}}(u)$ et $X = \text{Mat}_{\mathcal{B}}(x)$. Notons $(m_{ij})_{(i,j) \in \llbracket 1,n \rrbracket \times \llbracket 1,p \rrbracket}$ les coefficients de M , $(x_j)_{j \in \llbracket 1,p \rrbracket}$ ceux de X , $(y_i)_{i \in \llbracket 1,n \rrbracket}$ ceux de MX , $(e_j)_{j \in \llbracket 1,p \rrbracket}$ les vecteurs de la base $\mathcal{B}$ et $(f_i)_{i \in \llbracket 1,n \rrbracket}$ ceux de $\mathcal{C}$.

Alors, par définition du produit matriciel, on a

$$\forall i \in \llbracket 1,n \rrbracket \quad y_i = \sum_{j=1}^p m_{ij} x_j.$$

$$\text{Alors on a } x = \sum_{j=1}^p x_j e_j, \text{ donc } u(x) = \sum_{j=1}^p x_j u(e_j).$$

$$\text{Par ailleurs, pour tout } j \in \llbracket 1,p \rrbracket, u(e_j) = \sum_{i=1}^n m_{ij} f_i.$$

On a donc

$$\begin{aligned} u(x) &= \sum_{j=1}^p \sum_{i=1}^n x_j m_{ij} f_i \\ &= \sum_{i=1}^n \sum_{j=1}^p x_j m_{ij} f_i \\ &= \sum_{i=1}^n y_i f_i. \end{aligned}$$

Ainsi, $\text{Mat}_{\mathcal{C}}(u(x))$ a pour coefficients la famille $(y_i)_{i \in \llbracket 1,n \rrbracket}$. $\square$

Exemple 2.2.13.

Reprendre les deux premiers exemples de la série d'exemples précédente avec le vecteur $(17, 42)$.

Remarque 2.2.14.

On pourra représenter schématiquement ce résultat comme dans la figure XXVI.2 : avec $M = \text{Mat}_{\mathcal{B},\mathcal{C}}(u)$ et $\text{Mat}_{\mathcal{B}}(x)$, on a $\text{Mat}_{\mathcal{C}}(u(x)) = MX$.

Corollaire 2.2.15.

Avec les mêmes notations, soit $\mathcal{F}$ une famille de vecteurs de E , alors

$$\text{Mat}_{\mathcal{C}}(u(\mathcal{F})) = \text{Mat}_{\mathcal{B},\mathcal{C}}(u) \times \text{Mat}_{\mathcal{B}}(\mathcal{F}).$$

$$\begin{array}{ccc} x & & u(x) \\ E, \mathcal{B} & \xrightarrow[\quad M \quad]{\quad u \quad} & F, \mathcal{C} \\ X & & MX \end{array}$$

FIGURE XXVI.2 – Matrice de l'image d'un vecteur par une application linéaire.

Démonstration.

Il suffit d'appliquer la proposition 2.2.12 colonne par colonne. $\square$

Théorème 2.2.16.

Soient E, F, G trois $\mathbb{K}$ -ev de bases $\mathcal{B}, \mathcal{C}, \mathcal{D}$. Soient $f \in \mathcal{L}(F, G)$, $g \in \mathcal{L}(E, F)$. Alors

$$\text{Mat}_{\mathcal{B},\mathcal{D}}(f \circ g) = \text{Mat}_{\mathcal{C},\mathcal{D}}(f) \times \text{Mat}_{\mathcal{B},\mathcal{C}}(g).$$

Démonstration.

En utilisant le corollaire 2.2.15 :

$$\begin{aligned} \text{Mat}_{\mathcal{B},\mathcal{D}}(f \circ g) &= \text{Mat}_{\mathcal{D}}(f \circ g(\mathcal{B})) \\ &= \text{Mat}_{\mathcal{D}}(f(g(\mathcal{B}))) \\ &= \text{Mat}_{\mathcal{C},\mathcal{D}}(f) \times \text{Mat}_{\mathcal{C}}(g(\mathcal{B})) \\ &= \text{Mat}_{\mathcal{C},\mathcal{D}}(f) \times \text{Mat}_{\mathcal{B},\mathcal{C}}(g). \end{aligned}$$

$\square$

Remarque 2.2.17.

Ce résultat peut être vu comme LA raison pour laquelle le produit matriciel est associatif. On peut en effet en tirer une démonstration non calculatoire de l'associativité du produit matriciel : étant donné trois matrices A, B, C telles que le produit $A(BC)$ soit bien défini, il suffit de choisir quatre espaces vectoriels, des bases de ces espaces vectoriels et trois applications f, g et h telles que les matrices A, B et C soient respectivement celles de f, g et h . Alors $A(BC)$ est la matrice de $f \circ (g \circ h)$ et $(AB)C$ est celle de $(f \circ g) \circ h$. Or la composition d'application est associative donc ces deux applications sont égales, donc $A(BC) = (AB)C$.

On laisse au lecteur le soin de vérifier que la propriété d'associativité du produit matriciel n'a pas été utilisée dans la démonstration ci-dessus ni dans les résultats ou définitions qu'elle utilise.

Remarque 2.2.18.

On pourra représenter schématiquement ce résultat comme dans la figure XXVI.3 : avec

$M = \text{Mat}_{\mathcal{C}, \mathcal{D}}(f)$ et $N = \text{Mat}_{\mathcal{B}, \mathcal{C}}(g)$, on a $\text{Mat}_{\mathcal{B}, \mathcal{D}}(f \circ g) = MN$. On réalise alors ce que

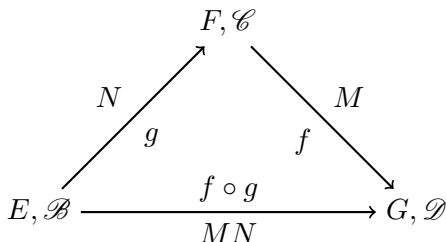


FIGURE XXVI.3 – Diagramme de composition d'applications linéaires et de leurs représentations matricielles.

l'on peut appeler un *diagramme de composition commutatif* : les applications obtenues en composant plusieurs flèches ayant même départ et même origine sont identiques.

Exemple 2.2.19.

Choisir deux applications $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ et $g : \mathbb{R}^2 \rightarrow \mathbb{R}^3$, faire les calculs.

Définition 2.2.20.

Soient $(A_1, +, \times)$ et $(A_2, +, \times)$ deux anneaux, et $\varphi : A_1 \rightarrow A_2$. On dit que φ est un morphisme d'anneaux si c'est un morphisme de groupes pour la loi $+$ et $\varphi(1_{A_1}) = 1_{A_2}$ et $\forall x, y \in A_1 \quad \varphi(x \times y) = \varphi(x) \times \varphi(y)$

Remarque 2.2.21.

Ne pas oublier la condition $\varphi(1_{A_1}) = 1_{A_2}$. L'application suivante, qui vérifie toutes les autres conditions, n'est en effet pas un morphisme d'anneau :

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \rightarrow & \mathbb{Z}/6\mathbb{Z} \\ 0 & \mapsto & 0 \\ 1 & \mapsto & 3 \end{array}$$

Corollaire 2.2.22.

Soit E un $\mathbb{K}$ -ev de dim n , et $\mathcal{B}$ une base de E . Alors, l'application

$$\varphi : \left\{ \begin{array}{ccc} (\mathcal{L}(E), +, \circ) & \rightarrow & (\mathcal{M}_n(\mathbb{K}), +, \times) \\ u & \mapsto & \text{Mat}_{\mathcal{B}}(u) \end{array} \right.$$

est un isomorphisme d'anneaux.

Démonstration.

Le théorème 2.2.10 assure que c'est un isomorphisme de groupes pour la loi $+$, le théorème 2.2.16 montre que l'image du produit est le produit des images et l'image du neutre de $\mathcal{L}(E)$ pour la composition (qui est l'application identité sur E) est le neutre de $\mathcal{M}_n(\mathbb{K})$ pour le produit (qui est I_n). $\square$

2.3 Inversibilité.

Proposition 2.3.1.

La matrice d'une application linéaire est inversible si et seulement si cette application linéaire est un isomorphisme. Dans ce cas, l'inverse de la matrice considérée est la matrice de l'application réciproque de l'isomorphisme considéré.

Démonstration.

Soit E et F deux espaces vectoriels de dimensions finies respectives p et n . Soit $\mathcal{B}$ une base de E et $\mathcal{C}$ une base de F . Soit $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, E)$. Posons $A = \text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$ et $B = \text{Mat}_{\mathcal{C}, \mathcal{B}}(v)$.

On a :

$$\begin{aligned} u \circ v = \text{Id}_F &\iff \text{Mat}_{\mathcal{C}, \mathcal{C}}(u \circ v) = I_n \\ &\iff \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) \times \text{Mat}_{\mathcal{C}, \mathcal{B}}(v) = I_n \\ &\iff AB = I_n \end{aligned}$$

De même

$$v \circ u = \text{Id}_E \iff BA = I_p$$

En particulier, si u est un isomorphisme, d'isomorphisme réciproque v , alors $AB = I_n$ et $BA = I_p$. De plus, on a alors $\dim E = \dim F$, donc $n = p$. Donc A est une matrice carrée et B est son inverse.

Réciproquement, si $u \in \mathcal{L}(E, F)$ possède une matrice inversible A , alors en notant v l'unique application linéaire telle que $A^{-1} = \text{Mat}_{\mathcal{C}, \mathcal{B}}(v)$, on a $u \circ v = \text{Id}_F$ et $v \circ u = \text{Id}_E$. $\square$

Remarque 2.3.2.

Soit M une matrice carrée, u l'endomorphisme qui lui est canoniquement associé. On peut utiliser la proposition précédente pour montrer que M est inversible et déterminer, le cas échéant, son inverse.

- On commence par prendre X, Y deux vecteurs colonne ayant autant de lignes que M .
- On résout en X le système $MX = Y$.
- S'il y a toujours existence et unicité de la solution, on lit $X = M^{-1}Y$.

Cela correspond bien à ce qui était fait auparavant, la proposition précédente justifie bien que l'on puisse conclure à l'inversibilité de M directement, et obtenir son inverse.

Exemple 2.3.3.

Montrer que la matrice

$$M = \begin{pmatrix} 4 & 2 & -1 \\ 1 & 0 & 1 \\ 3 & -1 & 2 \end{pmatrix}$$

est inversible et déterminer son inverse.

Corollaire 2.3.4.

Soit A et B deux matrices carrées de taille n . Alors $AB = I_n$ si et seulement si A et B sont inversibles et sont inverses l'une de l'autre.

Il est donc équivalent pour une matrice (carrée) d'être :

1. inversible ;
2. inversible à gauche ;
3. inversible à droite.

Démonstration.

Pour montrer cette équivalence, il suffit de montrer le sens direct, l'autre découlant directement de la définition d'inverse.

Supposons donc $AB = I_n$.

Notons u et v les applications linéaires canoniquement associées respectivement à A et B relativement à la base canonique.

En reprenant la démonstration précédente, on peut remarquer que $u \circ v = \text{Id}_{\mathbb{K}^n}$, donc v est un endomorphisme injectif et u un endomorphisme surjectif.

La dimension de $\mathbb{K}^n$ étant finie, u et v sont donc des automorphismes et on a $v = u^{-1} \circ u \circ v = u^{-1} \circ \text{Id}_{\mathbb{K}^n} = u^{-1}$.

Donc d'après la proposition précédente A et B sont inversibles et sont inverses l'une de l'autre. $\square$

Corollaire 2.3.5.

Dans un espace vectoriel E de dimension finie n , la matrice d'une famille de vecteurs est inversible si et seulement si cette famille de vecteurs est une base.

Démonstration.

Pour que la matrice soit inversible, il est nécessaire qu'elle soit carrée. Pour que la famille de vecteurs soit une base, il est nécessaire qu'elle possède exactement n vecteurs. On

peut donc se restreindre au cas d'une famille de n vecteurs $v_1, \dots, v_n$ et de la matrice M associée relativement à une base $\mathcal{B}$ de E . Notons $(e_1, \dots, e_n)$ les vecteurs de $\mathcal{B}$.

Notons u l'unique endomorphisme de E tel que $\text{Mat}_{\mathcal{B}}(u) = M$.

M est inversible si et seulement si u est un automorphisme. E étant de dimension finie, cela est équivalent à u surjective, c'est-à-dire à $\text{rg } u = n$. Or $\text{rg } u = \text{rg}(u(e_1), \dots, u(e_n)) = \text{rg}(v_1, \dots, v_n)$. Donc M est inversible si et seulement si $(v_1, \dots, v_n)$ est génératrice. Or $\dim E = n$ donc cela est équivalent à $(v_1, \dots, v_n)$ est une base. $\square$

Corollaire 2.3.6.

Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si ses colonnes forment une base de $\mathcal{M}_{n,1}(\mathbb{K})$ et si et seulement si ses lignes forment une base de $\mathcal{M}_{1,n}(\mathbb{K})$.

Démonstration.

Considérer la famille des colonnes de M et la base canonique de $\mathbb{K}^n$, puis transposer. $\square$

Remarque 2.3.7.

Ainsi, s'il y a une relation de dépendance entre les colonnes de M , M n'est pas inversible.

Exemple 2.3.8.

$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ -1 & 1 & 0 \end{pmatrix}$ n'est pas inversible.

Remarque 2.3.9.

Retour sur $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, qui est inversible si et seulement si $ad - bc \neq 0$, i.e. si et seulement si les colonnes $\begin{pmatrix} a \\ c \end{pmatrix}$ et $\begin{pmatrix} b \\ d \end{pmatrix}$ sont linéairement indépendantes.

2.4 Matrices de passage.

Dans cette section E est un $\mathbb{K}$ -ev de dimension finie n , et $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ sont des bases de E .

Une question se pose maintenant naturellement : peut-on relier les matrices d'un vecteur ou d'une application linéaire exprimées dans des bases différentes ?

Définition 2.4.1.

On appelle *matrice de passage de $\mathcal{B}$ dans $\mathcal{B}'$* la matrice $\text{Mat}_{\mathcal{B}}(\mathcal{B}')$. On la note parfois $P_{\mathcal{B}}^{\mathcal{B}'}$.

Exemple 2.4.2.

$E = \mathbb{R}^2$: $\mathcal{B} = ((0, 1), (1, 1)) = (f_1, f_2)$, $\mathcal{B}' = ((1, -1), (0, 1)) = (g_1, g_2)$.

$g_1 = f_2 - 2f_1$ et $g_2 = f_1$, donc $\text{Mat}_{\mathcal{B}}(\mathcal{B}') = \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}$.

Théorème 2.4.3.

On note $P = \text{Mat}_{\mathcal{B}}(\mathcal{B}')$ et $P' = \text{Mat}_{\mathcal{B}'}(\mathcal{B}'')$.

1. $P = \text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E)$.
2. P est inversible et son inverse est $\text{Mat}_{\mathcal{B}'}(\mathcal{B})$ (matrice de passage de $\mathcal{B}'$ dans $\mathcal{B}$).
3. La matrice de passage de $\mathcal{B}$ dans $\mathcal{B}''$ est $\text{Mat}_{\mathcal{B}}(\mathcal{B}'') = PP' = \text{Mat}_{\mathcal{B}}(\mathcal{B}') \times \text{Mat}_{\mathcal{B}'}(\mathcal{B}'')$ (« transitivité »).

Remarque 2.4.4.

On pourra représenter schématiquement le point 1 comme dans la figure XXVI.4.

$$E, \mathcal{B} \xleftarrow[\underset{P_{\mathcal{B}}^{\mathcal{B}'}}]{\overset{\text{Id}_E}{\longrightarrow}} E, \mathcal{B}'$$

FIGURE XXVI.4 – Application linéaire représentée par une matrice de passage.

Ce schéma sera le bloc fondamental de tous les schémas que nous écrirons lors de changements de base : retenez-le bien !

Remarque 2.4.5.

On pourra représenter schématiquement le point 2 comme dans la figure XXVI.5.

Remarque 2.4.6.

On pourra représenter schématiquement le point 3 comme dans la figure XXVI.6.

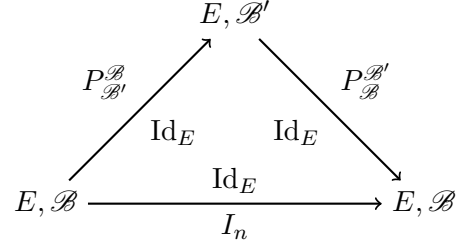


FIGURE XXVI.5 – Inverse d'une matrice de passage.

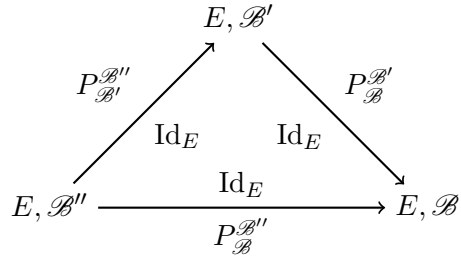


FIGURE XXVI.6 – Composition de changements de base.

Démonstration. 1. Notons $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (f_1, \dots, f_n)$. On a

$$\begin{aligned} \text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E) &= \text{Mat}_{\mathcal{B}}(\text{Id}_E(f_1), \dots, \text{Id}_E(f_n)) \\ &= \text{Mat}_{\mathcal{B}}(f_1, \dots, f_n) \\ &= \text{Mat}_{\mathcal{B}}(\mathcal{B}') \end{aligned}$$

2. $P = \text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E)$, or $\text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E) \cdot \text{Mat}_{\mathcal{B}, \mathcal{B}'}(\text{Id}_E) = \text{Mat}_{\mathcal{B}, \mathcal{B}}(\text{Id}_E \circ \text{Id}_E) = \text{Mat}_{\mathcal{B}, \mathcal{B}}(\text{Id}_E) = I_n$, donc P est inversible et $P^{-1} = \text{Mat}_{\mathcal{B}, \mathcal{B}'}(\text{Id}_E)$ d'après le corollaire 2.3.4, et donc $P^{-1} = \text{Mat}_{\mathcal{B}'}(\mathcal{B})$ d'après le premier point.

3. On utilise à nouveau (i) : $\text{Mat}_{\mathcal{B}}(\mathcal{B}') \cdot \text{Mat}_{\mathcal{B}', \mathcal{B}''}(\text{Id}_E) = \text{Mat}_{\mathcal{B}, \mathcal{B}''}(\text{Id}_E \circ \text{Id}_E) = \text{Mat}_{\mathcal{B}, \mathcal{B}''}(\text{Id}_E) = \text{Mat}_{\mathcal{B}}(\mathcal{B}'')$. □

Le théorème suivant motive l'utilisation des matrices de passage.

Théorème 2.4.7 (Changement de base).

Les matrices de passages permettent de relier les matrices d'un même vecteur ou d'une même application relativement à des bases différentes :

Pour un vecteur Soit $x \in E$. On note $X = \text{Mat}_{\mathcal{B}}(x)$ et $X' = \text{Mat}_{\mathcal{B}'}(x)$, et $P = \text{Mat}_{\mathcal{B}}(\mathcal{B}')$. Alors $X = PX'$.

Pour une application linéaire Avec les mêmes notations et en notant de plus F un $\mathbb{K}$ -ev de dimension finie, $\mathcal{C}$ et $\mathcal{C}'$ deux bases de F , $u \in \mathcal{L}(E, F)$, et enfin $Q = \text{Mat}_{\mathcal{C}}(\mathcal{C}')$. Alors $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u) = Q^{-1} \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) P$.



La formule de changement de base pour un vecteur s'écrit $X = PX'$, et non $X' = PX$ (c'est une source d'erreur fréquente). Au moindre doute, n'hésitez pas à tracer le schéma correspondant.

Remarque 2.4.8.

Le premier point correspond au schéma de la figure XXVI.7.

$$\begin{array}{ccc} x & & x \\ E, \mathcal{B} & \xleftarrow[\text{Mat}_{\mathcal{B}}(\mathcal{B}')]{\text{Id}_E} & E, \mathcal{B}' \\ X & & X' \end{array}$$

FIGURE XXVI.7 – Illustration de la relation de changement de bases pour un vecteur.

Remarque 2.4.9.

Le second point correspond au schéma de la figure XXVI.8.

Démonstration. Pour un vecteur il suffit de traduire l'égalité $x = \text{Id}_E(x)$ dans les bonnes bases : x dans la base $\mathcal{B} = \text{Id}(x)$ dans la base $\mathcal{B}'$, soit : $X = \text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E) X' = P X'$.

Pour une application linéaire On traduit à nouveau $u(x) = u(x)$ dans les bonnes bases :

$$\begin{aligned} \text{Mat}_{\mathcal{B}', \mathcal{C}'}(u) &= \text{Mat}_{\mathcal{B}', \mathcal{C}'}(\text{Id}_F \circ u \circ \text{Id}_E) \\ &= \text{Mat}_{\mathcal{C}, \mathcal{C}'}(\text{Id}_F) \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) \text{Mat}_{\mathcal{B}', \mathcal{B}}(\text{Id}_E) \\ &= Q^{-1} \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) P \end{aligned}$$

□

Remarque 2.4.10.

Avec $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et $f \in \mathcal{L}(E)$, on a $\text{Mat}_{\mathcal{B}'}(f) = [P_{\mathcal{B}}^{\mathcal{B}'}]^{-1} \times \text{Mat}_{\mathcal{B}}(f) \times P_{\mathcal{B}}^{\mathcal{B}'}$. On essaiera, pour chaque changement de base, de

$$\begin{array}{ccc} E, \mathcal{B} & \xrightarrow[\text{Mat}_{\mathcal{B}, \mathcal{C}}(f)]{\text{Id}_E} & F, \mathcal{C} \\ \uparrow P_{\mathcal{B}}^{\mathcal{B}'} & & \downarrow \text{Id}_F \\ E, \mathcal{B}' & \xrightarrow[\text{Mat}_{\mathcal{B}', \mathcal{C}'}(f)]{f} & F, \mathcal{C}' \end{array} \quad \left[P_{\mathcal{C}}^{\mathcal{C}'} \right]^{-1} = P_{\mathcal{C}'}^{\mathcal{C}}$$

FIGURE XXVI.8 – Illustration de la relation de changement de bases pour une application linéaire.

$$\begin{array}{ccc} \mathcal{B} & \xrightarrow[\text{Mat}_{\mathcal{B}}(f)]{\text{Id}} & \mathcal{B} \\ \uparrow P_{\mathcal{B}}^{\mathcal{B}'} & & \downarrow \text{Id} \\ \mathcal{B}' & \xrightarrow[\text{Mat}_{\mathcal{B}'}(f)]{f} & \mathcal{B}' \end{array} \quad \left[P_{\mathcal{B}}^{\mathcal{B}'} \right]^{-1} = P_{\mathcal{B}'}^{\mathcal{B}}$$

FIGURE XXVI.9 – Illustration de la relation de changement de bases pour un endomorphisme.

reproduire le schéma de la figure XXVI.9 pour se rappeler de cette formule.

Exemple 2.4.11.

Mêmes choses que dans l'exemple 2.4.2. $F = \mathbb{R}^3$, $\mathcal{C} = (e_1, e_2, e_3)$ (base canonique), $\mathcal{C}' = (h_1, h_2, h_3)$ avec $h_1 = e_1$, $h_2 = (1, 1, 0) = e_1 + e_2$, $h_3 = (-1, 0, 1) = -e_1 + e_3$.

On considère

$$u : \begin{cases} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ (x, y) & \longmapsto & (x - y, x, 2x + y). \end{cases}$$

1. Déterminer $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$.
2. Déterminer P et Q^{-1} , en déduire $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u)$.

3. Vérifier en exprimant $u(g_i)$ en fonction des h_j .

Exemple 2.4.12.

On donne $\mathcal{C}$ = base canonique de $\mathbb{R}^3$ et $\mathcal{B}' = ((1, 0, -1), (1, 0, 2), (0, 1, -1)) = (v_1, v_2, v_3)$, et $x = 2v_1 + 2v_2 - v_3$. Exprimer x en fonction de e_1, e_2, e_3 .

Remarque 2.4.13.

Ceci permet de voir que pour inverser une matrice, il suffit d'inverser la matrice de passage sous-jacente, et donc d'inverser un système linéaire.

Exemple 2.4.14.

Inverser $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & -1 & 1 \end{pmatrix}$ en passant par des matrices de passage.

Remarque 2.4.15.

On appelle $P = \text{Mat}_{\mathcal{B}}(\mathcal{B}')$ « matrice de passage de $\mathcal{B}$ dans $\mathcal{B}'$ » car elle permet de transformer une équation exprimée dans $\mathcal{B}$ en équation exprimée dans $\mathcal{B}'$. En effet, avec φ une forme linéaire et $L = \text{Mat}_{\mathcal{B},1}(\varphi)$, l'équation cartésienne de $\text{Ker } \varphi$ (c'est un hyperplan) s'écrit, dans la base $\mathcal{B}$, $LX = 0$. Dans la base $\mathcal{B}'$, cela s'écrit alors $LPX' = 0$. La ligne donnant l'équation dans la base $\mathcal{B}'$ est donc LP .

3 Matrices remarquables.

3.1 Matrices triangulaires.

Définition 3.1.1.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. On dit que A est *triangulaire supérieure* (resp. *inférieure*) si $\forall i, j \in \llbracket 1, n \rrbracket$ tels que $i > j$ (resp. $i < j$), $a_{ij} = 0$.

On note $\tau_n^+(\mathbb{K})$ (resp. $\tau_n^-(\mathbb{K})$) l'ensemble des matrices triangulaires supérieures (resp. inférieures) d'ordre n .

Théorème 3.1.2.

$(\tau_n^\pm(\mathbb{K}), +, \times)$ est un anneau et $(\tau_n^\pm(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$ -ev de dimension $\frac{n(n+1)}{2}$.

Démonstration.

• $\mathbb{K}$ -ev : élémentaire.

• Anneau : soient $A, B \in \tau_n^+(\mathbb{K})$. On note $AB = (\gamma_{ij})$. On

suppose $i > j$, alors $\gamma_{ij} = \sum_{k=1}^{i-1} a_{ik}b_{kj} + \sum_{k=i}^n a_{ik}b_{kj}$, et tous les termes sont nuls.

• Dimension : les E_{ij} avec $i \leq j$ est une famille libre (déjà vu) et génératrice. Elle comporte $\frac{n(n+1)}{2}$ vecteurs. $\square$

Remarque 3.1.3.

Avec cette démonstration on voit que $\gamma_{ii} = a_{ii}b_{ii}$.

Théorème 3.1.4.

Une matrice triangulaire est inversible si et seulement si elle n'a aucun zéro sur sa diagonale.

Démonstration.

Soit A triangulaire sup. d'ordre n . On note $(v_1, \dots, v_n)$ la famille de vecteurs telle que $A = \text{Mat}_{\mathcal{B}}(v_1, \dots, v_n)$, avec $\mathcal{B}$ base canonique de $\mathbb{K}^n$.

• Si pas de zéro sur la diag. : on montre que $(v_1, \dots, v_n)$ est libre, avec $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$, on pose le système, on résout : même pas besoin de faire de pivot de Gauss. Donc c'est une base, donc c'est inversible.

• S'il y a un zéro à la k^e position, alors $(v_1, \dots, v_k)$ ont tous des zéros après leur $(k-1)^e$ coordonnées, donc sont dans $\text{Vect}(e_1, \dots, e_{k-1})$, ils sont donc liés. $\square$

Lemme 3.1.5.

Soit E un espace vectoriel de dimension n et $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . Pour $k \in \llbracket 1, n \rrbracket$, on pose $E_k = \text{Vect}(e_1, \dots, e_k)$. Soit $u \in \mathcal{L}(E)$ et $M = \text{Mat}_{\mathcal{B}}(u)$.

Alors M est triangulaire supérieure si et seulement si pour tout $k \in \llbracket 1, n \rrbracket$, E_k est stable par u .

Démonstration.

Soit $k \in \llbracket 1, n \rrbracket$. Pour que E_k soit stable par u , il faut que $u(e_k) \in E_k$, c'est-à-dire que seuls les k premières lignes de la matrice colonne des coordonnées de $u(e_k)$ dans $\mathcal{B}$ soient non nulles.

Or la matrice M de u est la matrice formée de ces colonnes. Pour que tous les E_k , pour $k \in \llbracket 1, n \rrbracket$ soient stables par u , il est donc nécessaire qu'elle soit triangulaire supérieure.

Réciproquement, supposons que cette matrice soit triangulaire supérieure. Alors pour tout $k \in \llbracket 1, n \rrbracket$ et tout $i \in \llbracket 1, k \rrbracket$, on a $u(e_i) \in E_i \subset E_k$. Donc pour tout $k \in \llbracket 1, n \rrbracket$, $u(E_k) \subset \text{Vect}(u(e_1), \dots, u(e_k)) \subset E_k$. $\square$

Remarque 3.1.6.

Ce résultat s'adapte aux matrices triangulaires inférieures, en posant $E_1 = \text{Vect}(e_k)$, $E_2 = \text{Vect}(e_{k-1}, e_k), \dots$

Théorème 3.1.7.

L'inverse d'une matrice triangulaire supérieure (resp. inférieure) inversible est également triangulaire supérieure (resp. inférieure).

Démonstration.

Nous donnons la démonstration pour les matrices triangulaires supérieures. Pour les matrices triangulaires inférieures, on peut exploiter la remarque ci-dessus ou utiliser les résultats sur la transposée en remarquant que la transposée d'une matrice triangulaire supérieure est triangulaire inférieure et vice-versa.

Soit $M \in \tau_n^+(\mathbb{K}) \cap \text{GL}_n(\mathbb{K})$.

On choisit E un espace vectoriel de dimension n , $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et on note u l'endomorphisme de E de matrice M relativement à $\mathcal{B}$.

M étant inversible, u est bijective.

D'après le lemme, tous les E_k sont stables par u . En appliquant le lemme, il suffit de montrer qu'ils sont stables par u^{-1} pour montrer que $\text{Mat}_{\mathcal{B}}(u^{-1}) = M^{-1}$ est triangulaire supérieure.

Soit $k \in \llbracket 1, n \rrbracket$. On a $u(E_k) \subset E_k$, donc $E_k \subset u^{-1}(E_k)$. Or $\dim u^{-1}(E_k) = \dim E_k$ (image d'un sous-espace vectoriel par un morphisme bijectif), donc $u^{-1}(E_k) = E_k$. On a donc l'inclusion souhaitée : u^{-1} est donc triangulaire supérieure. $\square$

3.2 Matrices diagonales.

Définition 3.2.1.

On appelle *matrice diagonale* toute matrice carrée $(a_{ij})_{1 \leq i, j \leq n}$ telle que pour tous $i, j \in \llbracket 1, n \rrbracket$, $i \neq j \Rightarrow a_{ij} = 0$.

On note $\mathcal{D}_n(\mathbb{K})$ l'ensemble des matrices diagonales d'ordre n .

Remarque 3.2.2.

- On note $\text{diag}(\lambda_1, \dots, \lambda_n)$ la matrice diagonale dont les termes diagonaux sont $(\lambda_1, \dots, \lambda_n)$.
- $\mathcal{D}_n(\mathbb{K}) = \tau_n^+(\mathbb{K}) \cap \tau_n^-(\mathbb{K})$.

Définition 3.2.3.

On appelle *matrice scalaire* toute matrice diagonale dont les coeffs de la diagonale sont tous égaux, i.e. de la forme λI_n .

Théorème 3.2.4.

$(\mathcal{D}_n(\mathbb{K}), +, \times)$ est un anneau et $(\mathcal{D}_n(\mathbb{K}), +, \cdot)$ est un $\mathbb{K}$ -ev de dimension n .

Démonstration.

Anneau et ev : immédiat avec $\mathcal{D}_n(\mathbb{K}) = \tau_n^+(\mathbb{K}) \cap \tau_n^-(\mathbb{K})$.
Dimension : $(E_{ii})_{1 \leq i \leq n}$ en forme une base. $\square$

Remarque 3.2.5.

Une matrice diagonale est inversible si et seulement si tous ses coefficients diagonaux sont non nuls. Et dans ce cas $\text{diag}(\lambda_1, \dots, \lambda_n)^{-1} = \text{diag}\left(\frac{1}{\lambda_1}, \dots, \frac{1}{\lambda_n}\right)$.

De plus, pour tout $p \in \mathbb{N}$, $(\text{diag}(\lambda_1, \dots, \lambda_n))^p = \text{diag}(\lambda_1^p, \dots, \lambda_n^p)$. Et si aucun coefficient diagonal n'est nul, cette relation est aussi valable pour $p \in \mathbb{Z}$.

3.3 Matrices symétriques et antisymétriques.

Rappel 3.3.1.

$A \in \mathcal{M}_n(\mathbb{K})$ est dite *symétrique* (resp. *antisymétrique*) si $A = A^\top$ (resp. $A = -A^\top$).

On note souvent $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques de dimension n à coefficients dans $\mathbb{K}$, et $\mathcal{A}_n(\mathbb{K})$ celui des matrices antisymétriques.

Théorème 3.3.2.

L'ensemble des matrices symétriques (resp. antisymétriques) muni de $+$ et $\cdot$ est un $\mathbb{K}$ -ev de dimension $\frac{n(n+1)}{2}$ (resp. $\frac{n(n-1)}{2}$).

De plus, $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont supplémentaires dans $\mathcal{M}_n(\mathbb{K})$.

Démonstration.

Ce sont respectivement les noyaux de $A \mapsto A^\top - A$ et $A \mapsto A^\top + A$, donc ce sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$.

Soit $M = (m_{ij}) \in \mathcal{M}_n(\mathbb{K})$. On a $M \in \mathcal{S}_n(\mathbb{K})$ si et seulement si pour tout i, j , $m_{i,j} = m_{j,i}$. Si $M \in \mathcal{S}_n(\mathbb{K})$, on a donc

$$M = \sum_{i=1}^n m_{i,i} E_{i,i} + \sum_{1 \leq i < j \leq n} m_{i,j} (E_{i,j} + E_{j,i}).$$

Ainsi, la famille $(E_{i,i})_{1 \leq i \leq n} \cup (E_{i,j} + E_{j,i})_{1 \leq i < j \leq n}$ engendre $\mathcal{S}_n(\mathbb{K})$. On vérifie aisément que cette famille est libre : c'est

donc une base de $\mathcal{S}_n(\mathbb{K})$, et elle contient bien $n(n+1)/2$ vecteurs.

De même, si $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{K})$, on a $M \in \mathcal{A}_n(\mathbb{K})$ si et seulement si pour tout i, j , $m_{i,j} = -m_{j,i}$. La famille $(E_{i,j} - E_{j,i})_{1 \leq i < j \leq n}$ est libre, c'est donc une base de $\mathcal{A}_n(\mathbb{K})$, et elle contient bien $n(n-1)/2$ vecteurs.

Enfin, si $M \in \mathcal{A}_n(\mathbb{K}) \cap \mathcal{S}_n(\mathbb{K})$, on a $M = M^\top = -M^\top$, donc $M = 0$. $\mathcal{A}_n(\mathbb{K})$ et $\mathcal{S}_n(\mathbb{K})$ sont donc en somme directe, la somme de leurs dimensions vaut n^2 , d'où le résultat.

On pouvait aussi observer que $s : A \mapsto A^\top$ est une symétrie vectorielle de $\mathcal{M}_n(\mathbb{K})$, donc que $\mathcal{A}_n(\mathbb{K}) = \text{Ker}(s + \text{Id})$ et $\mathcal{S}_n(\mathbb{K}) = \text{Ker}(s - \text{Id})$ sont supplémentaires. $\square$



Ce ne sont pas des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$!

Exemple 3.3.3.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Exercice 3.3.4.

Montrer, sans utiliser leurs dimensions, que $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont supplémentaires dans $\mathcal{M}_n(\mathbb{K})$.

4 Rang d'une matrice.

4.1 Définitions.

Remarque 4.1.1. 1. Soit E et F deux $\mathbb{K}$ -espaces vectoriels et $\varphi : E \rightarrow F$ un isomorphisme de E sur F .

Soit $p \in \mathbb{N}$ et $(x_i)_{i \in [1,p]}$ une famille d'éléments de E .

Alors φ réalise une bijection de $\text{Vect}(x_1, \dots, x_p)$ sur $\text{Vect}(\varphi(x_1), \dots, \varphi(x_p))$, donc les familles $(x_i)_{i \in [1,p]}$ et $(\varphi(x_i))_{i \in [1,p]}$ ont même rang.

2. En particulier, soit n un entier et soit F un espace vectoriel de dimension finie n , muni d'une base $\mathcal{B}$. L'application

$$\begin{aligned} \varphi : F &\rightarrow \mathcal{M}_{n,1}(\mathbb{K}) \\ x &\mapsto \text{Mat}_{\mathcal{B}}(x) \end{aligned}$$

est une bijection, donc pour toute famille $(x_i)_{i \in [1,p]}$ d'éléments de F , $(\text{Mat}_{\mathcal{B}}(x_i))_{i \in [1,p]}$ est une famille de même rang.

3. Par ailleurs, soit E et F deux espaces vectoriels de dimensions finies respectives p et n et $(e_1, \dots, e_p)$ une base de E . Alors pour toute application linéaire u de E dans F , on a

$$\begin{aligned} \text{Im}(u) &= u(\text{Vect}(e_1, \dots, e_p)) \\ &= \text{Vect}(u(e_1), \dots, u(e_p)) \end{aligned}$$

$$\text{donc } \text{rg}(u) = \text{rg}(u(e_1), \dots, u(e_p)).$$

Définition 4.1.2.

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. Notons $C_1, \dots, C_p$ les colonnes de A . Alors on appelle *rang de A* et on note $\text{rg}(A)$ l'entier $\text{rg}(C_1, \dots, C_p)$.

Remarque 4.1.3.

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors

1. Pour tout $r \in [0, p]$ et tout choix de r colonnes $C_1, \dots, C_r$ de A , la famille $(C_1, \dots, C_r)$ est de rang inférieur ou égal à $\text{rg } A$. C'est une conséquence du fait que l'espace engendré par $C_1, \dots, C_r$ est inclus dans $\text{Im } A$.
2. Il existe un choix de $\text{rg}(A)$ colonnes de A , $C_1, \dots, C_{\text{rg}(A)}$ tel que $\text{Vect}(C_1, \dots, C_{\text{rg}(A)}) = \text{Im}(A)$. En effet, la famille des colonnes de A est une famille génératrice d'un sous-espace vectoriel de $\mathbb{K}^n$ de dimension $\text{rg}(A)$, on peut donc en extraire une base, qui comporte nécessairement $\text{rg}(A)$ vecteurs colonnes.

Théorème 4.1.4.

Soit E et F deux espaces vectoriels de dimensions finies respectives p et n , de bases respectives $\mathcal{B}$ et $\mathcal{C}$, et $u \in \mathcal{L}(E, F)$. Alors $\text{rg}(u) = \text{rg}(\text{Mat}_{\mathcal{B}, \mathcal{C}}(u))$.

Démonstration.

En notant A la matrice $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$, $C_1, \dots, C_p$ ses colonnes et $e_1, \dots, e_p$ les vecteurs de $\mathcal{B}$, on a

$$\text{rg}(A) = \text{rg}(C_1, \dots, C_p) = \text{rg}(u(e_1), \dots, u(e_p)) = \text{rg}(u).$$

$\square$

Théorème 4.1.5.

Soit F un $\mathbb{K}$ -espace vectoriel de dimension finie de base $\mathcal{C}$, $(v_1, \dots, v_p)$ une famille de vecteurs de F . Alors $\text{rg}(\text{Mat}_{\mathcal{C}}(v_1, \dots, v_p)) = \text{rg}(v_1, \dots, v_p)$.

Démonstration.

En notant A la matrice $\text{Mat}_{\mathcal{C}}(v_1, \dots, v_p)$, et $C_1, \dots, C_p$ ses colonnes, on a

$$\text{rg}(A) = \text{rg}(C_1, \dots, C_p) = \text{rg}(v_1, \dots, v_p).$$

□

Théorème 4.1.6.

$A \in \mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si $\text{rg } A = n$.

Démonstration.

Soient $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$, et $(v_1, \dots, v_n)$ une famille de vecteurs de E telle que $A = \text{Mat}_{\mathcal{B}}(v_1, \dots, v_n)$. Alors A est inversible si et seulement si $(v_1, \dots, v_n)$ est une base de E si et seulement si $\text{rg}(v_1, \dots, v_n) = n$ si et seulement si $\text{rg } A = n$. □

Exercice 4.1.7.

Calculer les rangs suivants.

- $\text{rg} \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$;
- $\text{rg}(\text{diag}(\lambda_1, \dots, \lambda_n))$;
- $\text{rg} \begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Définition 4.1.8.

Soit n et p deux entiers. On dit qu'une matrice A de $\mathcal{M}_{n,p}(\mathbb{K})$ est *équivalente* à une autre matrice B de $\mathcal{M}_{n,p}(\mathbb{K})$ s'il existe deux matrices $P \in \mathcal{M}_n(\mathbb{K})$ et $Q \in \mathcal{M}_p(\mathbb{K})$ inversibles telles que $A = PBQ$.

Proposition 4.1.9.

La relation « être équivalente à » sur l'ensemble des matrices de $\mathcal{M}_{n,p}(\mathbb{K})$ est une relation d'équivalence.

Démonstration.

Cette relation est

Réflexive car pour toute $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $A = I_n A I_p$ et I_n et I_p sont inversibles ;

Symétrique car pour tout $(A, B) \in (\mathcal{M}_{n,p}(\mathbb{K}))^2$ tel que A et B sont équivalentes, il existe deux matrices $P \in \mathcal{M}_n(\mathbb{K})$ et $Q \in \mathcal{M}_p(\mathbb{K})$ inversibles telles que $A = PBQ$, et on a alors $B = P^{-1}AQ^{-1}$ et P^{-1} et Q^{-1} sont inversibles ;

Transitive car pour tout $(A, B, C) \in (\mathcal{M}_{n,p}(\mathbb{K}))^3$ tel que A et B sont équivalentes et B et C sont équivalentes. Alors il existe $P \in \mathcal{M}_n(\mathbb{K})$, $Q \in \mathcal{M}_p(\mathbb{K})$, $R \in \mathcal{M}_n(\mathbb{K})$ et $S \in \mathcal{M}_p(\mathbb{K})$ inversibles, telles que $A = PBQ$ et $B = RCS$, donc $A = (PR)C(SQ)$ et PR et SQ sont inversibles.

Il s'agit donc bien d'une relation d'équivalence. □

Proposition 4.1.10. 1. Soit E et F deux espaces vectoriels de dimensions finies et $u \in \mathcal{L}(E, F)$. Soit $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et $\mathcal{C}$ et $\mathcal{C}'$ deux bases de F . Alors $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$ et $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u)$ sont des matrices équivalentes.

2. Soit E et F deux espaces vectoriels de dimensions finies, munies de bases respectives $\mathcal{B}$ et $\mathcal{C}$. Soit $u \in \mathcal{L}(E, F)$. Soit A une matrice équivalente à $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$. Alors il existe une base $\mathcal{B}'$ de E et une base $\mathcal{C}'$ de F telles que $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u) = A$.

Démonstration. 1. D'après le théorème de changement de base, on a

$$\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u) = \text{Mat}_{\mathcal{C}}(\mathcal{C}')^{-1} \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) \text{Mat}_{\mathcal{B}}(\mathcal{B}')$$

et les matrices de changement de base sont inversibles, donc $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u)$ et $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$ sont équivalentes.

2. Posons $M = \text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$. A est équivalente à M , donc on peut trouver $P \in \mathcal{M}_n(\mathbb{K})$ et $Q \in \mathcal{M}_p(\mathbb{K})$ inversibles telles que $A = PMQ$. Soit $f \in \mathcal{L}(F)$ et $g \in \mathcal{L}(E)$ les applications vérifiant $P^{-1} = \text{Mat}_{\mathcal{C}}(f)$ et $Q = \text{Mat}_{\mathcal{B}}(g)$. P et Q étant inversibles, f et g sont des automorphismes. Notons $\mathcal{B}'$ et $\mathcal{C}'$ les images respectives de $\mathcal{B}$ de $\mathcal{C}$ par g et f . Alors $\text{Mat}_{\mathcal{B}}(\mathcal{B}') = Q$ et $\text{Mat}_{\mathcal{C}}(\mathcal{C}') = P^{-1}$. Donc d'après le théorème de changement de base $\text{Mat}_{\mathcal{B}', \mathcal{C}'}(u) = P \text{Mat}_{\mathcal{B}, \mathcal{C}}(u) Q$. □

Théorème 4.1.11 (Théorème de réduction).

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ une matrice de rang r .

1. Alors, $r \leq \min(n, p)$.

2. A est équivalente à la matrice $J_{n,p,r}$ définie par

$$J_{n,p,r} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Démonstration. 1. On note $V_1, \dots, V_p$ les colonnes de A . Il s'agit de p vecteurs de $\mathcal{M}_{n,1}(\mathbb{K})$, donc $\text{rg}(V_1, \dots, V_p) \leq p$ et de plus $\text{rg}(V_1, \dots, V_p) \leq \dim \mathcal{M}_{n,1}(\mathbb{K}) = n$.

2. Considérons $u : \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ canoniquement associée à la matrice A . u est de même rang que A .

On sait qu'on peut trouver un supplémentaire S de $\text{Ker } u$ tel que u réalise un isomorphisme de S sur $\text{Im } u$. De plus $\dim S = \text{rg}(u) = r$ et $\dim \text{Ker } u = p - r$. Soit $(e_1, \dots, e_r)$ une base de S , $(e_{r+1}, \dots, e_p)$ une base de $\text{Ker } u$. Posons $\mathcal{B} = (e_1, \dots, e_p)$. $\mathcal{B}$ est une base de $\mathbb{K}^p$. Posons $f_i = u(e_i)$ pour $i \in \llbracket 1, r \rrbracket$. Alors $(f_1, \dots, f_r)$ est une base de $\text{Im } u$, qu'on peut compléter en une base $\mathcal{C}$ de $\mathbb{K}^n$.

Alors $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u) = J_{n,p,r}$. Or u a pour matrice A dans les bases canoniques, donc A et $J_{n,p,r}$ sont équivalentes. $\square$

Remarque 4.1.12.

Nous venons de voir une interprétation géométrique de ce résultat. On peut aussi en donner une interprétation matricielle.

On applique l'algorithme du pivot de Gauss au système $AX = B$, avec $B \in \mathcal{M}_{n,1}(\mathbb{K})$ et $X \in \mathcal{M}_{p,1}(\mathbb{K})$. Après une phase de descente, on arrive à un système échelonné en lignes. Quitte à échanger quelques colonnes, A est donc équivalente à une matrice de la forme

$$\begin{pmatrix} J & * \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix} \text{ avec } J = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Remarquons qu'hormis ces échanges de colonnes, nous n'avons effectué que des opérations sur les

lignes. Après la phase de remontée (opérations sur les lignes, toujours), on obtient que A est équivalente à une matrice de la forme

$$\begin{pmatrix} I_r & * \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Il suffit donc d'effectuer quelques opérations élémentaires sur les colonnes de A pour obtenir que A est équivalente à $J_{n,p,r}$.

On remarquera donc que, en écrivant $A = PJ_{n,p,r}Q$, avec $P \in GL_n(\mathbb{K})$ et $Q \in GL_p(\mathbb{K})$, on lit dans P les opérations effectuées sur les lignes de A pendant l'algorithme du pivot de Gauss et dans Q celles effectuées sur les colonnes de A .

4.2 Opérations laissant le rang invariant.

Théorème 4.2.1.

Multiplier une matrice par une matrice inversible (à droite ou à gauche) ne change pas son rang.

Démonstration.

Ce n'est que le point de vue matriciel du résultat analogue sur les applications linéaires. $\square$

Tous les théorèmes suivants utiliseront ce résultat.

Théorème 4.2.2.

Deux matrices A et B sont équivalentes si et seulement si elles sont de même taille et de même rang.

Démonstration.

Dans un sens, utiliser le résultat précédent. Dans l'autre, utiliser le théorème de réduction. $\square$

Théorème 4.2.3 (Invariance par transposition). Si $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $\text{rg}(A) = \text{rg}(A^\top)$.

Démonstration.

C'est un corollaire du théorème de réduction : si $A = BJ_{n,p,r}C$, $A^\top = C^\top J_{n,p,r}^\top B^\top = C^\top J_{p,n,r} B^\top$, qui est de rang r , car $B^\top$ et $C^\top$ sont inversibles et $J_{p,n,r}$ est de rang r . $\square$

Corollaire 4.2.4.

Les résultats sur le rang applicables aux colonnes des matrices vus précédemment s'appliquent aussi aux lignes. Plus précisément :

1. Le rang d'une matrice est le rang de ses vecteurs lignes.
2. Le rang d'une famille de lignes d'une matrice est inférieur ou égal à celui de la matrice.
3. Pour toute matrice de rang r , il existe une famille de r lignes de cette matrice constituant une famille libre.

Exemple 4.2.5.

$$\text{rg} \begin{pmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ se calcule plus vite en}$$

passant à la transposée, *i.e.* en raisonnant sur les lignes au lieu des colonnes. On peut aussi faire un mix.

Théorème 4.2.6.

Les opérations élémentaires sur les lignes et colonnes préservent le rang.

Démonstration.

Facile car ces opérations reviennent à multiplier par des matrices inversibles. $\square$

Théorème 4.2.7.

Supprimer une ligne ou une colonne de zéros dans une matrice ne change pas son rang.

Démonstration.

Pour les colonnes : analogue du résultat sur les vecteurs.
Pour les lignes : passer à la transposée. $\square$

4.3 Calculs pratiques.**Remarque 4.3.1.**

Calcul du rang et de l'inverse d'une matrice grâce au pivot de Gauss.

Pour le rang On peut appliquer la méthode du pivot à une matrice $M \in \mathcal{M}_{n,p}(\mathbb{K})$ non nécessairement carrée.

On peut mélanger les opérations sur les lignes et les colonnes.

On arrive au final à une matrice contenant des lignes non nulles $L_1, \dots, L_k$, dont le premier élément est situé colonne $c_1, \dots, c_k$ avec $c_1 < \dots < c_k$, puis $n - k$ lignes nulles. Alors $\text{rg } M = \text{rg}(\text{Vect}(L_1, \dots, L_k)) = k$ car les lignes $L_1, \dots, L_k$ forment une famille libre.

Pour le calcul du noyau d'une matrice non nécessairement carrée, on peut remarquer que les opérations sur les lignes le laissent invariant car multiplier à gauche une matrice par une matrice inversible ne change pas son noyau.

Pour le calcul de l'image d'une matrice non nécessairement carrée, on peut remarquer que les opérations sur les colonnes la laissent invariante car multiplier à droite une matrice par une matrice inversible ne change pas son image.

Pour le calcul de l'inverse d'une matrice carrée on peut travailler sur les lignes ou sur les colonnes mais **surtout pas sur les deux**. En effet, l'algorithme du calcul de l'inverse consiste à multiplier la matrice A par des matrices élémentaires jusqu'à obtenir l'identité, et à multiplier en parallèle la matrice identité par les mêmes matrices.

4.4 Matrices extraites.**Définition 4.4.1.**

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. On appelle matrice extraite de M toute matrice obtenue en supprimant h des lignes de M et k de ses colonnes avec $h \in \llbracket 0, n-1 \rrbracket$ et $k \in \llbracket 0, p-1 \rrbracket$.

Proposition 4.4.2.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$ et A une matrice extraite de M . Alors $\text{rg}(A) \leq \text{rg}(M)$.

Démonstration.

Posons $r = \text{rg}(A)$. Alors on peut trouver r colonnes $C_1, \dots, C_r$ de A linéairement indépendantes. Notons $C'_1, \dots, C'_r$ les r colonnes de M correspondantes. Pour tout $i \in \llbracket 1, r \rrbracket$, C_i est obtenue en supprimant certaines lignes de C'_i . Soit $(\lambda_1, \dots, \lambda_r)$ r scalaires. Considérons les combinaisons linéaires $S' = \sum_{i=1}^r \lambda_i C'_i$ et $S = \sum_{i=1}^r \lambda_i C_i$. S est obtenue en rayant certaines lignes de S' , donc si S' est nulle, S l'est également et tous les λ_i , sont alors nuls.

$C'_1, \dots, C'_r$ sont donc linéairement indépendantes, donc $\text{rg}(M) \geq r$. $\square$

Proposition 4.4.3.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. Posons $r = \text{rg}(M)$. Alors il existe une matrice A extraite de M , carrée, de taille r et inversible (donc de rang r).

Démonstration.

On peut trouver des colonnes $C_1, \dots, C_r$ de M telles que $\text{rg}(C_1, \dots, C_r) = r$. Ces colonnes permettent donc de former une matrice B de taille $n \times r$ de rang r . B possède n lignes. Comme elle est de rang r , il existe une r lignes $L_1, \dots, L_r$ de B telles que $\text{rg}(B) = \text{rg}(L_1, \dots, L_r)$.

Or ces lignes $L_1, \dots, L_r$ permettent de former une matrice A , extraite de M . Cette matrice A est de taille $r \times r$ (donc carrée) et de rang r , donc inversible. $\square$

5 Systèmes d'équations linéaires.

5.1 Généralités.

Définition 5.1.1.

On appelle *système linéaire à n équations et p inconnues* tout système de la forme :

$$\begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = b_1 \\ \vdots \\ a_{n1}x_1 + \dots + a_{np}x_p = b_n \end{cases}$$

où les a_{ij} et les b_i sont dans $\mathbb{K}$, et les x_i sont les inconnues. Le *système homogène associé* correspond au cas où $b_1 = \dots = b_n = 0$.

On dit que le système est *compatible* s'il admet une solution.

Interprétation matricielle En écrivant le système $AX = B$, on voit que (S) est compatible si et seulement si $B \in \text{Im } A$.

Interprétation linéaire En choisissant un espace vectoriel E de dimension p et F de dimension n munis respectivement d'une base $\mathcal{B}$ et d'une base $\mathcal{C}$ et en notant u l'application linéaire de E dans F et b le vecteur de F tels que $A = \text{Mat}_{\mathcal{B},\mathcal{C}}(u)$ et $B = \text{Mat}_{\mathcal{C}}(b)$, on voit que (S) est compatible si et seulement si $b \in \text{Im } u$.

Interprétation vectorielle En notant C_j les colonnes de A , on note que (S) est compatible si et seulement si $B \in \text{Vect}(C_1, \dots, C_p)$.

Interprétation duale En notant L_i les lignes de A , et u_i les formes linéaires sur F telles que $L_i = \text{Mat}_{\mathcal{C},\mathbb{K}}(u_i)$, on note que (S) est compatible si et seulement si les $u_i^{-1}(\{b_i\})$, pour $i \in \llbracket 1, p \rrbracket$, contiennent au moins un vecteur en commun.

Interprétation géométrique Soit $i \in \llbracket 1, n \rrbracket$. En supposant que $u_i^{-1}(\{b_i\})$ est non vide, alors il s'agit d'un hyperplan affine (*i.e.* il est de la forme $X_0 + H$ où $H = \text{Ker } u_i$ est un hyperplan) si u_i n'est pas la forme linéaire nulle et il s'agit de F sinon. Donc l'ensemble des solutions est ou bien vide ou bien l'intersection d'un certain nombre d'hyperplans (autant que de lignes non nulles).

Exemple 5.1.2.

Écrire ces différents points de vue avec $\begin{pmatrix} 2 & -1 \\ 1 & 2 \\ 3 & -1 \end{pmatrix}$.

5.2 Solutions.

Définition 5.2.1.

Soit (S) un système linéaire écrit sous forme matricielle $AX = B$. On appelle *rang du système* le rang de la matrice A . On le note $\text{rg}(S)$.

Théorème 5.2.2.

Soit (S) un système linéaire de matrice associée $A \in \mathcal{M}_{n,p}(\mathbb{K})$.

1. L'ensemble des solutions du système homogène associé à (S) est un $\mathbb{K}$ -ev de dimension $p - \text{rg}(S)$ (p est le nombre d'inconnues).
2. L'ensemble des solutions de (S) est soit vide, soit un sous-espace affine de direction l'ensemble des solutions du système homogène associé à (S) .

Démonstration. 1. Cet ensemble $\mathcal{S}_0$ de solutions est tout simplement $\text{Ker } A$, et on utilise le théorème du rang.

2. On note $\mathcal{S}$ cet ensemble de solutions. Si (S) est compatible, soit $X_0 \in \mathcal{S}$ une solution. Soit X une autre solution. On montre alors facilement que $X - X_0$ est solution du système homogène, donc $X \in \mathcal{S}_0 + X_0$, et $\mathcal{S} \subset \mathcal{S}_0 + X_0$.

Réciproquement, soit $X \in \mathcal{S}_0 + X_0$. Il est facile de voir que $X \in \mathcal{S}$. $\square$

Définition 5.2.3.

Soit (S) un système linéaire écrit sous forme matricielle $AX = B$. Si A est inversible, on dit que (S) est un *système de Cramer*.

Théorème 5.2.4.

Tout système de Cramer a une unique solution, qui est $A^{-1}B$.

Démonstration.

Il est facile de voir que $A^{-1}B$ est une solution. C'est la seule car $\mathcal{S}$ est un sea dont la direction est de dimension $n - n = 0$. $\square$

6 Matrices semblables et trace.

Dans toute cette partie, on ne considère que des matrices carrées.

6.1 Matrices semblables.

a Changement de base pour un endomorphisme.

Proposition 6.1.1.

Soit E un $\mathbb{K}$ -ev de dimension finie, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et $u \in \mathcal{L}(E)$. Alors,

$$\text{Mat}_{\mathcal{B}'}(u) = \text{Mat}_{\mathcal{B}}(\mathcal{B}')^{-1} \text{Mat}_{\mathcal{B}}(u) \text{Mat}_{\mathcal{B}}(\mathcal{B}').$$

Démonstration.

C'est une conséquence immédiate de la formule de changement de base dans le cas où $F = E$, $\mathcal{C} = \mathcal{B}$ et $\mathcal{C}' = \mathcal{B}'$ (théorème 2.4.7). $\square$

Définition 6.1.2.

Soit A et B deux matrices carrées de taille n . Deux matrices A et B sont dites *semblables* si et seulement s'il existe $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$.

La relation « A est semblable à B » est appelée relation de *similitude*.

Proposition 6.1.3.

La relation de similitude est une relation d'équivalence sur $\mathcal{M}_n(\mathbb{K})$.

Démonstration.

Cette relation est

Réflexive car pour tout $A \in \mathcal{M}_n(\mathbb{K})$, on a $A = I_n^{-1}AI_n$.

Symétrique car pour tout $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ et tout $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$, alors $P^{-1} \in GL_n(\mathbb{K})$ et $B = (P^{-1})^{-1}AP^{-1}$.

Transitive car pour tout $(A, B, C) \in \mathcal{M}_n(\mathbb{K})^3$ et tout $(P, Q) \in GL_n(\mathbb{K})^2$ vérifiant $A = P^{-1}BP$ et $B = Q^{-1}CQ$, on a $A = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP)$. $\square$

Remarque 6.1.4.

Deux matrices semblables sont nécessairement équivalentes mais la réciproque n'est pas vraie. Par exemple, I_2 et $17I_2$ ont même rang (2) donc sont équivalentes mais ne sont pas semblables car pour tout matrice carrée P de taille 2 inversible, $P^{-1}(I_2)P = I_2 \neq 17I_2$.

Proposition 6.1.5.

Soit A et B deux matrices carrées de taille n . A et B sont semblables si et seulement si ce sont les

matrices d'un même endomorphisme u exprimées dans deux bases différentes.

Plus exactement, A et B sont semblables si et seulement s'il existe un espace vectoriel E de dimension n , deux bases $\mathcal{B}$ et $\mathcal{B}'$ et un endomorphisme u tel que $\text{Mat}_{\mathcal{B}}(u) = A$ et $\text{Mat}_{\mathcal{B}'}(u) = B$.

Démonstration.

Le sens indirect est une conséquence de la formule de changement de base pour un endomorphisme (proposition 6.1.1).

Montrons le sens direct. Supposons que A et B sont semblables, c'est-à-dire qu'il existe P tel que $A = P^{-1}BP$. Choisissons un espace vectoriel E de dimension n et une base $\mathcal{B} = (e_1, \dots, e_n)$ de cet espace (on peut par exemple prendre $E = \mathbb{K}^n$ et $\mathcal{B}$ la base canonique de $\mathbb{K}^n$). Notons $e'_1, \dots, e'_n$ les vecteurs de E dont les coordonnées dans la base $\mathcal{B}$ sont les colonnes de P . Alors $P = \text{Mat}_{\mathcal{B}}(\mathcal{B}')$.

Notons enfin u l'endomorphisme de E vérifiant $\text{Mat}_{\mathcal{B}}(u) = A$.

Alors,

$$\begin{aligned} \text{Mat}_{\mathcal{B}'}(u) &= \text{Mat}_{\mathcal{B}}(\mathcal{B}')^{-1} \text{Mat}_{\mathcal{B}}(u) \text{Mat}_{\mathcal{B}}(\mathcal{B}') \\ &= P^{-1}BP \\ &= A, \end{aligned}$$

donc A et B sont les deux matrices d'un même endomorphisme relativement aux bases respectives $\mathcal{B}'$ et $\mathcal{B}$. $\square$

Proposition 6.1.6.

Considérons deux matrices A et B semblables de taille n . Alors pour tout $k \in \mathbb{N}$, A^k et B^k sont des matrices semblables.

Démonstration.

Ce résultat peut être démontré au moins des deux manières suivantes :

Par le calcul On montre par récurrence sur k que pour tout k , on a $A^k = P^{-1}B^kP$. Pour montrer que ce prédicat est héréditaire, il suffit de constater que pour tout $k \in \mathbb{N}$ tel que le prédicat est vérifié, on a également $A^{k+1} = A^kA = P^{-1}B^kPP^{-1}BP$.

Géométriquement A et B sont deux matrices d'un même endomorphisme u , donc A^k et B^k sont deux matrices de u^k .

$\square$

6.2 Trace d'une matrice carrée.

a Définition.

Définition 6.2.1.

Soit A une matrice carrée de taille n . Alors la trace de A , notée $\text{tr}(A)$ (ou $\text{Tr}(A)$), est la somme des éléments diagonaux de A .

En notant $(a_{ij})_{(i,j) \in \llbracket 1, n \rrbracket \times \llbracket 1, n \rrbracket}$ les coefficients de A :

$$\text{tr}(A) = \sum_{i=1}^n a_{ii}.$$

Remarque 6.2.2.

Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, on a

$$\text{tr}(A^\top) = \text{tr}(A).$$

Démonstration.

Les matrices $A^\top$ et A ont les mêmes éléments diagonaux. $\square$

b Linéarité.

Proposition 6.2.3.

Pour tout $n \in \mathbb{N}^*$, l'application trace est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$.

Démonstration.

Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ et $\lambda \in \mathbb{K}$. Posons $C = \lambda A + B$ et montrons $\text{tr}(\lambda A + B) = \lambda \text{tr}(A) + \text{tr}(B)$. Notons (a_{ij}) , (b_{ij}) et c_{ij} les coefficients respectivement de A , de B et de C .

Alors, on a

$$\begin{aligned} \text{tr}(C) &= \sum_{i=1}^n c_{ii} \\ &= \sum_{i=1}^n (\lambda a_{ii} + b_{ii}) \\ &= \lambda \sum_{i=1}^n a_{ii} + \sum_{i=1}^n b_{ii} \\ &= \lambda \text{tr}(A) + \text{tr}(B). \end{aligned}$$

$\square$

c Propriété fondamentale de la trace.

Proposition 6.2.4.

Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$, alors,

$$\operatorname{tr}(AB) = \operatorname{tr}(BA).$$



$\operatorname{tr}(A \times B) \neq \operatorname{tr} A \times \operatorname{tr} B$; par exemple, dans $\mathcal{M}_2(\mathbb{K})$, $0 = \operatorname{tr}(E_{11} \times E_{22}) \neq 1 = \operatorname{tr}(E_{11}) \times \operatorname{tr}(E_{22})$.

Démonstration.

Posons $C = AB$ et $D = BA$. Notons (a_{ij}) , (b_{ij}) , (c_{ij}) et (d_{ij}) les coefficients respectifs de A , B , C et D .

On a, pour tout $(i, j) \in \llbracket 1, n \rrbracket^2$:

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj},$$

$$d_{ij} = \sum_{k=1}^n b_{ik} a_{kj}.$$

D'où, pour tout $i \in \llbracket 1, n \rrbracket$:

$$c_{ii} = \sum_{k=1}^n a_{ik} b_{ki},$$

$$d_{ii} = \sum_{k=1}^n b_{ik} a_{ki}.$$

D'où :

$$\operatorname{tr}(C) = \sum_{i=1}^n \sum_{k=1}^n a_{ik} b_{ki},$$

$$\operatorname{tr}(D) = \sum_{i=1}^n \sum_{k=1}^n a_{ki} b_{ik}.$$

Ainsi,

$$\operatorname{tr}(C) = \sum_{1 \leq \alpha, \beta \leq n} a_{\alpha\beta} b_{\beta\alpha},$$

$$\operatorname{tr}(D) = \sum_{1 \leq \alpha, \beta \leq n} a_{\alpha\beta} b_{\beta\alpha},$$

d'où l'égalité recherchée. $\square$

Remarque 6.2.5. 1. On peut déduire de cette égalité que la trace d'un produit de matrices est invariant par permutations circulaires : pour toutes matrices $A_1, \dots, A_k$ de taille n , on a

$$\begin{aligned} \operatorname{tr}(A_1 A_2 \dots A_{k-1} A_k) &= \operatorname{tr}(A_2 \dots A_k A_1) \\ &= \operatorname{tr}(A_3 \dots A_k A_1 A_2) \\ &\dots \end{aligned}$$

2. En revanche, la trace d'un produit de matrice n'est **pas** invariant par n'importe quelle permutation. Par exemple, dans $\mathcal{M}_2(\mathbb{K})$, en notant (E_{ij}) les matrices de la base canonique :

$$\operatorname{tr}(E_{21} E_{11} E_{12}) = 1 \neq 0 = \operatorname{tr}(E_{11} E_{21} E_{12}).$$

d Invariance par similitude.
Proposition 6.2.6.

Deux matrices semblables ont même trace (on dit que la trace est un *invariant de similitude*) : soit $A, B \in \mathcal{M}_n(\mathbb{K})$, deux matrices semblables. Alors $\operatorname{tr}(A) = \operatorname{tr}(B)$.

Démonstration.

Il existe $P \in GL_n(\mathbb{K})$ vérifiant $A = P^{-1}BP$. Alors on a

$$\begin{aligned} \operatorname{tr}(A) &= \operatorname{tr}(P^{-1}(BP)) \\ &= \operatorname{tr}((BP)P^{-1}) \\ &= \operatorname{tr}(B). \end{aligned}$$

$\square$

Remarque 6.2.7.

La réciproque de ce résultat est fausse. Par exemple, montrez que $A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$ et I_2 ne sont pas semblables.



Ce résultat n'est pas valable pour des matrices équivalentes. Par exemple I_2 et $2I_2$ sont équivalentes, mais n'ont pas la même trace.

e Trace d'un endomorphisme en dimension finie.
Définition 6.2.8.

Soit E un espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. La *trace de l'endomorphisme* u et on note $\operatorname{tr}(u)$ (ou $\operatorname{Tr}(u)$) est le scalaire défini par

$$\operatorname{tr}(u) = \operatorname{tr}(\operatorname{Mat}_{\mathcal{B}}(u)),$$

où $\mathcal{B}$ est une base quelconque de E . Cette valeur ne dépend pas du choix de la base $\mathcal{B}$.

Démonstration.

On a vu d'une part que deux matrices d'un même endomorphisme sont nécessairement semblables et d'autre part que la trace de matrices est un invariant de similitude. La valeur de $\text{tr}(u)$ ne dépend donc pas du choix de la base $\mathcal{B}$. $\square$

Exemple 6.2.9.

L'endomorphisme Id_E a pour trace $\dim(E)$.

Exercice 6.2.10.

Déterminer la trace de l'endomorphisme de dérivation dans $\mathbb{K}_n[X]$.

f Propriétés.
Proposition 6.2.11.

Soit E un espace vectoriel de dimension finie. La trace est une forme linéaire sur $\mathcal{L}(E)$.

Démonstration.

Il suffit de choisir une base de $\mathcal{B}$ de E et constater que pour tous endomorphismes u et v , de matrices respectives A et B , et pour tout scalaire λ , on a

$$\begin{aligned}\text{tr}(\lambda u + v) &= \text{tr}(\lambda A + B) \\ &= \lambda \text{tr}(A) + \text{tr}(B) \\ &= \lambda \text{tr}(u) + \text{tr}(v).\end{aligned}$$

$\square$

Proposition 6.2.12.

Soit E un espace vectoriel de dimension finie et v et u deux endomorphismes de E . Alors,

$$\text{tr}(v \circ u) = \text{tr}(u \circ v).$$

Démonstration.

Il suffit de choisir une base $\mathcal{B}$ de E . En notant A et B les matrices respectives de u et v , la matrice de $v \circ u$ est BA , celle de $u \circ v$ est AB et on sait que $\text{tr}(AB) = \text{tr}(BA)$, d'où le résultat. $\square$

Exemple 6.2.13.

Vérifier ce résultat sur deux endomorphismes de $\mathbb{R}^3$.

g Trace d'un projecteur.
Proposition 6.2.14.

Soit E un espace vectoriel de dimension finie et p un projecteur. Alors, la trace de p est la dimension de $\text{Im } p$:

$$\text{tr}(p) = \text{rg } p.$$

Démonstration.

Notons n la dimension de E , q celle de $\text{Im } p$. p étant un projecteur, on a $E = \text{Im } p \oplus \text{Ker } p$. Soit $(e_1, \dots, e_q)$ une base de $\text{Im } p$. On a $\dim \text{Ker } p = n - q$, donc on peut trouver une base $(e_{q+1}, \dots, e_n)$ de $\text{Ker } p$. La famille $(e_1, \dots, e_n)$ est alors une base $\mathcal{B}$ de E et relativement à cette base, la matrice de p est une matrice diagonale dont les q premiers coefficients valent 1 et tous les autres sont nuls. Sa trace est donc q . $\square$

Remarque 6.2.15.

Ce résultat est faux pour d'autres endomorphismes que les projecteurs. Considérer par exemple un endomorphisme de matrice E_{12} .

7 Matrices par blocs (HP).

Définition 7.0.1.

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. On peut écrire la matrice sous la forme

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1p} \\ m_{21} & m_{22} & \cdots & m_{2p} \\ \vdots & \vdots & & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{np} \end{pmatrix}.$$

En traçant $q - 1$ lignes horizontales distinctes et $r - 1$ lignes verticales distinctes dans le tableau représentant M , on peut décomposer M en $q \times r$ matrices extraites M_{ij} pour $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$:

$$M = \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1r} \\ M_{21} & M_{22} & \cdots & M_{2r} \\ \vdots & \vdots & & \vdots \\ M_{q1} & M_{q2} & \cdots & M_{qr} \end{pmatrix}.$$

Cette décomposition est appelée *décomposition par blocs* de M en $q \times r$ blocs.

Formellement, une décomposition par bloc de M est la donnée de $q \times r$ matrices M_{ij} pour $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$ telles que

1. Pour tout $i \in \llbracket 1, q \rrbracket$, les matrices $M_{i1}, \dots, M_{ir}$ ont un même nombre de lignes n_i (toutes les matrices d'une même ligne ont même nombre de lignes).
2. Pour tout $j \in \llbracket 1, r \rrbracket$, les matrices $M_{1j}, \dots, M_{qj}$ ont un même nombre de colonnes p_j (toutes les matrices d'une même colonne ont même nombre de colonnes).
3. En notant a_{hk}^{ij} le coefficient de la ligne h , colonne k de la matrice M_{ij} pour $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$ et $(h, k) \in \llbracket 1, n_i \rrbracket \times \llbracket 1, p_j \rrbracket$, on a $a_{hk}^{ij} = m_{(s+h)(t+k)}$ où $s = n_1 + \dots + n_{i-1}$ et $t = p_1 + \dots + p_{j-1}$.

On dira que la décomposition précédente est *triangulaire supérieure par blocs* si $n = p$ et que :

1. pour tout $i \in \llbracket 1, q \rrbracket$, M_{ii} est carrée ;
2. pour tout $(i, j) \in \llbracket 1, q \rrbracket^2$ avec $i > j$, M_{ij} est nulle.

On définit de même les décompositions *triangulaires inférieures par blocs*.

Enfin, les décompositions *diagonales par blocs* sont celles dont tous les blocs M_{ij} tels $i \neq j$ sont nuls et tous les blocs M_{ii} sont carrés.

Exemple 7.0.2.

En posant

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 & 17 & 18 \\ 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 \end{pmatrix},$$

A peut se décomposer par bloc en

$$\begin{pmatrix} B & C & D \\ E & F & G \\ H & I & J \end{pmatrix},$$

où

$$\begin{aligned} B &= \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}, & C &= \begin{pmatrix} 3 \\ 9 \end{pmatrix}, \\ D &= \begin{pmatrix} 4 & 5 & 6 \\ 10 & 11 & 12 \end{pmatrix}, & E &= \begin{pmatrix} 13 & 14 \end{pmatrix}, \\ F &= \begin{pmatrix} 15 \end{pmatrix}, & G &= \begin{pmatrix} 16 & 17 & 18 \end{pmatrix}, \\ H &= \begin{pmatrix} 19 & 20 \\ 25 & 26 \\ 31 & 32 \end{pmatrix}, & I &= \begin{pmatrix} 21 \\ 27 \\ 33 \end{pmatrix}, \\ J &= \begin{pmatrix} 22 & 23 & 24 \\ 28 & 29 & 30 \\ 34 & 35 & 36 \end{pmatrix}. \end{aligned}$$

Remarque 7.0.3.



Lorsqu'on parle de décomposition triangulaire supérieure (resp. triangulaire inférieure, diagonale) par bloc, c'est bien la décomposition qui est triangulaire supérieure (resp. triangulaire inférieure, diagonale). Toute matrice carrée admet en effet une décomposition (triviale) triangulaire supérieure (resp. triangulaire inférieure, diagonale) par bloc.

Proposition 7.0.4 (Interprétation géométrique).

On peut interpréter la décomposition par blocs de la façon suivante. Considérons la matrice $n \times p$ donnée dans la définition précédente :

$$M = \begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1r} \\ M_{21} & M_{22} & \cdots & M_{2r} \\ \vdots & \vdots & & \vdots \\ M_{q1} & M_{q2} & \cdots & M_{qr} \end{pmatrix},$$

où pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$, M_{ij} est de taille $n_i \times p_j$. Soit E et F des espaces vectoriels respectivement de dimension p et n , $\mathcal{B} = (e_1, \dots, e_p)$ une base de E , $\mathcal{C} = (f_1, \dots, f_n)$ une base de F et $u \in \mathcal{L}(E, F)$ vérifiant $\text{Mat}_{\mathcal{B}, \mathcal{C}}(u)$.

On note $\mathcal{B}_1$ la famille des p_1 premiers vecteurs de $\mathcal{B}$, $\mathcal{B}_2$ celle des p_2 suivants, ..., $\mathcal{B}_r$ celle des p_r derniers et $E_1 = \text{Vect}(\mathcal{B}_1)$, ..., $E_r = \text{Vect}(\mathcal{B}_r)$. Pour tout $j \in \llbracket 1, r \rrbracket$, $\mathcal{B}_j$ est une base de E_j .

On note $\mathcal{C}_1$ la famille des n_1 premiers vecteurs de $\mathcal{C}$, $\mathcal{C}_2$ celle des n_2 suivants, ..., $\mathcal{C}_r$ celle des

n_r derniers et $F_1 = \text{Vect}(\mathcal{C}_1), \dots, F_q = \text{Vect}(\mathcal{C}_q)$.
Pour tout $i \in \llbracket 1, q \rrbracket$, $\mathcal{C}_i$ est une base de F_i .

Alors

$$\begin{aligned} E &= E_1 \oplus \dots \oplus E_r, \\ F &= F_1 \oplus \dots \oplus F_q. \end{aligned}$$

Tout $y \in F$ s'écrit de façon unique $\pi'_1(y) + \dots + \pi'_q(y)$, où $\pi'_i(y) \in F_i$ pour tout $i \in \llbracket 1, q \rrbracket$ (π'_i est alors la projection sur F_i parallèlement à la somme des F_k pour $k \neq i$).

De même notons, pour tout $j \in \llbracket 1, r \rrbracket$, π_j la projection sur E_j parallèlement à la somme des E_k pour $k \neq j$.

Alors, pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$, on note

$$u_{ij} : \begin{cases} E_j & \longrightarrow F_i \\ x & \longmapsto \pi'_i(u(x)) \end{cases}.$$

Ainsi, u_{ij} est obtenu en restreignant u au départ à E_j et, comme il n'est pas a priori possible de le restreindre à l'arrivée à F_i en le composant à gauche par la projection sur F_i (par rapport à la somme des F_k pour $k \neq i$) : $u_{ij} = \pi'_i \circ u|_{E_j}$.

On a alors, pour tout $x \in E$:

$$u(x) = \sum_{(i,j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket} u_{ij}(\pi_j(x)).$$

De plus, pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$,

$$\text{Mat}_{\mathcal{B}_j, \mathcal{C}_i}(u_{ij}) = M_{ij}.$$

Démonstration.

Remarquons tout d'abord que pour tout $x \in E$, on a

$$\begin{aligned} u(x) &= u\left(\sum_{j=1}^r \pi_j(x)\right) \\ &= \sum_{j=1}^r u(\pi_j(x)) \\ &= \sum_{j=1}^r \sum_{i=1}^q \pi'_i(u(\pi_j(x))) \\ &= \sum_{(i,j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket} u_{ij}(\pi_j(x)). \end{aligned}$$

Soit $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$. On a

$$\begin{aligned} \mathcal{C}_i &= (f_{s+1}, f_{s+2}, \dots, f_{s+n_i}), \\ \mathcal{B}_j &= (e_{t+1}, e_{t+2}, \dots, e_{t+p_j}), \end{aligned}$$

où

$$\begin{aligned} s &= n_1 + \dots + n_{i-1}, \\ t &= p_1 + \dots + p_{j-1}. \end{aligned}$$

Soit $k \in \llbracket 1, p_j \rrbracket$. En notant $(m_{ij})_{(i,j) \in \llbracket 1, n \rrbracket \times \llbracket 1, q \rrbracket}$ les coefficients de M , on a

$$\begin{aligned} u_{ij}(e_k) &= \pi'_i(u(e_{t+k})) \\ &= \pi'_i\left(\sum_{h=1}^n m_{h(t+k)} f_h\right) \\ &= \sum_{h=s+1}^{s+n_i} m_{h(t+k)} f_h \\ &= \sum_{h=1}^{n_i} m_{(s+h)(t+k)} f_{s+h}. \end{aligned}$$

On en déduit que la matrice de u_{ij} est la matrice des $(m_{(s+h)(t+k)})_{(h,k) \in \llbracket 1, n_i \rrbracket \times \llbracket 1, p_j \rrbracket}$ qui est exactement la matrice M_{ij} . On a donc $\text{Mat}_{\mathcal{B}_j, \mathcal{C}_i}(u_{ij}) = M_{ij}$. $\square$

Proposition 7.0.5 (Addition par blocs).

Soit $(A, B) \in \mathcal{M}_{n,p}(\mathbb{K})^2$, admettant des décompositions par blocs

$$\begin{aligned} A &= \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1r} \\ A_{21} & A_{22} & \cdots & A_{2r} \\ \vdots & \vdots & & \vdots \\ A_{q1} & A_{q2} & \cdots & A_{qr} \end{pmatrix}, \\ B &= \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1r} \\ B_{21} & B_{22} & \cdots & B_{2r} \\ \vdots & \vdots & & \vdots \\ B_{q1} & B_{q2} & \cdots & B_{qr} \end{pmatrix}, \end{aligned}$$

où pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$, A_{ij} et B_{ij} sont de même taille.

Alors $A + B$ vaut

$$\begin{pmatrix} A_{11} + B_{11} & A_{12} + B_{12} & \cdots & A_{1r} + B_{1r} \\ A_{21} + B_{21} & A_{22} + B_{22} & \cdots & A_{2r} + B_{2r} \\ \vdots & \vdots & & \vdots \\ A_{q1} + B_{q1} & A_{q2} + B_{q2} & \cdots & A_{qr} + B_{qr} \end{pmatrix}.$$

Démonstration.

Notons, pour tout $i \in \llbracket 1, q \rrbracket$ (resp. pour tout $j \in \llbracket 1, r \rrbracket$), n_i (resp. p_j) le nombre de lignes (resp. de colonnes) des matrices de la ligne i (resp. de la colonne j) de ces décompositions par bloc.

Posons $C = A + B$ et pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$, $C_{ij} = A_{ij} + B_{ij}$.

Notons a_{ij} pour $(i, j) \in \llbracket 1, n \rrbracket \times \llbracket 1, p \rrbracket$ les coefficients de la matrice A , b_{ij} ceux de B , c_{ij} ceux de C et pour tout $(i, j) \in \llbracket 1, q \rrbracket \times \llbracket 1, r \rrbracket$ et tout $(k, h) \in \llbracket 1, n_i \rrbracket \times \llbracket 1, p_j \rrbracket$, a_{hk}^{ij} (resp. b_{hk}^{ij} , resp. c_{hk}^{ij}) ceux de A_{ij} (resp. B_{ij} , resp. C_{ij}). On a alors, en posant $s = n_1 + \dots + n_{i-1} + h$ et $t = p_1 + \dots + p_{j-1} + k$.

$$c_{st} = a_{st} + b_{st} = a_{hk}^{ij} + b_{hk}^{ij} = c_{hk}^{ij}$$

On a donc

$$C = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1r} \\ C_{21} & C_{22} & \cdots & C_{2r} \\ \vdots & \vdots & & \vdots \\ C_{q1} & C_{q2} & \cdots & C_{qr} \end{pmatrix}$$

D'où le résultat. $\square$

Proposition 7.0.6 (Multiplication par blocs).

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$.

On considère des décompositions de A en $r \times s$ blocs et de B en $s \times t$ blocs,

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ A_{21} & A_{22} & \cdots & A_{2s} \\ \vdots & \vdots & & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rs} \end{pmatrix},$$

$$B = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1t} \\ B_{21} & B_{22} & \cdots & B_{2t} \\ \vdots & \vdots & & \vdots \\ B_{s1} & B_{s2} & \cdots & B_{st} \end{pmatrix},$$

telles que pour tout pour tout $(i, k, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, s \rrbracket \times \llbracket 1, t \rrbracket$, les matrices A_{ik} et B_{kj} aient des tailles compatibles par la multiplication.

Alors le produit $A \times B$ s'écrit par blocs :

$$C = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1t} \\ C_{21} & C_{22} & \cdots & C_{2t} \\ \vdots & \vdots & & \vdots \\ C_{r1} & C_{r2} & \cdots & C_{rt} \end{pmatrix},$$

où pour tout $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, t \rrbracket$, on a

$$C_{ij} = \sum_{k=1}^s A_{ik} \times B_{kj}$$

Démonstration.

Nous donnons ici les grandes lignes de la démonstration, que nous traitons de façon géométrique.

Choisissons E, F, G trois espaces vectoriels de dimensions respectives q, p, n et trois bases respectives $\mathcal{B}, \mathcal{C}$ et $\mathcal{D}$ de ces espaces.

Notons $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$ les applications linéaires vérifiant $\text{Mat}_{(\mathcal{B}, \mathcal{C})}(u) = B$ et $\text{Mat}_{(\mathcal{C}, \mathcal{D})}(v) = A$.

Comme précédemment, on peut, à partir de la base $\mathcal{B}$, décomposer E en une somme directe $E_1 \oplus \dots \oplus E_t$ et construire des projections $\pi_1, \dots, \pi_t$ sur ces sous-espaces respectifs, parallèlement à la somme des autres.

On fait de même pour décomposer F en $F_1 \oplus \dots \oplus F_s$ et construire les projections $\pi'_1, \dots, \pi'_s$ associées et pour décomposer G en $G_1 \oplus \dots \oplus G_r$ et construire les projections $\pi''_1, \dots, \pi''_r$ associées.

Posons $w = v \circ u$.

On peut construire comme précédemment des $u_{ij} \in \mathcal{L}(E_j, F_i)$ pour $(i, j) \in \llbracket 1, s \rrbracket \times \llbracket 1, t \rrbracket$ pour décomposer u , des $v_{ij} \in \mathcal{L}(F_j, G_i)$ pour $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, s \rrbracket$ pour décomposer v et des $w_{ij} \in \mathcal{L}(E_j, G_i)$ pour $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, t \rrbracket$ pour décomposer w .

En posant $C_{ij} = \text{Mat}_{\mathcal{B}, \mathcal{D}}(w_{ij})$ pour $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, t \rrbracket$, on obtient une décomposition par bloc de la matrice $\text{Mat}_{\mathcal{B}, \mathcal{D}}(w)$ qui n'est autre que $A \times B$.

Soit alors $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 1, s \rrbracket$ et $x \in E_j$. On a

$$\begin{aligned} w_{ij} &= \pi''_i \circ w|_{E_j} \\ &= \pi''_i \circ v \circ u|_{E_j} \\ &= \pi''_i \circ v \circ \left(\sum_{k=1}^s \pi'_k \right) \circ u|_{E_j} \\ &= \sum_{k=1}^s \pi''_i \circ v \circ \pi'_k \circ u|_{E_j} \\ &= \sum_{k=1}^s \pi''_i \circ v|_{F_k} \circ \pi'_k \circ u|_{E_j} \\ &= \sum_{k=1}^s v_{ik} \circ u_{kj}. \end{aligned}$$

On en déduit

$$\begin{aligned} C_{ij} &= \text{Mat}_{\mathcal{B}, \mathcal{D}} \left(\sum_{k=1}^s v_{ik} \circ u_{kj} \right) \\ &= \sum_{k=1}^s \text{Mat}_{\mathcal{C}, \mathcal{D}}(v_{ik}) \times \text{Mat}_{\mathcal{B}, \mathcal{C}}(u_{kj}) \\ &= \sum_{k=1}^s A_{ik} \times B_{kj}. \end{aligned}$$

$\square$

Exercice 7.0.7.

Calculer A^2 , avec

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Chapitre XXVII

Déterminants

Sommaire

1	Groupe symétrique.	424
1.1	Permutations.	424
1.2	Permutations particulières.	424
1.3	Décomposition d'une permutation. . .	425
1.4	Signature d'une permutation.	426
2	Applications multilinéaires.	428
2.1	Définition et exemples.	428
2.2	Applications multilinéaires symétriques, antisymétriques et alternées.	428
3	Déterminant d'une famille de vecteurs. 430	
3.1	Définition en dimension finie.	430
3.2	Interprétation en géométrie réelle. . . .	432
a	Orientation d'un ev réel de dimension finie (HP).	432
b	Déterminant et aire dans le plan.	433
c	Déterminant et volume dans l'espace.	434
4	Déterminant d'un endomorphisme. . .	434
5	Déterminant d'une matrice carrée. . . .	435
5.1	Définitions et propriétés.	435
5.2	Matrices triangulaires et triangulaires par blocs.	436
5.3	Opérations élémentaires et pivot de Gauss.	437
5.4	Développement par rapport à une ligne ou une colonne.	438

Dans tout ce chapitre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Les lettres n, p, q et r désignent des entiers naturels non nuls.

1 Groupe symétrique.

Dans toute cette section, E désigne un ensemble.

1.1 Permutations.

Définition 1.1.1.

On appelle **permutation de E** toute bijection de E dans E . On note S_E l'ensemble des permutations de E . Alors $(S_E, \circ)$ est un groupe appelé **groupe des permutations de E** .

Définition 1.1.2.

Si $E = \llbracket 1, n \rrbracket$, on note S_n le groupe des permutations de E , qui est un groupe fini de cardinal $n!$. Ce groupe s'appelle le **groupe symétrique** d'ordre n (ou de degré n). Une permutation σ de S_n se note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Exemple 1.1.3.

- La permutation σ de $\llbracket 1, 5 \rrbracket$ vérifiant $\sigma(1) = 2$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 4$ et $\sigma(5) = 3$ se note $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$. On vérifie bien que 1, 2, 3, 4 et 5 apparaissent une et une seule fois par ligne.
 - Cette écriture permet de composer facilement des permutations :
- $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$
- et de facilement calculer les antécédents.

1.2 Permutations particulières.

Définition 1.2.1.

Soient $\sigma \in S_E$, et $x \in E$. On appelle **orbite** de x l'ensemble $\mathfrak{O}(x) = \{\sigma^k(x), k \in \mathbb{Z}\}$.

Exemple 1.2.2.

Si $E = \llbracket 1, 6 \rrbracket$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$, alors $\mathfrak{O}(1) = \mathfrak{O}(2) = \{1, 2\}$ et $\mathfrak{O}(3) = \mathfrak{O}(4) = \mathfrak{O}(5) = \mathfrak{O}(6) = \{3, 4, 5, 6\}$.

Définition 1.2.3.

On appelle **permutation circulaire** toute permutation $\sigma \in S_E$ telle qu'il existe $x \in E$ vérifiant $\mathfrak{O}(x) = E$.

Exemple 1.2.4.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ est une permutation circulaire.



Si une permutation a un point fixe et si $\text{card}(E) > 1$, alors la permutation n'est pas circulaire, mais la non existence de point fixe n'implique pas que la permutation est circulaire. Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ n'est pas circulaire.

Définition 1.2.5.

On dit qu'une permutation est un **cycle** lorsqu'elle admet exactement une orbite non réduite à un élément. Cette orbite s'appelle alors le **support** de ce cycle, et son cardinal s'appelle la **longueur** du cycle.

Remarque 1.2.6.

Les éléments qui sont hors du support d'un cycle sont des points fixes de cette permutation.

Exemple 1.2.7.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$ est un cycle de longueur 3 dont le support est $\{2, 3, 5\}$.

Remarque 1.2.8.

On note généralement les cycles de la manière suivante $(x_1, x_2, \dots, x_p)$, où p est la longueur du cycle et $\{x_1, x_2, \dots, x_p\}$ son support, dans l'ordre, c'est-à-dire que x_1 est envoyé sur x_2 , x_2 sur x_3 , ..., x_{p-1} sur x_p et enfin x_p sur x_1 . Les éléments

de $\llbracket 1, n \rrbracket$ autres que $x_1, \dots, x_p$ sont les points fixes de la permutation. Le cycle de l'exemple 1.2.7 est ainsi tout simplement noté $(2, 5, 3)$. Remarquons qu'on peut aussi l'écrire $(5, 3, 2)$ ou $(3, 2, 5)$, car un cycle est une « boucle ».

Définition 1.2.9.

On appelle **transposition** tout cycle de longueur 2. Une transposition échange ainsi deux éléments de E . Si a et b sont deux éléments de E , la transposition qui échange a et b est notée τ_{ab} .

Exemple 1.2.10.

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ est une transposition, notée τ_{24} .

Remarque 1.2.11.

Toute transposition est une involution, *i.e.* est sa propre inverse.

1.3 Décomposition d'une permutation.

Dans toute la suite de la section 1, $E = \llbracket 1, n \rrbracket$. On se place donc dans S_n .

Lemme 1.3.1.

Deux cycles de supports disjoints commutent.

Démonstration.

Ceci est dû au fait que deux cycles de supports disjoints agissent sur des éléments distincts. Soient σ_1 et σ_2 deux cycles de supports respectifs I et J inclus dans $\llbracket 1, n \rrbracket$ et tels que $I \cap J = \emptyset$. Soit $x \in I$, $y \in J$ et $z \in (I \cup J)^C$.

Alors $\sigma_1(x) \neq x$ et $\sigma_1(x) \in I$, donc $\sigma_1(x) \notin J$. Ainsi $\sigma_2(x) = x$ et $\sigma_2(\sigma_1(x)) = \sigma_1(x)$. On en tire $\sigma_1 \circ \sigma_2(x) = \sigma_1(x) = \sigma_2 \circ \sigma_1(x)$.

De même, $\sigma_2 \circ \sigma_1(y) = \sigma_2(y) = \sigma_1 \circ \sigma_2(y)$.

Enfin, $\sigma_1(z) = z = \sigma_2(z)$ et donc $\sigma_1 \circ \sigma_2(z) = z = \sigma_2 \circ \sigma_1(z)$.

Ainsi $\sigma_1 \circ \sigma_2$ et $\sigma_2 \circ \sigma_1$ coïncident en tous les éléments de $\llbracket 1, n \rrbracket$, et sont bien égaux. $\square$

Exemple 1.3.2.

Pour vous en assurer, calculez pour $n = 7$, $(1\ 4\ 3) \circ (2\ 5)$ et $(2\ 5) \circ (1\ 4\ 3)$.

Lemme 1.3.3.

Soit $\sigma \in S_n$. Tout point de $\llbracket 1, n \rrbracket$ est dans une et une seule orbite de σ . L'ensemble des orbites de σ forme donc une partition de E (c'est-à-dire que la réunion de ces orbites est $\llbracket 1, n \rrbracket$ mais ces orbites sont deux à deux disjointes).

Démonstration.

Tout point est dans au moins une orbite : la sienne. Si x est dans deux orbites distinctes, *i.e.* $x \in \mathfrak{O}(y)$ et $x \in \mathfrak{O}(z)$ avec $\mathfrak{O}(y) \neq \mathfrak{O}(z)$, alors il existe $k, \ell \in \mathbb{Z}$ tels que $x = \sigma^k(y) = \sigma^\ell(z)$. D'où $y = \sigma^{\ell-k}(z)$, et ainsi $y \in \mathfrak{O}(z)$. Il est alors facile de vérifier que $\mathfrak{O}(y) = \mathfrak{O}(z)$, ce qui est une contradiction. $\square$

Théorème 1.3.4.

Toute permutation se décompose en produit de cycles de supports disjoints. À l'ordre près des facteurs, cette décomposition est unique.

Démonstration.

D'après le lemme 1.3.1, si cette décomposition existe on peut permuter l'ordre des facteurs.

Notons $\mathfrak{O}_1, \dots, \mathfrak{O}_p$ les orbites de σ de cardinal au moins 2. Pour tout $i \in \llbracket 1, p \rrbracket$ on définit la permutation C_i de la manière suivante :

- (i) $\forall x \in \mathfrak{O}_i, C_i(x) = \sigma(x)$;
- (ii) $\forall x \in \llbracket 1, n \rrbracket \setminus \mathfrak{O}_i, C_i(x) = x$.

On vérifie que les C_i sont des cycles, que leurs supports sont deux à deux disjoints, et que $C_1 \circ C_2 \circ \dots \circ C_p = \sigma$.

La démonstration de l'unicité n'est pas exigible, nous la donnons à but d'information. Soit $(C_1, \dots, C_p)$ des cycles

à supports disjoints, vérifiant $\prod_{i=1}^p C_i = \sigma$. Soit $1 \leq i \leq p$,

soit x appartenant au support de C_i ($C_i(x) \neq x$ et si $j \neq i$, $C_j(x) = x$). Alors, comme les cycles C_j commutent, on a

$$\sigma(x) = \left(\prod_{j=1}^p C_j \right)(x) = C_i \left[\left(\prod_{j \neq i} C_j \right)(x) \right] = C_i(x).$$

Ainsi, l'orbite de x par C_i et par σ coïncident : l'orbite de x (par σ) est donc le support de C_i . Réciproquement, si $\sigma(x) \neq x$, alors il existe forcément un i tel que $C_i(x) \neq x$. Il y a donc exactement autant de cycles que d'orbites de σ non réduites à un élément, donc p est unique. De plus, chaque cycle a un support correspondant à une orbite de σ , non réduite à un point. Il suffit maintenant de voir que pour chaque orbite de σ de longueur $\ell > 1$, il existe un unique cycle dont le support est exactement cette orbite : c'est, avec un élément x de cette orbite, $(x, \sigma(x), \dots, \sigma^{\ell-1}(x))$. $\square$

Il faut savoir décomposer une permutation en produit de cycles de supports disjoints. Dans la pratique, voici comment l'on procède (le procédé est celui de la démonstration précédente). Soit $\sigma \in S_n$.

L'idée est la suivante : on part d'un élément de $\llbracket 1, n \rrbracket$, et on regarde ses images successives par σ . On parcourt alors son orbite. Au bout d'un nombre fini d'étapes, on revient au point de départ. On a alors parcouru une boucle, ce qui correspond à un cycle C_1 . Pour autant, tous les éléments de $\llbracket 1, n \rrbracket$ n'ont pas forcément été rencontrés lors de cette boucle. On peut donc recommencer une autre promenade en partant d'un élément que nous n'avons pas encore rencontré. On fait alors une nouvelle boucle qui est une deuxième orbite, ce qui correspond à un second cycle C_2 . En faisant cela pour toutes les orbites, on a construit autant de cycles que d'orbites. Ils ont tous des supports disjoints et leur composition donne σ . On remarque pour finir que puisque leurs supports sont disjoints, ils commutent. On peut donc composer ces cycles dans l'ordre que l'on veut. Un exemple pour illustrer tout cela :

Exemple 1.3.5.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$. Déterminons l'orbite de 1, par le schéma suivant, où une flèche va d'un élément à son image par σ : $1 \mapsto 5 \mapsto 4 \mapsto 1$, et la boucle est bouclée. L'orbite de 1 est donc, dans l'ordre, $\{1, 5, 4\}$. Prenons ensuite un élément qui n'est pas dans cette orbite, par exemple 2. On a alors : $2 \mapsto 2$, et la boucle est déjà bouclée, 2 est un point fixe de σ . Prenons un autre élément qui n'est dans aucune des deux orbites précédentes, par exemple 3 : $3 \mapsto 6 \mapsto 3$. L'orbite de 3 est donc $\{3, 6\}$. On s'arrête là car tous les éléments de $\llbracket 1, 6 \rrbracket$ ont été rencontrés. On peut donc écrire $\sigma = (1, 5, 4) \circ (2) \circ (3, 6)$. Comme (2) n'est en fait pas un cycle (c'est l'identité), on ne l'écrit pas. On n'écrit pas non plus les symboles $\circ$. On a donc $\sigma = (1, 5, 4)(3, 6)$, et on remarque que c'est aussi égal à $(3, 6)(1, 5, 4)$.

Cette écriture comme produit de cycles de supports disjoints est plus pratique que l'écriture sous forme de deux lignes : elle est plus courte et permet de repérer immédiatement les

orbites. L'écriture à deux lignes s'en déduit très simplement.

De la décomposition précédente découle une autre, primordiale pour la suite du chapitre :

Théorème 1.3.6.

Toute permutation se décompose en produit de transpositions (on dit que S_n est engendré par ses transpositions).

Démonstration.

D'après le théorème précédent, il suffit de savoir décomposer un cycle en produit de transpositions. Soit $C = (x_1, \dots, x_p)$ un cycle. On montre alors que $C = (x_1, x_2)(x_2, x_3) \dots (x_{p-1}, x_p)$, et c'est fini.

Notons $T = (x_1, x_2)(x_2, x_3) \dots (x_{p-1}, x_p)$. Si $x \in \llbracket 1, n \rrbracket \setminus \{x_1, \dots, x_p\}$, alors x est invariant par toutes les transpositions ainsi que par le cycle, donc $T(x) = C(x) = x$. Si $1 \leq i < p$, on a

$$\begin{aligned} T(x_i) &= \left(\prod_{j=1}^{p-1} (x_j, x_{j+1}) \right) (x_i) \\ &= \left(\prod_{j=1}^{i-1} (x_j, x_{j+1}) \right) (x_i, x_{i+1}) (x_i) \\ &= \left(\prod_{j=1}^{i-1} (x_j, x_{j+1}) \right) (x_{i+1}) \\ &= x_{i+1} \\ &= C(x_i). \end{aligned}$$

On conclut simplement en montrant que $T(x_p) = x_1 = C(x_p)$ par récurrence sur p . $\square$



Cette décomposition n'est pas unique.

Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \tau_{12} \circ \tau_{23} \circ \tau_{34} = \tau_{41} \circ \tau_{12} \circ \tau_{23}$.

De plus, deux transpositions ne commutent en général pas : $\tau_{12} \circ \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \tau_{23} \circ \tau_{12}$.

1.4 Signature d'une permutation.

Définition 1.4.1.

Soit $\sigma \in S_n$. On dit qu'un couple $(i, j) \in \llbracket 1, n \rrbracket^2$ est une **inversion** de σ si $i < j$ et $\sigma(i) > \sigma(j)$. On note alors $I(\sigma)$ le nombre d'inversions de σ , et on définit la **signature** de σ , notée $\varepsilon(\sigma)$, comme étant l'entier $\varepsilon(\sigma) = (-1)^{I(\sigma)}$, qui vaut donc ± 1 . Une permutation de signature 1 est dite **paire**, **impaire** sinon.

Exemple 1.4.2.

Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 1 & 4 & 6 \end{pmatrix}$, alors $I(\sigma) = 10$ et donc $\varepsilon(\sigma) = 1$.

Proposition 1.4.3.

Toute transposition est impaire.

Démonstration.

Il suffit de voir que, si $1 \leq i < j \leq n$, $\tau_{i,j}$ a pour inversions :

- le couple (i, j) ;
- les couples (i, x) et (x, j) pour $i < x < j$.

Il y a donc bien un nombre impair d'inversions pour une transposition. $\square$

Lemme 1.4.4 (non exigible).

Si $\sigma \in S_n$, on a

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Démonstration.

En effet, $\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \frac{\prod_{1 \leq i < j \leq n} \sigma(i) - \sigma(j)}{\prod_{1 \leq i < j \leq n} i - j}$. Or

σ est une bijection, donc tout couple (i, j) tel que $i < j$ est égal à un unique couple de la forme $(\sigma(k), \sigma(\ell))$, avec nécessairement $k \neq \ell$. Cependant, si $i < j$ on ne sait pas si $k < \ell$ ou $k > \ell$. Réciproquement, pour tout couple (i, j) tel que $i < j$, $(\sigma(i), \sigma(j))$ est égal à un unique couple de la forme (k, ℓ) , avec nécessairement $k \neq \ell$. Dans tous les cas, le numérateur et le dénominateur de la dernière fraction sont égaux au signe près. Donc $\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = \pm 1$.

Remarquons que si $i < j$, alors $\frac{\sigma(i) - \sigma(j)}{i - j}$ est négatif si et seulement si (i, j) est une inversion. Comme il y a $I(\sigma)$ inversions, ce produit vaut $(-1)^{I(\sigma)}$. $\square$

Théorème 1.4.5.

L'application signature

$$\varepsilon : \begin{cases} (S_n, \circ) & \rightarrow (\{-1, 1\}, \times) \\ \sigma & \mapsto \varepsilon(\sigma) \end{cases}$$

est un morphisme de groupes. Son noyau, noté $\mathfrak{A}_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = +1\}$ est un sous-groupe de S_n appelé **groupe alterné** d'ordre n .

Démonstration (non exigible).

On utilise directement le lemme 1.4.4 (qui n'est pas exigible lui non plus) : si $\sigma, \sigma' \in S_n$, on a :

$$\begin{aligned} & \varepsilon(\sigma \circ \sigma') \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\sigma'(i)) - \sigma(\sigma'(j))}{i - j} \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\sigma'(i)) - \sigma(\sigma'(j))}{\sigma'(i) - \sigma'(j)} \times \prod_{1 \leq i < j \leq n} \frac{\sigma'(i) - \sigma'(j)}{i - j} \\ &= \prod_{1 \leq I < J \leq n} \frac{\sigma(I) - \sigma(J)}{I - J} \times \prod_{1 \leq i < j \leq n} \frac{\sigma'(i) - \sigma'(j)}{i - j} \\ &= \varepsilon(\sigma) \times \varepsilon(\sigma'). \end{aligned}$$

$\square$

Corollaire 1.4.6.

Si σ est le produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.

Exemple 1.4.7.

Un cycle de longueur p est donc de signature $(-1)^{p+1}$.

Exemple 1.4.8.

Avec

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix} = (1, 5, 4)(3, 6),$$

on a $\varepsilon(\sigma) = 1 \times (-1) = -1$.

Remarque 1.4.9.

La signature d'une permutation est très souvent définie comme ceci, et il faut donc connaître cette caractérisation, qui est de plus très pratique pour le calcul de la signature. Si cette définition est choisie, il faut dans ce cas montrer que le nombre de transpositions de n'importe quelle décomposition en produit de transpositions a toujours la même parité.

Corollaire 1.4.10.

La signature est l'unique morphisme de groupes ε de S_n dans $\{-1, 1\}$ telle que $\varepsilon(\tau) = -1$ pour toute transposition τ .

Démonstration.

Soit ε un tel morphisme. Alors ε correspond avec la signature sur l'ensemble des transpositions, et puisque $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ pour toutes permutations σ et σ' , alors si σ est le produit de p transpositions, $\varepsilon(\sigma) = (-1)^p$, qui vaut donc la signature de σ . $\square$

2 Applications multilinéaires.

Désormais, E et F sont deux $\mathbb{K}$ -espaces vectoriels.

2.1 Définition et exemples.**Définition 2.1.1.**

Soient $E_1, \dots, E_n$ et F des $\mathbb{K}$ -espaces vectoriels et f une application de $E_1 \times \dots \times E_n$ dans F . On dit que f est ***n*-linéaire** si pour tout $k \in \llbracket 1, n \rrbracket$, tout $(x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n) \in E_1 \times \dots \times E_{k-1} \times E_{k+1} \times \dots \times E_n$ l'application

$$\begin{cases} E_k & \rightarrow F \\ x & \mapsto f(x_1, \dots, x_{k-1}, x, x_{k+1}, \dots, x_n) \end{cases}$$

est linéaire.

Si $n = 2$, on dit que f est ***bilinéaire*** et, si $F = \mathbb{K}$, on dit que f est une ***forme n-linéaire***.

L'ensemble des applications n -linéaires de $E_1 \times \dots \times E_n$ dans F est noté $\mathcal{L}(E_1, E_2, \dots, E_n; F)$. Si tous les E_i sont égaux et notés E , on utilise alors la notation $\mathcal{L}_n(E; F)$. Enfin l'ensemble des formes n -linéaires sur E^n est noté $\mathcal{L}_n(E)$ (c'est-à-dire si $F = \mathbb{K}$).

Remarque 2.1.2.

- On remarque facilement que tous ces ensembles d'applications multilinéaires sont des $\mathbb{K}$ -ev.
- Une application linéaire est une application 1-linéaire.
- Toute application multilinéaire s'annule sur un vecteur dont une coordonnée est nulle, par linéarité par rapport à cette coordonnée.

Exemple 2.1.3.

Les applications suivantes sont bilinéaires :

- $\mathbb{K} \times E \rightarrow E, (\lambda, x) \mapsto \lambda \cdot x$, où E est un $\mathbb{K}$ -ev.
- $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}, (u, v) \mapsto u \cdot v$.
- $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3, (u, v) \mapsto u \wedge v$.
- $\mathcal{M}_{n,p}(\mathbb{K}) \times \mathcal{M}_{p,q}(\mathbb{K}) \rightarrow \mathcal{M}_{n,q}(\mathbb{K}), (A, B) \mapsto AB$.
- $\mathcal{L}(E, E') \times \mathcal{L}(E', E'') \rightarrow \mathcal{L}(E, E''), (f, g) \mapsto g \circ f$, où E, E', E'' sont trois $\mathbb{K}$ -espaces vectoriels (la linéarité par rapport à g est vraie sans supposer que f et g sont linéaires ; pour la linéarité par rapport à f , g doit être linéaire).
- $\mathcal{C}^0([0, 1])^2 \rightarrow \mathbb{R}, (f, g) \mapsto \int_0^1 f(t)g(t) dt$.
- $(\mathbb{R}^2)^2 \rightarrow \mathbb{R}, (u, v) \mapsto \det(u, v)$.

2.2 Applications multilinéaires symétriques, antisymétriques et alternées.**Définition 2.2.1.**

Soit $f \in \mathcal{L}_n(E; F)$, et soit $\sigma \in S_n$. On définit l'application :

$$\sigma \star f : \begin{cases} E^n & \rightarrow F \\ (x_1, \dots, x_n) & \mapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \end{cases}.$$

On vérifie que $\sigma \star f$ est aussi une application n -linéaire.

Exemple 2.2.2.

Soit $f \in \mathcal{L}_3(\mathbb{R}; F)$, et $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$.

Alors $(\sigma \star f)(x_1, x_2, x_3) = f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = f(x_3, x_1, x_2)$.

Proposition 2.2.3.

Soit $f \in \mathcal{L}_n(E; F)$ et soit $\sigma_1, \sigma_2 \in S_n$. Alors $\sigma_1 \star (\sigma_2 \star f) = (\sigma_1 \circ \sigma_2) \star f$.

Démonstration.

Soit $(x_1, \dots, x_n) \in E^n$. Alors, avec $(x_{\sigma_1(1)}, \dots, x_{\sigma_1(n)}) = (x'_1, \dots, x'_n)$,

$$\begin{aligned} [\sigma_1 \star (\sigma_2 \star f)](x_1, \dots, x_n) &= [\sigma_2 \star f](x_{\sigma_1(1)}, \dots, x_{\sigma_1(n)}) \\ &= [\sigma_2 \star f](x'_1, \dots, x'_n) \\ &= f(x'_{\sigma_2(1)}, \dots, x'_{\sigma_2(n)}) \\ &= f(x_{\sigma_1(\sigma_2(1))}, \dots, x_{\sigma_1(\sigma_2(n))}) \\ &= [(\sigma_1 \circ \sigma_2) \star f](x_1, \dots, x_n). \end{aligned}$$

$\square$

Définition 2.2.4.

Une application n -linéaire f est dite **symétrique** si pour tout $\sigma \in S_n$, $\sigma \star f = f$. Elle est dite **antisymétrique** si pour tout $\sigma \in S_n$, $\sigma \star f = \varepsilon(\sigma)f$.

Remarque 2.2.5.

On remarque facilement que l'ensemble des applications symétriques est un $\mathbb{K}$ -ev, et qu'il en est de même pour celui des applications antisymétriques.



Les caractères « symétrique » et « antisymétrique » d'une application multilinéaire n'ont de sens que si les espaces vectoriels de départ sont tous égaux. Sinon, permuter des variables qui ne sont pas de même nature n'a pas de sens.

Exemple 2.2.6. • Le produit de deux fonctions $\mathcal{C}^0(\mathbb{R})^2 \rightarrow \mathcal{C}^0(\mathbb{R})$, $(f, g) \mapsto fg$ est une application bilinéaire symétrique.

- Le produit vectoriel de $\mathbb{R}^3 \times \mathbb{R}^3$ dans $\mathbb{R}^3$ est une application bilinéaire antisymétrique.
- Le déterminant de $\mathbb{R}^2 \times \mathbb{R}^2$ dans $\mathbb{R}$ est bilinéaire, antisymétrique. En effet, il suffit de voir que $\det(v, u) = -\det(u, v)$.
- Le déterminant de $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3$ dans $\mathbb{R}$ est une application trilinéaire antisymétrique. En effet, remarquons que si $\sigma \in S_3$, alors il existe p transpositions $\tau_1, \dots, \tau_p$ telles que $\sigma = \tau_p \circ \dots \circ \tau_1$. Dans ce cas $\sigma \star \det = \tau_p \star (\tau_{p-1} \star (\dots \tau_2 \star (\tau_1 \star \det)))$. Mais pour toute transposition τ , $\tau \star \det = -\det$, car échanger deux vecteurs dans un déterminant change le signe de ce déterminant. Ainsi $\sigma \star \det = (-1)^p \det = \varepsilon(\sigma) \det$.

Remarquons d'abord que l'on peut caractériser le caractère symétrique ou antisymétrique d'une application multilinéaire par l'action des transpositions sur cette dernière.

Proposition 2.2.7.

Soit f une application n linéaire. Si pour toute transposition τ , on a $\tau \star f = f$ alors f est symétrique. De même si, pour toute transposition τ , on a $\tau \star f = -f$ alors f est antisymétrique.

Démonstration.

Facile, une fois que l'on sait décomposer une permutation en produit de transpositions, avec la propriété de morphisme de la signature ainsi que la proposition 2.2.3. $\square$

Proposition 2.2.8.

Soit $f \in \mathcal{L}_n(E; F)$ une application n -linéaire antisymétrique. Soit $(x_1, \dots, x_n) \in E^n$.

- Si τ est une transposition de S_n , alors $\tau \star f = -f$, i.e. f est changée en son opposé si l'on échange deux variables ;
- S'il existe $i \neq j$ dans $\llbracket 1, n \rrbracket$ tels que $x_i = x_j$, alors $f(x_1, \dots, x_n) = 0$;
- On ne change pas la valeur de f si l'on ajoute à une variable une combinaison linéaire des autres ;
- Si $(x_1, \dots, x_n)$ est liée, alors $f(x_1, \dots, x_n) = 0$.

Démonstration. (i) Direct car $\varepsilon(\tau) = -1$;

- On note $X = (x_1, \dots, x_n)$ et $\tilde{X} = \tau_{x_i x_j}(X)$, c'est-à-dire le vecteur obtenu à partir de X en échangeant les i^e et j^e coordonnées. Si $x_i = x_j$, on a $X = \tilde{X}$, d'où $\tau_{x_i x_j} \star f(X) = f(\tilde{X}) = f(X)$. Or d'après (i), $\tau_{x_i x_j} \star f(X) = -f(X)$, d'où $f(X) = 0$;

- Considérons par exemple que l'on rajoute à x_n la combinaison linéaire $\sum_{i=1}^{n-1} \lambda_i x_i$, avec $\lambda_i \in \mathbb{K}$. Les autres cas se traitent de la même manière. Alors, par linéarité par rapport à la dernière variable, on a :

$$f\left(x_1, \dots, x_{n-1}, x_n + \sum_{i=1}^{n-1} \lambda_i x_i\right) =$$

$$f(x_1, \dots, x_n) + \sum_{i=1}^{n-1} \lambda_i f(x_1, \dots, x_{n-1}, x_i).$$

Or d'après le point (ii), pour tout $i \in \llbracket 1, n-1 \rrbracket$, on a $f(x_1, \dots, x_{n-1}, x_i) = 0$, d'où

$$f(x_1, \dots, x_{n-1}, x_n + \sum_{i=1}^{n-1} \lambda_i x_i) = f(x_1, \dots, x_n).$$

- Si $(x_1, \dots, x_n)$ est liée, alors on peut exprimer un des vecteurs de $x_1, \dots, x_n$ en fonction des autres. Par exemple (de même dans les autres cas), $x_n = \sum_{i=1}^{n-1} \lambda_i x_i$.

Alors d'après le point (iii), on a :

$$\begin{aligned} f(x_1, \dots, x_n) &= f(x_1, \dots, x_{n-1}, \sum_{i=1}^{n-1} \lambda_i x_i) \\ &= f(x_1, \dots, x_{n-1}, 0 + \sum_{i=1}^{n-1} \lambda_i x_i) \\ &= f(x_1, \dots, x_{n-1}, 0). \end{aligned}$$

Or, d'après la remarque 2.1.2, on a $f(x_1, \dots, x_{n-1}, 0) = 0$. $\square$

Définition 2.2.9.

Une application n -linéaire est dite **alternée** si elle s'annule sur tout n -uplet dont deux éléments au moins sont égaux.

Remarque 2.2.10.

Le point (ii) de la proposition 2.2.8 montre exactement que toute application antisymétrique est alternée. En fait, ces deux notions sont équivalentes, comme le montre le théorème suivant.

Théorème 2.2.11.

Si f est une application multilinéaire, f est antisymétrique si et seulement si elle est alternée.

Démonstration.

Il reste à montrer que si f est alternée, elle est antisymétrique. f va de E^n dans F . Soit τ_{ij} une transposition de S_n , avec $i, j \in \llbracket 1, n \rrbracket$, $i < j$. Soit $X = (x_1, \dots, x_n) \in E^n$. On appelle X' le vecteur dont les i^e et j^e coordonnées valent toutes les deux $x_i + x_j$, et dont les autres coordonnées sont les mêmes que celles de X . Ou encore, $X' = (x_1, \dots, x_{i-1}, x_i + x_j, x_{i+1}, \dots, x_{j-1}, x_i + x_j, x_{j+1}, \dots, x_n)$.

On en déduit que $f(X') = 0$. Or, par multilinéarité,

$$\begin{aligned} f(X') &= f(x_1, \dots, x_{i-1}, \underline{x_i + x_j}, x_{i+1}, \dots, x_{j-1}, \underline{x_i + x_j}, x_{j+1}, \dots, x_n) \\ &= f(x_1, \dots, x_{i-1}, \underline{x_i}, x_{i+1}, \dots, x_{j-1}, \underline{x_i + x_j}, x_{j+1}, \dots, x_n) \\ &\quad + f(x_1, \dots, x_{i-1}, \underline{x_j}, x_{i+1}, \dots, x_{j-1}, \underline{x_i + x_j}, x_{j+1}, \dots, x_n) \\ &= \underbrace{f(x_1, \dots, x_{i-1}, \underline{x_i}, x_{i+1}, \dots, x_{j-1}, \underline{x_i}, x_{j+1}, \dots, x_n)}_{=0} \\ &\quad + \underbrace{f(x_1, \dots, x_{i-1}, \underline{x_i}, x_{i+1}, \dots, x_{j-1}, \underline{x_j}, x_{j+1}, \dots, x_n)}_{=f(X)} \\ &\quad + \underbrace{f(x_1, \dots, x_{i-1}, \underline{x_j}, x_{i+1}, \dots, x_{j-1}, \underline{x_i}, x_{j+1}, \dots, x_n)}_{=f(\tau_{ij}(X))} \\ &\quad + \underbrace{f(x_1, \dots, x_{i-1}, \underline{x_j}, x_{i+1}, \dots, x_{j-1}, \underline{x_j}, x_{j+1}, \dots, x_n)}_{=0} \\ &= f(X) + f(\tau_{ij}(X)) \\ &= f(X) + \tau_{ij} \star f(X), \end{aligned}$$

d'où $\tau_{ij} \star f = -f$. On en déduit que pour toute transposition τ , et toute application multilinéaire f , $\tau \star f = -f$. Soit $\sigma \in S_n$. σ s'écrit comme le produit de p transpositions, $\sigma = \tau_1 \circ \dots \circ \tau_p$. D'après le point précédent on a $\sigma \star f = \tau_1 \star (\dots \star (\tau_p \star f) \dots) = -\tau_2 \star (\dots \star (\tau_p \star f) \dots) = \dots = (-1)^p f = \varepsilon(\sigma) f$, ce qui prouve bien le résultat voulu. $\square$

En général on utilise plutôt le mot « alternée » qu'« antisymétrique ».

Exemple 2.2.12. • Le produit vectoriel entre deux vecteurs de $\mathbb{R}^3$ est une application alternée.

- L'application qui, à une famille de deux vecteurs de $\mathbb{R}^2$, associe son déterminant est une forme bilinéaire alternée. Il en est de même pour le déterminant d'une famille de trois vecteurs de $\mathbb{R}^3$ (forme trilinéaire alternée).

3 Déterminant d'une famille de vecteurs.

3.1 Définition en dimension finie.

Désormais, E est un $\mathbb{K}$ -ev de dimension finie n . Notons $\mathcal{A}_n(E)$ l'ensemble des formes n -linéaires alternées sur E^n .

Exercice 3.1.1.

Si $n = 2$, soit $\mathcal{B} = (e_1, e_2)$ une base de E , soit $f \in \mathcal{A}_2(E)$ et soit les vecteurs $x = x_1 e_1 + x_2 e_2$ et $y = y_1 e_1 + y_2 e_2$.

Développer par linéarité $f(x, y)$ par rapport à sa première coordonnée, puis sa deuxième.

Faire de même en dimension 3.

Théorème 3.1.2.

Soit $\mathcal{B} = \{e_1, \dots, e_n\}$ une base de E . Pour $(X_1, \dots, X_n) \in E^n$ et $1 \leq j \leq n$, on note $(x_{i,j})_{1 \leq i \leq n}$ les coordonnées de X_j dans $\mathcal{B}$.

(i) $\mathcal{A}_n(E)$ est une droite vectorielle, i.e. est de dimension 1.

(ii) Considérons l'application

$$\det_{\mathcal{B}} : E^n \rightarrow \mathbb{K},$$

telle que pour tout $(X_1, \dots, X_n) \in E^n$,

$$\begin{aligned} \det_{\mathcal{B}}(X_1, \dots, X_n) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n x_{i, \sigma(i)} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n x_{\sigma(i), i}. \end{aligned}$$

C'est une forme n -linéaire alternée non nulle sur E^n , et c'est la seule vérifiant

$$\det_{\mathcal{B}}(\mathcal{B}) = \det_{\mathcal{B}}(e_1, \dots, e_n) = 1.$$

(iii) Si $f \in \mathcal{A}_n(E)$, on a $f = f(\mathcal{B}) \det_{\mathcal{B}}$ (avec $f(\mathcal{B}) = f(e_1, \dots, e_n)$) et donc $\mathcal{A}_n(E) = \text{Vect}(\det_{\mathcal{B}})$.



Ici la dimension de E doit être égale à la puissance de E .

Démonstration (non exigible).

Montrons déjà l'égalité des deux formes de la définition du déterminant. Soit $\sigma \in S_n$, comme σ est une permutation, on a

$$\prod_{i=1}^n x_{i, \sigma(i)} = \prod_{i=1}^n x_{\sigma^{-1}(i), i}.$$

On conclut en remarquant que comme $\sigma \circ \sigma^{-1} = \text{Id}$, alors $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ et que $\sigma \mapsto \sigma^{-1}$ est une permutation de S_n .

(i) Ce point découlera directement du point (iii).

(ii) À vous de montrer que $\det_{\mathcal{B}}$ est n -linéaire.

Montrons déjà qu'elle est non nulle. Pour

tout i , on peut écrire $e_i = \sum_{j=1}^n \delta_{i,j} e_j$

(δ étant le symbole de Kronecker), donc

$$\det_{\mathcal{B}}(\mathcal{B}) = \det_{\mathcal{B}}(e_1, \dots, e_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n \delta_{i, \sigma(i)}.$$

Mais si $\sigma \neq \text{Id}$, il existe i tel que $i \neq \sigma(i)$, et ainsi $\delta_{i, \sigma(i)} = 0$. Par conséquent,

$$\det_{\mathcal{B}}(\mathcal{B}) = \varepsilon(\text{Id}) \prod_{i=1}^n \delta_{i, \text{Id}(i)} = 1, \text{ ce qui montre}$$

d'ailleurs un autre point de (ii).

Montrons enfin qu'elle est alternée. Soit $(X_1, \dots, X_n) \in E^n$ tel qu'il existe $i, j \in \llbracket 1, n \rrbracket$ avec $i < j$ et $X_i = X_j$. Alors :

$$\begin{aligned} \det_{\mathcal{B}}(X_1, \dots, X_n) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^n x_{k, \sigma(k)} \\ &= \sum_{\sigma \in \mathfrak{A}_n} \prod_{k=1}^n x_{k, \sigma(k)} - \sum_{\sigma \in S_n \setminus \mathfrak{A}_n} \prod_{k=1}^n x_{k, \sigma(k)}. \end{aligned}$$

On utilise alors l'idée suivante : si l'on note $\tau = \tau_{i,j}$, l'application $\mathfrak{A}_n \rightarrow S_n \setminus \mathfrak{A}_n$, $\sigma \mapsto \tau \circ \sigma$ est une bijection.

Ainsi,

$$\begin{aligned} \sum_{\sigma \in S_n \setminus \mathfrak{A}_n} \prod_{k=1}^n x_{k, \sigma(k)} &= \sum_{\sigma \in \mathfrak{A}_n} \prod_{k=1}^n x_{k, \tau \sigma(k)} \\ &= \sum_{\sigma \in \mathfrak{A}_n} \prod_{k=1}^n x_{k, \sigma(k)}, \end{aligned}$$

car $X_i = X_j$ et si $\sigma(k) \neq i$ et $\sigma(k) \neq j$, $\tau(\sigma(k)) = \sigma(k)$. On obtient donc bien $\det_{\mathcal{B}}(X_1, \dots, X_n) = 0$.

Le fait que $\det_{\mathcal{B}}$ soit la seule à vérifier $\det_{\mathcal{B}}(e_1, \dots, e_n) = 1$ découlera du point (iii).

(iii) Soient $f \in \mathcal{A}_n(E)$ et $(X_1, \dots, X_n) \in E^n$. On a :

$$\begin{aligned}
 & f(X_1, \dots, X_n) \\
 = & f\left(\sum_{i_1=1}^n x_{i_1 1} e_{i_1}, \dots, \sum_{i_n=1}^n x_{i_n n} e_{i_n}\right) \\
 = & \sum_{i_1=1}^n x_{i_1 1} f\left(e_{i_1}, \sum_{i_2=1}^n x_{i_2 2} e_{i_2}, \dots, \sum_{i_n=1}^n x_{i_n n} e_{i_n}\right) \\
 = & \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n x_{i_1 1} x_{i_2 2} \dots x_{i_n n} f(e_{i_1}, \dots, e_{i_n}) \\
 = & \sum_{i_1, \dots, i_n \in [1, n]} x_{i_1 1} \dots x_{i_n n} f(e_{i_1}, \dots, e_{i_n}) \\
 = & \sum_{\substack{i_1, \dots, i_n \in [1, n] \\ \text{tq. si } k \neq \ell \text{ alors } i_k \neq i_\ell}} x_{i_1 1} \dots x_{i_n n} f(e_{i_1}, \dots, e_{i_n}) \\
 = & \sum_{\sigma \in S_n} x_{\sigma(1)1} \dots x_{\sigma(n)n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \\
 = & \sum_{\sigma \in S_n} \left(\left(\prod_{i=1}^n x_{\sigma(i)i} \right) \varepsilon(\sigma) f(e_1, \dots, e_n) \right) \\
 = & f(e_1, \dots, e_n) \sum_{\sigma \in S_n} \left(\varepsilon(\sigma) \prod_{i=1}^n x_{\sigma(i)i} \right) \\
 = & f(\mathcal{B}) \det_{\mathcal{B}}(X_1, \dots, X_n).
 \end{aligned}$$

□

Définition 3.1.3.

Cette fonction $\det_{\mathcal{B}}$ est appelée **déterminant dans la base $\mathcal{B}$** .

Exemple 3.1.4.

Si $n = 2$, remarquons que $S_n = \{\text{Id}, \tau_{12}\}$. Si $\mathcal{B} = \{e_1, e_2\}$ est une base de E , et si $x, y \in E$ ont pour coordonnées (x_1, x_2) et (y_1, y_2) dans $\mathcal{B}$, on a : $\det_{\mathcal{B}}(x, y) = \varepsilon(\text{Id})x_1y_2 + \varepsilon(\tau_{12})x_2y_1 = x_1y_2 - x_2y_1$, ce qui est la formule habituelle du déterminant en dimension 2.

De même, si $n = 3$, on remarque que $S_n = \{\text{Id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$, ce qui donne :

$$\det_{\mathcal{B}}(x, y, z) = \underbrace{x_1y_2z_3}_{\text{Id}} + \underbrace{x_2y_3z_1}_{(1,2,3)} + \underbrace{x_3y_1z_2}_{(1,3,2)} - \underbrace{x_3y_2z_1}_{(1,3)} - \underbrace{x_2y_1z_3}_{(1,2)} - \underbrace{x_1y_3z_2}_{(2,1,3)}.$$

Remarque 3.1.5.

Dans l'exemple ci-dessus et $\mathcal{B}$ étant la base canonique, on peut remarquer que $\det_{\mathcal{B}}(x, y, z) = x \cdot (y \wedge z)$. Pouvez-vous former d'autres relations de ce type ?



Attention, la valeur du déterminant varie suivant la base, comme le montre l'exemple suivant :

Exemple 3.1.6.

On pose $E = \mathbb{R}^2$, et $\mathcal{B} = \{(1, 0), (0, 1)\} = \{e_1, e_2\}$ et $\mathcal{B}' = \{(1, 1), (2, 0)\} = \{f_1, f_2\}$ deux bases de E . On pose $v = e_1 + e_2$ et $w = e_1 - e_2$. Alors $v = f_1$ et $w = -f_1 + f_2$. Alors $\det_{\mathcal{B}}(v, w) = -2$ et $\det_{\mathcal{B}'}(v, w) = 1$.

Théorème 3.1.7.

Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et $\mathcal{F}$ une famille de n vecteurs de E . On a alors :

- (i) **Formule de changement de base** : $\det_{\mathcal{B}}(\mathcal{F}) = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(\mathcal{F})$.
- (ii) $\mathcal{F}$ est une base ssi $\det_{\mathcal{B}}(\mathcal{F}) \neq 0$. Dans ce cas $\det_{\mathcal{F}}(\mathcal{B}) = \frac{1}{\det_{\mathcal{B}}(\mathcal{F})}$.

Démonstration.

Ces résultats découlent de résultats précédents :

- (i) On utilise le point (iii) du théorème 3.1.2. Si on appelle f l'application $\det_{\mathcal{B}}$, f est n -linéaire alternée et donc $f = f(\mathcal{B}') \det_{\mathcal{B}'}$, ce qui exactement le résultat voulu.
- (ii) On utilise le point (iv) de la proposition 2.2.8 : D'une part, si $\mathcal{F}$ est liée, on a $\det_{\mathcal{B}}(\mathcal{F}) = 0$, d'autre part, si $\mathcal{F}$ n'est pas liée, comme $\text{card}(\mathcal{F}) = n$, $\mathcal{F}$ est alors une base, donc $\det_{\mathcal{F}}(\mathcal{F}) = 1$, et le point i précédent assure que $\det_{\mathcal{F}}(\mathcal{F}) = \det_{\mathcal{F}}(\mathcal{B}) \det_{\mathcal{B}}(\mathcal{F})$.

□

Exemple 3.1.8.

En reprenant les bases $\mathcal{B}$ et $\mathcal{B}'$ de l'exemple précédent, on trouve bien $\det_{\mathcal{B}}(\mathcal{B}') = -2$ et $\det_{\mathcal{B}'}(\mathcal{B}) = -\frac{1}{2}$.

3.2 Interprétation en géométrie réelle.

On considère ici le cas où le corps de base est $\mathbb{K} = \mathbb{R}$.

a Orientation d'un ev réel de dimension finie (HP).
Définition 3.2.1.

On dit que deux bases $\mathcal{B}$ et $\mathcal{B}'$ de E ont la même orientation si $\det_{\mathcal{B}}(\mathcal{B}') > 0$. La relation « avoir la

même orientation » est une relation d'équivalence, et il y a exactement deux orientations possibles.

Démonstration.

Le fait qu'il s'agisse d'une relation d'équivalence ne pose aucune difficulté :

- *réflexivité* : $\det_{\mathcal{B}}(\mathcal{B}) = 1$.
- *symétrie* : $\det_{\mathcal{B}'}(\mathcal{B}) = \frac{1}{\det_{\mathcal{B}}(\mathcal{B}')}$, donc ces deux déterminants ont le même signe.
- *transitivité* : $\det_{\mathcal{B}}(\mathcal{B}'') = \det_{\mathcal{B}}(\mathcal{B}') \cdot \det_{\mathcal{B}'}(\mathcal{B}'')$.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E : elle définit une orientation. Soit $\mathcal{B}' = (-e_1, \dots, e_n)$ une seconde base. Puisque $\det_{\mathcal{B}}(\mathcal{B}') = -1$, $\mathcal{B}'$ définit une seconde orientation. Montrons qu'il n'y en pas d'autre : soit $\mathcal{B}''$ une troisième base. Puisque $\det_{\mathcal{B}}(\mathcal{B}'') = \det_{\mathcal{B}}(\mathcal{B}') \cdot \det_{\mathcal{B}'}(\mathcal{B}'')$, et $\det_{\mathcal{B}}(\mathcal{B}') < 0$, alors $\det_{\mathcal{B}}(\mathcal{B}'')$ et $\det_{\mathcal{B}'}(\mathcal{B}'')$ sont de signes opposés, donc l'un des deux est strictement positif, donc $\mathcal{B}''$ a la même orientation que $\mathcal{B}$ ou que $\mathcal{B}'$. $\square$

Orienter E , c'est dire que l'une de ces deux orientations est *directe*. Les bases représentant l'autre orientation seront alors dites *indirectes*.

Exemple 3.2.2.

Pour tout $\theta \in \mathbb{R}$, les bases $(\vec{u}_\theta, \vec{v}_\theta)$ ont la même orientation que la base canonique dans $\mathbb{R}^2$.

b Déterminant et aire dans le plan.

On considère ici que $E = \mathbb{R}^2$, que l'on munit du produit scalaire usuel ainsi que de la norme euclidienne induite. Notons (e_1, e_2) la base canonique de $\mathbb{R}^2$.

On considère que $\mathbb{R}^2$ est orienté par sa base canonique.

Proposition 3.2.3.

Soit (u, v) deux vecteurs de $\mathbb{R}^2$. Alors $\det_{(e_1, e_2)}(u, v)$ est l'aire algébrique du parallélogramme engendré par (u, v) (voir la figure XXVII.1). Elle est donc nulle si u et v sont colinéaires, strictement positive si (u, v) est orientée directement et strictement négative sinon.

Démonstration.

Posons $u = (u_1, u_2)$ et $v = (v_1, v_2)$ (voir la figure XXVII.2). Quitte à échanger u et v , on peut supposer que (u, v) est directe, l'aire algébrique du parallélogramme est donc positive.

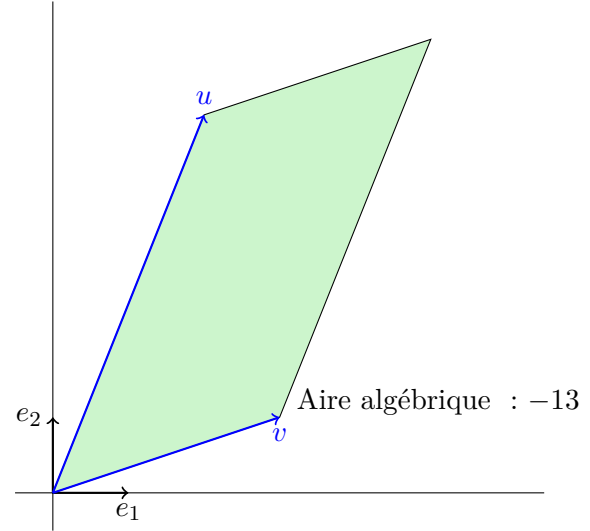


FIGURE XXVII.1 – Aire du parallélogramme engendré par (u, v) , avec $u = (2, 5)$ et $v = (3, 1)$.

On peut aussi supposer que $u \neq (0, 0)$. Rappelons que l'aire d'un parallélogramme est le produit de la longueur d'un de ses côtés par la hauteur correspondante. Avec $u' = (-u_2, u_1)$, on remarque que $u \cdot u' = 0$ donc que u et u' sont orthogonaux, ainsi que $\|u\| = \|u'\|$. La hauteur correspondant à u est donc $h = \left| \frac{u'}{\|u'\|} \cdot v \right|$ et l'aire du parallélogramme est donc $h \|u\| = |u' \cdot v| = |u_1 v_2 - u_2 v_1|$. $\square$

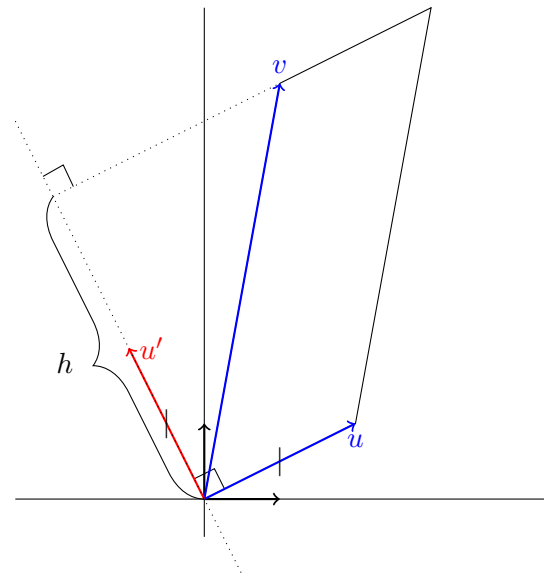


FIGURE XXVII.2 – Illustration du lien entre l'aire d'un parallélogramme et le déterminant.

Remarque 3.2.4.

Ce résultat est vrai en considérant le déterminant pris dans une base orthonormée directe quelconque, et non juste dans la base canonique.

Exemple 3.2.5.

Si u est un vecteur non nul de $\mathbb{R}^2$ et $\mathcal{B}$ est la base canonique de $\mathbb{R}^2$, on obtient directement une représentation cartésienne de la droite engendrée par u par :

$$\forall x \in \mathbb{R}^2, x \in \text{Vect } u \Leftrightarrow \det_{\mathcal{B}}(x, u) = 0.$$

c Déterminant et volume dans l'espace.

On considère ici que $E = \mathbb{R}^3$, que l'on munit du produit scalaire usuel ainsi que de la norme euclidienne induite. Notons (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$.

On considère que $\mathbb{R}^3$ est orienté par sa base canonique.

Proposition 3.2.6.

Soit (u, v, w) trois vecteurs de $\mathbb{R}^3$. Alors $\det_{(e_1, e_2, e_3)}(u, v, w)$ est le volume algébrique du pavé engendré par (u, v, w) (voir la figure XXVII.3). Elle est donc nulle si (u, v, w) sont coplanaires, strictement positive si (u, v, w) est orientée directement et strictement négative sinon.

Démonstration.

Cette preuve est laissée aux soins du lecteur : pensez à utiliser le produit vectoriel ! $\square$

Remarque 3.2.7.

Ce résultat est vrai en considérant le déterminant pris dans une base orthonormée directe quelconque, et non juste dans la base canonique.

Exemple 3.2.8.

Si u et v sont des vecteurs non colinéaires de $\mathbb{R}^3$ et $\mathcal{B}$ est la base canonique de $\mathbb{R}^3$, on obtient directement une représentation cartésienne du plan engendré par u et v par :

$$\forall x \in \mathbb{R}^3, x \in \text{Vect } (u, v) \Leftrightarrow \det_{\mathcal{B}}(x, u, v) = 0.$$

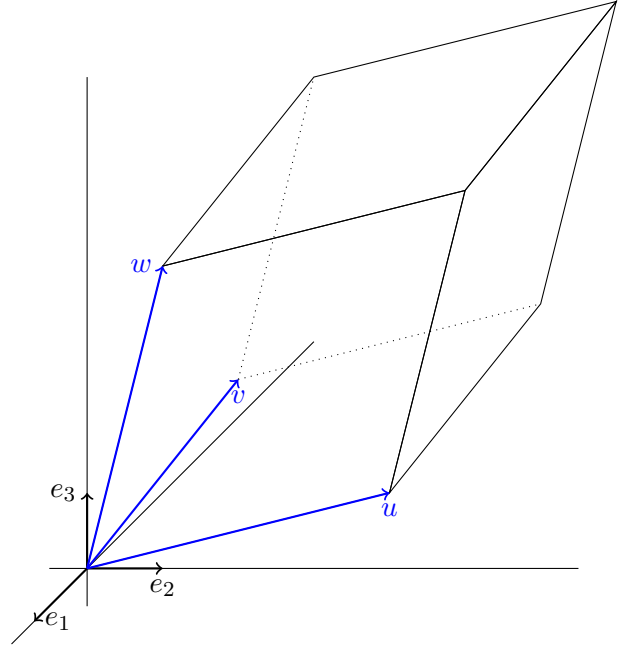


FIGURE XXVII.3 – Représentation du pavé engendré par (u, v, w) .

4 Déterminant d'un endomorphisme.

E est un $\mathbb{K}$ -ev- de dimension n , dont une base est $\mathcal{B} = (e_1, \dots, e_n)$. Soit $f \in \mathcal{L}(E)$.

Remarque 4.0.1.

Pour $\mathcal{F} = (x_1, \dots, x_n) \in E^n$, on commettra le (léger) abus de notation suivant :

$$f(\mathcal{F}) = (f(x_1), \dots, f(x_n)).$$

Définition 4.0.2.

On appelle *déterminant* de f le scalaire noté $\det f$ tel que

$$\det f = \det_{\mathcal{B}}(f(\mathcal{B})) = \det_{\mathcal{B}}(f(e_1), \dots, f(e_n)).$$

Ce scalaire ne dépend pas de la base $\mathcal{B}$ choisie.

Remarque 4.0.3.

Pour pouvoir calculer ce déterminant, il faut que pour tout i , $f(e_i) \in E$, donc que f soit un endomorphisme.

Démonstration.

On introduit l'application

$$\varphi : \begin{cases} E^n & \rightarrow \mathbb{K} \\ (v_1, \dots, v_n) & \mapsto \det_{\mathcal{B}}(f(v_1), \dots, f(v_n)) \end{cases}.$$

On montre que φ est n -linéaire (à vous de le faire) et alternée :

supposons qu'il existe $i, j \in \llbracket 1, n \rrbracket$ tels que $i \neq j$ et $v_i = v_j$. Il faut montrer que $\varphi(v_1, \dots, v_n) = 0$. On a $\varphi(v_1, \dots, v_n) = \det_{\mathcal{B}}(f(v_1), \dots, f(v_n))$. Mais $f(v_i) = f(v_j)$ donc $\det_{\mathcal{B}}(f(v_1), \dots, f(v_n)) = 0$, car $\det_{\mathcal{B}}$ est alterné.

Il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_{\mathcal{B}}$, et on a vu que $\lambda = \varphi(\mathcal{B})$.

Soit $\mathcal{B}'$ une seconde base de E .

Alors :

$$\begin{aligned} \det_{\mathcal{B}'}(f(\mathcal{B}')) &= \det_{\mathcal{B}'}(\mathcal{B}) \cdot \det_{\mathcal{B}} f(\mathcal{B}') \\ &= \det_{\mathcal{B}'}(\mathcal{B}) \cdot \varphi(\mathcal{B}') \\ &= \det_{\mathcal{B}'}(\mathcal{B}) \cdot \varphi(\mathcal{B}) \cdot \det_{\mathcal{B}}(\mathcal{B}') \\ &= \varphi(\mathcal{B}) \\ &= \det_{\mathcal{B}}(f(\mathcal{B})). \end{aligned}$$

□

Exemple 4.0.4.

Soit $g : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ une application linéaire tel que

$$g(e_1) = e_1 \text{ et } g(e_2) = 0. \text{ Alors } \det g = \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} = 0.$$

$$\text{Et d'autre part } \det(g + \text{Id}_{\mathbb{R}^2}) = \begin{vmatrix} 2 & 0 \\ 0 & 1 \end{vmatrix} = 2.$$

$$\begin{aligned} \text{Si l'on prend la base } \mathcal{B}' &= \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) = \\ (f_1, f_2), \text{ alors on trouve } g(f_1) &= e_1 = \frac{1}{2}(f_1 + f_2) \\ \text{et } g(f_2) &= e_1 = \frac{1}{2}(f_1 + f_2), \text{ d'où en effet } \det g = \\ \det_{\mathcal{B}'}(g(\mathcal{B}')) &= \begin{vmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{vmatrix} = 0 \text{ et } \det(g + \text{Id}_{\mathbb{R}^2}) = \\ \begin{vmatrix} 3/2 & 1/2 \\ 1/2 & 3/2 \end{vmatrix} &= 9/4 - 1/4 = 2. \end{aligned}$$

Proposition 4.0.5.

Soit $\mathcal{F}$ une famille de n vecteurs de E .

1. $\det_{\mathcal{B}}(f(\mathcal{F})) = \det f \times \det_{\mathcal{B}}(\mathcal{F})$;
2. si $g \in \mathcal{L}(E)$, $\det(g \circ f) = \det f \times \det g$;
3. $\det(\text{Id}_E) = 1$;
4. f est un automorphisme de E ssi $\det f \neq 0$;
5. Si $\det f \neq 0$, alors $\det(f^{-1}) = \frac{1}{\det f}$.
6. $\det(\lambda f) = \lambda^n \det f$.

Démonstration. 1. En utilisant la démonstration précédente, on a : $\det_{\mathcal{B}}(f(\mathcal{F})) = \varphi(\mathcal{F}) = \varphi(\mathcal{B}) \times \det_{\mathcal{B}}(\mathcal{F})$, et on a montré que $\varphi(\mathcal{B}) = \det f$.

2.

$$\begin{aligned} \det(g \circ f) &= \det_{\mathcal{B}}(g(f(e_1)), \dots, g(f(e_n))) \\ &= \det_{\mathcal{B}} \underbrace{g(f(e_1), \dots, f(e_n))}_{=\mathcal{F}} \\ &= \det_{\mathcal{B}} g(\mathcal{F}) = \det g \times \det_{\mathcal{B}} \mathcal{F} \\ &= \det g \times \det f. \end{aligned}$$

3. $\det(\text{Id}_E) = \det_{\mathcal{B}}(\text{Id}_E(\mathcal{B})) = \det_{\mathcal{B}}(\mathcal{B}) = 1$.

4. $(\Rightarrow)$: f^{-1} existe et donc $\det(f \circ f^{-1}) = \det \text{Id}_E = 1$. Or d'après le point 2, $\det(f \circ f^{-1}) = \det f \times \det(f^{-1})$, donc on obtient $\det f \neq 0$, et aussi $\det f^{-1} = \frac{1}{\det f}$ (ce qui par ailleurs prouve le point 5).
 $(\Leftarrow)$: On suppose que $\det f \neq 0$. Donc $\det_{\mathcal{B}}(f(\mathcal{B})) \neq 0$, d'où $f(\mathcal{B})$ est une base de E , et ainsi f est un automorphisme.

6. Par multilinéarité du déterminant,
 $\det(\lambda f) = \det_{\mathcal{B}}(\lambda f(e_1), \dots, \lambda f(e_n)) = \lambda^n \det_{\mathcal{B}}(f(e_1), \dots, f(e_n)) = \lambda^n \det f$.

□

Exemple 4.0.6.

$\det(2\text{Id}_{\mathbb{R}^2}) = 2^2 \det \text{Id}_{\mathbb{R}^2} = 4$, mais $\det(2\text{Id}_{\mathbb{R}^3}) = 2^3 \det \text{Id}_{\mathbb{R}^3} = 8$.

Remarque 4.0.7.

Le déterminant est un morphisme de groupes de $\mathcal{GL}(E)$ dans $\mathbb{K}^*$.



De manière générale, $\det(f + g) \neq \det f + \det g$.

5 Déterminant d'une matrice carrée.

5.1 Définitions et propriétés.

Définition 5.1.1.

Soit $A \in \mathcal{M}_n(\mathbb{K})$ et $\mathcal{C} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$. Alors, il existe une unique $f \in \mathcal{L}(\mathbb{K}^n)$ telle que $A = \text{Mat}_{\mathcal{C}}(f)$. On définit alors le déterminant de A comme étant le scalaire $\det f$.

Ainsi, si $A = (a_{i,j})_{1 \leq i,j \leq n}$, en notant $(C_1, \dots, C_n)$ les colonnes de A , on a

$$\det A = \det_{\mathcal{C}}(C_1, \dots, C_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}.$$

On retrouve les mêmes propriétés que pour le déterminant d'une application linéaire :

Théorème 5.1.2.

Soit E un $\mathbb{K}$ -espace vectoriel et $f \in \mathcal{L}(E)$, et soit $\mathcal{B}$ une base quelconque de E . Alors,

$$\det(f) = \det(\text{Mat}_{\mathcal{B}}(f)).$$

De même, si $\mathcal{F}$ est une famille de n vecteurs de E , $\det_{\mathcal{B}}(\mathcal{F}) = \det(\text{Mat}_{\mathcal{B}}(\mathcal{F}))$.

Démonstration.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . Avec $A = (a_{i,j}) = \text{Mat}_{\mathcal{B}}(f)$, on a, d'une part,

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i\sigma(i)}.$$

De plus,

$$\begin{aligned} \det(f) &= \det_{\mathcal{B}}(f(\mathcal{B})) = \det_{\mathcal{B}} \left(\sum_{i=1}^n a_{i,j} e_i \right)_{j \in \llbracket 1, n \rrbracket} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i\sigma(i)} \\ &= \det A \end{aligned}$$

On procède de même pour une famille de vecteurs. $\square$

Proposition 5.1.3.

Soit $A, B \in \mathcal{M}_n(\mathbb{K})$.

1. $\det(A \times B) = \det A \times \det B$.
2. $\det I_n = 1$.
3. A est inversible si et seulement si $\det A \neq 0$.
Si $\det A \neq 0$, on a $\det A^{-1} = \frac{1}{\det A}$.
4. $\det A^{\top} = \det A$.
5. Si $\lambda \in \mathbb{K}$, $\det(\lambda A) = \lambda^n \det(A)$.

Démonstration.

1., 2., 3. et 5. immédiats d'après les propriétés du déterminant d'une application linéaire.

4. si $A = (a_{ij})$, on note $A^{\top} = (b_{ij})$ avec $b_{ij} = a_{ji}$.

Alors :

$$\begin{aligned} \det A^{\top} &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n b_{i,\sigma(i)} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{\sigma(i),i} \\ &\stackrel{\text{déjà vu}}{=} \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)} \\ &= \det A. \end{aligned}$$

$\square$

Remarque 5.1.4.

Le déterminant d'une matrice carrée est donc une forme n -linéaire alternée de la famille de ses colonnes, ainsi que de ses lignes.

Remarque 5.1.5.

Le déterminant est un morphisme de groupes de $\text{GL}_n(\mathbb{K})$ dans $\mathbb{K}^*$.

Exercice 5.1.6.

Montrer de deux manières différentes que deux matrices semblables ont même déterminant.

5.2 Matrices triangulaires et triangulaires par blocs.

Lemme 5.2.1.

Soit $\sigma \in S_n$ tel que pour tout $i \in \llbracket 1, n \rrbracket$, $i \leq \sigma(i)$. Alors $\sigma = \text{Id}$.

Démonstration.

Posons l'hypothèse de récurrence (H_i) : pour tout k de $n-i$ à n , $\sigma(k) = k$.

→ Initialisation : par hypothèse on a $\sigma(n) \geq n$. Mais $\sigma(n) \in \llbracket 1, n \rrbracket$, donc nécessairement $\sigma(n) = n$. (H_0) est donc vraie.

→ Hérité : supposons (H_i) vraie pour $i \in \llbracket 0, n-1 \rrbracket$. Alors pour tout $k \geq n-i$, $\sigma(k) = k$. Par injectivité de σ il vient donc : pour tout $k < n-i$, $\sigma(k) < n-i$. En particulier $n-i-1 \leq \sigma(n-i-1) < n-i$, et donc $\sigma(n-i-1) = n-i-1$, et (H_{i+1}) est vérifiée.

On a donc bien $\sigma = \text{Id}$. $\square$

Théorème 5.2.2.

Soit $A = (a_{i,j})$ une matrice triangulaire. Alors,

$$\det A = \prod_{i=1}^n a_{i,i}.$$

Démonstration.

Supposons A triangulaire supérieure. Alors pour tous $i, j \in \llbracket 1, n \rrbracket$, $i > j \Rightarrow a_{i,j} = 0$. On sait que

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}.$$

Soit $\sigma \in S_n$ tel que $\sigma \neq \text{Id}$. Alors d'après le lemme 5.2.1, il existe i_0 tel que $\sigma(i_0) < i_0$. Alors $a_{i_0\sigma(i_0)} = 0$ donc $\prod_{i=1}^n a_{i,\sigma(i)} = 0$. Ainsi, dans la somme $\sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$, seule le terme pour $\sigma = \text{Id}$ est non nul, et donc

$$\det A = \prod_{i=1}^n a_{i,\text{Id}(i)} = \prod_{i=1}^n a_{i,i}.$$

On a évidemment le même résultat pour les matrices triangulaires inférieures. $\square$

Exemple 5.2.3.

Une matrice A dont les coefficients sont écrits entre barres verticales signifie $\det A$.

$$\begin{vmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ -51 & -4 & 2 \end{vmatrix} = \begin{vmatrix} 3 & 1 & -16 \\ 0 & 1 & 15 \\ 0 & 0 & 2 \end{vmatrix} = 6.$$

Remarque 5.2.4.

Avec ce résultat on retrouve facilement qu'une matrice triangulaire est inversible si et seulement si elle n'a pas de zéro sur la diagonale.

Proposition 5.2.5.

Soit $M = \begin{pmatrix} A & B \\ 0 & I_p \end{pmatrix}$ une matrice par blocs de $\mathcal{M}_{n+p}(\mathbb{K})$, avec $A \in \mathcal{M}_n(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. Alors

$$\det M = \det A.$$

Démonstration.

Considérons l'application $f : (\mathcal{M}_{n,1}(\mathbb{K}))^n \rightarrow \mathbb{K}$ telle que $f(x_1, \dots, x_n) = \det M$, avec $M = \begin{pmatrix} A & B \\ 0_{p,n} & \text{Id}_n \end{pmatrix}$ et B fixée, où A est la matrice de $(x_1, \dots, x_n)$ dans la base canonique. Avec un léger abus de notation, on notera ceci $f(A)$. Cette

application est n -linéaire alternée, donc il existe $k \in \mathbb{K}$ telle que pour tout $A \in \mathcal{M}_n(\mathbb{K})$, $f(A) = k \det A$. Or pour $A = I_p$, M est une matrice triangulaire de déterminant 1, donc $k = 1$, et le résultat est démontré. $\square$

Remarque 5.2.6.

Nous avons bien sûr de la même manière $\det \begin{pmatrix} I_n & B \\ 0 & C \end{pmatrix} = \det C$.

Théorème 5.2.7 (Déterminant d'une matrice triangulaire par blocs).

Soit $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ une matrice triangulaire par blocs. Alors,

$$\det M = \det A \times \det C.$$

Démonstration.

Il suffit d'écrire

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & C \end{pmatrix} \begin{pmatrix} A & B \\ 0 & I_p \end{pmatrix}.$$

$\square$

Remarque 5.2.8.

Le résultat s'adapte évidemment dans le cas des matrices triangulaires inférieures par blocs, ainsi que dans le cas de matrices triangulaires par blocs avec plus de deux blocs sur la diagonale.



La formule ne se généralise pas aux matrices par blocs non triangulaires. Ainsi,

$$\begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \neq \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} - \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}.$$

5.3 Opérations élémentaires et pivot de Gauss.

La méthode présentée ci-après est la méthode de base : elle fonctionne toujours, et est la plus rapide dans la grande majorité des cas.

On fixe $A \in \mathcal{M}_n(\mathbb{K})$.

Théorème 5.3.1. 1. Ajouter à une ligne ou une colonne de A une combinaison linéaire des autres lignes ou colonnes ne change pas le déterminant de A .

2. Multiplier une ligne ou une colonne de A par une constante $\lambda \in \mathbb{K}$, change le déterminant de A en $\lambda \det A$.

3. Échanger deux lignes ou deux colonnes de A change le déterminant de A en $-\det A$.

Démonstration.

C'est direct, car le déterminant est une fonction n -linéaire alternée de ses lignes, ainsi que de ses colonnes.

On peut aussi en donner une preuve matricielle. Effectuer chacune de ces opérations élémentaires revient à multiplier A par une certaine matrice inversible M . Ainsi le déterminant de A est changé en $\det M \times \det A$. Il suffit donc de calculer le déterminant de M , ce qui ne pose aucun problème dans les deux premiers cas, car alors M est triangulaire. Dans le cas 3, remarquons (par exemple pour les lignes) que $L_i \leftrightarrow L_j$ est équivalente à la suite d'opérations suivantes :

Ligne n° i	Ligne n° j	Opération effectuée
L_i	L_j	
$L_i + L_j$	L_j	$L_i \leftarrow L_i + L_j$
$L_i + L_j$	$-L_i$	$L_j \leftarrow L_j - L_i$
L_j	$-L_i$	$L_i \leftarrow L_i + L_j$
L_j	L_i	$L_i \leftarrow -L_i$

Il suffit donc de multiplier $\det A$ par le produit des déterminants de ces opérations successives, qui sont tous 1, sauf le dernier qui vaut -1 : ce produit vaut bien -1 . $\square$

Remarque 5.3.2.

À l'instar d'un calcul de rang, il est possible de mélanger des opérations sur les lignes et sur les colonnes pour calculer un déterminant de matrice.

Exemple 5.3.3.

Avec l'opération $C_2 \leftarrow 2C_2 - 3C_1$, on a

$$\begin{vmatrix} 2 & 3 \\ 5 & 7 \end{vmatrix} = \frac{1}{2} \begin{vmatrix} 2 & 0 \\ 5 & -1 \end{vmatrix} \underset{\text{triang.}}{=} -1.$$

Exemple 5.3.4.

Avec les opérations $C_2 \leftarrow 2C_2 - 3C_1$ et $C_3 \leftarrow$

$2C_3 - 5C_1$, on a

$$\begin{vmatrix} 2 & 3 & 5 \\ 4 & 3 & -1 \\ 3 & -1 & 2 \end{vmatrix} = \frac{1}{2^2} \begin{vmatrix} 2 & 0 & 0 \\ 4 & -6 & -22 \\ 3 & -11 & -11 \end{vmatrix} \\ = \frac{1}{4} \times 2 \times \begin{vmatrix} -6 & -22 \\ -11 & -11 \end{vmatrix} \\ = -88.$$

5.4 Développement par rapport à une ligne ou une colonne.

Définition 5.4.1.

Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$.

1. On appelle *mineur d'ordre* (i, j) de A le scalaire $\Delta_{i,j} = \det A_{i,j}$ où $A_{i,j}$ est la matrice de $\mathcal{M}_{n-1}(\mathbb{K})$ obtenue à partir de A en supprimant la i^{e} ligne et la j^{e} colonne.
2. On appelle *cofacteur d'ordre* (i, j) de A le scalaire $(-1)^{i+j} \Delta_{i,j}$.
3. On appelle *comatrice* de A notée $\text{com}(A)$ la matrice des cofacteurs *i.e.* $\text{com}(A) = ((-1)^{i+j} \Delta_{i,j})_{1 \leq i, j \leq n} \in \mathcal{M}_n(\mathbb{K})$.

Exemple 5.4.2.

Soit $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 2 & 0 \\ 0 & 1 & -2 \end{pmatrix}$. On a alors $\text{com } A = \begin{pmatrix} -4 & 6 & 3 \\ 4 & -2 & -1 \\ 0 & 0 & -4 \end{pmatrix}$.

Théorème 5.4.3 (Développement par rapport à une ligne ou une colonne).

Soit $A \in \mathcal{M}_n(\mathbb{K})$, $A = (a_{i,j})$, soit $i, j \in \llbracket 1, n \rrbracket$.

1. Développement par rapport à la i^{e} ligne :

$$\det A = \sum_{k=1}^n (-1)^{i+k} a_{i,k} \Delta_{i,k}.$$

2. Développement par rapport à la j^{e} colonne :

$$\det A = \sum_{k=1}^n (-1)^{k+j} a_{k,j} \Delta_{k,j}.$$

Démonstration.

On ne démontre que le développement par rapport à la première ligne :

$$\begin{aligned}
 \det A &= |a_{ij}| = \begin{vmatrix} L_1 \\ M \end{vmatrix} \\
 &= \begin{vmatrix} a_{11} & 0 & \dots & 0 \\ M & & & \end{vmatrix} + \begin{vmatrix} 0 & a_{12} & 0 & \dots & 0 \\ M & & & & \end{vmatrix} + \dots + \begin{vmatrix} 0 & \dots & 0 & a_{1n} \\ M & & & \end{vmatrix} \\
 &= a_{11} \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ M & & & \end{vmatrix}}_{=\delta_1} + a_{12} \underbrace{\begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ M & & & & \end{vmatrix}}_{=\delta_2} + \dots + a_{1n} \underbrace{\begin{vmatrix} 0 & \dots & 0 & 1 \\ M & & & \end{vmatrix}}_{=\delta_n} \\
 &= \sum_{j=1}^n a_{1j} \delta_j.
 \end{aligned}$$

Calculons δ_j . Pour cela on note $C_1, \dots, C_n$ les n colonnes

de la matrice $M = \begin{pmatrix} a_{21} & \dots & a_{2n} \\ \dots & & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$:

$$\begin{aligned}
 \delta_j &= \begin{vmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ C_1 & \dots & C_{j-1} & C_j & C_{j+1} & \dots & C_n \end{vmatrix} \\
 &= (-1)^{j-1} \begin{vmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ C_j & C_1 & \dots & C_{j-1} & C_{j+1} & \dots & C_n \end{vmatrix} \\
 &= (-1)^{j-1} \begin{vmatrix} C_1 & \dots & C_{j-1} & C_{j+1} & \dots & C_n \end{vmatrix},
 \end{aligned}$$

car c'est une matrice triangulaire par blocs.

Or $(C_1 \dots C_{j-1} C_{j+1} \dots C_n) = A_{1j}$, d'où $\delta_j = (-1)^{j+1} \Delta_{1j}$ et on a le résultat voulu.

On peut aussi observer ce résultat directement dans la définition du déterminant :

$$\begin{aligned}
 \det(A) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^n a_{k, \sigma(k)} \\
 &= \sum_{j=1}^n \sum_{\sigma \in S_n, \sigma(i)=j} \varepsilon(\sigma) \prod_{k=1}^n a_{k, \sigma(k)} \\
 &= \sum_{j=1}^n a_{1j} \sum_{\sigma \in S_n, \sigma(i)=j} \varepsilon(\sigma) \prod_{\substack{k=1 \\ k \neq j}}^n a_{k, \sigma(k)}
 \end{aligned}$$

Il suffit ensuite de remarquer que, pour chaque $1 \leq j \leq n$, il y a bien $(n-1)!$ permutations σ vérifiant $\sigma(i) = j$ puis que le terme

$$\sum_{\sigma \in S_n, \sigma(i)=j} \varepsilon(\sigma) \prod_{\substack{k=1 \\ k \neq j}}^n a_{k, \sigma(k)}$$

correspond bien au cofacteur d'ordre i, j de A . Nous laissons le lecteur intéressé montrer cela. $\square$

Remarque 5.4.4.

Dans $\mathbb{R}^3$ et la base canonique $\mathcal{B}$, on retrouve les relations observées en début de chapitre : $\det_{\mathcal{B}}(x, y, z) = x \cdot (y \wedge z)$ etc.

Remarque 5.4.5.

• Cette méthode n'est à utiliser que lorsqu'il y a une ligne ou une colonne contenant un ou deux coefficients non nuls seulement, sinon elle est beaucoup plus longue que la méthode du pivot de Gauss.

N'oubliez pas non plus que si l'on veut développer par rapport à une ligne ou une colonne, il existe d'autres lignes ou colonnes que les premières !

• Pour démontrer le théorème 5.4.3, nous avons utilisé le résultat 5.2.7. Il est possible de démontrer ces deux résultats dans l'autre sens, mais attention à ne pas utiliser un résultat dans sa propre démonstration.

Exemple 5.4.6.

Comparer le calcul de $\begin{vmatrix} 1 & 3 & 4 \\ 2 & -1 & 2 \\ -5 & 1 & 7 \end{vmatrix}$ avec les deux méthodes (développement ou pivot de Gauss).

Corollaire 5.4.7.

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors $A \times (\text{com } A)^\top = (\text{com } A)^\top \times A = (\det A) \cdot I_n$. En particulier, si A est inversible, alors $A^{-1} = \frac{1}{\det A} \cdot (\text{com } A)^\top$.

Remarque 5.4.8.

Ce résultat est inutilisable en pratique pour calculer des inverses de matrices. Si $n = 2$, ça va (on retrouve la formule de l'inverse d'une matrice 2×2), pour $n = 3$, c'est trop long, et pour $n \geq 4$ c'est un cauchemar. Essayez !

Démonstration.

On note $A = (a_{ij})$ et $(\text{com } A)^\top = (b_{ij})$ avec $b_{ij} = (-1)^{i+j} \Delta_{ji}$. On note également $A \cdot (\text{com } A)^\top = (C_{ij})_{i,j}$, donc

$$C_{ij} = \sum_{k=1}^n a_{ik} b_{kj} = \sum_{k=1}^n (-1)^{k+j} a_{ik} \Delta_{jk}.$$

→ si $i = j$: grâce à la formule de développement par rapport à la j^{e} ligne, on trouve $C_{ij} = \det A$.

→ si $i \neq j$: on note Δ la matrice obtenue à partir de A en remplaçant la j^{e} ligne par la i^{e} ligne : cette matrice a deux lignes égales, donc $\det \Delta = 0$. On développe $\det \Delta$ par rapport à la j^{e} ligne, et on a :

$$0 = \det \Delta = \sum_{k=1}^n (-1)^{k+j} a_{ik} \Delta_{jk} = C_{ij},$$

d'où le résultat.

On procède de la même manière pour calculer $(\text{com } A)^\top \times A$. $\square$

Proposition 5.4.9 (Déterminant de Vandermonde).

Soit $n \in \mathbb{N}^*$ et $x_0, \dots, x_n$ $n+1$ scalaires. On définit le *déterminant de Vandermonde* par :

$$V(x_0, x_1, \dots, x_n) = \begin{vmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{vmatrix}.$$

Alors,

$$V(x_0, \dots, x_n) = \prod_{0 \leq i < j \leq n} (x_j - x_i).$$

Démonstration.

Ce déterminant est un classique parmi les classiques. Il est possible de le calculer directement par pivot de Gauss. Ici, on le démontre par récurrence.

Les cas $n = 0$ ou $n = 1$ sont évidents : $V(x_0) = 1$ et $V(x_0, x_1) = x_1 - x_0$.

Soit $n \in \mathbb{N}$ tel que le résultat soit vrai au rang n . Considérons le polynôme $V(x_0, \dots, x_n, X)$. En le développant par rapport à la dernière ligne, on voit qu'il est de degré au plus $n+1$, et que le terme en X^{n+1} a pour coefficient $V(x_0, \dots, x_n)$. Or il est aisé de voir qu'il a pour racines $x_0, \dots, x_n$. Il existe donc un scalaire $k \in \mathbb{K}$ tel que

$$V(x_0, \dots, x_n, X) = k \prod_{i=0}^n (X - x_i).$$

Ce scalaire k est le coefficient dominant de $V(x_0, \dots, x_n, X)$, c'est donc en développant sur la dernière ligne : $V(x_0, \dots, x_n)$. Ainsi, en évaluant ce polynôme en x_{n+1} , il vient :

$$V(x_0, \dots, x_n, x_{n+1}) = V(x_0, \dots, x_n) \prod_{i=0}^n (x_{n+1} - x_i)$$

ce qui, en utilisant l'hypothèse de récurrence, est bien le résultat recherché. $\square$

Remarque 5.4.10.

On peut utiliser la matrice de Vandermonde pour résoudre le problème d'interpolation polynomial, déjà étudié différemment avec les polynômes de Lagrange.

Chapitre XXVIII

Séries numériques

Sommaire

1	Prolégomènes	442
2	Séries à termes réels positifs	444
3	Comparaison série-intégrale	446
4	Séries absolument convergentes	447
5	Familles sommables	449
5.1	Familles sommables de réels positifs	450
5.2	Familles sommables de nombres complexes	453
6	Annexe : compléments	457

Dans tout ce chapitre, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$, et $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ et $(w_n)_{n \in \mathbb{N}}$ sont des suites à valeurs dans $\mathbb{K}$.

1 Prolégomènes

Définition 1.1.

À toute suite $(u_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ on associe la suite $(S_n)_{n \in \mathbb{N}}$ définie par

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^n u_k.$$

- Cette suite (S_n) est appelée *série de terme général* u_n . On la note $\sum u_n$ ou $\sum_{n \geq 0} u_n$. L'indice n est bien entendu muet.
- Lorsque la suite (u_n) n'est définie qu'à partir d'un certain rang n_0 , la série de terme général u_n est définie par la suite $S_n = \sum_{k=n_0}^n u_k$, pour tout $n \geq n_0$. Elle est notée $\sum_{n \geq n_0} u_n$.
- Le terme d'indice n de la suite (S_n) s'appelle la *somme partielle d'indice* (ou d'ordre) n , ou n^e *somme partielle* de la série $\sum u_n$.
- On dit que la série $\sum u_n$ *converge* si la suite (S_n) converge. Dans ce cas la limite de (S_n) est appelée *somme de la série* $\sum u_n$ et notée $\sum_{n=0}^{+\infty} u_n$.

Dans le cas contraire on dit que la série *diverge*.

- La *nature* d'une série est sa convergence ou sa divergence. Deux séries sont dites *de même nature* si elles sont toutes les deux convergentes ou toutes les deux divergentes.

Remarque 1.2.

Une série n'est donc qu'une suite, et on peut donc lui appliquer tous les résultats connus sur les suites. Réciproquement, toute suite est une série (cf. 1.9).

Remarque 1.3.

Si (u_n) est complexe, notons (a_n) sa partie réelle

et (b_n) sa partie imaginaire. Alors, en vertu du cours sur les suites, $\sum u_n$ converge si et seulement si $\sum a_n$ et $\sum b_n$ convergent, et dans le cas de convergence, $\sum_{n=0}^{+\infty} u_n = \sum_{n=0}^{+\infty} a_n + i \sum_{n=0}^{+\infty} b_n$.

Exemple 1.4 (Séries arithmétiques).

Les séries de la forme $\sum na$, avec $a \in \mathbb{C}$, ne sont convergentes que si $a = 0$.

Dans tous les cas la somme partielle S_n vaut $a \frac{n(n+1)}{2}$.

Définition 1.5.

Soit $\sum_{n \geq 0} u_n$ une série convergente, alors pour tout $n \in \mathbb{N}$, la série $\sum_{k \geq n} u_k$ converge également. Sa somme $R_n = \sum_{k=n+1}^{+\infty} u_k$ est appelée *reste d'ordre* (ou d'indice) n de la série $\sum u_n$.

De plus, pour tout $n \in \mathbb{N}$, on a

$$\sum_{k=0}^n u_k + \sum_{k=n+1}^{+\infty} u_k = \sum_{k=0}^{+\infty} u_k,$$

soit, en notant S_n la somme partielle d'ordre n et R_n le reste d'ordre n ,

$$S_n + R_n = \sum_{k=0}^{+\infty} u_k.$$

Démonstration.

Soit $n \in \mathbb{N}$ et $N \geq n$. Alors,

$$\sum_{k=n+1}^N u_k = \sum_{k=0}^N u_k - \sum_{k=0}^n u_k = S_N - S_n.$$

Comme (S_N) converge vers $\sum_{k=0}^{+\infty} u_k$, alors $\sum_{k \geq n+1} u_k$ converge et sa somme est donc

$$\sum_{k=n+1}^{+\infty} u_k = \sum_{k=0}^{+\infty} u_k - S_n.$$

□

Exemple 1.6 (Séries géométriques).

Les séries de la forme $\sum z^n$, avec $z \in \mathbb{C}$, sont

convergentes si et seulement si $|z| < 1$. Dans tous les cas la somme partielle S_n vaut $\frac{1 - z^{n+1}}{1 - z}$ si $z \neq 1$, et $n + 1$ si $z = 1$.

Si $|z| < 1$, alors la somme de la série est

$$\sum_{n=0}^{+\infty} z^n = \frac{1}{1 - z}.$$

Le reste de la série est

$$R_n = \sum_{k=n+1}^{+\infty} z^k = \frac{z^{n+1}}{1 - z}.$$

Remarque 1.7.

Soit $\sum u_n$ une série convergente, dont on note respectivement S_n et R_n la somme partielle et le reste à l'ordre n .

Alors $\sum_{n=0}^{+\infty} u_n = S_n + R_n$ et $R_n \xrightarrow{n \rightarrow +\infty} 0$.

En particulier, si $|R_n| < \varepsilon$, on peut dire que S_n est une approximation de $\sum_{n=0}^{+\infty} u_n$ à ε près.

Proposition 1.8.

Deux séries dont les termes généraux sont égaux à partir d'un certain rang ont même nature.

Démonstration.

Soient (u_n) et (v_n) deux suites égales à partir du rang N .

On note $S_n = \sum_{k=0}^n u_k$ et $S'_n = \sum_{k=0}^n v_k$.

Alors pour tout $n \geq N$, $S_n = S'_n + (S_N - S'_N)$. $\square$

Proposition 1.9 (Lien suite-série).

L'application

$$\varphi : \begin{cases} \mathbb{K}^{\mathbb{N}} & \longrightarrow & \mathbb{K}^{\mathbb{N}} \\ u & \longmapsto & S = \left(\sum_{k=0}^n u_k \right)_{n \in \mathbb{N}} \end{cases}$$

est un automorphisme d'espaces vectoriels.

Sa réciproque est l'application $\varphi^{-1} : \mathbb{K}^{\mathbb{N}} \rightarrow \mathbb{K}^{\mathbb{N}}$, où pour tout $S \in \mathbb{K}^{\mathbb{N}}$, $u = \varphi^{-1}(S)$ est la suite définie par

$$u_0 = S_0 \text{ et } \forall n \in \mathbb{N}^*, u_n = S_n - S_{n-1}.$$

Démonstration.

La linéarité de φ est facile à vérifier. Il est également aisé de montrer que $\varphi \circ \psi = \psi \circ \varphi = \text{Id}$. $\square$

Remarque 1.10.

En posant $S_{-1} = 0$, on peut écrire que, pour tout $n \in \mathbb{N}$,

$$S_n = \sum_{k=0}^n u_k = \sum_{k=0}^n S_k - S_{k-1}.$$

Toute série peut donc être vue comme une série télescopique.

Proposition 1.11 (Séries télescopiques).

La suite (u_n) et la série $\sum (u_{n+1} - u_n)$ ont même nature.

Dans le cas de convergence,

$$u_n - u_0 \xrightarrow{n \rightarrow +\infty} \sum_{n=0}^{+\infty} u_{n+1} - u_n.$$

Démonstration.

Nous savons déjà que les suites $(u_n)_{n \in \mathbb{N}}$ et $(u_{n+1})_{n \in \mathbb{N}}$ ont même nature.

De plus la somme partielle d'indice n de la série $\sum (u_{n+1} - u_n)$ vaut $u_{n+1} - u_0$ par sommation télescopique. Elle est donc égale au terme u_{n+1} , à une constante près, et a donc la même nature que la suite $(u_{n+1})_{n \in \mathbb{N}}$.

Dans le cas de convergence, il reste à passer à la limite dans la relation $\sum_{n=0}^N (u_{n+1} - u_n) = u_{N+1} - u_0$. $\square$

Exemple 1.12.

La série $\sum_{n>0} \frac{1}{n(n+1)}$ converge. En effet pour tout $n \in \mathbb{N}^*$, $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$, et la suite $\left(\frac{1}{n}\right)_{n>0}$ converge.

Nous pouvons même aller plus loin : $\sum_{k=1}^n \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$ donc $\sum_{n=1}^{+\infty} \frac{1}{n(n+1)} = 1$.

On voit aussi que le reste d'ordre n vaut $\frac{1}{n+1}$.

Exercice 1.13.

En simplifiant $\frac{(n+1) - n}{1 + n(n+1)}$, montrer que $\sum \arctan \frac{1}{1 + n + n^2}$ converge et calculer sa somme.

Proposition 1.14 (Linéarité de la somme).

L'ensemble des suites dont la série est convergente, muni des lois $+$ et $\cdot$, forme un $\mathbb{K}$ -espace vectoriel et l'application qui à une telle suite associe la somme de sa série est linéaire.

Démonstration.

Élémentaire, d'après les résultats sur les suites. $\square$

Finissons par le résultat principal de cette première partie :

Théorème 1.15 (Divergence grossière). (i) Si

la série $\sum u_n$ converge, alors $u_n \xrightarrow{n \rightarrow +\infty} 0$.

(ii) Si la suite (u_n) ne tend pas vers 0, on dit que la série $\sum u_n$ *diverge grossièrement*.

Démonstration. (i) Supposons que la série $\sum u_n$ converge. Puisque pour tout $n > 0$, $u_n = S_n - S_{n-1}$, alors u_n est la différence des termes généraux de deux suites convergeant vers la même limite. La suite (u_n) tend donc vers 0.

(ii) C'est la contraposée du premier point. $\square$

Exemple 1.16.

La série $\sum \cos n$ diverge grossièrement. En effet, en supposant que $\cos n \xrightarrow{n \rightarrow +\infty} 0$, la relation $\cos(2n) = 2\cos^2 n - 1$ donne une contradiction.

Remarque 1.17 .

La réciproque du premier point du théorème 1.15 est fausse. On peut citer en exemple la série harmonique $\sum_{n \geq 1} \frac{1}{n}$, qui sera revue plus tard.

Donnons également l'exemple de la suite $u_n = \ln(n+2) - \ln(n+1) = \ln\left(1 + \frac{1}{n+1}\right)$. Évidemment, $u_n \xrightarrow{n \rightarrow +\infty} 0$.

Mais $\sum_{k=0}^n u_k = \ln(n+2)$, par sommation télescopique. La série $\sum u_n$ diverge donc.

Concluons sur un dernier exemple, fondamental.

Proposition 1.18 (série exponentielle).

Pour tout $z \in \mathbb{C}$, $\sum_{n \geq 0} \frac{z^n}{n!}$ converge et

$$e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}.$$

Démonstration.

Soit $z \in \mathbb{C}$, soit $f : t \mapsto e^{tz}$, que l'on définit sur $\mathbb{R}$. Alors, f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et pour tout $n \in \mathbb{N}$:

$$f^{(n)} : t \mapsto z^n e^{tz}.$$

Alors, par l'inégalité de Taylor-Lagrange entre 0 et 1, pour $N \in \mathbb{N}$:

$$\left| e^z - \sum_{n=0}^N \frac{z^n}{n!} \right| \leq \frac{1^{N+1}}{(N+1)!} \sup \{ |z^{N+1} e^{tz}| \mid t \in [0, 1] \}.$$

Or, si $0 \leq t \leq 1$, en écrivant sous forme algébrique $z = a + ib$, on a

$$|z^{N+1} e^{tz}| = |z|^{N+1} |e^{ta} e^{itb}| = |z|^{N+1} e^{ta} \leq |z|^{N+1} \max(1, e^a).$$

Ainsi,

$$\left| e^z - \sum_{n=0}^N \frac{z^n}{n!} \right| \leq \frac{(|z|)^{N+1}}{(N+1)!} \max(1, e^a)$$

Par croissances comparées, $\frac{(|z|)^{N+1}}{(N+1)!} \xrightarrow{N \rightarrow +\infty} 0$, ce qui permet de conclure. $\square$

2 Séries à termes réels positifs

Étudions maintenant le cas particulier où tous les termes d'une série sont des réels positifs ou nuls. La propriété fondamentale est dans ce cas la suivante.

Proposition 2.1.

Soit (u_n) une suite à valeurs positives et $S_n = \sum_{k=0}^n u_k$. Alors la suite (S_n) est croissante.

Démonstration.

Tout simplement, $S_{n+1} - S_n = u_{n+1} \geq 0$. $\square$

Remarque 2.2.

Attention, une série peut ne pas être à terme positifs mais avoir toutes ses sommes partielles positives, comme la série $\sum_{n \geq 0} (-1)^n$.

Proposition 2.3.

Une série à termes positifs converge si et seulement si la suite de ses sommes partielles est majorée.

Démonstration.

La suite des sommes partielles est croissante. Elle est donc convergente si et seulement si elle est majorée, comme conséquence directe du théorème de la limite monotone. $\square$

Proposition 2.4.

Soient (u_n) et (v_n) deux suites réelles telles que pour tout $n \in \mathbb{N}$, $0 \leq u_n \leq v_n$.

- (i) Si $\sum v_n$ converge, alors $\sum u_n$ également et

$$0 \leq \sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n.$$
- (ii) Si $\sum u_n$ diverge, alors $\sum v_n$ également.

Démonstration.

Il suffit de remarquer que si (S_n) est la suite des sommes partielles de $\sum u_n$ et (S'_n) celle de $\sum v_n$, alors $0 \leq S_n \leq S'_n$.

- (i) (S'_n) converge, donc est majorée, donc (S_n) est également majorée, et comme elle est croissante, elle converge également. Il reste alors à passer à la limite dans la relation $0 \leq S_n \leq S'_n$.
- (ii) c'est le théorème de minoration. $\square$

Remarque 2.5.

Si la relation $0 \leq u_n \leq v_n$ n'est vérifiée qu'à partir d'un certain rang, le résultat du théorème 2.4 est valable, à ceci près que dans le point (i) on ne

peut pas conclure que $0 \leq \sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n$, mais

seulement $0 \leq \sum_{n=N}^{+\infty} u_n \leq \sum_{n=N}^{+\infty} v_n$.

Exemple 2.6.

$\sum \frac{1}{(n+1)^2}$ converge et

$$1 < \sum_{n=0}^{+\infty} \frac{1}{(n+1)^2} < 2.$$

En effet, pour tout $n > 0$, $0 < \frac{1}{(n+1)^2} <$

$\frac{1}{n(n+1)}$, donc $0 < \sum_{n=1}^{+\infty} \frac{1}{(n+1)^2} < 1$ car

$$\sum_{n=1}^{+\infty} \frac{1}{n(n+1)} = 1. \text{ Puisque pour } n = 0, \frac{1}{(n+1)^2} = 1, \text{ il vient le résultat.}$$

Corollaire 2.7.

Soient (u_n) et (v_n) deux suites réelles positives, (v_n) ne s'annulant pas à partir d'un certain rang.

- (i) Si $u_n = O(v_n)$, alors la convergence de $\sum v_n$ entraîne celle de $\sum u_n$.
- (ii) Si $u_n = o(v_n)$, alors la convergence de $\sum v_n$ entraîne celle de $\sum u_n$.
- (iii) Si $u_n \sim v_n$ (donc (u_n) ne s'annule pas à partir d'un certain rang), alors $\sum v_n$ et $\sum u_n$ sont de même nature.

Démonstration. (i) $\frac{u_n}{v_n}$ est bornée par un certain réel $M > 0$, donc à partir d'un certain rang, $0 \leq u_n \leq M v_n$ car (u_n) et (v_n) sont positives. On conclut donc avec 2.4.

- (ii) si $u_n = o(v_n)$, alors en particulier $u_n = O(v_n)$.
- (iii) si $u_n \sim v_n$, alors $u_n = O(v_n)$ et $v_n = O(u_n)$. $\square$

Exemple 2.8.

Puisque $\sin\left(\frac{1}{2^n}\right) \sim \frac{1}{2^n}$, d'après le résultat sur les séries géométriques, $\sum \sin\left(\frac{1}{2^n}\right)$ converge.

Pour pouvoir utiliser le dernier corollaire, nous avons besoin de « séries étalon », dont la nature est bien connue, et auxquelles on compare les séries à étudier. Les quelques exemples déjà étudiés font partie de ces séries de référence standard, mais la famille de séries la plus utilisée est celle des *séries de Riemann*, dont font partie la série harmonique et la série $\sum \frac{1}{(n+1)^2}$.

Théorème 2.9.

Soit $\alpha \in \mathbb{R}$. La série $\sum_{n \geq 1} \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Démonstration.

Si $\alpha = 1$, remarquons que $\frac{1}{n} \sim \ln(n+1) - \ln n$. Donc

$\sum_{n \geq 1} \frac{1}{n^\alpha}$ est de même nature que $\sum_{n \geq 1} (\ln(n+1) - \ln n)$, qui elle-même est de même nature que la suite $(\ln n)$ d'après 1.11, d'où la divergence.

Si $\alpha \neq 1$, $\frac{1}{n^\alpha} \sim \frac{1}{\alpha-1} \left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}} \right)$ (effectuer un développement asymptotique de $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ ou appliquer l'inégalité des accroissements finis à $x \mapsto x^{1-\alpha}$). La série de terme général $\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}$ est de même nature que la suite $\left(\frac{1}{n^{\alpha-1}} \right)$, d'où le résultat.

On peut aussi remarquer que si $\alpha \leq 0$, la divergence est grossière, et si $0 < \alpha < 1$, la série diverge car $\frac{1}{n^\alpha} > \frac{1}{n}$. $\square$

Le résultat classique suivant est une application directe de 2.7 et 2.9 :

Remarque 2.10 (Règle $n^\alpha u_n$).

Soient (u_n) une suite réelle positive et $\alpha \in \mathbb{R}$.

- (i) S'il existe $\alpha > 1$ telle que $n^\alpha u_n \xrightarrow{n \rightarrow +\infty} 0$, alors $\sum u_n$ converge.
- (ii) S'il existe $\alpha \leq 1$ telle que $n^\alpha u_n \xrightarrow{n \rightarrow +\infty} +\infty$, alors $\sum u_n$ diverge.
- (iii) Si la suite $(n^\alpha u_n)$ converge vers une limite non nulle, la série $\sum u_n$ converge si et seulement si $\alpha > 1$.

Démonstration. (i) si $n^\alpha u_n \xrightarrow{n \rightarrow +\infty} 0$ alors $u_n = o\left(\frac{1}{n^\alpha}\right)$, et $\sum \frac{1}{n^\alpha}$ converge.

(ii) si $n^\alpha u_n \xrightarrow{n \rightarrow +\infty} +\infty$ alors $\frac{1}{n^\alpha} = o(u_n)$, et $\sum \frac{1}{n^\alpha}$ diverge.

(iii) si la suite $n^\alpha u_n \xrightarrow{n \rightarrow +\infty} \ell$ avec $\ell \in \mathbb{R}_+^*$, $\sum u_n$ et $\sum \frac{1}{n^\alpha}$ ont même nature. $\square$

Exemple 2.11 (Séries de Bertrand).

Soient $\alpha, \beta \in \mathbb{R}$. On considère la série $\sum_{n \geq 2} \frac{1}{(\ln n)^\beta n^\alpha}$.

- Si $\alpha > 1$: il existe $\gamma \in]1, \alpha[$ et $n^\gamma \frac{1}{(\ln n)^\beta n^\alpha} \xrightarrow{n \rightarrow +\infty} 0$ par croissances comparées, car $\alpha - \gamma > 0$. Ainsi la série converge.
- Si $\alpha < 1$: il existe $\gamma \in]\alpha, 1[$ et $n^\gamma \frac{1}{(\ln n)^\beta n^\alpha} \xrightarrow{n \rightarrow +\infty} +\infty$ par croissances comparées, car $\alpha - \gamma < 0$. Ainsi la série diverge.
- Si $\alpha = 1$: si $\beta \leq 0$, le terme général est plus

grand que $\frac{1}{n}$, donc la série diverge. Nous traitons le cas $\beta > 0$ en 3.3.

3 Comparaison série-intégrale

Proposition 3.1.

Soit $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ une fonction continue par morceaux et décroissante.

Alors la série $\sum f(n)$ converge si et seulement si la suite $\left(\int_0^n f(t) dt \right)$ est convergente.

De plus la suite définie par $u_n = \sum_{k=0}^n f(k) - \int_0^n f(t) dt$ converge.

Démonstration.

Soit $k \in \mathbb{N}$. Par décroissance de f , on a :

$$\forall t \in [k, k+1], 0 \leq f(k+1) \leq f(t) \leq f(k).$$

Puis, par intégration de cet encadrement sur $[k, k+1]$:

$$0 \leq f(k+1) \leq \int_k^{k+1} f(t) dt \leq f(k) \quad (\text{XXVIII.1})$$

et par sommation, pour $n \geq 1$:

$$0 \leq \sum_{k=0}^{n-1} f(k+1) \leq \int_0^n f(t) dt \leq \sum_{k=0}^{n-1} f(k)$$

ou encore

$$0 \leq \sum_{k=0}^n f(k) - f(0) \leq \int_0^n f(t) dt \leq \sum_{k=0}^n f(k) - f(n). \quad (\text{XXVIII.2})$$

Or les suites $\left(\sum_{k=0}^n f(k) \right)_{n \in \mathbb{N}}$ et $\left(\int_0^n f(t) dt \right)_{n \in \mathbb{N}}$ sont croissantes, et ont donc la même nature. De plus, il vient $0 \leq f(n) \leq \sum_{k=0}^n f(k) - \int_0^n f(t) dt$, soit $0 \leq u_n$. Ainsi (u_n) est minorée. Enfin, on a

$$u_{n+1} - u_n = f(n+1) - \int_n^{n+1} f(t) dt \leq 0.$$

La suite (u_n) est donc décroissante et minorée et converge donc. $\square$

Remarque 3.2.

L'encadrement XXVIII.1 est à rapprocher de la méthode des rectangles, vue dans le chapitre sur l'intégration.

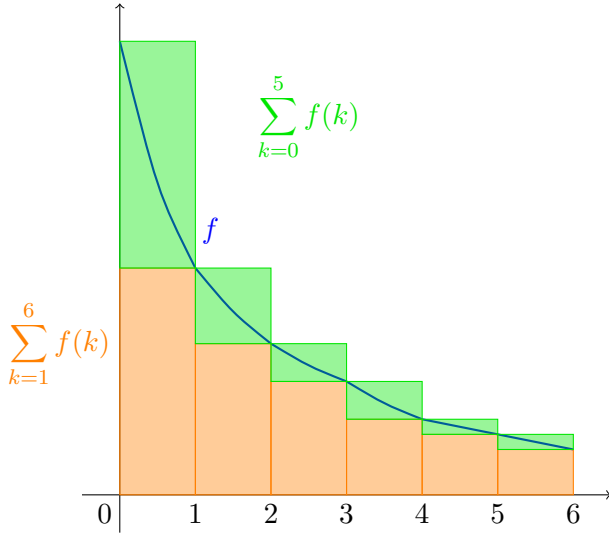


FIGURE XXVIII.1 – Exemple de comparaison série-intégrale pour une fonction f décroissante, positive.

Exemple 3.3.

Achevons l'étude des séries de Bertrand commencée en 2.11.

Si $\beta > 0$, considérons l'application $f : t \mapsto \frac{1}{t(\ln t)^\beta}$. Elle est continue et décroissante sur $[2, +\infty[$.

Si $\beta = 1$, une primitive de f est $F : t \mapsto \ln(\ln t)$ et $\int_2^n f(t) dt = F(n) - F(2)$. Or $F(n) \xrightarrow{n \rightarrow +\infty} +\infty$ donc la série diverge.

Par comparaison, la série diverge également si $0 \leq \beta < 1$.

Si $\beta > 1$, une primitive de f est $F : t \mapsto \frac{(\ln t)^{1-\beta}}{1-\beta}$ et $\int_2^n f(t) dt = F(n) - F(2)$. Or $F(n) \xrightarrow{n \rightarrow +\infty} 0$ car $1 - \beta < 0$, donc la série converge.

Exercice 3.4.

Redémontrer le résultat 2.9 en utilisant 3.1.

Exemple 3.5.

On pose $f : x \mapsto \frac{1}{1+x}$. On sait alors que la suite de terme général $u_n = \sum_{k=0}^{n-1} f(k) - \int_0^{n-1} f(t) dt =$

$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \ln n$ converge, vers une limite notée γ et nommée *constante d'Euler*.

Exemple 3.6.

L'encadrement (XXVIII.2) permet d'avoir une estimation du reste d'une série convergente de la forme $\sum f(n)$ avec f décroissante.

Par exemple, soit $f : x \mapsto \frac{1}{x^2}$. Alors

$$\begin{aligned} \frac{1}{n+1} - \frac{1}{N} &= \int_{n+1}^N \frac{dt}{t^2} \leq \sum_{n+1}^N \frac{1}{n^2} \leq \int_n^{N-1} \frac{dt}{t^2} \\ &\leq \frac{1}{n} - \frac{1}{N-1} \end{aligned}$$

et en passant à la limite quand $N \rightarrow +\infty$,

$$\frac{1}{n+1} \leq \sum_{n+1}^{+\infty} \frac{1}{n^2} \leq \frac{1}{n}.$$

Si l'on veut une approximation de $\sum_{n=1}^{+\infty} \frac{1}{n^2}$ à 10^{-3} près, il suffit donc de choisir $n = 1000$ et de calculer $\sum_{n=1}^{1000} \frac{1}{n^2}$.

Exercice 3.7.

On peut obtenir une approximation de cette somme en calculant seulement la somme d'une trentaine de termes. Comment ?

4 Séries absolument convergentes

Revenons à des séries à termes quelconques dans $\mathbb{K}$. Nous allons étudier une convergence plus restreinte que la convergence définie en 1.1 : la *convergence absolue*.

Définition 4.1.

On dit que la série $\sum u_n$ est *absolument convergente* si la série à termes positifs $\sum |u_n|$ converge.

Exemple 4.2.

Si $z \in \mathbb{C}$, alors $\sum_{n \geq 0} \frac{z^n}{n!}$ converge absolument.

Proposition 4.3.

Toute série absolument convergente est convergente.

Démonstration.

Commençons par établir le résultat pour des suites à valeurs réelles. Pour cela, définissons pour une suite (u_n) les deux suites (u_n^-) et (u_n^+) définies par : $u_n^+ = \max(u_n, 0)$ et $u_n^- = \max(-u_n, 0)$. Nous avons alors :

$$\begin{aligned} u_n^+ &= \begin{cases} 0 & \text{si } u_n < 0 \\ |u_n| & \text{si } u_n \geq 0 \end{cases} \\ u_n^- &= \begin{cases} 0 & \text{si } u_n > 0 \\ |u_n| & \text{si } u_n \leq 0 \end{cases} \\ 0 \leq u_n^+ &\leq |u_n| & \text{(XXVIII.3)} \\ 0 \leq u_n^- &\leq |u_n| & \text{(XXVIII.4)} \\ u_n &= u_n^+ - u_n^- & \text{(XXVIII.5)} \end{aligned}$$

$$|u_n| = u_n^+ + u_n^-.$$

De (XXVIII.3) et (XXVIII.4) on tire que $\sum u_n^+$ et $\sum u_n^-$ sont convergentes car $\sum |u_n|$ est convergente.

De (XXVIII.5) on tire que $\sum u_n$ est convergente.

Étendons maintenant ce résultat au cas d'une suite (u_n) à valeurs complexes absolument convergente. Pour tout n , on a $0 \leq |\operatorname{Re} u_n| \leq |u_n|$, or la série $\sum |u_n|$ converge, donc la série $\sum |\operatorname{Re} u_n|$ est convergente, donc $\sum \operatorname{Re} u_n$ est absolument convergente, donc convergente d'après le premier point. De même $\sum \operatorname{Im} u_n$ converge. Donc $\sum u_n$ converge. $\square$



La réciproque est fausse. Soit par exemple la suite de terme général $u_n = \frac{(-1)^n}{n} - \frac{(-1)^{n+1}}{n+1} = v_n - v_{n+1}$, avec $v_n = \frac{(-1)^n}{n}$. La série $\sum u_n$ est donc de même nature que la suite (v_n) , elle converge donc.

Mais $|u_n| = \frac{1}{n} + \frac{1}{n+1} \sim \frac{2}{n}$, donc $\sum u_n$ n'est pas absolument convergente. On dit qu'une telle suite, convergente mais pas absolument, est *semi-convergente*. L'étude de telles suites est souvent délicate !

Corollaire 4.4.

Soit (u_n) une suite complexe et (v_n) une suite à termes positifs telles que $|u_n| = O(v_n)$. Alors si $\sum v_n$ converge, $\sum u_n$ également.

Démonstration.

Par comparaison de séries à termes positifs, $\sum u_n$ converge absolument, donc converge. $\square$

Remarque 4.5.

Une série à termes de signe constant converge absolument si et seulement si elle converge.

Proposition 4.6.

L'ensemble des séries absolument convergentes est un sous-espace vectoriel de l'ensemble des séries convergentes.

Démonstration.

Élémentaire par l'inégalité triangulaire. $\square$

Proposition 4.7.

Soit $\sum u_n$ une série absolument convergente. Alors

$$\left| \sum_{n=0}^{+\infty} u_n \right| \leq \sum_{n=0}^{+\infty} |u_n|.$$

Démonstration.

Soit $N \in \mathbb{N}$, alors, par l'inégalité triangulaire,

$$\left| \sum_{n=0}^N u_n \right| \leq \sum_{n=0}^N |u_n| \leq \sum_{n=0}^{+\infty} |u_n|.$$

On conclut par passage à la limite en N . $\square$

Un exemple important est celui de la série exponentielle.

Théorème 4.8.

Pour tout $z \in \mathbb{C}$, la série $\sum_{n \geq 0} \frac{z^n}{n!}$ converge absolument.

Démonstration.

$\sum_{n \geq 0} \left| \frac{z^n}{n!} \right| = \sum_{n \geq 0} \frac{|z|^n}{n!}$, qui est une série exponentielle, donc converge. $\square$

Les séries convergeant mais ne convergeant pas absolument sont appelées *séries semi-convergentes*. Leur étude est délicate, deux outils principaux étant souvent utilisés : le critère spécial des séries alternées (*cf. infra*) et la transformation d'Abel (voir la feuille de TD).

Théorème 4.9 (critère spécial des séries alternées, ou CSSA).

Soit (u_n) une suite de réels positifs, décroissante et convergeant vers 0.

Alors, $\sum_{n \geq 0} (-1)^n u_n$ converge.

De plus, en notant R_n le reste d'ordre n de la série et S_n sa somme partielle d'ordre n , alors pour tout $n \in \mathbb{N}$

1. $S_{2n+1} \leq \sum_{n=0}^{+\infty} (-1)^n u_n \leq S_{2n}$,
2. $R_n \leq 0$ si n est pair,
3. $R_n \geq 0$ si n est impair,
4. $|R_n| \leq u_{n+1}$

Démonstration.

Notons S_n la somme partielle d'ordre n de cette série. Il suffit de montrer que (S_{2n}) et (S_{2n+1}) sont adjacentes, pour obtenir qu'elles convergent vers une même limite et donc que (S_n) converge, c'est-à-dire que $\sum_{n \geq 0} (-1)^n u_n$ converge.

Tout ceci est élémentaire. Considérons $n \in \mathbb{N}$.

- $S_{2n+1} - S_{2n} = -u_{2n+1} \xrightarrow{n \rightarrow +\infty} 0$.
- $S_{2n+2} - S_{2n} = u_{2n+2} - u_{2n+1} \leq 0$ par décroissance de (u_n) , donc (S_{2n}) est décroissante.
- $S_{2n+3} - S_{2n+1} = u_{2n+2} - u_{2n+3} \geq 0$ par décroissance de (u_n) , donc (S_{2n+1}) est croissante.

Ainsi, (S_{2n}) et (S_{2n+1}) sont adjacentes.

Par adjacence de ces suites, on a donc pour tout $n \in \mathbb{N}$:

$$S_{2n+1} \leq \sum_{n=0}^{+\infty} (-1)^n u_n \leq S_{2n}.$$

On obtient donc immédiatement que

$$\begin{aligned} R_{2n} &= \sum_{n=0}^{+\infty} (-1)^n u_n - S_{2n} \leq 0 \\ R_{2n+1} &= \sum_{n=0}^{+\infty} (-1)^n u_n - S_{2n+1} \geq 0 \end{aligned}$$

On a aussi immédiatement

$$0 \leq -R_{2n} = S_{2n} - \sum_{n=0}^{+\infty} (-1)^n u_n \leq S_{2n} - S_{2n+1} = u_{2n+1}$$

et de même, par l'encadrement,

$$S_{2n+1} \leq \sum_{n=0}^{+\infty} (-1)^n u_n \leq S_{2n+2},$$

on a

$$0 \leq R_{2n+1} = \sum_{n=0}^{+\infty} (-1)^n u_n - S_{2n+1} \leq S_{2n+2} - S_{2n+1} = u_{2n+2}.$$

On a donc pour tout $n \in \mathbb{N}$, par disjonction de cas sur la parité de n :

$$|R_n| \leq u_{n+1}.$$

□

Remarque 4.10.

Comme $S_1 = u_0 - u_1 \geq 0$, on a alors $\sum_{n=0}^{+\infty} (-1)^n u_n \geq 0$.

Remarque 4.11.

Le critère spécial des séries alternées est parfois formulé de la manière suivante : si $(|u_n|)$ est décroissante, si $|u_n| \xrightarrow{n \rightarrow +\infty} 0$ et si (u_n) est à signes alternées (*i.e.* pour tout $n \in \mathbb{N}$, $u_n u_{n+1} \leq 0$), alors $\sum_{n \geq 0} u_n$ converge. On a alors la majoration

$|R_n| \leq |u_n|$, et l'on sait aussi que $\sum_{n=0}^{+\infty} u_n$ est du même signe que u_0 .

Exercice 4.12.

Montrer que $\sum_{n \geq 1} \frac{(-1)^n}{n}$ converge, et donner une valeur approchée rationnelle à 10^{-2} près de la somme de cette série.

5 Familles sommables

Nous allons maintenant nous intéresser à des situations où l'on somme des familles de nombres qui ne sont pas indicées par $\mathbb{N}$ (par exemple, on peut vouloir sommer des familles de nombres indicées par $\mathbb{Z}$, par $\mathbb{Q}$ ou par $\mathbb{N}^2$).

En pratique, l'ensemble d'indices ne peut pas être trop gros (on peut supposer qu'il est au plus *dénombrable*), vous étudierez cela plus en détail l'année prochaine.

Dans toute cette partie, I désigne un ensemble quelconque, non vide.

5.1 Familles sommables de réels positifs

Commençons par étudier les processus sommatoires de nombres positifs (en se permettant de sommer aussi $+\infty$). La positivité de ces nombres permet de s'affranchir de bon nombre de précautions, et de donner un sens très large à la notion de somme.

Notation 5.1.

On note $\bar{\mathbb{R}}_+ = \mathbb{R}_+ \cup \{+\infty\}$, que l'on pourra aussi noter $[0, +\infty]$.

On se placera dans cette partie dans la droite numérique achevée $\bar{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$, avec son ordre usuel et les conventions de calcul habituelles.

Exemple 5.2.

Si $A \subset \mathbb{R}$ est une partie non vide et non majorée, on se permettra de plus d'écrire $\sup(A) = +\infty$.

Dans toute cette sous-partie, $(u_i)_{i \in I}$ est une famille d'éléments de $\bar{\mathbb{R}}_+$, indicée par I .

Remarque 5.3.

On se permet donc d'avoir un $i \in I$ vérifiant $u_i = +\infty$.

Définition 5.4 (somme).

On appelle somme de la famille $(u_i)_{i \in I} \in (\bar{\mathbb{R}}_+)^I$ l'élément de $\bar{\mathbb{R}}_+$ défini par

$$\sum_{i \in I} u_i = \sup \left\{ \sum_{i \in F} u_i \mid F \subset I \text{ t.q. } F \text{ est fini} \right\}.$$

Exemple 5.5.

On a $\sum_{(i,j) \in (\mathbb{N}^*)^2} \frac{1}{ij} = +\infty$.

En effet, si pour $n \in \mathbb{N}^*$, si l'on considère $F_n = \{(i, 1) \mid 1 \leq i \leq n\}$, qui est bien une partie finie de $(\mathbb{N}^*)^2$, alors

$$\sum_{(i,j) \in F_n} \frac{1}{ij} = \sum_{i=1}^n \frac{1}{i} \xrightarrow{n \rightarrow +\infty} +\infty.$$

Ainsi,

$$\sup \left\{ \sum_{i \in F} u_i \mid F \subset (\mathbb{N}^*)^2 \text{ t.q. } F \text{ est fini} \right\} = +\infty.$$

Remarque 5.6.

On a donc toujours, pour toute $F \subset I$ finie,

$$\sum_{i \in F} u_i \leq \sum_{i \in I} u_i.$$

Définition 5.7 (famille sommable).

Une famille $(u_i)_{i \in I} \in (\bar{\mathbb{R}}_+)^I$ est dite sommable si l'ensemble des $\sum_{i \in F} u_i$, pour F parcourant les parties finies de I , est majoré.

La nature d'une famille est son caractère sommable ou non.

Remarque 5.8.

Pour une famille de réels positifs, la famille $(u_i)_{i \in I} \in (\bar{\mathbb{R}}_+)^I$ est sommable si et seulement si $\sum_{i \in I} u_i < +\infty$.

Exemple 5.9 (sommes finies).

Dans le cas où $I = \{i_1, \dots, i_p\}$ est un ensemble fini, alors

$$\sum_{i \in I} u_i = u_{i_1} + \dots + u_{i_p},$$

et la famille $(u_i)_{i \in I} \in (\bar{\mathbb{R}}_+)^I$ est sommable si et seulement si tous les u_i sont réels.

Exemple 5.10 (séries numériques).

Si $I = \mathbb{N}$ et si $(u_i) \in (\bar{\mathbb{R}}_+)^{\mathbb{N}}$, alors la famille $(u_i)_{i \in \mathbb{N}}$ est sommable si et seulement si la série $\sum_{i \geq 0} u_i$ converge. On a alors

$$\sum_{i \in \mathbb{N}} u_i = \sum_{i=0}^{+\infty} u_i.$$

En cas de divergence de la série, on a toujours l'écriture

$$\sum_{i \in \mathbb{N}} u_i = +\infty.$$

On se permet donc d'écrire

$$\sum_{i=0}^{+\infty} u_i = +\infty.$$

Théorème 5.11 (invariance de la somme par permutation).

Soit $(u_i)_{i \in I} \in (\mathbb{R}_+)^I$, soit $\sigma \in S_I$ une permutation de I . Alors,

$$\sum_{i \in I} u_i = \sum_{i \in I} u_{\sigma(i)}.$$

Notamment, les familles $(u_i)_{i \in I}$ et $(u_{\sigma(i)})_{i \in I}$ ont même nature.

Démonstration.

Il suffit de voir que si F parcourt toutes les parties finies de I , alors $\sigma(F)$ parcourt aussi toutes les parties finies de I . Ainsi,

$$\begin{aligned} & \left\{ \sum_{i \in F} u_i \mid F \subset (\mathbb{N}^*)^2 \text{ t.q. } F \text{ est fini} \right\} \\ &= \left\{ \sum_{i \in \sigma(F)} u_i \mid F \subset (\mathbb{N}^*)^2 \text{ t.q. } F \text{ est fini} \right\} \\ &= \left\{ \sum_{i \in F} u_{\sigma(i)} \mid F \subset (\mathbb{N}^*)^2 \text{ t.q. } F \text{ est fini} \right\} \end{aligned}$$

□

Bien entendu, les opérations usuelles sont toujours valides sur cette notion de somme.

Proposition 5.12 (opérations).

Soit $(u_i)_{i \in I}, (v_i)_{i \in I} \in (\mathbb{R}_+)^I$, soit $\lambda \in \mathbb{R}_+^*$, alors

1. $\sum_{i \in I} (u_i + v_i) = \sum_{i \in I} u_i + \sum_{i \in I} v_i$.
2. $\sum_{i \in I} \lambda u_i = \lambda \sum_{i \in I} u_i$.

Démonstration.

Remarquons d'abord que toutes ces familles sont bien à valeurs dans $\mathbb{R}_+$. De plus, s'il existe $i \in I$ tel que $u_i = +\infty$ ou $v_i = +\infty$, alors les résultats sont immédiats. On peut donc supposer que pour tout $i \in I$, $u_i, v_i \in \mathbb{R}_+$.

Soit F une partie finie de I , alors

$$\begin{aligned} \sum_{i \in F} (u_i + v_i) &= \sum_{i \in F} u_i + \sum_{i \in F} v_i \\ &\leq \sum_{i \in I} u_i + \sum_{i \in I} v_i. \end{aligned}$$

Ainsi, par passage à la borne supérieure,

$$\sum_{i \in I} (u_i + v_i) \leq \sum_{i \in I} u_i + \sum_{i \in I} v_i.$$

Supposons que $\sum_{i \in I} u_i = +\infty$. Pour tout $A \in \mathbb{R}_+$, il existe donc $F \subset I$ finie telle que

$$\sum_{i \in F} u_i \geq A.$$

Comme tous les v_i sont positifs, on a donc

$$\sum_{i \in F} u_i + v_i \geq \sum_{i \in F} u_i \geq A.$$

Ainsi, $\sum_{i \in I} (u_i + v_i) = +\infty$. On a le même résultat si $\sum_{i \in I} v_i = +\infty$.

Si $\sum_{i \in I} u_i < +\infty$ et $\sum_{i \in I} v_i < +\infty$, considérons $\varepsilon > 0$. Il existe donc $F, G \subset I$ finies telles que

$$\begin{aligned} \sum_{i \in F} u_i &\geq \sum_{i \in I} u_i - \varepsilon \\ \sum_{i \in G} v_i &\geq \sum_{i \in I} v_i - \varepsilon. \end{aligned}$$

Ainsi, par positivité des u_i et des v_i , en remarquant que $F \cup G$ est une partie finie de I .

$$\begin{aligned} \sum_{i \in F \cup G} (u_i + v_i) &= \sum_{i \in F \cup G} u_i + \sum_{i \in F \cup G} v_i \\ &\geq \sum_{i \in F} u_i + \sum_{i \in G} v_i \\ &\geq \sum_{i \in I} u_i + \sum_{i \in I} v_i - 2\varepsilon. \end{aligned}$$

Par la caractérisation de la borne supérieure,

$$\sum_{i \in I} (u_i + v_i) = \sum_{i \in I} u_i + \sum_{i \in I} v_i$$

Soit F une partie finie de I , alors

$$\sum_{i \in F} \lambda u_i = \lambda \sum_{i \in F} u_i \leq \lambda \sum_{i \in I} u_i.$$

Ainsi, par passage à la borne supérieure,

$$\sum_{i \in I} \lambda u_i \leq \lambda \sum_{i \in I} u_i.$$

Il suffit d'appliquer ce qui précède à la famille des $(\lambda u_i)_{i \in I}$ et au scalaire λ^{-1} , ce qui donne

$$\sum_{i \in I} u_i \leq \lambda^{-1} \sum_{i \in I} \lambda u_i,$$

soit

$$\lambda \sum_{i \in I} u_i \leq \sum_{i \in I} \lambda u_i$$

Ainsi, $\sum_{i \in I} \lambda u_i = \lambda \sum_{i \in I} u_i$.

□

Exemple 5.13.

On sait que $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Alors,

$$\sum_{n \in 2\mathbb{N}^*} \frac{1}{n^2} = \frac{\pi^2}{24}.$$

Proposition 5.14 (comparaison).

Soit $(u_i)_{i \in I}, (v_i)_{i \in I} \in (\overline{\mathbb{R}}_+)^I$.

Si pour tout $i \in I$, $u_i \leq v_i$, alors

$$\sum_{i \in I} u_i \leq \sum_{i \in I} v_i.$$

Démonstration.

Soit $F \subset I$ finie, alors

$$\sum_{i \in F} u_i \leq \sum_{i \in F} v_i \leq \sum_{i \in I} v_i.$$

Par passage à la borne supérieure,

$$\sum_{i \in I} u_i \leq \sum_{i \in I} v_i.$$

□

Remarque 5.15.

Si on a $\forall i \in I$, $u_i \leq v_i$, et si la famille $(v_i)_{i \in I}$ est sommable, alors $(u_i)_{i \in I}$ est aussi sommable.

Proposition 5.16 (sous-famille).

Soit $(u_i)_{i \in I} \in (\overline{\mathbb{R}}_+)^I$, soit $J \subset I$. Alors,

$$\sum_{j \in J} u_j \leq \sum_{i \in I} u_i.$$

Notamment, si $(u_i)_{i \in I}$ est sommable, alors $(u_j)_{j \in J}$ l'est aussi.

Démonstration.

Soit $F \subset J$ finie, alors F est une partie finie de I , donc

$$\sum_{j \in F} u_j \leq \sum_{i \in I} u_i.$$

Par passage à la borne supérieure, on obtient le résultat. □

L'outil principal de calcul de somme est le théorème de sommation par paquets. En pratique, il conviendra de procéder à un regroupement par paquets judicieux pour calculer les sommes en jeu.

Théorème 5.17 (sommation par paquets).

Soit J un ensemble. Pour chaque $j \in J$, on considère $I_j \subset I$ et l'on suppose que I est la réunion disjointe des I_j :

$$I = \bigsqcup_{j \in J} I_j.$$

Soit $(u_i)_{i \in I} \in (\overline{\mathbb{R}}_+)^I$.

Alors,

$$\sum_{i \in I} u_i = \sum_{j \in J} \left(\sum_{i \in I_j} u_i \right).$$

Lemme 5.18.

Soit A, B deux parties disjointes de I , soit $(u_i)_{i \in I} \in (\overline{\mathbb{R}}_+)^I$. Alors,

$$\sum_{i \in A \sqcup B} u_i = \sum_{i \in A} u_i + \sum_{i \in B} u_i.$$

Démonstration.

Soit $F \subset A \sqcup B$ finie. Posons $G = F \cap A$ et $H = F \cap B$, de sorte que G et H soient finies, $F = G \sqcup H$, $G \subset A$ et $H \subset B$. Alors

$$\sum_{i \in F} u_i = \sum_{i \in G} u_i + \sum_{i \in H} u_i \leq \sum_{i \in A} u_i + \sum_{i \in B} u_i.$$

Par passage à la borne supérieure,

$$\sum_{i \in A \sqcup B} u_i \leq \sum_{i \in A} u_i + \sum_{i \in B} u_i$$

S'il existe $i \in A \sqcup B$ tel que $u_i = +\infty$, le résultat est immédiat. Supposons donc que pour tout $i \in A \sqcup B$, $u_i < +\infty$.

Si $\sum_{i \in A} u_i = +\infty$, soit $M \in \mathbb{R}_+$. Il existe donc $F \subset A$

finie telle que $\sum_{i \in F} u_i \geq M$. Comme F est une partie finie

de $A \sqcup B$, on a immédiatement $\sum_{i \in A \sqcup B} u_i = +\infty$. On a le

même résultat si $\sum_{i \in B} u_i = +\infty$.

Enfin, supposons que $\sum_{i \in A} u_i < +\infty$ et $\sum_{i \in B} u_i < +\infty$.

Soit $\varepsilon > 0$. Il existe $F \subset A$ et $G \subset B$ finies telles que

$$\begin{aligned} \sum_{i \in F} u_i &\geq \sum_{i \in A} u_i - \varepsilon \\ \sum_{i \in G} u_i &\geq \sum_{i \in B} u_i - \varepsilon \end{aligned}$$

Alors, F et G sont disjointes et $F \sqcup G$ est une partie finie de $A \sqcup B$. De plus,

$$\sum_{i \in F \sqcup G} u_i = \sum_{i \in F} u_i + \sum_{i \in G} u_i \geq \sum_{i \in A} u_i + \sum_{i \in B} u_i - 2\varepsilon.$$

Par la caractérisation de la borne supérieure,

$$\sum_{i \in A \sqcup B} u_i = \sum_{i \in A} u_i + \sum_{i \in B} u_i.$$

□

Remarque 5.19.

Par récurrence, on généralise le lemme à une somme finie sur des parties disjointes deux à deux.

Démonstration (théorème de sommation par paquets, hors programme).

S'il existe $i \in I$ vérifiant $u_i = +\infty$, le résultat est immédiat. Supposons donc que pour tout $i \in I$, $u_i \in \mathbb{R}_+$.

Soit F une partie finie de I . Si $j \in J$, notons $F_j = F \cap I_j$. Remarquons :

- que F_j est une partie finie de I_j ;
- qu'il existe un nombre fini de $j \in J$ pour lesquels $F_j \neq \emptyset$.

Notons $K = \{j \in J \mid F_j \neq \emptyset\}$. Ainsi, K est une partie finie de J et

$$F = \bigsqcup_{j \in K} F_j.$$

Ainsi,

$$\begin{aligned} \sum_{i \in F} u_i &= \sum_{j \in K} \sum_{i \in F_j} u_i \\ &\leq \sum_{j \in K} \sum_{i \in I_j} u_i \\ &\leq \sum_{j \in J} \sum_{i \in I_j} u_i. \end{aligned}$$

Ainsi, par passage à la borne supérieure,

$$\sum_{i \in I} u_i \leq \sum_{j \in J} \sum_{i \in I_j} u_i.$$

Réciproquement, soit $K \subset J$ finie. Comme $I' = \bigsqcup_{j \in K} I_j$ est une union finie de parties de I , on a par le lemme 5.18,

$$\sum_{j \in K} \sum_{i \in I_j} u_i = \sum_{i \in I'} u_i \leq \sum_{i \in I} u_i.$$

Ainsi, par passage à la borne supérieure,

$$\sum_{j \in J} \sum_{i \in I_j} u_i \leq \sum_{i \in I} u_i.$$

On a donc bien l'égalité. □

Remarque 5.20.

Ce théorème, fondamental, a deux usages principaux : montrer qu'une famille est sommable, et calculer la somme d'une famille.

Exercice 5.21.

On sait que $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Calculer $\sum_{n \in \mathbb{Z}^*} \frac{1}{n^2}$.

Corollaire 5.22 (théorème de Fubini positif).

Soit I, J deux ensembles, soit $(u_{i,j})_{(i,j) \in I \times J} \in (\mathbb{R}_+)^{I \times J}$. Alors,

$$\sum_{(i,j) \in I \times J} u_{i,j} = \sum_{i \in I} \left(\sum_{j \in J} u_{i,j} \right) = \sum_{j \in J} \left(\sum_{i \in I} u_{i,j} \right).$$

Démonstration.

Il suffit de considérer les paquets $I_j = \{(i,j) \mid i \in I\}$ et $J_i = \{(i,j) \mid j \in J\}$, puis d'appliquer le théorème de sommation par paquets. □

Remarque 5.23.

Bien entendu, ce résultat s'étend à tous les produits cartésiens finis.

Exercice 5.24.

On sait que $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Calculer $\sum_{(i,j) \in (\mathbb{N}^*)^2} \frac{1}{i^2 2^j}$.

5.2 Familles sommables de nombres complexes

L'extension de la notion de somme à un ensemble quelconque est bien plus délicate, dès lors que l'on abandonne l'hypothèse de positivité des nombres sommés.

Prenons l'exemple de la somme $\sum_{n \in \mathbb{Z}} n$. Le découpage

$$0 + \underbrace{1-1} + \underbrace{2-2} + \underbrace{3-3} + \dots$$

donne un regroupement par paquets de somme nulle, tandis que le regroupement

$$0 + 1 + \underbrace{2-1} + \underbrace{3-2} + \underbrace{4-3} + \dots$$

donne un regroupement par paquets de somme $+\infty$. Pire, le regroupement

$$\sum_{n=0}^{+\infty} k + \sum_{n=1}^{+\infty} (-k)$$

donne un regroupement par paquets n'ayant aucun sens.

Ainsi, les procédés sommatoires généraux font apparaître des hypothèses que ne connaissent pas les procédés sommatoires positifs.

Définition 5.1 (famille sommable).

Une famille $(u_i)_{i \in I} \in \mathbb{C}^I$ est sommable si $\sum_{i \in I} |u_i| < +\infty$, i.e. si la famille positive $(|u_i|)_{i \in I}$ est sommable.

Notation 5.2.

On note $\ell^1(I)$ l'ensemble des familles sommables de nombres complexes indicées par I .

Définition 5.3 (somme d'une famille réelle).

Soit $(u_i)_{i \in I} \in \mathbb{R}^I$ sommable. Si $i \in I$, on définit

$$\begin{aligned} u_i^+ &= \max(0, u_i), \\ u_i^- &= \max(0, -u_i). \end{aligned}$$

Alors, $(u_i^+)_{i \in I}$ et $(u_i^-)_{i \in I}$ sont sommables et l'on définit la somme de la famille $(u_i)_{i \in I}$ comme

$$\sum_{i \in I} u_i = \sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^-.$$

Démonstration.

On a pour tout $i \in I$, $0 \leq u_i^+ \leq |u_i|$ et $0 \leq u_i^- \leq |u_i|$, ce qui justifie la sommabilité des familles $(u_i^+)_{i \in I}$ et $(u_i^-)_{i \in I}$ ainsi que la validité de la différence dans la définition de $\sum_{i \in I} u_i$. $\square$

Définition 5.4 (somme d'une famille complexe).

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ sommable. Alors, $(\operatorname{Re}(u_i))_{i \in I}$ et $(\operatorname{Im}(u_i))_{i \in I}$ sont sommables et l'on définit la somme de la famille $(u_i)_{i \in I}$ comme

$$\sum_{i \in I} u_i = \sum_{i \in I} \operatorname{Re}(u_i) + i \sum_{i \in I} \operatorname{Im}(u_i).$$

Démonstration.

On a pour tout $i \in I$, $0 \leq |\operatorname{Re}(u_i)| \leq |u_i|$ et $0 \leq |\operatorname{Im}(u_i)| \leq |u_i|$, ce qui justifie la sommabilité des familles $(\operatorname{Re}(u_i))_{i \in I}$ et $(\operatorname{Im}(u_i))_{i \in I}$, et donc la validité de la définition de $\sum_{i \in I} u_i$. $\square$

Remarque 5.5.

Sous réserve de sommabilité, on a donc par définition

$$\operatorname{Re} \left(\sum_{i \in I} u_i \right) = \sum_{i \in I} \operatorname{Re}(u_i)$$

et

$$\operatorname{Im} \left(\sum_{i \in I} u_i \right) = \sum_{i \in I} \operatorname{Im}(u_i)$$

Remarque 5.6 (séries et convergence absolues).

Dans le cas d'une suite $(u_n) \in \mathbb{C}^{\mathbb{N}}$, la famille $(u_n)_{n \in \mathbb{N}}$ est sommable si et seulement si la série $\sum_{n \geq 0} u_n$ converge absolument. En cas de convergence absolue, on a alors

$$\sum_{n \in \mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n.$$

Remarque 5.7 (sommes finies).

Une famille finie de nombres complexes est toujours sommable.

Proposition 5.8.

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ une famille sommable. Pour tout $\varepsilon > 0$, il existe $F \subset I$ finie telle que

$$\left| \sum_{i \in I} u_i - \sum_{i \in F} u_i \right| \leq \varepsilon.$$

Démonstration.

On traite d'abord le cas où $\forall i \in I$, $u_i \in \mathbb{R}$. Il existe $F_+, F_- \subset I$ finies telles que

$$\begin{aligned} \sum_{i \in I} u_i^+ &\geq \sum_{i \in F_+} u_i^+ && \geq \sum_{i \in I} u_i^+ - \varepsilon, \\ \sum_{i \in I} u_i^- &\geq \sum_{i \in F_-} u_i^- && \geq \sum_{i \in I} u_i^- - \varepsilon. \end{aligned}$$

Ainsi, avec $F = F_+ \cup F_-$, qui est bien une partie finie de I , on a

$$\begin{aligned} \sum_{i \in I} u_i^+ &\geq \sum_{i \in F} u_i^+ && \geq \sum_{i \in I} u_i^+ - \varepsilon, \\ \sum_{i \in I} u_i^- &\geq \sum_{i \in F} u_i^- && \geq \sum_{i \in I} u_i^- - \varepsilon, \end{aligned}$$

donc notamment

$$-\sum_{i \in I} u_i^- + \varepsilon \geq -\sum_{i \in F} u_i^- \geq -\sum_{i \in I} u_i^-.$$

Comme pour tout $i \in F$, $u_i = u_i^+ - u_i^-$, on a

$$\sum_{i \in F} u_i = \sum_{i \in F} u_i^+ - \sum_{i \in F} u_i^- ,$$

comme par définition on a

$$\sum_{i \in I} u_i = \sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^- ,$$

on a en sommant les encadrements précédents :

$$\sum_{i \in I} u_i + \varepsilon \geq \sum_{i \in F} u_i \geq \sum_{i \in I} u_i - \varepsilon ,$$

ce qui est l'encadrement demandé.

Remarquons que, par construction, pour toute $G \subset I$ finie vérifiant $F \subset G$, alors

$$\left| \sum_{i \in I} u_i - \sum_{i \in G} u_i \right| \leq \varepsilon .$$

Pour le cas général, il existe $F_r, F_i \subset I$ finies telles que,

$$\begin{aligned} \left| \sum_{i \in I} \operatorname{Re}(u_i) - \sum_{i \in F_r} \operatorname{Re}(u_i) \right| &\leq \varepsilon , \\ \left| \sum_{i \in I} \operatorname{Im}(u_i) - \sum_{i \in F_i} \operatorname{Im}(u_i) \right| &\leq \varepsilon , \end{aligned}$$

Par la remarque précédente, on peut considérer $F = F_r \cup F_i$ (qui est une partie finie de I) et supposer que

$$\begin{aligned} \left| \sum_{i \in I} \operatorname{Re}(u_i) - \sum_{i \in F} \operatorname{Re}(u_i) \right| &\leq \varepsilon , \\ \left| \sum_{i \in I} \operatorname{Im}(u_i) - \sum_{i \in F} \operatorname{Im}(u_i) \right| &\leq \varepsilon , \end{aligned}$$

Alors, par l'inégalité triangulaire

$$\begin{aligned} \left| \sum_{i \in I} u_i - \sum_{i \in F} u_i \right| &\leq \left| \sum_{i \in I} \operatorname{Re}(u_i) - \sum_{i \in F} \operatorname{Re}(u_i) \right| \\ &\quad + \left| \sum_{i \in I} \operatorname{Im}(u_i) - \sum_{i \in F} \operatorname{Im}(u_i) \right| \\ &\leq 2\varepsilon . \end{aligned}$$

Quitte à changer ε et $\frac{\varepsilon}{2}$, on a donc le résultat demandé. $\square$

Théorème 5.9 (invariance de la somme par permutation).

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ sommable, soit $\sigma \in S_I$ une permutation de I . Alors,

$$\sum_{i \in I} u_i = \sum_{i \in I} u_{\sigma(i)} .$$

Notamment, les familles $(u_i)_{i \in I}$ et $(u_{\sigma(i)})_{i \in I}$ ont même nature.

Démonstration.

Il suffit d'appliquer le résultat analogue de la question précédentes :

- aux parties positives et négatives des u_i , en supposant que pour tout $i \in I$, $u_i \in \mathbb{R}$;
- aux parties réelles et imaginaires des u_i , dans le cas général.

$\square$

Une conséquence intéressante de ce résultat est le point suivant.

Exemple 5.10.

Soit $\sum_{n \geq 0} u_n$ une série complexe convergeant absolument. Alors, quelque soit la permutation σ de $\mathbb{N}$, la série $\sum_{n \geq 0} u_{\sigma(n)}$ converge absolument et

$$\sum_{n=0}^{+\infty} u_{\sigma(n)} = \sum_{n=0}^{+\infty} u_n .$$

Pour les séries semi-convergentes, on a le résultat suivant.

Exercice 5.11 (culturel, intéressant et difficile).

Soit $\sum_{n \geq 0} u_n$ une série réelle semi-convergente.

Alors, pour tout $\ell \in \mathbb{R}$, il existe une permutation σ de $\mathbb{N}$ telle que la série $\sum_{n \geq 0} u_{\sigma(n)}$ converge et

$$\sum_{n=0}^{+\infty} u_{\sigma(n)} = \ell .$$

Montrer aussi le résultat analogue pour $\ell = +\infty$ et $\ell = -\infty$.

Théorème 5.12 (argument de comparaison).

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ et $(v_i)_{i \in I} \in (\mathbb{R}_+)^I$ vérifiant

$$\forall i \in I, |u_i| \leq v_i .$$

Alors, si la famille $(v_i)_{i \in I}$ est sommable, la famille $(u_i)_{i \in I}$ l'est aussi.

Démonstration.

Immédiat par les résultats de la partie précédente. $\square$

Proposition 5.13 (linéarité de la somme).

Soit $(u_i)_{i \in I}, (v_i)_{i \in I} \in \mathbb{C}^I$ deux familles sommables, soit $\lambda, \mu \in \mathbb{C}$. Alors, la famille $(\lambda u_i + \mu v_i)_{i \in I}$ est sommable et

$$\sum_{i \in I} (\lambda u_i + \mu v_i) = \lambda \sum_{i \in I} u_i + \mu \sum_{i \in I} v_i.$$

Démonstration (fastidieuse et peu intéressante).

Traiter d'abord le cas réel, en décomposant λ, μ, u_i, v_i en parties positives, puis traiter le cas complexe en écrivant tout ceci sous forme algébrique. $\square$

Lemme 5.14 (sous-famille).

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ une famille sommable, soit $J \subset I$. Alors, $(u_j)_{j \in J}$ est une famille sommable.

Démonstration.

Immédiat d'après les résultats de la partie précédente. $\square$

Un résultat important est le théorème de sommation par paquets. Remarquons toutefois que, contrairement au cas des réels positifs, ce théorème ne peut s'appliquer qu'après avoir démontré que la famille étudiée est sommable.

Théorème 5.15 (sommation par paquets).

Soit J un ensemble. Pour chaque $j \in J$, on considère $I_j \subset I$ et l'on suppose que I est la réunion disjointe des I_j :

$$I = \bigsqcup_{j \in J} I_j.$$

Soit $(u_i)_{i \in I} \in \mathbb{C}^I$ une famille sommable.

Alors,

$$\sum_{i \in I} u_i = \sum_{j \in J} \left(\sum_{i \in I_j} u_i \right).$$

Démonstration (hors programme).

Admis

Remarquons toutefois que le lemme 5.14 assure que les familles $(u_i)_{i \in I_j}$ sont sommables, les sommes $\sum_{i \in I_j} u_i$ ont donc bien un sens. $\square$

Corollaire 5.16 (théorème de Fubini).

Soit I, J deux ensembles, soit $(u_{i,j})_{(i,j) \in I \times J} \in \mathbb{C}^{I \times J}$ une famille sommable. Alors,

$$\sum_{(i,j) \in I \times J} u_{i,j} = \sum_{i \in I} \sum_{j \in J} u_{i,j} = \sum_{j \in J} \sum_{i \in I} u_{i,j}.$$

Démonstration.

Il suffit de considérer les paquets $I_j = \{(i, j) \mid i \in I\}$ et $J_i = \{(i, j) \mid j \in J\}$, puis d'appliquer le théorème de sommation par paquets. $\square$

Le théorème de regroupement par paquets, et donc le théorème de Fubini, ne s'appliquent qu'une fois la sommabilité démontrée. Cette sommabilité s'obtient en étudiant une famille de réels positifs, étude pour laquelle nous disposons d'outils puissants (voir la partie précédente).

Exercice 5.17.

Pour $x \in \mathbb{C}$, étudier la somme

$$\sum_{n,p \in \mathbb{N}} \frac{x^n p^n}{n! p!}.$$

Dans le cas particulier (et courant) d'une somme double factorisée, on a toutefois une réciproque, qui permet d'appliquer le théorème de Fubini automatiquement.

Théorème 5.18.

Soit I, J deux ensembles, soit $(u_i)_{i \in I} \in \mathbb{C}^I$ et $(v_j)_{j \in J} \in \mathbb{C}^J$ deux familles sommables.

Alors, la famille $(u_i v_j)_{(i,j) \in I \times J}$ est sommable et

$$\sum_{(i,j) \in I \times J} u_i v_j = \left(\sum_{i \in I} u_i \right) \left(\sum_{j \in J} v_j \right).$$

Démonstration.

Il suffit de démontrer la sommabilité, l'égalité venant ensuite directement du théorème de Fubini. Soit $F \subset I \times J$ finie, il existe $G \subset I$ et $H \subset J$ finies telles que $F \subset G \times H$

(prendre $G = \{ i \in I \mid \exists j \in J, (i, j) \in F \}$). Alors,

$$\begin{aligned} \sum_{(i,j) \in F} |u_i v_j| &\leq \sum_{(i,j) \in G \times H} |u_i v_j| \\ &\leq \left(\sum_{i \in G} |u_i| \right) \left(\sum_{j \in H} |v_j| \right) \\ &\leq \left(\sum_{i \in I} |u_i| \right) \left(\sum_{j \in J} |v_j| \right). \end{aligned}$$

Par majoration, $\sum_{(i,j) \in I \times J} u_i v_j$ est sommable.

□

Remarque 5.19.

Cela se généralise par récurrence des sommes doubles aux sommes multiples.

Exemple 5.20.

Si $q \in]-1, 1[$, alors la famille $\left(\frac{q^{n+p}}{n!} \right)_{n,p \in \mathbb{N}}$ est sommable et

$$\sum_{n,p \in \mathbb{N}} \frac{q^{n+p}}{n!} = \frac{e^q}{1-q}.$$

Une utilisation importante de tous ces résultats concerne le produit de Cauchy de deux séries.

Corollaire 5.21 (produit de Cauchy).

Soit $\sum_{n \geq 0} a_n$, $\sum_{n \geq 0} b_n$ deux séries absolument convergentes. On définit pour $n \geq 0$:

$$c_n = \sum_{p=0}^n a_p b_{n-p}.$$

Alors, $\sum_{n \geq 0} c_n$ converge absolument et

$$\sum_{n=0}^{+\infty} c_n = \left(\sum_{n=0}^{+\infty} a_n \right) \left(\sum_{n=0}^{+\infty} b_n \right).$$

Démonstration.

Il suffit d'appliquer le théorème 5.18 aux deux familles sommables $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ pour obtenir que la famille $(a_n b_m)_{(n,m) \in \mathbb{N}^2}$ est sommable, puis de procéder par regroupement par paquets avec les paquets

$$I_n = \{ (p, n-p) \mid 0 \leq p \leq n \}.$$

□

Exercice 5.22.

Pour $x \in \mathbb{C}$, montrer que les deux séries $\sum_{n \geq 0} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$ et $\sum_{n \geq 0} (-1)^n \frac{x^{2n}}{(2n)!}$ convergent absolument.

On note alors

$$\begin{aligned} \sin(x) &= \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}, \\ \cos(x) &= \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n}}{(2n)!}. \end{aligned}$$

Montrer que $2 \sin(x) \cos(x) = \sin(2x)$.

6 Annexe : compléments

Voici deux critères de convergence qui peuvent être utiles.

Proposition 6.1 (Test de comparaison logarithmique).

Soient (u_n) et (v_n) deux suites à termes réels strictement positifs telles que pour tout $n \in \mathbb{N}$, $\frac{u_{n+1}}{u_n} \leq \frac{v_{n+1}}{v_n}$.

Alors :

- (i) si $\sum v_n$ converge, il en est de même de $\sum u_n$;
- (ii) si $\sum u_n$ diverge, il en est de même de $\sum v_n$.

Démonstration.

Nous avons pour tout n , $\frac{u_{n+1}}{v_{n+1}} \leq \frac{u_n}{v_n}$, et donc par récurrence : $\frac{u_n}{v_n} \leq \frac{u_0}{v_0}$. En posant $\mu = \frac{u_0}{v_0}$, il vient donc : $u_n \leq \mu v_n$. Le résultat découle alors directement de 2.4. □

Proposition 6.2 (Règle de d'Alembert).

Soit (u_n) une suite à termes réels strictement positifs.

- (i) S'il existe $q \in]0, 1[$ tel que pour tout $n \in \mathbb{N}$, $\frac{u_{n+1}}{u_n} \leq q$, alors la série $\sum u_n$ est convergente.
- (ii) S'il existe $q \in [1, +\infty[$ tel que pour tout $n \in \mathbb{N}$, $\frac{u_{n+1}}{u_n} \geq q$, alors la série $\sum u_n$ est divergente.

- (iii) en particulier, si $\lim_{n \rightarrow +\infty} \frac{u_{n+1}}{u_n} = \ell \in \overline{\mathbb{R}}$:
- si $\ell \in [0, 1[$, la série $\sum u_n$ est convergente ;
 - si $\ell > 1$, la série $\sum u_n$ est divergente ;
 - si $\ell = 1$, on ne peut rien dire, sauf dans le cas $u_n \leq u_{n+1}$ à partir d'un certain rang, où il y a divergence grossière.

Démonstration. (i) Posons $v_n = q^n$. Alors $\sum v_n$ converge, et pour tout n , $\frac{u_{n+1}}{u_n} \leq \frac{v_{n+1}}{v_n}$. Le critère de comparaison logarithmique 6.1 permet alors de conclure.

(ii) Même démonstration (ou même divergence grossière).

(iii) Découle des deux points précédents. $\square$

Exemple 6.3.

- Soient $x \in \mathbb{R}^*$ et $u_n = \frac{x^n}{n!}$. Alors $\frac{u_{n+1}}{u_n} \xrightarrow{n \rightarrow +\infty} 0$, donc $\sum u_n$ converge, et de plus on en tire que $u_n \xrightarrow{n \rightarrow +\infty} 0$.
- Soient $\alpha \in \mathbb{R}$ et $u_n = n^\alpha$. Alors $\frac{u_{n+1}}{u_n} \xrightarrow{n \rightarrow +\infty} 1$, et pourtant, suivant la valeur de α , $\sum u_n$ peut aussi bien diverger que converger.

Chapitre XXIX

Espaces euclidiens et préhilbertiens réels

Sommaire

1	Produit scalaire, norme et distance. . .	460
2	Orthogonalité.	463
2.1	Premières définitions.	463
2.2	Familles orthogonales.	463
2.3	Sous-espaces vectoriels orthogonaux. .	465
2.4	Formes linéaires et hyperplans d'un es- pace euclidien.	466
2.5	Symétries et projecteurs orthogonaux.	467
2.6	Distance à un sous ev.	467
2.7	Distance et projection sur un hyperplan	467

Le corps de base est $\mathbb{R}$. n, p, q, r et s désignent des entiers naturels non nuls. E désigne un espace vectoriel.

1 Produit scalaire, norme et distance.

Définition 1.1.

On appelle *produit scalaire sur E* toute application $\varphi : E \times E \rightarrow \mathbb{R}$ bilinéaire symétrique et telle que pour tout $x \in E$, on ait d'une part $\varphi(x, x) \geq 0$ et d'autre part $\varphi(x, x) = 0$ si et seulement si $x = 0$. Un espace vectoriel réel muni d'un produit scalaire est dit *préhilbertien*. Si de plus il est de dimension finie, il est dit *euclidien*.

Remarque 1.2. • Différentes notations sont utilisées couramment pour le produit scalaire de x et y : $(x | y), \langle x | y \rangle, (x, y), \langle x, y \rangle, x \cdot y$.

- Par bilinéarité, si x ou $y = 0$, $\langle x | y \rangle = 0$.
- La symétrie et la linéarité par rapport à une variable suffisent à montrer la bilinéarité.
- Jusqu'à maintenant on définissait le produit scalaire à partir d'angles. En fait c'est l'inverse que l'on fait lorsque l'on théorise tout cela.

Exemple 1.3. • Les produits scalaires usuels vus en début d'année sur $\mathbb{R}^2$ et $\mathbb{R}^3$ sont bien évidemment des produits scalaires.

- Il existe de nombreux produits scalaires sur $\mathbb{R}^2$; par exemple $((x_1, y_1), (x_2, y_2)) \mapsto x_1x_2 - y_1x_2 + 2y_1y_2 - x_1y_2$.
- Il existe également sur $\mathbb{R}^n$ un produit scalaire canonique ; $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = \sum_{k=1}^n x_k y_k$.
- Par extension, tout $\mathbb{R}$ -ev de dimension n , étant isomorphe à $\mathbb{R}^n$, est muni d'un produit scalaire. Ainsi, sur $\mathbb{R}_n[X]$ le produit scalaire usuel est $\left(\sum_{k=0}^n a_k X^k \right) \cdot \left(\sum_{k=0}^n b_k X^k \right) = \left(\sum_{k=0}^n a_k b_k \right)$.

- Soit a et b deux réels avec $a < b$. Sur $\mathcal{C}([a, b], \mathbb{R})$, l'application $(f, g) \mapsto \int_a^b fg$ est un produit scalaire (attention : cet espace est de dimension infinie, donc n'est pas euclidien, mais préhilbertien réel).

Exercice 1.4.

L'espérance munit-elle l'ensemble des variables aléatoires réelles sur un espace probabilisé fini d'un produit scalaire (via $\langle X, Y \rangle = E(XY)$) ?

Proposer une solution à ce « problème ».

Définition 1.5 (Norme).

Soit E un $\mathbb{R}$ -espace vectoriel. On appelle *norme sur E* toute application $\|\cdot\| : E \rightarrow \mathbb{R}^+$ vérifiant les trois conditions suivantes :

- (i) $\forall x \in E \quad \|x\| = 0 \iff x = 0$;
- (ii) $\forall \lambda \in \mathbb{R}, \forall x \in E \quad \|\lambda x\| = |\lambda| \|x\|$ (homogénéité) ;
- (iii) $\forall (x, y) \in E^2 \quad \|x + y\| \leq \|x\| + \|y\|$ (inégalité triangulaire).

Remarque 1.6.

Il convient de ne pas oublier la positivité dans la définition d'une norme.

Exemple 1.7.

Sur $\mathbb{R}^n$ et pour $p \in \{1, 2\}^1$, les applications

$$\|\cdot\|_p : (x_1, \dots, x_n) \mapsto \left(\sum_{k=1}^n |x_k|^p \right)^{1/p}$$

et

$$\|\cdot\|_\infty : (x_1, \dots, x_n) \mapsto \max_{k \in [1, n]} |x_k|$$

sont des normes.

Exercice 1.8.

Pour une norme $\|\cdot\|$, on appelle *boule centrée en $a \in E$ et de rayon $r \geq 0$* l'ensemble

$$B(a, r) = \{ x \in E \mid \|a - x\| \leq r \}.$$

Tracer les boules centrées en 0 et de rayon 1 pour les normes $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$ sur $\mathbb{R}^2$.

1. et même pour tout $p \in [1, +\infty[$

Remarque 1.9.

Soit E un $\mathbb{R}$ -espace vectoriel muni d'une norme $\|\cdot\|$. Alors pour tout $(x, y) \in E^2$, on a

$$|\|x\| - \|y\|| \leq \|x - y\|.$$

Démonstration.

Soit $(x, y) \in E^2$. Remarquons qu'on a $\|x\| = \|x + y - y\| \leq \|x + y\| + \|y\|$ par l'inégalité triangulaire, d'où l'on déduit $\|x\| - \|y\| \leq \|x + y\|$. Symétriquement, on remarque qu'on a $\|y\| - \|x\| \leq \|x + y\|$. Or $\|x\| - \|y\| = \max(\|x\| - \|y\|, \|y\| - \|x\|)$. On en déduit le résultat. $\square$

Définition 1.10 (Distance associée à une norme).

Soit E un $\mathbb{R}$ -espace vectoriel muni d'une norme $\|\cdot\|$. On appelle *distance associée à la norme* $\|\cdot\|$ l'application $d : (x, y) \mapsto \|x - y\|$.

Remarque 1.11.

Plus généralement, si E est un ensemble (quelconque, pas nécessairement un espace vectoriel), on appelle *distance sur E* toute application $d : E^2 \rightarrow \mathbb{R}^+$ vérifiant les trois conditions suivantes :

- (i) $\forall (x, y) \in E^2 \quad d(x, y) = 0 \iff x = y$;
- (ii) $\forall (x, y) \in E^2 \quad d(x, y) = d(y, x)$ (symétrie) ;
- (iii) $\forall (x, y, z) \in E^3 \quad d(x, z) \leq d(x, y) + d(y, z)$ (inégalité triangulaire).

Un ensemble muni d'une distance est appelé *espace métrique*.

Par exemple, la distance usuelle dans le plan est une distance ; le nombre minimal d'arêtes à parcourir sur ce graphe pour relier deux points donnés définit une distance.

On pourra vérifier que la distance associée à une norme est bien une distance.

Exemple 1.12.

La distance associée à $\|\cdot\|_1$ est parfois appelée *distance de Manhattan*. Dans Manhattan, les rues forment un damier « orthogonal », on ne peut donc que se déplacer parallèlement à ces axes. La distance parcourue entre deux points n'est donc pas la distance « euclidienne » usuelle ...

Définition 1.13 (Norme associée à un produit scalaire).

Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien. On appelle *norme associée au produit scalaire* $\langle \cdot | \cdot \rangle$ l'application $x \mapsto \sqrt{\langle x | x \rangle}$.

Remarque 1.14. 1. Il est clair, par positivité du produit scalaire, que cette application est bien définie. La racine carrée étant à valeurs dans $\mathbb{R}^+$, elle est de plus à valeurs dans $\mathbb{R}^+$. Il reste à voir si cette application est bien une norme.

- 2. La norme associée à un produit scalaire dépend évidemment du produit scalaire. Par exemple sur $\mathbb{R}^2$, les normes associées respectivement au produit scalaire usuel et au produit scalaire $((x, y), (x', y')) \mapsto \frac{1}{2}xx' + 2yy'$ sont différentes (regarder par exemple les valeurs pour les vecteurs $(1, 0)$ et $(0, 1)$).
- 3. On a directement que pour une famille $(x_1, \dots, x_n)$ de vecteurs,

$$\begin{aligned} \left\| \sum_{i=1}^n x_i \right\|^2 &= \sum_{1 \leq i, j \leq n} \langle x_i | x_j \rangle \\ &= \sum_{i=1}^n \|x_i\|^2 + 2 \sum_{1 \leq i < j \leq n} \langle x_i | x_j \rangle. \end{aligned}$$

Pour deux vecteurs, on retrouve $\|x \pm y\|^2 = \|x\|^2 \pm 2 \langle x | y \rangle + \|y\|^2$.

Dans tout ce qui suit, sauf mention expresse du contraire, $(E, \langle \cdot | \cdot \rangle)$ désigne un espace vectoriel préhilbertien, et $\|\cdot\|$ la norme associée à son produit scalaire.

Proposition 1.15.

Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien et $\|\cdot\|$ la norme associée. On a

- 1. $\forall x \in E \quad \|x\| = 0 \iff x = 0$;
- 2. $\forall \lambda \in \mathbb{R} \quad \forall x \in E \quad \|\lambda x\| = |\lambda| \cdot \|x\|$.

Démonstration. 1. Soit $x \in E$. On a $\|x\| = 0 \iff \langle x | x \rangle = 0$. $\langle \cdot | \cdot \rangle$ étant un produit scalaire, on a donc $\|x\| = 0 \iff x = 0$.

2. Soit $\lambda \in \mathbb{R}$ et $x \in E$. On a $\|\lambda x\| = \sqrt{\langle \lambda x | \lambda x \rangle} = \sqrt{\lambda^2 \langle x | x \rangle} = |\lambda| \sqrt{\langle x | x \rangle}$. $\square$

Avec ce qui précède, il suffit maintenant de démontrer que $\|\cdot\|$ vérifie l'inégalité triangulaire pour démontrer qu'il s'agit bien d'une norme. Pour cela, on démontre tout d'abord le théorème suivant.

Théorème 1.16 (Inégalité de Cauchy-Schwarz). Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien et $\|\cdot\|$ la norme associée. Alors pour tout $(x, y) \in E^2$, on a

$$|\langle x | y \rangle| \leq \|x\| \cdot \|y\|.$$

L'égalité a lieu si et seulement si x et y sont colinéaires.

Démonstration.

Soient $x, y \in E$. Pour $y = 0$ le résultat est évident. Sinon, on peut donner deux démonstrations

Géométrique Posons $u = \frac{1}{\|y\|}y$. On vérifie aisément $\|u\| = 1$. Posons alors $x' = \langle x | u \rangle u$ et $x'' = x - x'$ (faire un dessin). On a alors

$$\langle x' | x'' \rangle = \langle x' | x \rangle - \langle x' | x' \rangle = \langle x | u \rangle^2 - \langle x | u \rangle^2 = 0.$$

On en déduit

$$\begin{aligned} \|x\|^2 &= \|x'\|^2 + 2\langle x' | x'' \rangle + \|x''\|^2 \\ &= \|x'\|^2 + \|x''\|^2 \\ &\geq \|x'\|^2. \end{aligned}$$

On en déduit $\|x\| \cdot \|y\| \geq \|x'\| \cdot \|y\|$. Or on a :

$$\begin{aligned} \|x'\| \cdot \|y\| &= |\langle x | u \rangle| \cdot \|y\| \\ &= |\langle x | y \rangle|. \end{aligned}$$

D'où le résultat.

Algébrique pour tout $t \in \mathbb{R}$, on a : $\|x + ty\|^2 = \|x\|^2 + 2t\langle x | y \rangle + t^2\|y\|^2$. C'est un polynôme toujours positif, donc son discriminant est négatif ou nul.

Il y a égalité dans l'inégalité de Cauchy-Schwarz si et seulement si ce discriminant est nul, donc si et seulement si ce polynôme a une racine réelle, donc si et seulement si il existe t tel que [à vous de l'écrire], donc si et seulement si x et y sont colinéaires.

Une idée calculatoire astucieuse Si $x = 0$ ou $y = 0$, le résultat est évident. Sinon, on remarque que $\left\| \frac{x}{\|x\|} \right\| = 1$ et l'on écrit ($\pm$ signifie qu'on le fait pour $+$ puis pour $-$) :

$$0 \leq \left\| \frac{x}{\|x\|} \pm \frac{y}{\|y\|} \right\|^2 = \left\| \frac{x}{\|x\|} \right\|^2 + \left\| \frac{y}{\|y\|} \right\|^2 \pm 2 \frac{\langle x | y \rangle}{\|x\| \|y\|}$$

ce qui donne

$$0 \leq 1 \pm \frac{\langle x | y \rangle}{\|x\| \|y\|}$$

et c'est fini ! $\square$

Proposition 1.17 (Inégalité triangulaire).

Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien, $x, y \in E$. Alors,

$$\|x + y\| \leq \|x\| + \|y\|.$$

De plus, on a l'égalité si et seulement si x et y sont colinéaires et de même sens.

Démonstration.

On a $\|x + y\|^2 = \langle x + y | x + y \rangle = \|x\|^2 + 2\langle x | y \rangle + \|y\|^2$. Or $(\|x\| + \|y\|)^2 = \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2$ et $\langle x | y \rangle \leq \|x\| \cdot \|y\|$, donc $\|x + y\|^2 \leq (\|x\| + \|y\|)^2$. $\|x + y\|$ et $\|x\| + \|y\|$ étant positifs, on en déduit le résultat.

L'égalité a lieu si et seulement si $\langle x | y \rangle = \|x\| \cdot \|y\|$. Pour cela, il est nécessaire d'avoir $\langle x | y \rangle \geq 0$ (car le produit de deux normes est positif ou nul) et x et y colinéaires (cas d'égalité de Cauchy-Schwarz), donc il est nécessaire que x et y soient colinéaires — l'un s'écrit comme produit de l'autre par un scalaire — et de même sens — ce scalaire est positif ou nul. Cette condition est clairement suffisante. $\square$

Théorème 1.18.

Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien, $x, y \in E$.

1. Identité du parallélogramme :

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2).$$

2. Identité de polarisation :

$$\begin{aligned} \langle x | y \rangle &= \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2) \\ &= \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2). \end{aligned}$$

Remarque 1.19.

Faire le dessin d'un parallélogramme, on utilise le théorème d'Al-Kashi deux fois (une par hypothèse).

Démonstration.

Il suffit de développer les normes. $\square$

Remarque 1.20.

Ces identités permettent de retrouver l'expression du produit scalaire quand on ne connaît que la norme.

Exemple 1.21.

Existe-t-il un produit scalaire donnant la norme $\|(x, y)\|^2 = (x + y)^2 + x^2$?

2 Orthogonalité.

Soit $(E, \langle \cdot | \cdot \rangle)$ un ev préhilbertien et $\|\cdot\|$ la norme associée.

2.1 Premières définitions.

Définition 2.1.

Soient $x, y \in E$. On dit que x est *unitaire* (ou *normé*) si $\|x\| = 1$. On dit que x et y sont *orthogonaux* et l'on note $x \perp y$ si $\langle x | y \rangle = 0$.

Remarque 2.2.

Si $x \neq 0_E$, il y a exactement deux vecteurs unitaires colinéaires à x .

Exemple 2.3.

- Tout vecteur est toujours orthogonal au vecteur nul.
- Dans $\mathbb{R}^2$ muni du produit scalaire usuel, $(1, 3)$ et $(-6, 2)$ sont orthogonaux.
- Dans $\mathbb{R}^2$ muni du produit scalaire $(x, y) \cdot (x', y') = 2xx' - xy' - x'y + 3yy'$, les vecteurs $(1, 1)$ et $(2, -1)$ sont orthogonaux.

2.2 Familles orthogonales.

Définition 2.1.

Une famille de vecteurs est dite *orthogonale* s'ils sont 2 à 2 orthogonaux. Si les vecteurs sont de plus unitaires, la famille est dite *orthonormale* (ou *orthonormée*).

Exemple 2.2.

Les $f_n : x \mapsto \cos(nx)$, $n \in \mathbb{N}$, forment une famille orthogonale pour le produit scalaire usuel de $\mathcal{C}([0, 2\pi], \mathbb{R})$.

Théorème 2.3 (Pythagore).

Soit $(v_1, \dots, v_n)$ une famille orthogonale de n vecteurs. Alors $\left\| \sum_{k=1}^n v_k \right\|^2 = \sum_{k=1}^n \|v_k\|^2$.

Démonstration.

On développe le produit scalaire : $\left\| \sum_{k=1}^n v_k \right\|^2 = \sum_{i=1}^n \sum_{j=1}^n \langle v_i | v_j \rangle$. □

Exemple 2.4.

Dans $\mathbb{R}^3$ muni du produit scalaire usuel, on pose $v_1 = (1, 2, 3)$, $v_2 = (-5, 1, 1)$ et $v_3 = (-1, -16, 11)$. Vérifier que la famille (v_1, v_2, v_3) est orthogonale et s'assurer que l'égalité donnée par le théorème de Pythagore est vérifiée.

Théorème 2.5.

Toute famille orthogonale ne comportant **aucun vecteur nul** est libre.

Démonstration.

Soient λ_k tels que $\sum_{k=1}^n \lambda_k v_k = 0$. Alors pour tout i , $\left\langle \sum_{k=1}^n \lambda_k v_k | v_i \right\rangle = 0$ or quand on développe la somme on a $\lambda_i \langle v_i | v_i \rangle$. □

Remarque 2.6.

Toute famille orthonormale est une famille orthogonale ne comportant aucun vecteur nul.

Corollaire 2.7.

Toute famille orthogonale ne comportant **aucun vecteur nul** et de cardinal $\dim E$ est une base de E .

Exemple 2.8.

$\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$, $\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$ et $\begin{pmatrix} 5 \\ 2 \\ -1 \end{pmatrix}$ forment une famille orthogonale de trois vecteurs non nuls de $\mathbb{R}^3$, et donc une base de $\mathbb{R}^3$.

Théorème 2.9 (orthonormalisation de Gram-Schmidt).

On suppose E euclidien de dim n . Soit $(u_1, \dots, u_n)$ une base de E . Alors il existe une base $(v_1, \dots, v_n)$ de E telle que :

1. $(v_1, \dots, v_n)$ est orthonormale ;
2. pour tout $k \in \llbracket 1, n \rrbracket$,

$$\text{Vect}(u_1, \dots, u_k) = \text{Vect}(v_1, \dots, v_k).$$

Les v_k sont uniques au signe près et on peut

$$\text{choisir : } v_k = \frac{u_k - \sum_{i=1}^{k-1} \langle u_k | v_i \rangle v_i}{\left\| u_k - \sum_{i=1}^{k-1} \langle u_k | v_i \rangle v_i \right\|}.$$

Démonstration.

Explication pour le choix de v_1 .

• Analyse : on suppose la famille construite jusqu'au rang k . Construisons le $k+1$ vecteur.

Il faut choisir v_{k+1} dans $\text{Vect}(u_1, \dots, u_k, u_{k+1}) = \text{Vect}(v_1, \dots, v_k, u_{k+1})$: $v_{k+1} = \lambda_1 v_1 + \dots + \lambda_k v_k + \mu u_{k+1}$. $\langle v_{k+1} | v_j \rangle = 0$ donne $\lambda_j + \mu \langle u_{k+1} | v_j \rangle = 0$, donc $v_{k+1} = \mu \left(- \sum_{i=1}^k \langle u_{k+1} | v_i \rangle v_i + u_{k+1} \right)$. Reste à choisir μ pour avoir $\|v_{k+1}\| = 1$ (2 choix possibles).

• Synthèse : on a vu unicité au signe près. On vérifie que les vecteurs trouvés conviennent bien. $\square$

Exemple 2.10.

Orthonormaliser $(1, X, X^2)$ pour le produit scalaire de $\mathbb{R}_2[X]$ défini par $\langle P | Q \rangle = \int_0^1 P(t)Q(t) dt$.

On trouve (P_0, P_1, P_2) , où

$$P_0 = 1,$$

$$P_1 = \frac{X - 1/2}{1/(2\sqrt{3})} = \sqrt{3}(2X - 1),$$

$$P_2 = \frac{X^2 - X + 1/6}{\|\dots\|} = \sqrt{5}(6X^2 - 6X + 1).$$

Corollaire 2.11.

Tout espace euclidien a une base orthonormale. Toute famille orthonormale peut être complétée en une base orthonormale.

Démonstration.

Pour l'existence, il suffit d'orthonormaliser une base quelconque.

Soit $(e_1, \dots, e_p)$ une famille orthonormale de E . On peut la compléter en base de E : $(e_1, \dots, e_p, e'_{p+1}, \dots, e'_n)$.

On orthonormalise ensuite cette base : pour les p premiers vecteurs, on a à chaque fois le choix entre e_i et $-e_i$, on choisit bien entendu e_i .

On obtient donc une base orthonormée de E dont les p premiers vecteurs sont $e_1, \dots, e_p$. $\square$

Proposition 2.12 (Coordonnées dans une base orthonormale).

Soit E euclidien, $(v_1, \dots, v_n)$ base orthonormale de E . Alors, pour tout $x \in E$, $x = \sum_{k=1}^n \langle x | v_k \rangle v_k$.

Démonstration.

Soit $x \in E$, soit $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tels que $x = \sum_{k=1}^n \lambda_k v_k$. Si $1 \leq k \leq n$, on a par bilinéarité du produit scalaire

$$\begin{aligned} \langle x | v_k \rangle &= \sum_{i=1}^n \lambda_i \langle v_k | v_i \rangle \\ &= \sum_{i=1}^n \lambda_i \delta_{i,k} \\ &= \lambda_k. \end{aligned}$$

$\square$

Exemple 2.13.

Trouver les coordonnées de $(1, -3)$ dans la base $\left(\frac{1}{\sqrt{2}}(1, 1), \frac{1}{\sqrt{2}}(1, -1) \right)$ (pour le produit scalaire usuel).

Exercice 2.14.

Exprimer la formule de la proposition 2.12 dans le cas où $(v_1, \dots, v_n)$ base orthogonale de E .

Proposition 2.15 (Expression du produit scalaire dans une base orthonormale).

Soit E euclidien, $(v_1, \dots, v_n)$ une base orthonormale de E . x et y de coordonnées (x_i) et (y_i) dans la base $(v_1, \dots, v_n)$. Alors $\langle x | y \rangle = \sum_{k=1}^n x_k y_k$.

Remarque 2.16 (Écriture matricielle du produit scalaire).

Notons X et Y les matrices respectives de x et y dans la base orthonormale $(v_1, \dots, v_n)$, alors $\langle x | y \rangle = X^\top \cdot Y$ (en identifiant la matrice $X^\top \cdot Y$ et son unique coefficient).

Corollaire 2.17.

Avec les mêmes notations,

$$\|x\|^2 = \sum_{i=1}^n x_i^2.$$

Remarque 2.18.

Tous les produits scalaires ont la même expression «usuelle» à condition de se placer dans une base orthonormale **pour ce produit scalaire**.

Remarque 2.19.

Ces formules d'adaptent encore dans le cas de bases orthogonales.

2.3 Sous-espaces vectoriels orthogonaux.

Définition 2.1.

Soit F et G deux sous-espaces vectoriels de E . On dit que F et G sont des sous-espaces orthogonaux et on écrit $F \perp G$ si

$$\forall x \in F \quad \forall y \in G \quad x \perp y.$$

Exemple 2.2.

Dans $\mathbb{R}^3$ avec le produit scalaire usuel, $\text{Vect}(1, -1, 0) \perp \text{Vect}((1, 1, 0), (0, 0, 1))$.

Remarque 2.3.

Si F et G sont orthogonaux, alors ils sont en somme directe. En effet, soit alors $x \in F \cap G$. On a alors $x \perp x$, donc $\langle x | x \rangle = 0$, donc $x = 0$. Donc $F \cap G \subset \{0\}$, d'où on déduit le résultat.

Théorème 2.4.

Soient F et G deux sev de dimension finies de E . On note $(f_1, \dots, f_q)$ une famille génératrice de F et $(g_1, \dots, g_p)$ une famille génératrice de G . Alors

$F \perp G$ si et seulement si pour tout $i \in \llbracket 1, q \rrbracket$ et $j \in \llbracket 1, p \rrbracket$ on a $\langle f_i | g_j \rangle = 0$.

Démonstration.

$(\Rightarrow)$ par définition de $F \perp G$.

$(\Leftarrow)$ soient $f = \sum \lambda_i f_i$ et $g = \sum \mu_j g_j$. Alors $\langle f | g \rangle = \sum_i \sum_j \lambda_i \mu_j \langle f_i | g_j \rangle = 0$. $\square$

Définition 2.5.

Soit X une partie (quelconque) de E . On appelle *orthogonal* de X et on note $X^\perp$ (ou X^o) l'ensemble $\{y \in E \mid \forall x \in X \quad \langle x | y \rangle = 0\}$.

Proposition 2.6.

Soit X une partie de E . Alors

1. $X^\perp$ est un sev de E ;
2. Pour toute partie Y de E telle que $X \subset Y$, on a $Y^\perp \subset X^\perp$;
3. $X \subset (X^\perp)^\perp$.

Démonstration. 1. On a $0 \in X^\perp$ car 0 est orthogonal à tout vecteur, donc à tout vecteur de X ; de plus toute combinaison linéaire de vecteurs orthogonaux à tout vecteur de X est orthogonale à tout vecteur de X .

Sinon, il suffit de voir que

$$X^\perp = \bigcap_{x \in X} \text{Ker } \langle x | \cdot \rangle.$$

2. Tout élément de $Y^\perp$ est orthogonal à tout vecteur de Y , donc a fortiori à tout vecteur de X .
3. Soit x un vecteur de X . Tout vecteur de $X^\perp$ est orthogonal à tout vecteur de X , donc en particulier à x . Donc x est orthogonal à tout vecteur de $X^\perp$, donc appartient à $(X^\perp)^\perp$. $\square$

Remarque 2.7.

Il n'y a pas forcément égalité dans le dernier point. Par exemple, avec $X = \emptyset$, $(X^\perp)^\perp = \{0\}$.

Théorème 2.8.

Soit F un sev de E . Alors $F^\perp$ est le plus grand sous-espace vectoriel orthogonal à F (et F et $F^\perp$ sont de plus en somme directe).

Si de plus F est de dimension finie, alors $E = F \oplus F^\perp$ et $F^\perp$ est l'unique sous-espace vectoriel G vérifiant $E = F \oplus G$ et $F \perp G$. C'est pourquoi on appelle $F^\perp$ **le** supplémentaire orthogonal de F dans E .

Enfin, si F est de dimension finie, alors $F = (F^\perp)^\perp$.

Démonstration.

On sait déjà que $F^\perp$ est un sous-espace vectoriel. F et $F^\perp$ sont clairement orthogonaux (donc en somme directe) et de plus pour tout sous-espace vectoriel G tel que F et G sont orthogonaux, tout élément x de G est orthogonal à tout élément de F , donc appartient à $F^\perp$, donc $G \subset F^\perp$.

Supposons de plus que le sous-espace vectoriel F est de dimension finie. Alors F est aussi un espace vectoriel euclidien, donc possède une base orthonormale $(f_1, \dots, f_q)$.

Soit $x \in E$. Posons $y = \sum_{i=1}^q \langle x | f_i \rangle f_i$ et $z = x - y$, alors $x = y + z$ et $y \in F$. Par ailleurs, si $1 \leq k \leq q$, par bilinéarité du produit scalaire

$$\begin{aligned} \langle z | f_k \rangle &= \langle x | f_k \rangle - \langle y | f_k \rangle \\ &= \langle x | f_k \rangle - \sum_{i=1}^q \langle x | f_i \rangle \delta_{i,k} \\ &= 0. \end{aligned}$$

Par conséquent, $z \in F^\perp$. Cela assure que $E = F \oplus F^\perp$.

Démontrons l'unicité : soit G un sev de E vérifiant $E = F \oplus G$ et $F \perp G$. Alors $G \subset F^\perp$.

Par ailleurs, soit $x \in F^\perp$. Il existe $(f, g) \in F \times G$ tel que $x = f + g$, et comme $x \in F^\perp$, $\langle x | f \rangle = 0$. Or $\langle x | f \rangle = \langle f | f \rangle + \langle g | f \rangle = \langle f | f \rangle$, donc $f = 0$ et $x \in G$.

On en déduit que $G = F^\perp$.

Enfin, F est un sev de E vérifiant $E = F^\perp \oplus F$ et $F^\perp \perp F$. Comme l'unicité ne fait pas intervenir l'hypothèse sur la dimension finie, on peut en déduire que $F = (F^\perp)^\perp$. $\square$

Remarque 2.9 (Important).

Le résultat ne se généralise pas à des sev F qui ne sont pas de dimension finie. Dans ce cas, on peut trouver des sous-espaces vectoriels F tels que F et $F^\perp$ ne soient pas supplémentaires et tels que $(F^\perp)^\perp \neq F$ (on peut même trouver F tel que $F \neq E$ et $F^\perp = \{0\}$). On verra ce résultat en exercice dans le cas de $\mathbb{R}[X]$.

Exemple 2.10.

On pose, pour tout couple (P, Q) d'éléments de $\mathbb{R}_2[X]$, $\langle P | Q \rangle = P'(1)Q'(1) + P(-1)Q(-1) + P(0)Q(0)$. Vérifier qu'il s'agit d'un produit scalaire et trouver $\mathbb{R}_1[X]^\perp$ dans $\mathbb{R}_2[X]$.

Exercice 2.11.

On considère dans $\mathbb{R}[X]$ le sev $F = \text{Vect}(1+X, 1+X^2, \dots, 1+X^n, \dots)$. On rappelle qu'un hyperplan est un sev admettant un supplémentaire de dimension 1.

On munit $\mathbb{R}[X]$ du produit scalaire

$$\left(\sum_{k=0}^{+\infty} a_k X^k, \sum_{k=0}^{+\infty} b_k X^k \right) = \sum_{k=0}^{+\infty} a_k b_k.$$

1. Montrer que F est un hyperplan de $\mathbb{R}[X]$.
2. Déterminer $F^\perp$ pour le produit scalaire usuel de $\mathbb{R}[X]$.
3. Quel résultat vrai en dimension finie est ici mis en défaut ?

2.4 Formes linéaires et hyperplans d'un espace euclidien.

Dans toute cette partie, $(E, \langle \cdot, \cdot \rangle)$ désigne un espace euclidien de dimension n .

Définition 2.1.

Soit H un hyperplan d'un espace euclidien, alors $H^\perp$ est une droite vectorielle appelée *droite normale* à H .

Tout vecteur v vérifiant $H^\perp = \text{Vect}(v)$ est appelé *vecteur normal* à H .

Proposition 2.2.

Soit H un hyperplan d'un espace euclidien E , soit $v \in E$. Alors v est un vecteur normal à H si et seulement si $v \neq 0_E$ et $v \in H^\perp$.

Démonstration.

Immédiat. $\square$

2.5 Symétries et projecteurs orthogonaux.

Définition 2.1.

Soit F sev de dimension finie d'un espace préhilbertien E . On appelle *projection orthogonale* (resp. *symétrie orthogonale*) toute projection (resp. symétrie) sur (resp. par rapport à un) F parallèlement à $F^\perp$.

Proposition 2.2.

Un projecteur p est orthogonal si et seulement si $\text{Im } p \perp \text{Ker } p$. Une symétrie s est orthogonale si et seulement si $\text{Ker}(s - \text{Id}) \perp \text{Ker}(s + \text{Id})$.

Démonstration.

Direct. $\square$

Théorème 2.3 (expression d'un projecteur orthogonal dans une base orthonormée).

Soit F sev de dimension finie d'un espace préhilbertien E . Soit $(f_1, \dots, f_p)$ une base orthonormale de F . Soit $x \in E$. Le projeté orthogonal de x sur F est $p(x) = \sum_{i=1}^p \langle x | f_i \rangle f_i$.

Démonstration.

Démontré dans 2.8 $\square$

Exemple 2.4.

Déterminer la projection orthogonale (et la symétrie orthogonale) de $(2, 1)$ sur $\text{Vect}(-1, 2)$, ainsi que sur son supplémentaire orthogonal, pour le produit scalaire

$$((x_1, y_1) | (x_2, y_2)) = 5x_1x_2 + 2y_1x_2 + 2x_1y_2 + y_1y_2.$$

Remarque 2.5.

On peut ré-écrire le procédé d'orthonormalisation de Gram-Schmidt comme suit.

Avec $F_k = \text{Vect}(e_1, \dots, e_k)$, en notant p_k le projeté de e_{k+1} sur F_k , on procède comme suit.

- On renormalise e_1 pour obtenir v_1 .
- Pour chaque $1 \leq k \leq p-1$, on remarque que $e_{k+1} - p_k \in F_k^\perp$. On renormalise donc $e_k - p_k$ pour obtenir v_{k+1} .

2.6 Distance à un sous ev.

Définition 2.1 (distance d'un point à une partie d'un espace préhilbertien).

Soit A une partie non vide de E et $x \in E$. On appelle distance de x à A et on note $d(x, A)$ le réel $\inf_{a \in A} d(x, a)$.

Théorème 2.2.

Soit F un sev de dimension finie de E . Alors la distance de x à F est atteinte en un seul point, qui est la projection orthogonale de x . De plus : $d(x, F)^2 = \|x - p(x)\|^2$. En particulier $d(x, F) = 0$ si et seulement si $x \in F$.

Démonstration.

Soit $f \in F$. On a la décomposition dans $F^\perp \oplus F$: $x - f = x - p(x) + p(x) - f$. On conclut en appliquant le théorème de Pythagore. $\square$

Exemple 2.3.

Le minimum de la fonction

$$f : \begin{cases} \mathbb{R}^2 & \rightarrow \mathbb{R} \\ (a, b) & \mapsto \int_0^1 (-a - bx + x^2)^2 dx \end{cases}$$

est atteint pour $a = -1/6$ et $b = 1$ et vaut $1/180$.

2.7 Distance et projection sur un hyperplan

Dans toute cette partie, $(E, \langle \cdot, \cdot \rangle)$ désigne un espace euclidien, H un hyperplan de E et u un vecteur normal à H .

Notamment, $H = \text{Vect}(u)^\perp$.

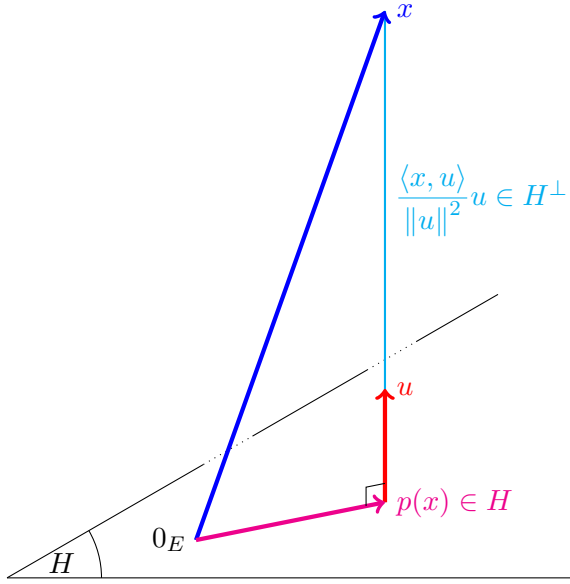
Proposition 2.1 (voir figure XXIX.1).

Soit $x \in E$, le projeté orthogonal de x sur H est

$$p(x) = x - \frac{\langle x, u \rangle}{\|u\|^2} u.$$

La distance de x à H est

$$d(x, H) = \frac{|\langle x, u \rangle|}{\|u\|}.$$


 FIGURE XXIX.1 – Projection orthogonale sur un hyperplan H .

Démonstration.

Immédiat.

□

Démonstration.

Il suffit d'observer que

$$x = x - \frac{\langle x, u \rangle}{\|u\|^2} u + \frac{\langle x, u \rangle}{\|u\|^2} u$$

et que

$$\langle x - \frac{\langle x, u \rangle}{\|u\|^2} u, u \rangle = \langle x, u \rangle - \langle x, u \rangle = 0,$$

donc que

$$x - \frac{\langle x, u \rangle}{\|u\|^2} u \in H.$$

 On peut aussi observer que $\frac{u}{\|u\|}$ est une b.o.n. de $H^\perp$,

 et donc que $\frac{\langle x, u \rangle}{\|u\|^2} u$ est le projeté orthogonal de x sur

 $\text{Vect}(u)$. Ainsi, $x - \frac{\langle x, u \rangle}{\|u\|^2} u$ est le projeté orthogonal de x sur $\text{Vect}(u)^\perp$. □

Corollaire 2.2.

 Soit $(e_1, \dots, e_n)$ une b.o.n. de E , dans laquelle on écrit

$$u = u_1 e_1 + \dots + u_n e_n,$$

$$x = x_1 e_1 + \dots + x_n e_n.$$

 Alors, la distance de x à H est

$$\frac{|x_1 u_1 + \dots + x_n u_n|}{\sqrt{u_1^2 + \dots + u_n^2}}.$$

Chapitre XXX

Fonctions de deux variables

Sommaire

1	Fonctions numériques à deux variables	470
1.1	Petite topologie du plan	470
1.2	Représentation d'une fonction de deux variables	470
1.3	Continuité	471
2	Introduction au calcul différentiel . . .	472
2.1	Dérivées partielles	472
2.2	Fonctions de classe $\mathcal{C}^1$	473
2.3	Dérivées directionnelles	474
2.4	Composition, règle de la chaîne	475
2.5	Recherche d'extrema	477

On se place dans $\mathbb{R}^2$ muni de sa norme euclidienne canonique.

1 Fonctions numériques à deux variables

1.1 Petite topologie du plan

Définition 1.1 (boules).

Soit $a \in \mathbb{R}^2$ et $r > 0$.

On appelle *boule ouverte* de centre a et de rayon r l'ensemble

$$B(a, r) = \left\{ x \in \mathbb{R}^2 \mid \|a - x\| < r \right\}.$$

On appelle *boule fermée* de centre a et de rayon r l'ensemble

$$\overline{B}(a, r) = \left\{ x \in \mathbb{R}^2 \mid \|a - x\| \leq r \right\}.$$

On appelle *sphère* de centre a et de rayon r l'ensemble

$$\overline{S}(a, r) = \left\{ x \in \mathbb{R}^2 \mid \|a - x\| = r \right\}.$$

Remarque 1.2.

La boule fermée s'obtient en ajoutant à la boule ouverte la sphère qui la délimite.

Définition 1.3 (ouverts du plan).

Une partie A du plan est dite *ouverte* si

$$\forall a \in A, \exists r > 0, B(a, r) \subset A.$$

Exemple 1.4 (exemples fondamentaux).

Sont des parties ouvertes du plan : le plan, $\emptyset$, toute boule ouverte, un produit d'intervalles ouverts.

Proposition 1.5 (voir figure XXX.1).

Soit $A \subset \mathbb{R}^2$ un ouvert, soit $(x_0, y_0) \in A$. Alors, il existe deux intervalles ouverts I et J tels que

- $x_0 \in I$;

- $y_0 \in J$;
- $I \times J \subset A$.

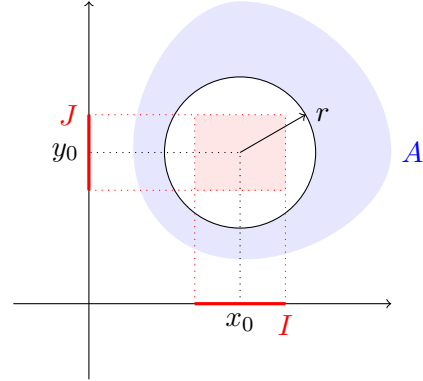


FIGURE XXX.1 – Un ouvert A , contenant un disque, contenant un rectangle.

Démonstration.

Il existe $r > 0$ tel que le $B((x_0, y_0), r) \subset A$. En posant

$$I = \left] x_0 - \frac{r}{\sqrt{2}}; x_0 + \frac{r}{\sqrt{2}} \right[$$

$$J = \left] y_0 - \frac{r}{\sqrt{2}}; y_0 + \frac{r}{\sqrt{2}} \right[$$

on vérifie aisément que $I \times J \subset B((x_0, y_0), r)$, I et J étant bien des intervalles ouverts contenant respectivement x_0 et y_0 . $\square$

1.2 Représentation d'une fonction de deux variables

Dans cette partie, on considère un ouvert A de $\mathbb{R}^2$ et une fonction $f : A \rightarrow \mathbb{R}$.

Rappel 1.2.1.

Le graphe de f est

$$\Gamma = \{ (a, f(a)) \mid a \in A \}.$$

Remarque 1.2.

Le graphe de f est formellement une partie de $\mathbb{R}^2 \times \mathbb{R}$, que l'on identifie à $\mathbb{R}^3$. On considère donc que le graphe de f est

$$\{ (x, y, f(x, y)) \mid (x, y) \in A \}.$$

Ainsi, le graphe de f se représente comme une « nappe » au dessus de la partie A , $f(x, y)$ désignant

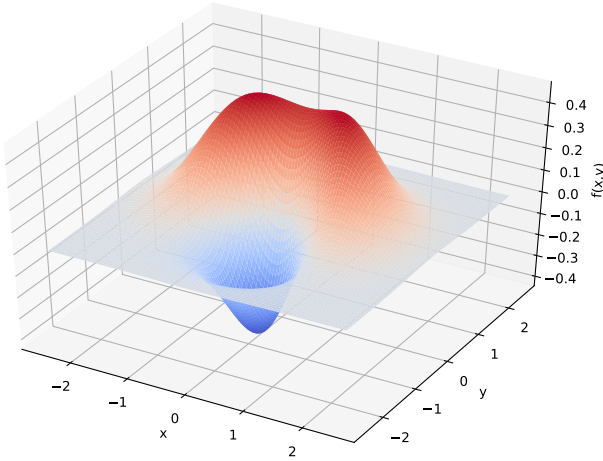


FIGURE XXX.2 – Représentation de $f : (x, y) \mapsto (x^2 + y^2)e^{-(x^2 + y^2)}$.

l'altitude du point d'abscisse x et d'ordonnée y (voir figure XXX.2).

1.3 Continuité

Dans cette partie, on considère un ouvert A de $\mathbb{R}^2$ et une fonction $f : A \rightarrow \mathbb{R}$.

Définition 1.1.

Soit $a \in A$, la fonction f est continue en a si

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in A, \|x - a\| \leq \alpha \Rightarrow |f(x) - f(a)| < \varepsilon.$$

La fonction f est continue sur A si elle est continue en tout point a de A .

Proposition 1.2 (opérations).

Soit $f, g : A \rightarrow \mathbb{R}$ deux fonctions continues sur A .

1. Si $\lambda, \mu \in \mathbb{R}$, alors $\lambda f + \mu g$ est continue sur A .
2. Les fonctions fg , $|f|$, $\min(f, g)$ et $\max(f, g)$ sont continues sur A .

Démonstration.

C'est la même chose que pour les fonctions réelles. $\square$

Proposition 1.3 (composition à gauche).

Soit $f : A \rightarrow \mathbb{R}$ une fonction continue sur A , soit $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ continue.

Alors, $\varphi \circ f$ est continue sur A .

Démonstration.

C'est la même chose que pour les fonctions réelles. $\square$

Proposition 1.4 (composition à droite).

Soit A, B deux ouverts de $\mathbb{R}^2$, Soit $f : A \rightarrow \mathbb{R}$ une fonction continue sur A , soit $u, v : B \rightarrow \mathbb{R}$ continues telles que $u(B) \times v(B) \subset A$.

Alors, $(x, y) \mapsto f(u(x, y), v(x, y))$ est continue sur B .

Démonstration.

C'est la même chose que pour les fonctions réelles. $\square$

Lemme 1.5 (continuité des projections).

Les fonctions $\pi_1 : (x, y) \mapsto x$ et $\pi_2 : (x, y) \mapsto y$ sont continues sur $\mathbb{R}^2$.

Démonstration.

Il suffit de voir que pour tout $a, b \in \mathbb{R}^2$ et pour $i \in \{1, 2\}$,

$$|\pi_i(a) - \pi_i(b)| = |\pi_i(a - b)| \leq \|a - b\|.$$

$\square$

Définition 1.6.

On appelle *fonction polynomiale de deux variables* toute fonction $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ combinaison linéaire des fonctions de la forme

$$(x, y) \mapsto x^p y^q,$$

pour $p, q \in \mathbb{N}$.

Proposition 1.7.

Toute fonction polynomiale de deux variables est continue sur $\mathbb{R}^2$.

Démonstration.

Il suffit d'utiliser le résultat du lemme 1.5, puis la stabilité de l'ensemble des fonctions continues par combinaison linéaire et produit. $\square$

Exercice 1.8.

En quels points les fonctions

$$f : (x, y) \mapsto \begin{cases} \frac{x^2 y}{x^2 + y^2} & \text{si } (x, y) \neq (0, 0) \\ 0 & \text{si } x = y = 0 \end{cases}$$

et

$$g : (x, y) \mapsto \begin{cases} \frac{xy}{x^2 + y^2} & \text{si } (x, y) \neq (0, 0) \\ 0 & \text{si } x = y = 0 \end{cases}$$

sont-elles continues ?

2 Introduction au calcul différentiel

Dans cette partie on considère U un ouvert de $\mathbb{R}^2$, et f une application de U dans $\mathbb{R}$.

2.1 Dérivées partielles

Définition 2.1.

Soit $(x_0, y_0) \in U$. Alors d'après le lemme 1.5 assure qu'il existe deux intervalles ouverts I et J tels que $x_0 \in I$, $y_0 \in J$ et $I \times J \subset U$. On considère alors les deux *fonctions partielles* de f :

- y_0 étant fixé, la première fonction partielle de f est $f_1 : I \rightarrow \mathbb{R}$, $x \mapsto f(x, y_0)$.
- x_0 étant fixé, la seconde fonction partielle de f est $f_2 : J \rightarrow \mathbb{R}$, $y \mapsto f(x_0, y)$.

Définition 2.2.

Nous gardons les notations précédentes f_1 et f_2 pour les fonctions partielles de f .

On dit que la fonction f est dérivable en un point (x_0, y_0) par rapport à sa première variable si la fonction partielle $f_1 : x \mapsto f(x, y_0)$ est dérivable en x_0 . On note alors

$$\frac{\partial f}{\partial x}(x_0, y_0) = f'_1(x_0) = \lim_{x \rightarrow x_0} \frac{f(x, y_0) - f(x_0, y_0)}{x - x_0}.$$

La fonction f est dite dérivable par rapport à sa première variable sur U si elle l'est en tout point de U .

De même, on dit que la fonction f est dérivable en un point (x_0, y_0) par rapport à sa deuxième variable si la fonction partielle $f_2 : y \mapsto f(x_0, y)$ est dérivable en y_0 . On note alors

$$\frac{\partial f}{\partial y}(x_0, y_0) = f'_2(y_0) = \lim_{y \rightarrow y_0} \frac{f(x_0, y) - f(x_0, y_0)}{y - y_0}.$$

La fonction f est dite dérivable par rapport à sa deuxième variable sur U si elle l'est en tout point de U .

Remarque 2.3.

La notation $\frac{\partial f}{\partial x}$ signifie la dérivation par rapport à la *première* variable de la fonction f , et est parfois notée $D_1 f$, ou $\partial_1 f$, *idem* pour la dérivation par rapport à la seconde variable.

Si l'on a noté une fonction $f : (u, v) \mapsto [\dots]$, on pourra bien entendu écrire $\frac{\partial f}{\partial u}$ pour signifier la dérivation par rapport à la première variable de f , *idem* pour la dérivation par rapport à la seconde variable.

On évitera absolument de considérer une fonction $f : (y, x) \mapsto [\dots]$.

On pourra aussi utiliser le symbole $\frac{\partial}{\partial \heartsuit}$ pour signifier la dérivation partielle d'une expression par rapport à la variable $\heartsuit$, toutes les autres variables étant considérées comme fixées.

Exemple 2.4.

Avec $f : (x, y) \mapsto x^2 e^{-x+y^2}$, définie sur $\mathbb{R}^2$, on a pour tout $(x, y) \in \mathbb{R}^2$:

$$\begin{aligned} \frac{\partial f}{\partial x}(x, y) &= (2x - x^2)e^{-x+y^2}, \\ \frac{\partial f}{\partial y}(x, y) &= 2x^2 y e^{-x+y^2}. \end{aligned}$$

Remarque 2.5 ().

Une fonction de deux variables peut être dérivable par rapport à chacune de ses deux variables, sans pour autant être continue.

Par exemple, la fonction définie par

$$f : (x, y) \mapsto \begin{cases} \frac{xy}{x^2 + y^2} & \text{si } (x, y) \neq (0, 0) \\ 0 & \text{si } x = y = 0 \end{cases}$$

admet des dérivées partielles en tout point de $\mathbb{R}^2$, mais n'est pas continue.

La dérivabilité par rapport à chacune des variables est élémentaire, la non continuité en 0 découle par exemple du fait que pour tout $x \in \mathbb{R}^*$,

$$f(x, x) = \frac{1}{2}.$$

Il suffit ensuite prendre x suffisamment petit pour nier la continuité de f .

2.2 Fonctions de classe $\mathcal{C}^1$

Définition 2.1.

La fonction f est dite de classe $\mathcal{C}^1$ sur U si f est dérivable par rapport à ses deux variables sur U et si les deux fonctions $\frac{\partial f}{\partial x}$ et $\frac{\partial f}{\partial y}$ sont continues sur U .

Proposition 2.2.

Toute fonction polynomiale de deux variables est de classe $\mathcal{C}^1$.

Démonstration.

Une fonction polynomiale de deux variables est dérivable par rapport à chacune de ses variables, et ses dérivées partielles sont polynomiales, donc continues. $\square$

Définition 2.3 (notation o).

Soit $f, g : U \rightarrow \mathbb{R}$, soit $a \in U$.

On dit que f est négligeable devant g au voisinage de a s'il existe une fonction $\varepsilon : U \rightarrow \mathbb{R}$ continue en a et vérifiant $\varepsilon(a) = 0$ telle que, pour tout $(x, y) \in U$,

$$f(x, y) = g(x, y)\varepsilon(x, y).$$

On note ceci

$$f(x, y) \underset{(x, y) \rightarrow a}{=} o(g(x, y)).$$

Théorème 2.4 (DL à l'ordre 1).

Soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ sur U , soit $(x_0, y_0) \in U$. Alors

$$\begin{aligned} f(x_0 + h, y_0 + k) &\underset{(h, k) \rightarrow (0, 0)}{=} f(x_0, y_0) \\ &+ h \frac{\partial f}{\partial x}(x_0, y_0) + k \frac{\partial f}{\partial y}(x_0, y_0) + o(\|(h, k)\|). \end{aligned}$$

Démonstration (hors-programme).

Pour alléger les notations, on note $a = (x_0, y_0)$.

Soit I et J deux intervalles ouverts vérifiant $I \times J \subset U$, et tels que $x_0 \in I$ et $y_0 \in J$. Il existe notamment $\alpha_0 > 0$ tel que, pour tout $u \in U$, si $\|a - u\| \leq \alpha_0$, alors $u \in I \times J$. Notons B la boule ouverte de centre 0 et de rayon α_0 .

On définit $\varepsilon : B \rightarrow \mathbb{R}$ par $\varepsilon(0, 0) = 0$ et si $(h, k) \neq (0, 0)$:

$$\varepsilon(h, k) = \frac{1}{\|(h, k)\|} \left(f(a + (h, k)) - f(a) - h \frac{\partial f}{\partial x}(a) - k \frac{\partial f}{\partial y}(a) \right)$$

Montrons que la fonction ε est continue en $(0, 0)$. Considérons $\eta > 0$.

Pour $u = (h, k)$ suffisamment petit, on a

$$\begin{aligned} \Delta &= \left| f(a + u) - f(a) - h \frac{\partial f}{\partial x}(a) - k \frac{\partial f}{\partial y}(a) \right| \\ &= \left| f(x_0 + h, y_0 + k) - f(x_0, y_0 + k) - h \frac{\partial f}{\partial x}(a) \right. \\ &\quad \left. + f(x_0, y_0 + k) - f(x_0, y_0) - k \frac{\partial f}{\partial y}(a) \right| \\ &\leq \underbrace{\left| f(x_0 + h, y_0 + k) - f(x_0, y_0 + k) - h \frac{\partial f}{\partial x}(a) \right|}_{\Delta_1} \\ &\quad + \underbrace{\left| f(x_0, y_0 + k) - f(x_0, y_0) - k \frac{\partial f}{\partial y}(a) \right|}_{\Delta_2} \end{aligned}$$

Comme $f(\cdot, y_0 + k)$ est dérivable sur I , par le théorème des accroissements finis, il existe t_1 entre x_0 et $x_0 + h$ vérifiant

$$f(x_0 + h, y_0 + k) - f(x_0, y_0 + k) = h \frac{\partial f}{\partial x}(t_1, y_0 + k).$$

On a donc

$$\Delta_1 = |h| \left| \frac{\partial f}{\partial x}(t_1, y_0 + k) - \frac{\partial f}{\partial x}(x_0, y_0) \right|.$$

Comme $\frac{\partial f}{\partial x}$ est continue en $a = (x_0, y_0)$, il existe $\alpha_1 > 0$ tel que pour tout $(h, k) \in \mathbb{R}^2$, si $\|(h, k)\| \leq \alpha_1$, alors

$$\left| \frac{\partial f}{\partial x}(t_1, y_0 + k) - \frac{\partial f}{\partial x}(x_0, y_0) \right| \leq \eta,$$

ce qui donne $|\Delta_1| \leq \eta \|(h, k)\|$.

On procède de même pour Δ_2 , et il existe donc $\alpha_2 > 0$ tel que pour tout $(h, k) \in \mathbb{R}^2$, si $\|(h, k)\| \leq \alpha_2$, alors $|\Delta_1| \leq \eta \|(h, k)\|$.

Ainsi, pour tout $(h, k) \in \mathbb{R}^2$, si $\|(h, k)\| \leq \min(\alpha_0, \alpha_1, \alpha_2)$, alors $|\varepsilon(h, k)| \leq 2\eta$, ce qui est bien le résultat demandé. $\square$

Remarque 2.5 (plan tangent).

Sous les mêmes hypothèses,

$$z - f(x_0, y_0) = (x - x_0) \frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0) \frac{\partial f}{\partial y}(x_0, y_0)$$

est l'équation d'un plan, appelé *plan tangent* au graphe de f en (x_0, y_0) .

Corollaire 2.6.

Si $f : U \rightarrow \mathbb{R}$ est de classe $\mathcal{C}^1$, alors f est continue.

Définition 2.7 (gradient).

Soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ sur U , soit $(x_0, y_0) \in U$. On définit le *gradient* de f en (x_0, y_0) comme le vecteur

$$\nabla f(x_0, y_0) = \left(\frac{\partial f}{\partial x}(x_0, y_0), \frac{\partial f}{\partial y}(x_0, y_0) \right).$$

Remarque 2.8.

Le théorème 2.4 s'écrit alors ainsi, avec $a = (x_0, y_0)$:

$$f(a + u) \underset{u \rightarrow (0,0)}{=} f(a) + \langle \nabla f(a), u \rangle + o(\|u\|).$$

Exemple 2.9.

Le champ de vecteur de l'exemple du début du chapitre est tracé dans la figure XXX.3.

2.3 Dérivées directionnelles

Définition 2.1 (dérivée selon un vecteur).

Soit $a \in U$, soit $v \in \mathbb{R}^2 \setminus \{(0, 0)\}$, soit $f : U \rightarrow \mathbb{R}$. La fonction f est dite *dérivable selon le vecteur v en a* si la fonction $t \mapsto f(a + tv)$ est dérivable en 0.

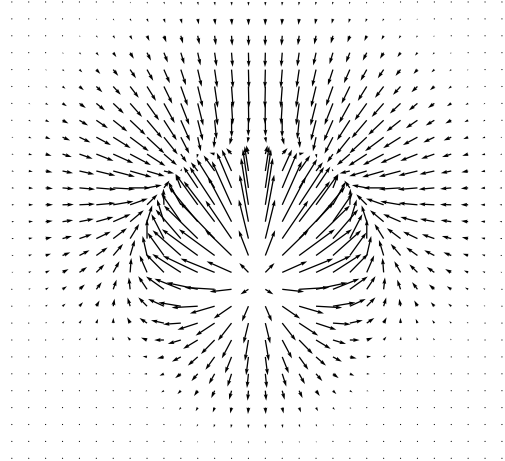


FIGURE XXX.3 – Champ de vecteurs de ∇f , pour $f : (x, y) \mapsto (x^2 + y)e^{-(x^2 + y^2)}$.

La dérivée de cette fonction en 0 est alors appelée *dérivée* de f selon v en a , et est notée $D_v f(a)$:

$$D_v f(a) = \lim_{t \rightarrow 0} \frac{f(a + tv) - f(a)}{t}.$$

Remarque 2.2.

En notant (e_1, e_2) la base canonique de $\mathbb{R}^2$, on a sous réserve d'existence :

$$\frac{\partial f}{\partial x}(a) = D_{e_1} f(a), \text{ et } \frac{\partial f}{\partial y}(a) = D_{e_2} f(a).$$

Remarque 2.3.

Si $\|v\| = 1$, $D_v f(a)$ est la pente de la droite tangente au graphe de f en a et dirigée par v .

Théorème 2.4.

Si f est de classe $\mathcal{C}^1$ sur U et si $a \in U$, alors f admet des dérivées selon tous les vecteurs en a , et pour tout $v \in \mathbb{R}^2 \setminus (0, 0)$:

$$D_v f(a) = \langle \nabla f(a), v \rangle.$$

Remarque 2.5.

On a donc pour tout $(h, k) \in \mathbb{R}^2$ non nuls :

$$D_{(h,k)} f(a) = h \frac{\partial f}{\partial x}(a) + k \frac{\partial f}{\partial y}(a).$$

Démonstration.

Notons $v = (h, k)$ et $a = (x_0, y_0)$. Soit $t \neq 0$. Soit $\alpha > 0$ tel que la boule ouverte de centre a et de rayon α soit incluse dans U . Notons alors B la boule ouverte de centre 0 et de rayon α .

Par le théorème de développement limité à l'ordre 1 de f , qui est de classe $\mathcal{C}^1$, il existe donc une fonction ε définie sur B , continue en $(0, 0)$ et vérifiant $\varepsilon(0, 0) = 0$ telle que, pour tout réel t tel que $tv \in B$,

$$f(a + tv) = f(a) + th \frac{\partial f}{\partial x}(a) + tk \frac{\partial f}{\partial y}(a) + |t| \|v\| \varepsilon(tv),$$

dont on peut déduire

$$f(a + tv) \underset{t \rightarrow 0}{=} f(a) + th \frac{\partial f}{\partial x}(a) + tk \frac{\partial f}{\partial y}(a) + o(t).$$

Ainsi, $t \mapsto f(a + tv)$ admet un DL à l'ordre 1 en 0, donc est dérivable en 0, et immédiatement

$$D_v f(a) = h \frac{\partial f}{\partial x}(a) + k \frac{\partial f}{\partial y}(a).$$

□

Remarque 2.6.

Par l'inégalité de Cauchy-Schwarz, $\nabla f(a)$ est la direction selon laquelle f croît/décroît le plus vite, c'est-à-dire la direction de la pente la plus forte.

2.4 Composition, règle de la chaîne

Théorème 2.1 (règle de la chaîne).

Soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$, soit I un intervalle ouvert de $\mathbb{R}$ et $x, y : I \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ telles que $x(I) \times y(I) \subset U$.

Alors, $t \mapsto f(x(t), y(t))$ est de classe $\mathcal{C}^1$ sur I et pour tout $t \in I$

$$\frac{d}{dt}(f(x(t), y(t))) = x'(t) \frac{\partial f}{\partial x}(x(t), y(t)) + y'(t) \frac{\partial f}{\partial y}(x(t), y(t)).$$

Démonstration.

Soit $t_0 \in I$. Notons $a = (x(t_0), y(t_0))$. Pour $t \in I$, on note aussi $\gamma(t) = (x(t), y(t))$.

Comme f est de classe $\mathcal{C}^1$, on peut appliquer le théorème de développement limité à l'ordre 1. Il existe donc une fonction ε continue en 0, vérifiant $\varepsilon(0, 0) = 0$ et telle que pour tout $u = (h, k)$ tel que $a + u \in U$:

$$f(a + u) = f(a) + h \frac{\partial f}{\partial x}(a) + k \frac{\partial f}{\partial y}(a) + \|u\| \varepsilon(u).$$

On a donc pour $t \in I$:

$$f(\gamma(t)) = f(a) + (x(t) - x(t_0)) \frac{\partial f}{\partial x}(a) + (y(t) - y(t_0)) \frac{\partial f}{\partial y}(a) + \|\gamma(t) - a\| \varepsilon(\gamma(t) - a).$$

Comme x et y sont dérivables, on peut écrire leurs développements limités à l'ordre 1. Il existe donc deux fonctions ε_1 et ε_2 de limite nulle en t_0 telles que, pour tout $t \in I$,

$$\begin{aligned} x(t) - x(t_0) &= (t - t_0)x'(t_0) + (t - t_0)\varepsilon_1(t), \\ y(t) - y(t_0) &= (t - t_0)y'(t_0) + (t - t_0)\varepsilon_2(t). \end{aligned}$$

On a donc

$$f(\gamma(t)) = f(a) + (t - t_0) \left(x'(t_0) \frac{\partial f}{\partial x}(a) + y'(t_0) \frac{\partial f}{\partial y}(a) \right) + R(t),$$

$$\text{où } R(t) = (t - t_0) \left(\varepsilon_1(t) \frac{\partial f}{\partial x}(a) + \varepsilon_2(t) \frac{\partial f}{\partial y}(a) \right) + \|\gamma(t) - a\| \varepsilon(\gamma(t) - a).$$

Il suffit de montrer que $R(t) = o(t - t_0)$. Comme ε_1 et ε_2 tendent vers 0 en t_0 , on peut écrire que

$$\varepsilon_1(t) \frac{\partial f}{\partial x}(a) + \varepsilon_2(t) \frac{\partial f}{\partial y}(a) = o(1).$$

De plus, comme x et y sont dérivables en t_0 , par composition

$$\left\| \frac{\gamma(t) - \gamma(t_0)}{t - t_0} \right\| \underset{t \rightarrow t_0}{\rightarrow} \|(x'(t_0), y'(t_0))\| \text{ et donc,}$$

$$\begin{aligned} \|\gamma(t) - a\| &= |t - t_0| \left\| \frac{\gamma(t) - \gamma(t_0)}{t - t_0} \right\| \\ &= |t - t_0| \times O(1) \\ &= O(t - t_0) \end{aligned}$$

Par composition, on a $\varepsilon(\gamma(t) - a) = o(1)$, ce qui permet de conclure. □

Remarque 2.2.

Sous les mêmes hypothèses, notons $\gamma : t \mapsto (x(t), y(t))$. Cette fonction γ est appelée *arc de classe $\mathcal{C}^1$* . La règle de la chaîne donne la dérivée de f suivant l'arc γ , et peut s'écrire comme suit :

$$(f \circ \gamma)'(t) = \langle \nabla f(\gamma(t)), \gamma'(t) \rangle.$$

Définition 2.3.

Soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$. Si $z \in \mathbb{R}$, on appelle *ligne de niveau de f d'altitude z* la partie

$$\{a \in \mathbb{R}^2 \mid f(a) = z\}.$$

Exemple 2.4.

On a tracé dans la figure XXX.4 les lignes de niveau correspondant à la fonction tracée dans la figure XXX.2.

Exemple 2.5.

Vous trouverez dans la figure XXX.5 un exemple

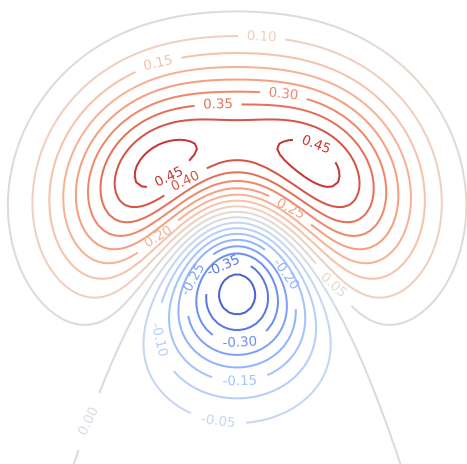


FIGURE XXX.4 – Lignes de niveau de $f : (x, y) \mapsto (x^2 + y)e^{-(x^2 + y^2)}$.

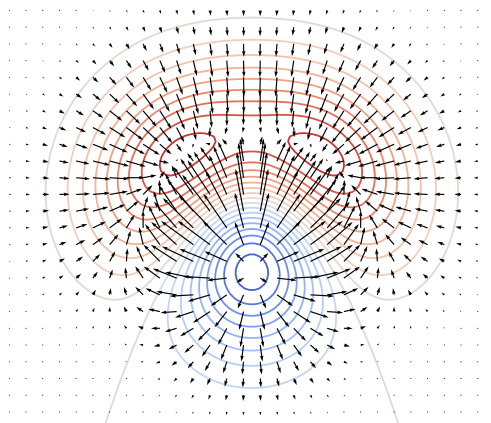


FIGURE XXX.6 – Champ de vecteurs de ∇f , et lignes de niveau de f .

de carte IGN, faisant figurer les lignes de niveau du terrain. Avec un peu d'habitude, on arrive très bien à se représenter le terrain !

Remarque 2.6.

La ligne de niveau d'altitude z est donc $f^{-1}(\{z\})$.

Proposition 2.7.

Soit $f : U \rightarrow \mathbb{R}$, soit $\gamma : I \rightarrow U$ un arc de classe $\mathcal{C}^1$ tel que $\gamma(I)$ est inclus dans une ligne de niveau de f .

Alors, pour tout $t \in I$, $\nabla f(\gamma(t))$ est orthogonal à $\gamma'(t)$.

Démonstration.

Immédiat, étant donné que pour tout $t \in I : (f \circ \gamma)'(t) = 0$. $\square$

Remarque 2.8.

La propriété précédente est souvent résumée sous la locution « le gradient de f est orthogonal aux lignes de niveau de f ». En effet, $\gamma'(t)$ dirige la droite tangente à l'arc γ au point $\gamma(t)$ (voir Figure XXX.6).

En vertu de la remarque 2.6, la direction de plus forte pente est donc orthogonale aux lignes de niveau.

Le théorème des fonctions implicites (hors programme) permet de montrer que, sous certaines hypothèses, les lignes de niveau d'une fonction forment des arcs de classe $\mathcal{C}^1$.



FIGURE XXX.5 – Exemple de carte IGN (source : géoportail).

Théorème 2.9.

Soit U, V deux ouverts de $\mathbb{R}^2$, soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$, soit $\varphi, \psi : V \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ telles que $\varphi(V) \times \psi(V) \subset U$.

Soit

$$g : \begin{cases} V & \longrightarrow \mathbb{R} \\ (u, v) & \longmapsto f(\varphi(u, v), \psi(u, v)) \end{cases}.$$

Alors, g est de classe $\mathcal{C}^1$ sur V et pour tout $(u, v) \in V$:

$$\begin{aligned} \frac{\partial g}{\partial u}(u, v) &= \frac{\partial f}{\partial x}(\varphi(u, v), \psi(u, v)) \frac{\partial \varphi}{\partial u}(u, v) \\ &\quad + \frac{\partial f}{\partial y}(\varphi(u, v), \psi(u, v)) \frac{\partial \psi}{\partial u}(u, v) \end{aligned}$$

$$\begin{aligned} \frac{\partial g}{\partial v}(u, v) &= \frac{\partial f}{\partial x}(\varphi(u, v), \psi(u, v)) \frac{\partial \varphi}{\partial v}(u, v) \\ &\quad + \frac{\partial f}{\partial y}(\varphi(u, v), \psi(u, v)) \frac{\partial \psi}{\partial v}(u, v) \end{aligned}$$

Remarque 2.10 (à la physicienne).

Les formules précédentes sont quelque peu difficiles à retenir. En notant x la fonction φ et y la fonction ψ , en notant $t = (u, v)$ et $a(t) = (x(t), y(t))$, on a alors

$$\frac{\partial(f \circ a)}{\partial u}(t) = \frac{\partial f}{\partial x}(a(t)) \frac{\partial x}{\partial u}(t) + \frac{\partial f}{\partial y}(a(t)) \frac{\partial y}{\partial u}(t),$$

ce que l'on peut (abusivement) écrire

$$\frac{\partial(f \circ a)}{\partial u} = \frac{\partial f}{\partial x} \frac{\partial x}{\partial u} + \frac{\partial f}{\partial y} \frac{\partial y}{\partial u}.$$

2.5 Recherche d'extrema

Définition 2.1 (extremum global).

Soit $a \in U$.

1. On dit que a est le lieu d'un *maximum global* de f si $\forall u \in U, f(u) \leq f(a)$.
2. On dit que a est le lieu d'un *minimum global* de f si $\forall u \in U, f(u) \geq f(a)$.

3. On dit que a est le lieu d'un *extremum global* de f si c'est le lieu d'un minimum ou d'un maximum global de f .

Remarque 2.2.

On dit aussi que f admet un maximum global en a (*idem* pour minimum et extremum).

Définition 2.3 (extremum local).

Soit $a \in U$.

1. On dit que a est le lieu d'un *maximum local* de f s'il existe $r > 0$ tel que

$$\forall u \in U, \|a - u\| \leq r \Rightarrow f(u) \leq f(a).$$

2. On dit que a est le lieu d'un *minimum local* de f s'il existe $r > 0$ tel que

$$\forall u \in U, \|a - u\| \leq r \Rightarrow f(u) \geq f(a).$$

3. On dit que a est le lieu d'un *extremum local* de f si c'est le lieu d'un minimum ou d'un maximum local de f .

Remarque 2.4.

On dit aussi que f admet un maximum local en a (*idem* pour minimum et extremum).

Remarque 2.5.

Tout extremum global est aussi un extremum local, la réciproque étant bien évidemment fausse.

Définition 2.6 (point critique).

Soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$, un *point critique* de f est un point $a \in U$ vérifiant

$$\nabla f(a) = (0, 0).$$

Théorème 2.7 (condition du premier ordre).

Soit $U \subset \mathbb{R}^2$ un ouvert, soit $f : U \rightarrow \mathbb{R}$ de classe $\mathcal{C}^1$, soit $a \in U$.

Si f admet un extremum local en a , alors a est un point critique de f .

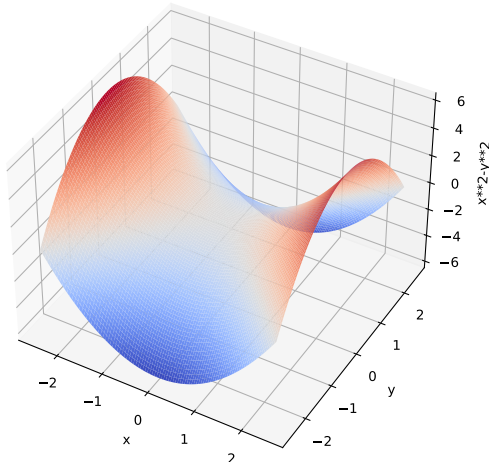


FIGURE XXX.7 – Représentation d'un point selle.

Démonstration.

Notons $a = (x_0, y_0)$. Les deux fonctions partielles de f en a admettent chacune un extremum local en x_0/y_0 , intérieur à leur ensemble de définition. Elles y admettent donc chacune un point critique, donc les dérivées partielles de f sont nulles en a , d'où le résultat. $\square$

Remarque 2.8.

Il est ici primordial que U soit un ouvert.

Ce théorème ne donne qu'une condition *nécessaire* pour qu'un point soit un extremum local (et *a fortiori* global) d'une fonction.

Cette condition n'est pas suffisante, comme on le peut le voir sur la figure XXX.7.

Exercice 2.9.

Soit $a \in \mathbb{R}_+^*$. On pose $f : (x, y) \mapsto x + y - (x^2 + y^2 + ay)$ et $D = \{(x, y) \in]0, 1[^2, x + y < 1\}$.

1. Représenter D dans le plan.
2. Discuter l'existence d'extrema locaux de f sur D en fonction de la valeur de a .