المملكة المغربية
وزارة التربية الوطنية
والتعليم الأولي والرياضة
المركز الجهوي لمهن التربية والتكوين
الرباط-سلا-القنيطرة

Exercices corrigés

Complément de formation

Logique, Ensembles et Arithmétique

Auteur : Nouira Redouane

Année scolaire 2024 - 2025

Module :
Complément de formation
Logique, Ensembles et Arithmétique

Exercices corrigés

Nouira Redouane

CRMEF de la région de Rabat-Salé-Kénitra,
Annexe de Kénitra

Année scolaire 2024-2025

Avant-propos

Ce polycopié constitue un recueil d'exercices destiné aux professeurs stagiaires du cycle qualifiant au Maroc. S'inscrivant dans le cadre du module « Complément de formation - Logique, ensembles et Arithmétique », il est conçu dans le but de fournir un support pédagogique complet et adapté pour renforcer les compétences nécessaires à l'enseignement, conformément aux programmes officiels.

Les exercices présentés couvrent les quatre thématiques fondamentales de ce module :

— *Logique et ensembles :* Cette partie explore les principes de base de la logique mathématique, les opérations sur les ensembles et leurs propriétés, permettant de structurer des raisonnements rigoureux.

— *Arithmétique des entiers :* Elle inclut des exercices sur la divisibilité, les nombres premiers, les congruences et les algorithmes fondamentaux comme celui d'Euclide.

— *Arithmétique des polynômes :* Comme pour l'arithmétique des entiers, nombreux types d'exercices sont proposés allant de la divisibilité jusqu'à la décomposition en facteurs irréductibles. Une importance particulière est accordée aux racines d'un polynôme, ainsi qu'à l'étude de certains polynômes classiques.

— *Fractions rationnelles :* Cette section est l'occasion de présenter les différentes techniques de la décomposition d'une fraction rationnelle en élément simple, ainsi que ses applications, montrant ainsi la puissance de l'usage de ces décompositions. Aussi, outre les exercices d'ordre calculatoire, d'autres d'ordre théorique sont largement représentées.

Chaque chapitre est conçu pour offrir une progression pédagogique claire, allant des exercices de base, destinés à consolider les notions essentielles, jusqu'à des problèmes plus complexes favorisant l'approfondissement et le développement des capacités d'analyse et de synthèse. Les solutions fournies permettent de guider les stagiaires dans leur apprentissage autonome.

Ce recueil se veut à la fois un outil de formation et une référence pratique pour les futurs enseignants. En s'exerçant sur ces différents thèmes, ils pourront non seulement maîtriser les concepts et techniques fondamentaux de l'algèbre, mais aussi développer des stratégies pédagogiques efficaces pour transmettre ces savoirs à leurs élèves.

Nous espérons que ce polycopié répondra aux attentes des utilisateurs et contribuera à la réussite de leur parcours professionnel.

Nouira Redouane

Table des matières

Chapitre 1

Élements de logique

1.1 Connecteurs logiques, négation d'une proposition

Exercice 1

Donner la valeur de vérité de chacune des propositions suivantes

1. $0 = 0$ et $2 + 1 = 8$
2. $0 = 0$ ou $2 + 1 = 8$
3. $0 = 0 \Longrightarrow 2 + 1 = 8$
4. $0 = 1 \Longrightarrow 2 + 1 = 8$
5. « $0 = 0 \Longrightarrow 2 + 1 = 3$ »
6. $\forall x \in \mathbb{R}, (x \geq 0 \Longrightarrow 2 = 4)$
7. $(\forall x \in \mathbb{R}, x \geq 0) \Longrightarrow 2 = 4$

Réponse 1

1. « $0 = 0$ et $2 + 1 = 8$ » est fausse ; car la proposition « $2 + 1 = 8$ » est fausse.
2. « $0 = 0$ ou $2 + 1 = 8$ » est vraie ; car la proposition « $0 = 0$ » est vraie.
3. « $0 = 0 \Longrightarrow 2 + 1 = 8$ » est fausse ; car la proposition « $0 = 0$ » est vraie et la proposition « $2 + 1 = 8$ » est fausse.
4. « $0 = 1 \Longrightarrow 2 + 1 = 8$ » est vraie ; car la proposition « $0 = 1$ » est fausse.
5. « $0 = 0 \Longrightarrow 2 + 1 = 3$ » est vraie ; car la proposition « $2 + 1 = 3$ » est vraie.
6. « $\forall x \in \mathbb{R}, (x \geq 0 \Longrightarrow 2 = 4)$ » est fausse ; car pour $x = 1$ on a $x \geq 0$ mais $2 \neq 4$.
7. « $(\forall x \in \mathbb{R}, x \geq 0) \Longrightarrow 2 = 4$ » est vraie ; car la proposition « $(\forall x \in \mathbb{R}, x \geq 0)$ » fausse, puisque pour $x = -1$ on a $x < 0$

Exercice 2

1. Déterminer les valeurs de vérité ainsi que les négations des assertions suivantes :
   - P « $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R}, \quad x + y > 0$ ».
   - Q « $\forall y \in \mathbb{R},\ \exists x \in \mathbb{R}, \quad x + y > 0$ ».
   - R « $\exists x \in \mathbb{R}\ /\ \forall y \in \mathbb{R}, \quad y^2 > x$ ».
2. Étant donné deux ensembles non vides E et F, et une fonction propositionnelle $P(x, y)$ de variables $x \in E$ et $y \in F$, montrer que si la proposition « $\exists x \in E\ /\ \forall y \in F,\ P(x, y)$ » est vraie, alors la proposition « $\forall y \in F\ /\ \exists x \in E,\ P(x, y)$ » l'est aussi.

Réponse 2

1. — P est fausse ; car pour tout $x \in \mathbb{R}$, il existe $y = -x \in \mathbb{R}$ tel que $x + y = 0 \not> 0$.
   Sa négation est :
   $\neg P$ « $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\quad x + y \leq 0$ ».
   — Q est vraie ; car pour tout $y \in \mathbb{R}$, il existe $x = -y + 1 \in \mathbb{R}$ tel que $x + y = 1 > 0$.
   Sa négation est :
   $\neg Q$ « $\exists y \in \mathbb{R},\ \forall x \in \mathbb{R},\quad x + y \leq 0$ ».
   — R est vraie ; car pour $x = -1$, pour tout $y \in \mathbb{R}$ on a $y^2 > x$.
   Sa négation est :
   $\neg R$ « $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\quad y^2 \leq x$ ».
2. Supposons qu'il existe un $x_0 \in E$ tel que pour tout $y \in F$ on a $P(x_0, y)$ est vraie. Donc, pour tout $y \in F$, il existe un $x \in E$ (on peut prendre $x = x_0$ par exemple) tel que $P(x, y)$ soit vraie. D'où le résultat.

Exercice 3

Soit f, g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Traduire en termes de quantificateurs les expressions suivantes :

1. f est majorée ;
2. f est bornée ;
3. f est paire ;
4. f est impaire ;
5. f ne s'annule jamais ;
6. f n'est pas la fonction nulle ;
7. f est périodique ;
8. f est croissante ;
9. f est strictement décroissante ;
10. f n'a jamais les mêmes valeurs en deux points distincts ;
11. f atteint toutes les valeurs de $\mathbb{N}$;
12. f est inférieure à g ;
13. f n'est pas inférieure à g.

Réponse 3

1. $\exists M \in \mathbb{R}\ :\ \forall x \in \mathbb{R},\ f(x) \leq M$
2. $\exists m \in \mathbb{R},\ \exists M \in \mathbb{R}\ :\ \forall x \in \mathbb{R},\ m \leq f(x) \leq M$
3. $\forall x \in \mathbb{R},\ f(-x) = f(x)$
4. $\forall x \in \mathbb{R},\ f(-x) = -f(x)$
5. $\forall x \in \mathbb{R},\ f(x) \neq 0$
6. $\exists x \in \mathbb{R},\ f(x) \neq 0$
7. $\exists T \in \mathbb{R}_+^*\ :\ \forall x \in \mathbb{R},\ f(x + T) = f(x)$
8. $\forall (x, y) \in \mathbb{R}^2,\ x \leq y \Longrightarrow f(x) \leq f(y)$
9. $\forall (x, y) \in \mathbb{R}^2,\ x < y \Longrightarrow f(x) < f(y)$
10. $\forall (x, y) \in \mathbb{R}^2,\ x \neq y \Longrightarrow f(x) \neq f(y)$
11. $\forall n \in \mathbb{N},\ \exists x \in \mathbb{R}\ :\ f(x) = n$
12. $\forall x \in \mathbb{R}\ :\ f(x) \leq g(x)$
13. $\exists x \in \mathbb{R}\ :\ f(x) > g(x)$

Exercice 4

Nier les assertions suivantes :

1. tout triangle rectangle possède un angle droit ;
2. dans toutes les écuries, tous les chevaux sont noirs ;
3. $\forall \varepsilon > 0\ \exists \alpha > 0\ \ /\ \ |x - 7/5| < \alpha \Longrightarrow |5x - 7| < \varepsilon$.
4. pour tout entier x, il existe un entier y tel que, pour tout entier z, la relation $z < x$ implique le relation $z < x + 1 < y$;

Réponse 4

1. Il existe au moins un triangle rectangle qui ne possède aucun angle droit ;
2. Il y a une écuries qui contient un cheval qui n'est pas noir ;
3. $\exists \varepsilon > 0\ :\ \forall \alpha > 0,\ |x - 7/5| < \alpha$ et $|5x - 7| \geq \varepsilon$.
4. Il existe un entier x tel que pour tout entier y, il existe un entier z tel que $z \geq x + 1$ ou $x + 1 \geq y$;

Exercice 5

Soit f une application de $\mathbb{R}$ dans $\mathbb{R}$. Nier, de la manière la plus précise possible, les énoncés qui suivent :

1. Pour tout $x \in \mathbb{R}\ f(x) \leq 1$.
2. L'application f est croissante.
3. L'application f est croissante et positive.
4. Il existe $x \in \mathbb{R}^+$ tel que $f(x) \leq 0$.
5. Il existe $x \in \mathbb{R}$ tel que quel que soit $y \in \mathbb{R}$, si $x < y$ alors $f(x) > f(y)$.

On ne demande pas de démontrer quoi que ce soit, juste d'écrire le contraire d'un énoncé.

Réponse 5

1. Il existe un $x \in \mathbb{R}$ tel que $f(x)) > 1$.
2. Il existe $(x, y) \in \mathbb{R}^2$ tels que $x \leq y$ et $f(x) > f(y)$.
3. Il existe $\in \mathbb{R}$ tels que $f(x) < 0$, ou il existe $(x, y) \in \mathbb{R}^2$ tels que $x \leq y$ et $f(x) > f(y)$
4. Pour tout $x \in \mathbb{R}^+,\ f(x) > 0$.
5. Pour tout $x \in \mathbb{R}$, il existe $y \in \mathbb{R}$ tel que $x < y$ et $f(x) \leq f(y)$.

Exercice 6

Compléter les pointillés par le connecteur logique qui s'impose : $\Longleftrightarrow$, $\Longleftarrow$, $\Longrightarrow$.

1. $\forall x \in \mathbb{R},\ x^2 = 4 \cdots\cdots\ x = 2$;
2. $\forall x \in \mathbb{R}+,\ x^2 = 4 \cdots\cdots\ x = 2$;
3. $\forall z \in \mathbb{C},\ z = \overline{z} \cdots\cdots\ z \in \mathbb{R}$;
4. $\forall x \in \mathbb{R},\ \forall n \in \mathbb{Z},\ x = 4n\pi \cdots\cdots e^{ix} = 1$.

Réponse 6

1. $\forall x \in \mathbb{R},\ x^2 = 4 \Longleftarrow x = 2$;
2. $\forall x \in \mathbb{R}+,\ x^2 = 4 \Longleftrightarrow x = 2$;
3. $\forall z \in \mathbb{C},\ z = \overline{z} \Longleftrightarrow z \in \mathbb{R}$;
4. $\forall x \in \mathbb{R},\ \forall n \in \mathbb{Z},\ x = 4n\pi \Rightarrow e^{ix} = 1$.

1.2 Modes de raisonnements

Exercice 7

1. Démontrer que la somme d'une suite convergente et d'une suite divergente, est une suite divergente.
2. Que dire de la somme de deux suites divergentes ?

Réponse 7

1. Soit (u_n) une suite convergente et (v_n) une suite divergente. Supposons que $(u_n + v_n)$ est convergente. Dans ce cas, la suite $((u_n + v_n) - u_n)$ est convergente comme somme de deux suites convergentes $(u_n + v_n)$ et $-u_n$. Or $(u_n + v_n) - u_n) = v_n$, ce qui est contradictoire. Ainsi, la somme d'une suite convergente et d'une suite divergente est une suite divergente.
2. Dans ce cas on ne pas conclure. En effet, les suites $(u_n), (v_n)$ et (w_n), définies par $u_n = w_n = n$ et $v_n = -n$ sont divergentes, la suite $(u_n + v_n)$ est convergente, mais $(u_n + w_n)$ est divergente.

Exercice 8

1. Démontrer que la somme d'un nombre rationnel et un nombre irrationnel est un nombre irrationnel.
2. le produit d'un rationnel non nul par un irrationnel est un nombre irrationnel.
3. l'inverse d'un nombre irrationnel est irrationnel.
4. Que dire de la somme de deux irrationnels ?

Réponse 8

Soit r un nombre rationnel et i un nombre réel irrationnel. Posons $s = r + i$, $p = r \times i$ et $y = \dfrac{1}{i}$.

1. Supposons que s est un nombre rationnel. Dans ce cas, $i = s - r$ est aussi rationnel, puisque c'est la somme de deux nombres rationnels, ce qui est faux. Donc, la somme d'un nombre rationnel et un nombre irrationnel est un nombre irrationnel.
2. On suppose ici que $r \neq 0$. Si p est un nombre rationnel alors $i = \dfrac{p}{r}$ est aussi rationnel, car c'est le produit de deux nombres rationnels, ce qui est faux. Donc, le produit d'un nombre rationnel non nul et un nombre irrationnel est un nombre irrationnel.
3. Même raisonnement. Si y est un nombre rationnel alors $x = \dfrac{1}{y}$ le sera aussi. Ainsi, l'inverse d'un nombre irrationnel est irrationnel.
4. On sait que $\sqrt{2}$ est irrationnel. Donc, d'après ce qui précède, $2\sqrt{2}$ et $-\sqrt{2}$ le sont aussi. D'autre part, $\sqrt{2} + \sqrt{2} = 2\sqrt{2}$ et $\sqrt{2} - \sqrt{2} = 0$, ce qui montre que la somme de deux irrationnels pourra être rationnel comme il pourra être irrationnel.

Exercice 9

Montrer qu'il existe une infinité de nombres premiers.

Réponse 9

Supposons que l'ensemble $\mathcal{P}$ des nombres premiers est fini. Donc $\mathcal{P}$ s'écrit sous la forme $\mathcal{P} =$

$\{p_1, p_2, \cdots, p_r\}$. Posant $N = p_1 p_2 \cdots p_r + 1$. Il est clair alors que $N \geq 2$, et par conséquent N admet un diviseur premier, donc un certain p_i avec $1 \leq i \leq r$. Comme p_i divise déjà $p_1 p_2 \cdots p_r$, alors il divise aussi $N - p_1 p_2 \cdots p_r$, qui n'est autre que 1. Absurde, car $p_i \geq 2$.
Conclusion, il existe une infinité de nombres premiers.

Exercice 10

Soit $(f_n)_{n\in\mathbb{N}}$ une suite d'applications de l'ensemble $\mathbb{N}$ dans lui-même. On définit une application f de $\mathbb{N}$ dans $\mathbb{N}$ en posant $f(n) = f_n(n) + 1$. Démontrer qu'il n'existe aucun $p \in \mathbb{N}$ tel que $f = f_p$.

Réponse 10

Supposons qu'il existe un certain $p \in \mathbb{N}$ tel que $f = f_p$. Dans ce cas, $f(p) = f_p(p)$. Or, par définition de f, on a $f(p) = f_p(p) + 1$, donc $f_p(p) = f_p(p) + 1$ puis $0 = 1$. Ceci étant faux, on conclut qu'il n'existe aucun $p \in \mathbb{N}$ tel que $f = f_p$.

Exercice 11

Montrer que

$$\forall \varepsilon > 0, \quad \exists N \in \mathbb{N} \ / \ (\forall n \in \mathbb{N}, \quad n \geq N \Longrightarrow 3 - \varepsilon < \frac{3n+2}{n+2} < 3 + \varepsilon.$$

Réponse 11

Soit $\varepsilon > 0$. Commençons d'abord par trouver une expression simple équivalente à l'expression $3 - \varepsilon < \frac{3n+2}{n+2} < 3 + \varepsilon$ pour tout $n \in \mathbb{N}$. En effet, pour tout $n \in \mathbb{N}$ on a :

$$\begin{array}{rcl} 3 - \varepsilon < \frac{3n+2}{n+2} < 3 + \varepsilon & \iff & 3 - \varepsilon < \frac{3(n+2)-4}{n+2} < 3 + \varepsilon \\ & \iff & 3 - \varepsilon < 3 - \frac{4}{n+2} < 3 + \varepsilon \\ & \iff & -\varepsilon < -\frac{4}{n+2} < \varepsilon \\ & \iff & \frac{4}{n+2} < \varepsilon \\ & \iff & \frac{4}{\varepsilon} < n + 2 \end{array}$$

Prenons alors $N = \mathrm{E}\left(\frac{4}{\varepsilon}\right)$; la partie entière de $\frac{4}{\varepsilon}$. Dans ce cas, pour tout $n \in \mathbb{N}$, si $n \geq N = \mathrm{E}\left(\frac{4}{\varepsilon}\right)$, alors $\frac{4}{\varepsilon} < n + 2$ et par conséquent $3 - \varepsilon < \frac{3n+2}{n+2} < 3 + \varepsilon$.
Conclusion : $\forall \varepsilon > 0, \quad \exists N \in \mathbb{N} \ / \ (\forall n \in \mathbb{N}, \quad n \geq N \Longrightarrow 3 - \varepsilon < \frac{3n+2}{n+2} < 3 + \varepsilon$.

Exercice 12 *Raisonnement par analyse et synthèse*

Montrer que toute application de $\mathbb{R}$ vers lui même s'écrit, de manière unique, comme somme de deux applications, l'une paire et l'autre impaire.

Réponse 12

Soit f une application de $\mathbb{R}$ vers lui même. Supposons qu'il existe une fonction paire g et une fonction impaire h de $\mathbb{R}$ vers $\mathbb{R}$ telles que $f = g + h$. Dans ce cas, pour tout $x \in \mathbb{R}$ on a

$$f = g + h \Longrightarrow \begin{cases} f(x) = g(x) + h(x) & (1) \\ f(-x) = g(x) - h(x) & (2) \end{cases}$$

$$\Longrightarrow \begin{cases} f(x) + f(-x) = 2g(x) & (1) + (2) \\ f(x) - f(-x) = 2h(x) & (1) - (2) \end{cases}$$

$$\Longrightarrow \begin{cases} g(x) = \dfrac{1}{2}\left(f(x) + f(-x)\right) \\ \\ h(x) = \dfrac{1}{2}\left(f(x) - f(-x)\right) \end{cases}$$

Ainsi, en cas d'existence, g et h sont uniques. Pour l'existence, posons

$$\begin{cases} g(x) = \dfrac{1}{2}\left(f(x) + f(-x)\right) \\ \\ h(x) = \dfrac{1}{2}\left(f(x) - f(-x)\right) \end{cases}$$

pour tout $x \in \mathbb{R}$. On vérifie facilement que pour tout $x \in \mathbb{R}$ on a

$$\begin{cases} g(-x) = \dfrac{1}{2}\left(f(-x) + f(+x)\right) = g(x) \\ \\ h(-x) = \dfrac{1}{2}\left(f(-x) - f(x)\right) = -h(x) \\ \\ g(x) + h(x) = f(x) \end{cases}$$

i.e. g est paire, h est impaire et $f = g + h$, d'où le résultat ?

Exercice 13

Montrer que : $\sqrt{30} \notin \mathbb{Q} \Longrightarrow \sqrt{2} + \sqrt{3} + \sqrt{5} \notin \mathbb{Q}$

Réponse 13

On montre le résultat par contraposée. Supposons que $\sqrt{2} + \sqrt{3} + \sqrt{5} \in \mathbb{Q}$. Dans ce cas on a $\left(\sqrt{2} + \sqrt{3} + \sqrt{5}\right)^2 \in \mathbb{Q}$. Comme

$$\left(\sqrt{2} + \sqrt{3} + \sqrt{5}\right)^2 = 10 + 2\left(\sqrt{2.3} + \sqrt{3.5} + \sqrt{2.5}\right)$$

alors $\sqrt{2.3} + \sqrt{3.5} + \sqrt{2.5} \in \mathbb{Q}$. En répétant la même technique on trouve que $\sqrt{2.30} + \sqrt{3.30} + \sqrt{5.30} \in \mathbb{Q}$. En divisant par $\sqrt{2} + \sqrt{3} + \sqrt{5}$ qui est un rationnel, on trouve que $\sqrt{30} \in \mathbb{Q}$.

Exercice 14

Montrer que pour tout entier $n \geq 1$ on a :

1. $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$
2. $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
3. $1^3 + 2^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$
4. $1.2 + 2.3 + \cdots + n.n + 1 = \dfrac{n(n+1)(n+2)}{3}$
5. $\dfrac{1}{1.3} + \dfrac{1}{3.5} + \cdots + \dfrac{1}{(2n-1).(2n+1)} = \dfrac{n}{2n+1}$
6. $\dfrac{1}{1.2} + \dfrac{1}{2.3} + \cdots + \dfrac{1}{n.(n+1)} = 1 - \dfrac{1}{n+1}$
7. $1.(1!) + 2.(2!) + \cdots + n.(n!) = (n+1)! - 1$

Réponse 14

1. — Pour $n = 1$ le résultat est évident : $1 = \dfrac{1(1+1)}{2}$.

   — Supposons que, pour un certain $n \geq 1$ on a $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$. Dans ce cas on a

$$\begin{aligned} 1 + 2 + \cdots + (n+1) &= 1 + 2 + \cdots + n + (n+1) \\ &= (\frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

   Le résultat est donc vrai pour $n + 1$.

   Donc : $\forall n \geq 1, \quad 1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

2. Soit, pour tout $n \in \mathbb{N}^*$, $\mathcal{A}_n$ l'assertion suivante :

$$(\mathcal{A}_n) \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

   — $\mathcal{A}_1$ est vraie ($1 = \dfrac{1(1+1)}{2}$).

   — Étant donné $n \in \mathbb{N}^*$ supposons que $\mathcal{A}_n$ soit vraie. Alors

$$\begin{aligned} \sum_{k=1}^{n+1} k^2 &= (n+1)^2 + \sum_{k=1}^{n} k^2 \\ &= (n+1)^2 + \frac{n(n+1)(2n+1)}{6} \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(n+2)(2(n+1)+1)}{6} \end{aligned}$$

   Ce qui prouve $\mathcal{A}_{n+1}$ est vrai.

   Conclusion : Par le principe de récurrence, $\mathcal{A}_n$ est vraie pour tout $n \in \mathbb{N}^*$.

3. — Pour $n = 1$ on a bien $1^3 = \left(\dfrac{1(1+1)}{2}\right)^2$

   — Supposons que $1^3 + 2^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$ pour un certain $n \geq 1$. Alors

$$\begin{aligned} 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\ &= (n+1)^2 \left(\frac{n^2}{4} + n + 1\right) \\ &= \frac{(n+1)^2(n^2+4n+4)}{4} \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 \end{aligned}$$

Conclusion : $\forall n \geq 1, \quad 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

4. Posons $A_n = 1.2 + 2.3 + \cdots + n.n + 1$ pour tout $n \in \mathbb{N}$.
   — Pour $n = 1$ on a bien $1.2 = \frac{1(1+1)(1+2)}{3}$
   — Supposons que $A_n = \frac{n(n+1)(n+2)}{3}$ pour un certain $n \geq 1$. Alors

$$\begin{aligned} A_{n+1} &= 1.2 + 2.3 + \cdots + n.n + 1 + (n+1)(n+2) \\ &= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\ &= (n+1)(n+2)\left(\frac{n}{3} + 1\right) \\ &= \frac{(n+1)(n+2)(n+3)}{3} \end{aligned}$$

   Conclusion : $\forall n \geq 1, \quad 1.2 + 2.3 + \cdots + n.n + 1 = \frac{n(n+1)(n+2)}{3}$.

5. Posons $A_n = \frac{1}{1.3} + \frac{1}{3.5} + \cdots + \frac{1}{(2n-1).(2n+1)}$ pour tout $n \geq 1$.
   — Pour $n = 1$ on a bien $\frac{1}{1.3} = \frac{1}{2+1}$
   — Supposons que $A_n = \frac{n}{2n+1}$ pour un certain $n \geq 1$. Alors

$$\begin{aligned} A_{n+1} &= \frac{1}{1.3} + \frac{1}{3.5} + \cdots + \frac{1}{(2n-1)(2n+1)} + \frac{1}{(2n+1)(2n+3)} \\ &= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \\ &= \frac{1}{2n+1}\left(n + \frac{1}{2n+3}\right) \\ &= \frac{2n^2+3n+1}{(2n+1)(2n+3)} \\ &= \frac{(2n+1)(n+1)}{(2n+1)(2n+3)} \\ &= \frac{n+1}{2n+3} \end{aligned}$$

   Conclusion : $\forall n \geq 1, \quad \frac{1}{1.3} + \frac{1}{3.5} + \cdots + \frac{1}{(2n-1).(2n+1)} = \frac{n}{2n+1}$.

6. Posons $A_n = \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n.(n+1)}$ pour tout $n \geq 1$.
   — Pour $n = 1$ on a bien $\frac{1}{1.2} = \frac{1}{1.(1+1)}$

— Supposons que $A_n = 1 - \dfrac{1}{n+1}$ pour un certain $n \geq 1$. Alors

$$\begin{aligned} A_{n+1} &= \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n.(n+1)} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= 1 - \frac{1}{n+1}\left(1 - \frac{1}{n+2}\right) \\ &= 1 - \frac{1}{n+1}.\frac{n+1}{n+2} \\ &= 1 - \frac{1}{n+2} \end{aligned}$$

Conclusion : $\forall n \geq 1, \quad \dfrac{1}{1.2} + \dfrac{1}{2.3} + \cdots + \dfrac{1}{n.(n+1)} = 1 - \dfrac{1}{n+1}$.

7. Posons $A_n = 1.(1!) + 2.(2!) + \cdots + n.(n!)$ pour tout $n \geq 1$.
   — Pour $n = 1$ on a bien $1.(1!) = (2+1)! - 1$
   — Supposons que $A_n = (n+1)! - 1$ pour un certain $n \geq 1$. Alors

$$\begin{aligned} A_{n+1} &= 1.(1!) + 2.(2!) + \cdots + n.(n!) + (n+1)\left((n+1)!\right) \\ &= (n+1)! - 1 + (n+1)\left((n+1)!\right) \\ &= (n+1)!\,(1 + n + 1) - 1 \\ &= (n+2)! - 1 \end{aligned}$$

Ainsi : $\forall n \geq 1, \quad 1.(1!) + 2.(2!) + \cdots + n.(n!) = (n+1)! - 1$.

Exercice 15

Montrer que pour tout $n \in \mathbb{N}$ on a :

1. $7^n - 1$ est divisible par 6.
2. $3^{2n+1} + 2^{n+2}$ est divisible par 7.
3. $2^{2n} + 15n - 1$ est divisible par 9.

Réponse 15

1. — Pour $n = 0$ le résultat est vrai.
   — Supposons qu'il l'est pour un certain $n \in \mathbb{N}$. Il existe alors un $k \in \mathbb{N}$ tel que $7^n - 1 = 6k$. Ainsi,

$$\begin{aligned} 7^{n+1} - 1 &= 7.7^n - 1 \\ &= (6+1).7^n - 1 \\ &= 6.7^n + (7^n - 1) \\ &= 6.7^n + 6k \\ &= 6(7^n + k) \end{aligned}$$

   Donc $7^{n+1} - 1$ est divisible par 6.

   Conclusion : Pour tout $n \in \mathbb{N}$, $7^n - 1$ est divisible par 6.

2. — Pour $n = 0$ le résultat est vrai.

— Supposons qu'il l'est pour un certain $n \in \mathbb{N}$. Il existe alors un $k \in \mathbb{N}$ tel que $3^{2n+1} + 2^{n+2} = 7k$. Ainsi,

$$\begin{aligned} 3^{2n+3} + 2^{n+3} &= 9.3^{2n+1} + 2.2^{n+2} \\ &= 7.3^{2n+1} + 2.3^{2n+1} + 2.2^{n+2} \\ &= 7.3^{2n+1} + 2\left(3^{2n+1} + 2^{n+2}\right) \\ &= 7.3^{2n+1} + 2.7.k \\ &= 7\left(3^{2n+1} + 2k\right). \end{aligned}$$

Donc, pour tout $n \in \mathbb{N}$, $2^{2n} + 15n - 1$ $3^{2n+3} + 2^{n+3}$ est divisible par 7.

Conclusion : Pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

3. $2^{2n} + 15n - 1$ est divisible par 9.
   — Pour $n = 0$ le résultat est vrai ; car 0 es divisible par 9.
   — Soit $n \in \mathbb{N}$ et supposons que $2^{2n} + 15n - 1$ est divisible par 9. Il existe alors un $k \in \mathbb{N}$ tel que $2^{2n} + 15n - 1 = 9k$. Ainsi,

$$\begin{aligned} 2^{2(n+1)} + 15(n+1) - 1 &= 4.2^{2n} + 15n + 14 \\ &= 4(2^{2n} + 15n - 1) - 45n + 18 \\ &= 4.9k - 45n + 18 \\ &= 9(4k - 5n + 2) \end{aligned}$$

Donc $2^{2(n+1)} + 15(n+1) - 1$ est divisible par 9.

Conclusion : Pour tout $n \in \mathbb{N}$, $2^{2n} + 15n - 1$ est divisible par 9.

Exercice 16

Montrer que le produit de n entiers consécutifs de $\mathbb{N}$ est divisible par $n!$, où $n \in \mathbb{N}^*$.

Réponse 16

Il s'agit de montrer que le nombre $A_{k,n} = k(k+1)\cdots(k+n-1)$ est divisible par $n!$, pour tout $k \in \mathbb{N}$, et tout $n \in \mathbb{N}^*$, avec bien entendu $A_{k,1} = k$. Montrons ce résultat par récurrence sur n.

— Pour $n = 1$ le résultat est évident ; pour tout $k \in \mathbb{N}$, $A_{k,1} = k$ est divisible par $1! = 1$.

— Soit $n \in \mathbb{N}^*$ et supposons que $A_{k,n}$ est divisible par $n!$ pour tout $k \in \mathbb{N}$. Montrons alors que $A_{k,n+1}$ est divisible par $(n+1)!$ pour tout $k \in \mathbb{N}$.
   — Pour $k = 0$ on a $A_{0,n+1} = 0$, donc divisible par $n(n+1)!$.
   — Soit $k \in \mathbb{N}$ et supposons que $A_{k,n+1}$ est divisible par $(n+1)!$. Donc donc $A_{k,n+1}$ et $A_{k+1,n}$ sont de la forme $A_{k,n+1} = (n+1)!d$ et $A_{k+1,n} = n!d'$ avec $d, d' \in \mathbb{N}$. Il suffit de montrer que $A_{k+1,n+1}$ est divisible par $(n+1)!$. En effet, ,

$$\begin{aligned} A_{k+1,n+1} &= (k+1)(k+2)\cdots(k+1+n) \\ &= (k+1)(k+2)\cdots(k+n)(k+1+n) \\ &= k(k+1)(k+2)\cdots(k+n) + \\ &\quad (1+n)(k+1)(k+2)\cdots(k+n) \\ &= A_{k,n+1} + (n+1)A_{k+1,n} \\ &= (n+1)!d + n!d'(n+1) \\ &= (n+1)!d + (n+1)!d' \\ &= (n+1)!(d+d') \end{aligned}$$

Donc $A_{k+1,n+1}$ est bien divisible par $(n+1)!$.

En conclusion : le produit de n entiers consécutifs de $\mathbb{N}$ est divisible par $n!$ pour tout $n \in \mathbb{N}^*$.

Exercice 17

Montrer que pour tout entier $n \geq 1$ on a :

1. $\forall a > 0, \quad (1+a)^n \geq 1 + na.$
2. $n! \leq \left(\dfrac{n+1}{2}\right)^n$. on pourra utiliser la question précédente 1.
3. $1 + \dfrac{1}{2^2} + \cdots + \dfrac{1}{n^2} \geq \dfrac{3n}{2n+1}.$
4. $2^n \leq 2^{n+1} - 2^{n-1} - 1$
5. $(1 - \dfrac{1}{2})(1 - \dfrac{1}{4})(1 - \dfrac{1}{8}) \cdots (1 - \dfrac{1}{2^n}) \geq \dfrac{1}{4} + \dfrac{1}{2^{n+1}}$
6. $1 + \dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{4} + \cdots + \dfrac{1}{2^n} \geq 1 + \dfrac{n}{2}$
7. $1!2! \cdots (2n+1)! \geq ((n+1)!)^{n+1}.$

Réponse 17

1. Soit $a > 0$.
   - Pour $n = 1$ le résultat est bien vérifié ; $(1+a)^0 = 1 + 0.a = 1$.
   - Soit $n \geq 1$ et supposons que $(1+a)^n \geq 1+na$. On a alors
   $$\begin{aligned}(1+a)^{n+1} &= (1+a)(1+a)^n \\ &\geq (1+a)(1+na) \\ &= 1 + na + a + na^2 \\ &\geq 1 + a + na \\ &\geq 1 + (n+1)a\end{aligned}$$

   Ainsi : $\forall a > 0, \quad (1+a)^n \geq 1 + na.$
2. - Pour $n = 1$ le résultat est vrai.
   - Soit $n \geq 1$. supposons que $n! \leq \left(\dfrac{n+1}{2}\right)^n$ et montrons que $(n+1)! \leq \left(\dfrac{n+2}{2}\right)^{n+1}$.

   On a
   $$\begin{aligned}(n+1)! &= n!(n+1) \\ &\leq \left(\frac{n+1}{2}\right)^n (n+1) \\ &= \frac{(n+1)^{n+1}}{2^n}\end{aligned}$$

   On est ramené à montrer que $\dfrac{(n+1)^{n+1}}{2^n} \leq \left(\dfrac{n+2}{2}\right)^{n+1}$. Or,

   $$\begin{aligned}\frac{(n+1)^{n+1}}{2^n} \leq \left(\frac{n+2}{2}\right)^{n+1} &\Leftrightarrow 2 \leq \left(\frac{n+2}{n+1}\right)^{n+1} \\ &\Leftrightarrow 2 \leq \left(1 + \frac{1}{n+1}\right)^{n+1}\end{aligned}$$

   Ce qui est vrai d'après la question précédente 1 en prenant $a = \dfrac{1}{n+1}$.

   D'où : $\forall n \geq 1, \quad n! \leq \left(\dfrac{n+1}{2}\right)^n$.
3. - Pour $n = 1$ le résultat est bien vérifié puisque $1 = \dfrac{3}{2.1+1}$.

— Soit $n \geq 1$. Supposons que $1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \geq \frac{3n}{2n+1}$ et montrons que $1 + \frac{1}{2^2} + \cdots + \frac{1}{(n+1)^2} \geq \frac{3n+3}{2n+3}$. On a :

$$\begin{aligned} 1 + \frac{1}{2^2} + \cdots + \frac{1}{(n+1)^2} &= 1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \\ &\geq \frac{3n}{2n+1} + \frac{1}{(n+1)^2} \end{aligned}$$

Or,

$$\begin{aligned} \frac{3n}{2n+1} + \frac{1}{(n+1)^2} \geq \frac{3n+3}{2n+3} &\Leftrightarrow \frac{1}{(n+1)^2} \geq \frac{3n+3}{2n+3} - \frac{3n}{2n+1} \\ &\Leftrightarrow \frac{1}{(n+1)^2} \geq \frac{3}{(2n+3)(2n+1)} \\ &\Leftrightarrow (2n+3)(2n+1) \geq 3(n+1)^2 \\ &\Leftrightarrow 4n^2 + 5n + 3 \geq 3n^2 + 6n + 3 \\ &\Leftrightarrow n^2 \geq n \\ &\Leftrightarrow n \geq 1 \end{aligned}$$

Ce qui est vrai. Donc $1 + \frac{1}{2^2} + \cdots + \frac{1}{(n+1)^2} \geq \frac{3n+3}{2n+3}$.

D'où, pour tout $n \geq 1$ on a $1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \geq \frac{3n}{2n+1}$.

4. — Pour $n = 1$ le résultat est vrai ; $2^1 = 2^{1+1} - 2^{1-1} - 1 = 2$.
   — Soit $n \geq 1$ et supposons que $2^n \leq 2^{n+1} - 2^{n-1} - 1$. Montrons alors que $2^{n+1} \leq 2^{n+2} - 2^n - 1$. On a

$$\begin{aligned} 2^{n+1} &= 2.2^n \\ &\leq 2\left(2^{n+1} - 2^{n-1} - 1\right) \\ &= 2^{n+2} - 2^n - 2 \\ &= 2^{n+2} - 2^n - 1 \end{aligned}$$

D'où : $\forall n \geq 1, \quad 2^n \leq 2^{n+1} - 2^{n-1} - 1$.

5. Posons $A_n = (1 - \frac{1}{2})(1 - \frac{1}{4})(1 - \frac{1}{8}) \cdots (1 - \frac{1}{2^n})$ pour tout $n \geq 1$.
   — Pour $n = 1$ le résultat est vrai ; en effet $A_1 = 1 - \frac{1}{2} = \frac{1}{4} + \frac{1}{2^{1+1}} = \frac{1}{2}$.
   — Supposons que $A_n \geq \frac{1}{4} + \frac{1}{2^{n+1}}$ pour un certain $n \geq 1$ et montrons que $A_{n+1} \geq \frac{1}{4} + \frac{1}{2^{n+2}}$. On a

$$\begin{aligned} A_{n+1} &= A_n(1 - \frac{1}{2^{n+1}}) \\ &\geq \left(\frac{1}{4} + \frac{1}{2^{n+1}}\right)(1 - \frac{1}{2^{n+1}}) \text{ ; car } 1 - \frac{1}{2^{n+1}} \geq 0 \\ &= \frac{1}{4} + \frac{1}{2^{n+1}} - \frac{1}{2^{n+3}} - \frac{1}{2^{2n+2}} \\ &= \frac{1}{4} + \frac{1}{2^{n+2}} - \frac{1}{2^{n+2}} + \frac{1}{2^{n+1}} - \frac{1}{2^{n+3}} - \frac{1}{2^{2n+2}} \\ &= \frac{1}{4} + \frac{1}{2^{n+2}} + \frac{1}{2^{n+2}} - \frac{1}{2^{n+3}} - \frac{1}{2^{2n+2}} \end{aligned}$$

Il suffit donc de montrer que $\frac{1}{2^{n+2}} - \frac{1}{2^{n+3}} - \frac{1}{2^{2n+2}} \geq 0$. En effet

$$\begin{aligned} \frac{1}{2^{n+2}} - \frac{1}{2^{n+3}} - \frac{1}{2^{2n+2}} \geq 0 &\Leftrightarrow 2^n - 2^{n-1} - 1 \geq 0 \\ &\Leftrightarrow 2^{n-1}(2-1) - 1 \geq 0 \\ &\Leftrightarrow 2^{n-1} - 1 \geq 0 \\ &\Leftrightarrow 2^{n-1} \geq 1 \end{aligned}$$

ce qui est vrai. Donc, $A_{n+1} \geq \frac{1}{4} + \frac{1}{2^{n+2}}$.

D'où : $\forall n \geq 1, \quad A_n \geq \frac{1}{4} + \frac{1}{2^{n+1}}$.

6. Posons $A_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n}$ pour tout $n \geq 1$
   - — Pour $n = 1$ le résultat est évident.
   - — Supposons que $A_n \geq 1 + \frac{n}{2}$ pour un certain $n \geq 1$ et montrons que $A_{n+1} \geq 1 + \frac{n+1}{2}$. On a

$$\begin{aligned} A_{n+1} &= A_n + \frac{1}{1+2^n} + \cdots + \frac{1}{2^{n+1}} \\ &\geq 1 + \frac{n}{2} + \frac{1}{1+2^n} + \frac{1}{2+2^n} + \cdots + \frac{1}{2^{n+1}} \\ &\geq 1 + \frac{n+1}{2} - \frac{1}{2} + \frac{1}{1+2^n} + \cdots + \frac{1}{2^{n+1}} \end{aligned}$$

   Il suffit donc de montrer que $-\frac{1}{2} + \frac{1}{1+2^n} + \cdots + \frac{1}{2^{n+1}} \geq 0$, ou encore que $\frac{1}{1+2^n} + \cdots + \frac{1}{2^{n+1}} \geq \frac{1}{2}$. En effet

$$\begin{cases} \frac{1}{1+2^n} & \geq \frac{1}{2^{n+1}} \\ \frac{1}{2+2^n} & \geq \frac{1}{2^{n+1}} \\ \vdots & \\ \frac{1}{2^{n+1}} & \geq \frac{1}{2^{n+1}} \end{cases}$$

   d'où, $\frac{1}{1+2^n} + \cdots + \frac{1}{2^{n+1}} \geq 2^n . \frac{1}{2^{n+1}} = \frac{1}{2}$ et par suite $A_{n+1} q \geq 1 + \frac{n+1}{2}$.

   Conclusion : $\forall n \geq 1, \quad 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$.

7. Posons $A_n = 1!2! \cdots (2n+1)!$ pour tout $n \geq 1$.
   - — Pour $n = 1$ le résultat est évident ; $1!2!3! = 6 \geq ((1+1)!)^{1+1} = 4$.
   - — Supposons que $A_n \geq ((n+1)!)^{n+1}$ pour un certain $n \geq 1$ et montrons que $A_{n+1} \geq ((n+2)!)^{n+2}$. On a

$$\begin{aligned} A_{n+1} &= A_n . (2n+2)!(2n+3)! \\ &\geq ((n+1)!)^{n+1} . (2n+2)!(2n+3)! \end{aligned}$$

   On est ramené alors à montrer que

$$B_n \geq ((n+2)!)^{n+2}; \text{ où } B_n = ((n+1)!)^{n+1} . (2n+2)!(2n+3)!.$$

   Comme $((n+2)!)^{n+2} = ((n+2)!)^{n+1}((n+2)!)$ alors,

$$\begin{aligned} B_n \geq ((n+2)!)^{n+2} &\Leftrightarrow (2n+2)!(2n+3)! \geq (n+2)^{n+1} . (n+2)! \\ &\Leftrightarrow (2n+2)! \frac{(2n+3)!}{(n+2)!} \geq (n+2)^{n+1} \end{aligned}$$

Or, $\dfrac{(2n+3)!}{(n+2)!} = (n+3)(n+4)\cdots(2n+3)$, et

$$\begin{cases} n+3 & \geq n+2 \\ n+4 & \geq n+2 \\ & \vdots \\ 2n+3 & \geq n+2 \end{cases}$$

donc

$$(n+3)(n+4)\cdots(2n+3) \geq (n+2)^{n+1}$$

et par suite

$$(2n+2)!\frac{(2n+3)!}{(n+2)!} \geq (2n+2)!(n+2)^{n+1} \geq (n+2)^{n+1}.$$

Ainsi $B_{n+1} \geq ((n+2)!)^{n+2}$.

Conclusion : $\forall n \geq 1, \quad 1!2!\cdots(2n+1)! \geq ((n+1)!)^{n+1}$.

Exercice 18

Soit la suite $(x_n)_{n\geq 1}$ définie par : $x_1 = 1$ et $x_{k+1} = \dfrac{x_k}{x_k+2}$. Montrer que

$$\forall n \geq 1, \quad x_n = \frac{1}{2^n - 1}.$$

Réponse 18

Le résultat étant évident pour $n = 1$, supposons qu'il l'est pour un certain $n \geq 1$ et montrons qu'il l'est pour $n+1$. En effet,

$$\begin{aligned} x_{n+1} &= \frac{x_n}{x_n+2} \\ &= \frac{x_n(2^n-1)}{(x_n+2)(2^n-1)} \\ &= \frac{1)}{2^{n+2}-1)} \end{aligned}$$

Le résultat est donc bien vérifié pour $n+1$. En conclusion, $\forall n \geq 1, \quad x_n = \dfrac{1}{2^n-1}$.

Exercice 19

Considérons la suite réelle $(u_n)_{n\geq 0}$ définie par $u_0 = 2,\ u_1 = 3$ et pour $u_{n+2} = 3u_{n+1} - 2u_n$ tout $n \in \mathbb{N}$. Montrer que

$$\forall n \in \mathbb{N},\ u_n = 2^n + 1.$$

Réponse 19

On a bien $u_0 = 2^0 + 1 = 2$ et $u_1 = 2^1 + 1 = 3$. Supposons que pour un $n \in \mathbb{N}$ on a $u_n = 2^n + 1$ et $u_{n+} = 2^{n+1} + 1$, et montrons que $u_{n+2} = 2^{n+2} + 1$. Effectivement,

$$\begin{aligned} u_{n+2} &= 3u_{n+1} - 2u_n \\ & 3(2^{n+1}+1) - 2(2^n+1) \\ & 3.2^{n+1} + 3 - 2^{n+1} - 2 \\ & 2.2^{n+1} + 1 \\ & = 2^{n+2} + 1 \end{aligned}$$

Conclusion : $\forall n \in \mathbb{N},\ u_n = 2^n + 1$.

Exercice 20

Donner une expression simple de

$$S_n = \sum_{p=0}^{n} \frac{1}{p^2 + 3p + 2}$$

Réponse 20

— On a $S_0 = \frac{1}{2}$, $S_1 = \frac{2}{3}$, $S_2 = \frac{3}{4}$ et $S_3 = \frac{4}{5}$. Remarquons que, pour ces premières valeurs, S_n est de la forme $S_n = \frac{n+1}{n+2}$. Supposons donc que, un certain $n \in \mathbb{N}$, on a bien $S_n = \frac{n+1}{n+2}$. Dans ce cas,

$$\begin{aligned} S_{n+1} &= S_n + \frac{1}{(n+1)^2 + 3(n+1) + 2} \\ &= \frac{n+1}{n+2} + \frac{1}{n^2 + 5n + 6} \\ &= \frac{n+1}{n+2} + \frac{1}{(n+2)(n+3)} \\ &= \frac{(n+1)(n+3)+1}{(n+2)(n+3)} \\ &= \frac{n^2 + 4n + 4}{(n+2)(n+3)} \\ &= \frac{n+2}{n+3} \end{aligned}$$

Finalement, pour tout $n \in \mathbb{N}$ on a $S_n = \frac{n+1}{n+2}$.

Exercice 21

soit $(u_n)_n$ une suite réelle telle que

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N},\ u_{n+1} = (1 + \frac{1}{n+1})u_n \end{cases}$$

Donner l'expression général de u_n.

Réponse 21

On a $u_0 = 1$, $u_1 = 2$ et $u_2 = 3$. Supposons que pour un $n \geq 0$ on a $u_n = n + 1$. Dans ce cas on a

$$u_{n+1} = (1 + \frac{1}{n+1})u_n = (1 + \frac{1}{n+1})(n+1) = n + 2$$

Ainsi, $\forall n \in \mathbb{N},\ u_n = n + 1$

Exercice 22

On considère la fonction f (dite d'Ackermann) définie sur $\mathbb{N}^2$ par :

$$\begin{cases} \forall n \geq 0, \quad f(0,n) = n+1, \\ \forall m \geq 1, \quad f(m,0) = f(m-1,1), \\ \forall m,n \geq 1, \quad f(m,n) = f(m-1, f(m,n-1)), \end{cases}$$

Montrer que pour tout $n \in \mathbb{N}$ on a :

$$f(1,k) = k+2, \quad f(2,k) = 2k+3 \text{ et } f(3,k) = 2^{k+3} - 3.$$

Réponse 22

Montrons chacune de ces identités par récurrence sur k.

— Pour $k = 0$ on a $f(1,0) = f(0,1) = 2 = 0+2$. Supposons que pour un certain $k \in \mathbb{N}$ on a $f(1,k) = k+2$. Dans ce cas on aura $f(1,k+1) = f(0, f(1,k)) = f(0,k+2) = k+3$. On peut conclure donc que :

$$\forall k \in \mathbb{N}, \quad f(1,k) = k+2.$$

— Pour $k = 0$ on a $f(2,0) = f(1,1) = 1+2 = 2.0+3$. Supposons que pour un certain $k \in \mathbb{N}$ on a $f(2,k) = 2k+3$. Dans ce cas on aura $f(2,k+1) = f(1, f(2,k)) = f(1, 2k+3) = 2k+5+2(k+1)+3$. Ainsi :

$$\forall k \in \mathbb{N}, \quad f(2,k) = 2k+3.$$

— Pour $k = 0$ on a $f(3,0) = f(2,1) = 2.1+3 = 2^{0+3}-3$. Supposons que pour un certain $k \in \mathbb{N}$ on a $f(3,k) = 2^{k+3} - 3$. Dans ce cas on aura $f(3,k+1) = f(2, f(3,k)) = f(2, 2^{k+3}-3) = 2(2^{k+3}-3)+3 = 2^{(k+1)+3} - 3$. Ainsi :

$$\forall k \in \mathbb{N}, \quad f(3,k) = 2^{k+3} - 3.$$

Exercice 23

1. Montrer que $\forall n \in \mathbb{N}, \quad (n+4)^2 - (n+3)^2 - (n+2)^2 + (n+1)^2 = 4$
2. En déduire que tout entier m peut s'écrire comme somme et différence des carrés $1^2, 2^2, 3^2, \cdots, n^2$ pour un certain n.

Réponse 23

1. Car pour pour tout $n \in \mathbb{N}$ on a

$$(n+4)^2 - (n+3)^2 = 2n+7 \text{ et } (n+2)^2 + (n+1)^2 = 2n+3$$

2. On a déjà

$$\begin{aligned} 1 &= 1^2, \\ 3 &= 2^2 - 1^2, \\ 2 &= 1^2 - 2^2 + 3^2 - 4 = 1^2 - 2^2 + 3^2 - 4^1 - 5^2 - 6^2 + 7^2 \end{aligned}$$

Ainsi le résultat est vrai pour $1, 2, 3$ et 4. Soit $m \in \mathbb{N}^*$. La division Euclidienne de m par 4 s'écrit : $m = 4n + r$ avec $0 \leq r \leq 3$. Donc, d'après 2, r s'écrit sous la forme

$$r = \sum_{i=1}^{k} \varepsilon_i . i$$

où $\varepsilon_i = \pm 1$ et $k = 1, 2$ ou 7. Il suffit de montrer que $4n$ s'écrit sou la forme :

$$4n = \sum_{i=k+1}^{l} \varepsilon_i i$$

où $l \in \mathbb{N}^*$ et $\varepsilon_i = \pm 1$. D'après la première question, ce résultat est vrais si $n = 1$. Supposons qu'il l'est pour un certain $n \in \mathbb{N}^*$. Dans ce cas

$$\begin{aligned} 4(n+1) &= 4n + 4 \\ &= 4 + \sum_{i=k+1}^{l} \varepsilon_i i \\ &= (l+4)^2 - (l+3)^2 - (l+2)^2 + (l+1)^2 + \sum_{i=k+1}^{l} \varepsilon_i i \\ &= \sum_{i=k+1}^{l+4} \varepsilon_i i \end{aligned}$$

d'où le résultat.

Exercice 24

On se propose d'établir par deux méthodes que

$$\forall n \in \mathbb{N}^* \ \exists! (p, q) \in \mathbb{N}^2; \ \ n = 2^p(2q+1)$$

Pour cela, pour tout $n \in \mathbb{N}^*$ fixé on pose

$$A_n = \{m \in \mathbb{N} \ / \ 2^m \text{ divise } n\}.$$

1. **L'unicité**
   (a) *1-ère méthode* : On suppose qu'il existe deux couples $(p, q) \in \mathbb{N}^2$ et $(p', q') \in \mathbb{N}^2$ tels que $n = 2^p(2q+1) = 2^{p'}(2q'+1)$. Montrer que $p = p'$ puis $q = q'$ puis conclure.
   (b) *2-ème méthode* : $n \in \mathbb{N}^*$. Montrer que s'il existe un couple $(p, q) \in \mathbb{N}^2$ tel que $n = 2^p(2q+1)$ alors $p = \max A_n$ puis conclure.
2. **L'existence**
   (a) *1-ère méthode* : Montrer que A_n admet un plus grand élèment p, et en déduire que n peut écrire sous la forme $n = 2^p(2q+1)$ avec $q \in \mathbb{N}$
   (b) *2-ème méthode* : Procéder par récurence forte.

Réponse 24

1. **L'unicité**
   (a) *1-ère méthode* : On suppose qu'il existe deux couples $(p, q) \in \mathbb{N}^2$ et $(p', q') \in \mathbb{N}^2$ tels que $n = 2^p(2q+1) = 2^{p'}(2q'+1)$. Supposons que $p < p'$. Dans ce cas $2q + 1 = 2^{p'-p}(2q'+1)$ ce qui montre que $2q+1$ est un nombre pair. Ceci étant faux, alors $p \geq p'$. De la même façon on a $p \leq p'$, donc $p = p'$. On en déduit alors que $2q+1 = 2q'+1$ puis $q = q'$. Finalement, en cas d'existence, le couple $(p, q) \in \mathbb{N}^2$ vérifiant $n = 2^p(2q+1)$, est unique.
   (b) *2-ème méthode* : $n \in \mathbb{N}^*$. Supposons qu'il existe un couple $(p, q) \in \mathbb{N}^2$ tel que $n = 2^p(2q+1)$. Il est clair alors que 2^p divise n. Supposons qu'il existe un entier $p' > p$ tel que 2^p divise n. Dans ce cas n s'écrit sous la forme $n = 2^{p'}k$ avec $k \in \mathbb{N}^*$. Ainsi

$n = 2^p(2q+1) = 2^{p'}k$ puis $2q+1 = 2^{p'-p}k$. Ceci est contradictoire car $2q+1$ est impair et $2^{p'-p}k$ est pair. Donc $p = \max A_n$ et p est alors unique. Comme $q = \frac{1}{2}\left(\frac{n}{2^p} - 1\right)$ alors q est à son tout unique. D'où, en cas d'existence, le couple $(p, q) \in \mathbb{N}^2$ vérifiant $n = 2^p(2q+1)$, est unique.

2. **L'existence**
   (a) *1-ère méthode* : Soit $n \in \mathbb{N}^*$. L'ensemble $A_n = \left\{k \in \mathbb{N} \ / \ 2^k/n\right\}$ est non vide car il contient 0, et il est majoré par n, donc il admet un plus grand élément noté p. Par définition de p, on a $2^p/n$, donc il existe $m \in \mathbb{N}$ tel que $n = 2^p m$. Si m est pair alors m s'écrit sous la forme $m = 2s$ avec $s \in \mathbb{N}$. Dans ce cas, $n = 2^{p+1}s$ et alors $p+1 \in A_n$, ce qui contredit la définition de p. Donc m est impair et par suite il existe $q \in \mathbb{N}$ tel que $m = 2q+1$. Ainsi, $n = 2^p(2q+1)$.
   (b) *2-ème méthode* :
   — Pour $n = 1$ le résultat estt vrai, $p = q = 0$.
   — Supposons que ce reste reste vrai jusqu'à un certain $n \geq 1$, c'est à dire qu'il est vrai pour tout $k \in [\![1, n]\!]$. Deux cas se présentent,
   — Si $n+1$ est impair, alors il est de la forme $n+1 = 2q+1$ pour un $q \in \mathbb{N}$.
   — Si $n+1$ est pair, alors il est de la forme $n+1 = 2k$ pour un $k \in \mathbb{N}^*$. Dans ce cas, $1 \leq k \leq n$. D'après l'hypothèse de récurrence, k est de la forme $k = 2^p(2q+1)$ avec $p, q \in \mathbb{N}$. Ainsi $n+1 = 2^{p+1}(2q+1)$ et le résultat est établit à l'ordre $n+1$.

   En conclusion, $\forall n \in \mathbb{N}^* \ \exists (p, q) \in \mathbb{N}^2; \ \ n = 2^p(2q+1)$.

Exercice 25

Soit f une application de $\mathbb{N}$ vers $\mathbb{N}$ telle que

$$\forall n \in \mathbb{N}, \ f(f(n)) < f(n+1).$$

On veut montrer que f est l'application identique.

1. Montrer que : $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, m \geq n \Rightarrow f(m) \geq n$.
2. Soit $n \in \mathbb{N}$. Justifier pourquoi l'ensemble $A_n = \{f(x) \ , \ x \geq n\}$ admet un plus petit élément de la forme $f(a)$ pour un certain $a \in \mathbb{N}$, puis montrer que $n = a$.
3. En déduire que f est strictement croissante.
4. Conclure.

Réponse 25

1. Raisonnons par récurrence sur n
   Initialisation : Si $n = 0$, on a $\forall x \geq 0 \ , \ f(x) \geq 0$ car f est à valeurs dans $\mathbb{N}$, d'où le résultat pour $n = 0$
   Hérédité : Soit $n \in \mathbb{N}^*$ et supposons que

   $$\forall m \in \mathbb{N}, m \geq n \Rightarrow f(m) \geq n.$$

   Soit $m \geq n+1$. On a alors $m - 1 \geq n$ et par suite, d'après hypothèse de récurrence, on a $f(m-1) \geq n$ et $f(f(m-1)) \geq n$. Or $f(f(m-1)) < f(m)$, donc $f(m) > n$ c'est a dire que $f(m) \geq n+1$ d'où le résultat a l'ordre $n+1$.
   Ainsi, $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, m \geq n \Rightarrow f(m) \geq n$.

2. L'ensemble A_n est une partie non vide de $\mathbb{N}$ car $f(n) \in A_n$, donc elle admet un plus petit élément de la forme $f(a)$ avec $a \geq n$. Supposons que $a > n$. Dans ce cas $a - 1 \geq n$ et par suite $f(a-1) \geq n$. Ceci montre que $f(f(a-1)) \in A_n$, et puisque $f(a) = \min A_n$, alors $f(a) \leq f(f(a-1))$. Or par hypothèse on a $f(f(a-1)) < f(a)$, ce qui est contradictoire. Comme conclusion, $f(n) = \min A_n$.
3. Soit n un entier naturel. On a $n+1 \geq n$, donc $f(n+1) \in A_n$ et par suite $f(n+1) \geq f(n)$. si $f(n+1) = f(n)$ alors d'après la question précédente on aura $n = n+1$, ce qu'est absurde , donc $f(n+1) > f(n)$ et f est alors strictement croissante.
4. Soit n un entier naturel. Puisque f est strictement croissante et $f(f(n)) < f(n+1)$ alors $f(n)) < n+1$; c'est à dire que $f(n) \leq n$. Or, d'après la question 1 ona $f(n) \geq n$, donc puis $f(n) = n$. Conclusion : f est l'application identique.

Exercice 26

Trouver l'erreur dans le raisonnement de récurrence suivant :
Soit $P(n)$, pour $n \in \mathbb{N}$, la propriété : « n points quelconques du plan sont toujours alignés, »

— Pour $n = 1$ et $n = 2$ la propriété $P(n)$ est vraie.

— Soit $n \geq 2$ supposons la propriété établie au rang n. Considérons alors $n+1$ points deux à deux distincts $A_1, A_2, \cdots, A_{n+1}$. D'après l'hypothèse de récurrence, les points $A_1, A_2, \cdots, A_n$ appartiennent à une même droite D. De même, les points $A_2, A_3, \cdots, A_{n+1}$ appartiennent à une même droite (D'). Or (D) et (D') contiennent deux points distincts A_2 et A_n, donc $(D) = (D')$. Ainsi $A_1, A_2, \cdots, A_{n+1}$ sont alignés. D'ou le résultat est vrai au rang $n+1$.

— Conclusion : pour tout $n \in \mathbb{N}$, n points quelconques du plan sont toujours alignés.

Réponse 26

Le raisonnement est faux parce qu'on en supposant que le résultat est vrai pour un certain n, rien ne garantit que A_2 et A_n soient deux points distincts ; ce qui est bien le cas lorsque $n = 2$.

Chapitre 2

Ensembles et applications

2.1 Inclusion, opérations sur les ensembles

Exercice 27

Soit E un ensemble et A, B, C trois parties de E. Montrer que :

1. $(A \cap B) \setminus C = (A \setminus C) \cap (B/C)$.
2. $(A \cup B) \setminus C = (A/C) \cup (B \setminus C)$.
3. $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C) = A \setminus (B \cup C)$.
4. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Réponse 27

1. — Soit $x \in E$. Alors

$$\begin{aligned} x \in (A \cap B) \setminus C &\Leftrightarrow \begin{cases} x \in A \cap B \\ x \notin C \end{cases} \\ &\Leftrightarrow \begin{cases} x \in A \text{ et } x \notin C \\ x \in B \text{ et } x \notin C \end{cases} \\ &\Leftrightarrow \begin{cases} x \in A \setminus C \\ x \in B \setminus C \end{cases} \\ &\Leftrightarrow x \in (A \cap B) \setminus C. \end{aligned}$$

   Donc $(A \cap B) \setminus C = (A \setminus C) \cap (B/C)$.

2. $\begin{aligned}(A \cup B) \setminus C &= (A \cup B) \cap \complement_E^C \\ &= (A \cap \complement_E^C) \cup (B \cap \complement_E^C \\ &= (A \setminus C) \cup (B \setminus C).\end{aligned}$

3. — Soit $x \in (A \setminus B) \setminus C$. Donc $x \in (A \setminus B)$ et $x \notin C$. Ainsi, $x \in A$, $x \notin B$ et $x \notin C$ et par la suite $x \in A$ et $x \notin B \cup C$, c'est à dire que $x \in A \setminus (B \cup C)$. Donc $(A \setminus B) \setminus C \subset A \setminus (B \cup C)$.
   — Soit $x \in A \setminus (B \cup C)$. Donc $x \in A$ et $x \notin B \cup C$, ce qui est équivalent à dire $x \in A$ et $x \notin B$ et $x \notin C$. Ainsi, $x \in A \setminus C$ et $x \notin B$. Et comme $B \setminus C \subset B$, alors $x \notin B \setminus C$. On en déduit que $x \in (A \setminus C) \setminus (B \setminus C)$. D'où $A \setminus (B \cup C) \subset (A \setminus C) \setminus (B \setminus C)$.
   — Soit $x \in (A \setminus C) \setminus (B \setminus C)$. Donc $x \in A \setminus C$ et $x \notin B \setminus C$. ceci veut dire que $x \in A$, $x \notin C$ et ($x \notin B$ ou $x \in C$. Et comme $x \notin C$, alors $x \in A$, $x \notin C$ et $x \notin B$. D'où, $x \in (A \setminus B)$ et $x \notin C$, ce qui équivalent à dire que$x \in (A \setminus B) \setminus C$. Ainsi $(A \setminus C) \setminus (B \setminus C) \subset (A \setminus B) \setminus C$.

   Conclusion : $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C) = A \setminus (B \cup C)$.

4. — Soit $x \in A \cap (B \triangle C)$. Donc $x \in A$ et $x \in (B \triangle C$. D'où $x \in B \setminus C$ ou $x \in C \setminus B$. Si $x \in B \setminus C$ alors $x \in B$ et $x \notin C$. On en déduit que $x \notin A \cap C$, et sachant que $x \in A$, on a $x \in A \cap B$. Ceci montre que $x \in (A \cap B) \setminus (A \cap C)$. Si $x \in C \setminus B$, le même raisonnement montre que $x \in (A \cap C) \setminus (A \cap B)$ et alors $x \in (A \cap B) \triangle (A \cap C)$.

   — Réciproquement, soit $x \in (A \cap B) \triangle (A \cap C)$. Donc, $x \in (A \cap B) \setminus (A \cap C)$ ou $x \in (A \cap C) \setminus (A \cap B)$.
   — *Premier cas :* Si $x \in (A \cap B) \setminus (A \cap C)$. Dans ce cas, $x \in A$, $x \in B$ et $x \notin (A \cap C)$. Comme $x \in A$ et $x \notin (A \cap C)$ alors $x \notin C$. Ceci montre que $x \in A$ $x \in A$ et $x \notin (A \cap C)$ alors $x \in B \setminus C \subset B \triangle C$.
   — *Deuxième cas :* Si $x \in (A \cap C) \setminus (A \cap B)$. De la même manière que précédemment, on montre que $x \in C \setminus B \subset B \triangle C$.

   Conclusion : $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Exercice 28

Soit E un ensemble et A, B, C, D des parties de E. Montrer que :

1. $A = B \iff A \cap B = A \cup B$.
2. $A \setminus B = A \iff B \setminus A = B$.
3. $A \subset B \iff \overline{B} \subset \overline{A}$.
4. $A \cap B = \emptyset \iff A \subset \overline{B}$.
5. $A \cup B = E \iff \overline{A} \subset B$.
6. $A \setminus B = A \iff B \setminus A = B$.
7. $(A \cup B \subset A \cup C \text{ et } A \cap B \subset A \cap C) \Longrightarrow B \subset C$.
8. $(A \cap B = A \cap C \text{ et } A \cup B = A \cup C) \Longrightarrow B = C$.
9. $(A \cap B = A \cup C \text{ et } A \cup B = A \cap C) \Longrightarrow A = B = C$.
10. $(A \subset C,\ B \subset D,\ A \cup B = C \cup D \text{ et } C \cap D = \emptyset) \Rightarrow (A = C \text{ et } B = D)$.

Réponse 28

1. L'inclusion directe étant évidente, nous montrons l'inclusion réciproque. Supposons donc que $A \cap B = A \cup B$ et montrons que $A = B$. En effet, On sait que $A \subset A \cup B$ et $A \cap B \subset B$, donc, puisque $A \cup B = A \cap B$, alors $A \subset B$. De la même façon, $B \subset A$ et finalement $A = B$.
2. On a
$$\begin{aligned} A \setminus B = A &\Leftrightarrow A \cap \overline{B} = A \\ &\Leftrightarrow A \subset \overline{B} \\ &\Leftrightarrow \overline{\overline{B}} \subset \overline{A} \\ &\Leftrightarrow B \subset \overline{A} \\ &\Leftrightarrow B \cap \overline{A} = B \\ &\Leftrightarrow B \setminus A = A \end{aligned}$$
   Conclusion : $A \setminus B = A \iff B \setminus A = B$.
3. — Supposons que $A \subset B$ et considérons $x \in \overline{B}$. Si $x \in A$ alors , puisque $A \subset B$ on aura $x \in B$, ce qui est faux car $x \in \overline{B}$. Donc $x \notin A$; c'est à dire que $x \in \overline{A}$. Donc $A \subset B \Rightarrow \overline{B} \subset \overline{A}$.
   — D'après l'étape précédente on a :
$$\begin{aligned} \overline{B} \subset \overline{A} &\Rightarrow \overline{\overline{A}} \subset \overline{\overline{B}} \\ &\Rightarrow A \subset BA \subset B \end{aligned}$$
   En conclusion : $A \subset B \iff \overline{B} \subset \overline{A}$.

4. — Supposons que $A \cap B = \emptyset$. Dans ce cas, pour tout $x \in A$ on a $x \notin B$ et par suite $x \in \overline{B}$. Ainsi, $A \subset \overline{B}$.
   — Supposons, par contraposée, que $A \cap B \neq \emptyset$ et soit $x \in A \cap B$. Alors, $x \in A$ et $x \in B$, donc $x \notin \overline{B}$, ce qui montre que $A \not\subseteq \overline{B}$.

   D'où : $A \cap B = \emptyset \iff A \subset \overline{B}$.

5. En effet,

$$\begin{aligned} A \cup B = E &\Leftrightarrow \overline{A \cup B} = \emptyset \\ &\Leftrightarrow \overline{A} \cap \overline{B} = \emptyset \\ &\Leftrightarrow \overline{A} \subset \overline{\overline{B}} = B \text{ ; c'est d'après la question précédente} \end{aligned}$$

   Ainsi : $A \cup B = E \iff \overline{A} \subset B$.

6. Supposons que $A \cup B \subset A \cup C$ et $A \cap B \subset A \cap C$ et soit $x \in B$. On étudiera les deux cas, $x \in A$ et $x \notin A$.
   — Supposons que $x \in A$. Dans ce cas, $x \in A \cap B$, et comme $A \cap B \subset A \cap C$ alors $x \in A \cap C$ et par suite $x \in C$.
   — Supposons maintenant que $x \notin A$. Puisque $x \in A$ et $A \subset A \cup B \subset A \cup C$ alors $x \in A \cup C$. Et comme $x \notin A$ alors $x \in C$.

   Finalement, dans les deux cas $x \in C$, ce qui achève la preuve.

7. Supposons que $A \cap B = A \cap C$ et $A \cup B = A \cup C$. on applique la question précédente on a $B \subset C$. Comme B et C jouent des rôles symétriques, alors $C \subset B$ puis $B = C$

8. Supposons que $A \cap B = A \cup C$ et $A \cup B = A \cap C$. On sait que $A \subset A \cup C$ et $A \cap B \subset B$. Comme on a supposé que $A \cup B = A \cap C$, alors $A \subset B$. Aussi, puisque $B \subset A \cup B$, $A \cup B = A \cap C$ et $A \cap C \subset C$, alors $B \subset C$. Il reste à montrer que $C \subset A$. De la même façon, $C \subset A \cup C = A \cap B \subset A$. D'où le résultat.

9. Supposons que $A \subset C,\ B \subset D,\ A \cup B = C \cup D$ et $C \cap D = \emptyset$. Il suffit de montrer que $C \subset A$ et $D \subset B$. Soit $x \in C$. Puisque $C \subset C \cup D$, $A \cup B = C \cup D$, alors $x \in A \cup B$; c'est à dire que $x \in A$ ou $x \in B$. Et comme $C \cap D = \emptyset$ et $x \in C$ alors $x \notin D$. Sachant que $B \subset D$, alors $x \notin B$. Ainsi $x \in A$, ce qui montre que $C \subset A$. De la même façon on a $D \subset B$. Fin de la démonstration.

Exercice 29

Soit , B des parties de E. Simplifier les expressions suivantes :

1. $(A \cap B) \cup (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap \overline{B})$.
2. $A \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B} \cap C)$
3. $A \backslash (A \backslash B)$

Réponse 29

1. D'après les lois de Morgan on a :

$$\begin{aligned} (A \cap B) \cup (\overline{A} \cap B) &= \left(A \cup \overline{A}\right) \cap B \\ &= E \cap B \\ &= B \end{aligned}$$

   On en déduit que $(A \cap \overline{B}) \cup (\overline{A} \cap \overline{B}) = \overline{B}$ puis

$$A \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B} \cap C) = B \cup \overline{B} = E$$

2. On a
$$A \cup (\overline{A} \cap B) = \big(A \cup \overline{A}\big) \cap (A \cup B) = E \cap (A \cup B) = A \cup B$$
En appliquant ce résultat, $A \cup B$ jouant le rôle de A et C jouant le rôle de B on aura :
$$(A \cup B) \cup (\overline{A} \cap \overline{B} \cap C) = (A \cup B) \cup (\overline{A \cup B} \cap C) = A \cup B \cup C$$
Donc $A \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B} \cap C) = A \cup B \cup C$

3. $$\begin{aligned} A\backslash(A\backslash B) &= A \cap \overline{A \cap \overline{B}} \\ &= A \cap \big(\overline{A} \cup B\big) \\ &= \big(A \cap \overline{A}\big) \cup (A \cap B) \\ &= \emptyset \cup (A \cap B) \\ &= A \cap B \end{aligned}$$

Exercice 30

Soit E un ensemble non vide. A chaque partie A de E, on fait assoicier l'application caractéristique χ_A définie par :
$$\begin{array}{rccl} \chi_A : & E & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \begin{cases} 1, & \text{si } x \in A \\ 0, & \text{si } x \notin A. \end{cases} \end{array}$$
Montrer que pour toutes parties A et B de E on a :

1. $A = B \Longleftrightarrow \chi_A = \chi_B$.
2. $\chi_{A\cap B} = \chi_A \chi_B$.
3. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \chi_B$
4. $\chi_{\overline{A}} = 1 - \chi_A$
5. $\chi_{A\backslash B} = \chi_A - \chi_A \chi_B$.
6. $\chi_{A\triangle B} = |\chi_A - \chi_B|$

Réponse 30

---

1. — Supposons que $A = B$ et soit $x \in E$.
   — Si $x \in A$ alors $\chi_A(x) = \chi_B(x) = 1$,
   — si $x \notin A$ alors $\chi_A(x) = \chi_B(x) = 0$.
   Donc, dans les deux cas on a $\chi_A(x) = \chi_B(x)$ et par suite $\chi_A = \chi_B$.
   — Réciproquement, supposons que $\chi_A = \chi_B$ et soit $x \in E$. Alors,
   $$\begin{aligned} x \in A &\Leftrightarrow \chi_A(x) = 1 \\ &\Leftrightarrow \chi_B(x) = 1, \text{ car } \chi_A = \chi_B \\ &\Leftrightarrow x \in B \end{aligned}$$
   Ainsi $A = B$.
   Finalement : $A = B \Longleftrightarrow \chi_A = \chi_B$.
2. Soit $x \in E$.
   — $x \in A \cap B$ alors $\chi_A(x) = \chi_B(x) = 1$ et par suite $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x) = 1$.
   — Si $x \notin A \cap B$ alors $x \notin A$ ou $x \notin \cap B$. Donc $\chi_A(x) = 0$ ou $\chi_B(x) = 0$ et par suite $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x) = 0$.
   Dans tous les cas $\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x)$, donc $\chi_{A\cap B} = \chi_A \chi_B$.
3. Soit $x \in E$.

— Si $x \in A$ et $x \in B$ alors $\chi_A(x) = \chi_B(x) = \chi_{A\cup B}(x) = 1$ et par suite $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x) = 1$.
— Si $x \notin A$ et $x \notin B$ alors $\chi_A(x) = 0 = \chi_B(x) = \chi_{A\cup B}(x) = 0$ et par suite $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x) = 0$.
— Si $x \in A$ et $x \notin B$ alors $\chi_A(x) = \chi_{A\cup B}(x) = 1$ et $\chi_B(x) = 0$ et par suite $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x) = 1$.
— De la même manière, si $x \in B$ et $x \notin A$ on aura $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x)\chi_B(x) = 1$.

Ainsi, $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A\chi_B$.

4. Soit $x \in E$.
— Si $x \in A$ alors $x \notin \overline{A}$ et par la suite $\chi_A(x) = 1$ et $\chi_{\overline{A}}(x) = 0$ puis $\chi_{\overline{A}}(x) = 1-\chi_A(x) = 0$.
— Si $x \notin A$ alors $x \in \overline{A}$ et par la suite $\chi_A(x) = 0$ et $\chi_{\overline{A}}(x) = 1$ ce qui implique $\chi_{\overline{A}}(x) = 1 - \chi_A(x) = 0$.

Conclusion : $\chi_{\overline{A}} = 1 - \chi_A$

5. D'après ce qui précède on a
$$\begin{aligned}\chi_{A\setminus B} &= \chi_{A\cap\overline{B}}\\ &= \chi_A\chi_{\overline{B}}\\ &= \chi_A\,(1-\chi_B)\\ &= \chi_A - \chi_A\chi_B\end{aligned}$$

6. Soit $x \in E$.
— Si $x \in A$ et $x \in B$ alors $x \notin A\triangle B$. Dans ce cas $\chi_A(x) = \chi_B(x) = 1$ et $\chi_{A\triangle B} = 0$ et par suite $\chi_{A\triangle B}(x) = |\chi_{A(x)} - \chi_B(x)| = 0$.
— Si $x \notin A$ et $x \notin B$ alors $x \notin A\triangle B$. Dans ce cas $\chi_A(x) = \chi_B(x) = \chi_{A\triangle B} = 0$ et par suite $\chi_{A\triangle B}(x) = |\chi_{A(x)} - \chi_B(x)| = 0$.
— Si $x \in A$ et $x \notin B$ alors $x \in A\triangle B$. Dans ce cas $\chi_B(x) = 0$ et $\chi_A(x) = \chi_{A\triangle B} = 1$ et par suite $\chi_{A\triangle B}(x) = |\chi_{A(x)} - \chi_B(x)| = 1$.
— Si $x \in B$ et $x \notin A$ alors $x \in A\triangle B$. Dans ce cas $\chi_A(x) = 0$ et $\chi_B(x) = \chi_{A\triangle B} = 1$ et par suite $\chi_{A\triangle B}(x) = |\chi_{A(x)} - \chi_B(x)| = 1$.

Conclusion : $\chi_{A\triangle B} = |\chi_A - \chi_B|$

2.2 Applications injectives, surjectives, bijectives

Exercice 31 Solution

Soit l'application $f : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R}\\ x & \longmapsto & \dfrac{2x}{1+x^2}\end{array}$

1. Étudier la nature de f, est elle injective ? surjective ? bijective ?
2. Montrer que $f(\mathbb{R}) = [-1, 1]$.
3. Montrer que l'application $g : \begin{array}{ccc}[-1,1] & \longrightarrow & [-1,1]\\ x & \longmapsto & \dfrac{2x}{1+x^2}\end{array}$ est bijective.

Réponse 31

1. Soit $y \in \mathbb{R}$ et résolvons dans $\mathbb{R}$ l'équation $f(x) = y$. Pour tout $x \in \mathbb{R}$ on a : $f(x) = y \iff yx^2 - 2x + y = 0$. Pour $y = 0$ l'équation admet une unique solution $x = 0$, et pour $y \neq 0$ on calcule le discriminant simplifié $\Delta' = 1 - y^2$. On peut déduire alors que si $|y| < 1$ alors l'équation admet deux solutions distinctes $x_1 = \dfrac{1 - \sqrt{1-y^2}}{y}$ et $x_2 = \dfrac{1 + \sqrt{1-y^2}}{y}$, et si $|y| > 1$ alors l'équation n'admet aucune solution, et$y = \pm$ alors l'équation admet une unique solution $x = \dfrac{1}{y} = y$. De là, n'est ni injective ni surjective.
2. Le calcul précédent montrer que, pour tout $y \in \mathbb{R}$, l'équation $f(x) = y$ admet une solution dans $\mathbb{R}$ si et seulement si $y \in [-1, 1]$. Ceci montre que $f(\mathbb{R}) = [-1, 1]$.
3. Toujours d'après la première question, pour $y = 0, 1$ ou -1, l'équation $f(x) = y$ admet une unique solution $x = y$ qui est dans $[-1, 1]$, et pour $y \in]-1, 1[\backslash\{0\}$ elle admet deux solutions distinctes $x_1 = \dfrac{1 - \sqrt{1-y^2}}{y}$ et $x_2 = \dfrac{1 + \sqrt{1-y^2}}{y}$. Mais puisque $x_1 x_2 = 1$ et que $x_1 \neq \pm 1$ et $x_2 \neq \pm 1$ alors une seule solution est dans $]-1, 1[$. Remarque : Par un calcul simple, ou en remarquant que $|x_1| \leq |x_1|$, on peut déduire que c'est x_1 qui est dans $]-1, 1[$. Conclusion : g est bijective.

Exercice 32

Montrer que l'application f définie de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ par

$$f(p, q) = p^2 + 2pq + q^2 + p$$

est injective. Est-elle surjective ?

Réponse 32

Soit $(p, q), (k, l) \in \mathbb{N}^2$ tels que $f(p, q) = f(k, l)$. Donc $(p+q)^2 + p = (k+l)^2 + k$. Commençons par montrer que $p+q = k+l$. Pour cela, supposons que $p+q \neq k+l$. Sans perdre de généralité, on peut supposer que $p + q > k + l$, ou encore $p + q \geq k + l + 1$. Dans ce cas,

$$\begin{aligned} f(p,q) &= (p+q)^2 + p \\ &\geq (k+l+1)^2 + p \\ &= k^2 + l^2 + 1 + 2kl + 2k + 2l + p \\ &= f(k,l) + 1 + 2k + l + p \\ &> f(k,l) \end{aligned}$$

Absurde. Donc $p + q = k + l$, puis $k = p$ et ensuite $q = l$. Ainsi f est injective.

Exercice 33

Soit E , F et G des ensembles non vides, f une application de E dans F et g une application de F dans G .

1. Montrer que si $g \circ f$ est injective, alors f est injective.
2. Montrer que si $g \circ f$ est surjective, alors g est surjective.

Réponse 33

1. Supposons que $g \circ f$ est injective et soit $(x, y) \in E^2$ tel que $f(x) = f(y)$. Comme g est une application on $g(f(x)) = g(f(y))$ c'est à dire que $g \circ f(x) = g \circ f(y)$. Et comme $g \circ f$ est injective, alors $x = y$, d'où le résultat.

2. Supposons que $g \circ f$ est surjective et considérons $z \in G$. Puisque $g \circ f$ est surjective, il existe $x \in E$ tel que $g \circ f(x) = z$, ou encore, $z = g(y)$ avec $y = f(x)$. Donc g est surjective.

Exercice 34

Soit E un ensemble, f, g et h des applications de E dans E. Montrer que :

1. Si $g \circ f$ et $h \circ g$ sont bijectives, alors f, g et h sont bijectives.
2. Si $h \circ g \circ f$ et $g \circ f \circ h$ sont surjectives et $f \circ h \circ g$ est injective, alors f,g et h sont bijectives.
3. Si $f \circ f = f$, et si f est surjective ou injective alors $f = \mathrm{id}_E$.
4. Si $f \circ f \circ f = f$ et f est surjective, alors f est bijective. quelle est son application réciproque f^{-1} ?

Réponse 34

1. Supposons que $g \circ f$ et $h \circ g$ sont bijectives. D'après l'exercice précédent, puisque $g \circ f$ est surjective, alors g est surjective, et puisque $h \circ g$ est injective, alors g est injective. On en déduit alors que g est bijective. En composant $g \circ f$ avec g^{-1} à gauche, et $h \circ g$ avec g^{-1} à droite, on déduit que f et h sont aussi bijectives.
2. Supposons que $h \circ g \circ f$ et $g \circ f \circ h$ sont surjectives et $f \circ h \circ g$ est injective. De l'exercice précédent, puisque $h \circ g \circ f$ et $g \circ f \circ h$ sont surjectives alors h, $h \circ g$, et g et $g \circ f$ sont aussi surjectives. Et puisque $f \circ h \circ g$ est injective alors g et $h \circ g$ sont injectives. On en déduit déjà que g et $h \circ g$ sont bijectives. En composant $g \circ f \circ h$ avec g^{-1} à gauche, et $f \circ h \circ g$ avec g à droite, on déduit que $f \circ h$ sont est surjective et injective, donc bijective. Maintenant, d'après la question précédente, puisque $h \circ g$ et $f \circ h$ sont bijectives, alors f, g et h sont bijectives.
3. Supposons que $f \circ f = f$.
   - Supposons que f est surjective et considérons $x \in E$. Il existe $a \in E$ tel que $x = f(a)$. Il s'ensuit que $x = f(a) = f \circ f(a) = f(x)$.
   - Supposons que f est injective et considérons $x \in E$. On a $f \circ f(x) = f(x)$, donc $f(f(x)) = f(x)$ et par suite $f(x) = x$

   Ainsi $f = \mathrm{id}_E$.
4. Supposons que $f \circ f \circ f = f$ et f est surjective. Soit $x \in E$. Il existe alors $a \in E$ tel que $x = f(a)$. Ainsi $x = f(a) = f \circ f \circ f(a) = f \circ f(x)$. On en déduit que $f \circ f = \mathrm{id}_E$; c'est à dire que f est bijective et $f^{-1} = f$.

Exercice 35

Soit E, F, G trois ensembles non vides et f une application de E vers F

1. Montrer que f est injective si et seulement si pour toutes applications g et h de G vers E on a
$$f \circ g = f \circ h \Longrightarrow g = h.$$
2. Montrer que si f est surjective alors pour toutes applications g et h de F vers G on a on a
$$g \circ f = h \circ f \Longrightarrow g = h.$$
Que dire de la réciproque.

Réponse 35

1. — Supposons que f est injective et soit g, h deux applications de G vers E tels que $f \circ g = f \circ h$. Soit $x \in E$. on a alors $f(g(x)) = f(h(x))$, et comme f est injective alors $g(x) = h(x)$. Donc $g = h$.
   — Réciproquement, supposons que pour toutes applications g et h de F vers G on a on a
   $$g \circ f = h \circ f \Longrightarrow g = h$$
   et montrons que f est bijective. Soit donc $x, y \in E$ tels que $f(x) = f(y)$. Considérons les applications g et h de G vers E définies par $g(t) = x$ et $h(t) = y$ pour tout $t \in G$. Il est clair que $f \circ g = f \circ h$, d'où $g = h$ et par la suite $x = y$. Ainsi f est injective.
2. — Supposons que f est surjective et considérons un $x \in F$. Il existe $a \in E$ tel que $x = f(a)$. On a alors $g(x) = g \circ f(a) = h \circ f(a) = h(x)$. Donc $h = g$.
   — Remarquons que si G est un singleton alors pour toutes applications g et h de F vers G on a
   $$f \circ g = f \circ h \Longrightarrow g = h,$$
   car dans ce cas, il existe une unique application de F vers G, donc $g = h$. Cependant, si F n'est pas réduit à un singleton, il existe au moins une application f de E vers F non surjective. On peut prendre par exemple $E = F = \{-1, 1\}$, $G = \{1\}$ et $f(1) = f(-1) = 1$. Cela montre que la réciproque est fausse.
   Remarquons aussi que si F est un singleton alors la réciproque est vraie, car dans ce cas il existe une unique application de E vers F et elle est surjective.
   Montrons, par contraposée, que la réciproque est aussi vraie si G n'est pas réduit à un singleton, donc contient au moins deux éléments distincts z et w. Supposons donc que f n'est pas surjective et soit b un élément de F n'ayant pas d'antécédent par f. Considérons les applications g et h de F vers G définies par
   $$\forall y \in F,\ g(y) = z, \quad \forall y \in F \setminus \{b\},\ h(y) = z \text{ et } h(b) = w.$$
   Il est clair que $g \circ f = h \circ f$ et $h \neq g$. Donc, la réciproque est vraie si et seulement si F est un singleton ou si G n'est pas réduit à un singleton.

Exercice 36

Soit E un ensemble non vide. Montrer qu'il n'existe pas de surjection de E dans $\mathcal{P}(E)$

Réponse 36

Supposons qu'il existe une surjection f de E dans $\mathcal{P}(E)$. L'idée est de chercher un élément X de $\mathcal{P}(E)$ n'admettant pas d'antécédent par f dans E pour aboutir à une contradiction et conclure. Posons $X = \{x \in E \,/\, x \notin f(x)\}$. Puisque f est surjective, il existe $a \in E$ tel que $f(a) = X$. Deux cas se pressentent alors :

— Si $a \in f(a) = X$ alors $a \notin X = f(a)$,

— et si $a \notin f(a) = X$ alors par définition de X on a $a \in X = f(a)$.

Les deux cas sont contradictoires. Donc, il n'existe pas de surjection de E dans $\mathcal{P}(E)$.

2.3 Image directe, image réciproque d'une partie par une application

Exercice 37

Soit E ,F deux ensembles non vides et f une application E dans F. Montrer que :

1. $\forall (A,B) \in \mathcal{P}(E)^2,\ A \subset B \Rightarrow\ f(A) \subset f(B)$.
2. $\forall (C,D) \in \mathcal{P}(F)^2,\ C \subset D \Rightarrow\ f^{-1}(C) \subset f^{-1}(D)$.
3. $\forall (A,B) \in \mathcal{P}(E)^2,\ f(A \cup B) = f(A) \cup f(B)$.
4. $\forall (C,D) \in \mathcal{P}(F)^2,\ f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
5. $\forall (A,B) \in \mathcal{P}(E)^2,\ f(A \cap B) \subset f(A) \cap f(B)$. A-t-on égalité ?
6. $\forall (A,B) \in \mathcal{P}(E)^2,\ f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
7. $\big(\forall (A,B) \in \mathcal{P}(E)^2,\ f(A \cap B) = f(A) \cap f(B)\big) \Leftrightarrow f$ est injective.

Réponse 37

1. Soit $(A,B) \in \mathcal{P}(E)^2$ tels que $A \subset B$ et soit $y \in f(A)$. Il existe alors $x \in A$ tel que $y = f(x)$. Comme $x \in A$ et $A \subset B$ alors $x \in B$ et par suite $y = f(x) \in f(B)$. Donc $f(A) \subset f(B)$. Comme conclusion :

$$\forall (A,B) \in \mathcal{P}(E)^2, A \subset B \Rightarrow\ f(A) \subset f(B).$$

2. Soit $(C,D) \in \mathcal{P}(F)^2$ tels que $C \subset D$ et soit $x \in f^{-1}(C)$. On a alors :

$$\begin{aligned} x \in f^{-1}(C) &\Rightarrow f(x) \in C \\ &\Rightarrow f(x) \in D \,;\, \text{car } C \subset D \\ &\Rightarrow x \in f^{-1}(D) \end{aligned}$$

   Donc $f^{-1}(C) \subset f^{-1}(D)$. Ainsi :

$$\forall (C,D) \in \mathcal{P}(F)^2, C \subset D \Rightarrow\ f^{-1}(C) \subset f^{-1}(D).$$

3. Soit $(A,B) \in \mathcal{P}(E)^2$. Comme $A \subset A \cup B$ et $B \subset A \cup B$ alors $f(A) \subset f(A \cup B)$ et $f(B) \subset f(A \cup B)$, puis $f(A) \cup f(B) \subset f(A \cup B)$. Pour la réciproque, considérons $y \in f(A \cup B)$. Il existe alors $x \in A \cup B$ tel que $y = f(x)$. puisque $x \in A \cup B$ alors $x \in A$ ou $x \in B$. Si $x \in A$ alors $y = f(x) \in f(A)$ et par suite $y \in f(A) \cup f(B)$. Et si $x \in B$ alors $y = f(x) \in f(B)$ et par suite $f(x) \in f(A) \cup f(B)$. Dans les deux cas $y \in f(A) \cup f(B)$ ce qui implique que $f(A \cup B) \subset f(A) \cup f(B)$. Finalement :

$$\forall (A,B) \in \mathcal{P}(E)^2,\ f(A \cup B) = f(A) \cup f(B).$$

4. Soit $(C,D) \in \mathcal{P}(F)^2$. Pour tout $x \in E$ n a :

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D \\ &\Leftrightarrow f(x) \in C \text{ ou } f(x) \in D \\ &\Leftrightarrow x \in f^{-1}(C) \text{ ou } x \in f^{-1}(D) \\ &\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D) \end{aligned}$$

   Ainsi $f^{-1}(C) \cup f^{-1}(D) = f^{-1}(C \cup D)$.

5. Soit $(A,B) \in \mathcal{P}(E)^2$. Comme $A \cap B \subset A$ et $A \cap B \subset B$ alors $f(A \cap B) \subset f(A)$ et $f(A \cap B) \subset f(B)$ et par suite $f(A \cap B) \subset f(A) \cap f(B)$.
   En général, on n'a pas égalité. En effet, si f n'est pas injective, il existe $x, y \in E$ tels que $x \neq y$ et $f(x) = f(y)$. On prend alors $A = \{x\}$ et $A = \{x\}$. Il s'ensuit que $A \cap B = \emptyset$, donc $f(A \cap B) = \emptyset$, mais $f(A) \cap f(B) = \{f(x)\} \neq \emptyset$.

6. ($\Rightarrow$) C'est déjà fait dans la question précédente. En effet, supposons, par contraposée, f n'est pas injective. Il existe alors $x, y \in E$ tels que $x \neq y$ et $f(x) = f(y)$. On prend alors $A = \{x\}$ et $A = \{x\}$. Dans ce cas, $f(A \cap B) = \emptyset$; car $A \cap B = \emptyset$, mais $f(A) \cap f(B) = \{f(x)\} \neq \emptyset$.

($\Leftarrow$) Supposons que f est injective. On a déjà $f(A\cap B)\subset f(A)\cap f(B)$. Soit $y\in f(A)\cap f(B)$. Il existe donc $(x,x')\in A\times B$ tel que $f(x)=y$ et $f(x')=y$, donc $f(x)=f(x')$. Puisque f est injective, alors $x=x'$ et par suite $y\in f(A\cap B)$, d'où le résultat.

Exercice 38

Soit E ,F deux ensembles non vides et f une application E dans F. Montrer que

1. $\forall B\subset F,\ \overline{f^{-1}(B)}=f^{-1}(\overline{B})$.
2. $\Big(\forall A\in\mathcal{P}(E),\ f(\overline{A})=\overline{f(A)}\Big)\Leftrightarrow f$ est bijective.

Réponse 38

1. Soit $B\subset F$. Pour tout $x\in E$ on a :

$$\begin{aligned} x\in f^{-1}(\overline{B}) &\Leftrightarrow f(x)\in\overline{B}\\ &\Leftrightarrow f(x)\notin B\\ &\Leftrightarrow x\notin f^{-1}(B)\\ &\Leftrightarrow x\in\overline{f^{-1}(B)}\end{aligned}$$

   Donc, $\overline{f^{-1}(B)}=f^{-1}(\overline{B})$.

2. ($\Rightarrow$) Supposons que

$$\forall A\in\mathcal{P}(E)\ ,\quad f(\overline{A})=\overline{f(A)}$$

   Posons $A=\emptyset$. On a $\overline{A}=E$, donc $f(E)=f(=\overline{f(\emptyset)}=\overline{\emptyset}=F$. Ainsi f est surjective. Considérons $(x,y)\in E^2$ tel que $x\neq y$ et prenons $A=\{y\}$. Comme $x\in\overline{A}$ alors $f(x)\in f(\overline{A})=\overline{f(A)}=F\setminus\{f(y)\}$. Ceci montre que $f(x)\neq f(y)$, et par suite f est injective. Ainsi f est bijective

   ($\Leftarrow$) Supposons que f est bijective et considérons une partie A de E.

   Première méthode.

   — Soit $y\in f(\overline{A})$. Il existe alors $x\in\overline{A}$ tel que $f(x)=y$. Montrons que $y\in\overline{f(A)}$. Pour cela, supposons que $y\notin\overline{f(A)}$; c'est à dire que $y\in f(A)$. Dans ce cas, il existe $x'\in A$ tel que $f(x')=y$. Ainsi $f(x)=f(x')$. Or f est injective, donc $x=x'$ ce qui faux car $x\in\overline{A}$ et $x'\in A$. Donc $f(\overline{A})\subset\overline{f(A)}$.

   — Soit $y\in\overline{f(A)}$ et montrons que $y\in f(\overline{A})$. Comme f est bijective, alors il existe un $x\in E$ tel que $f(x)=y$. Sachant que $y\in\overline{f(A)}$, alors $y\notin f(A)$ puis $x\notin A$; c'est à dire que $x\in\overline{A}$. Ceci montre que $y\in f(\overline{A})$ et en conséquence $\overline{f(A)}\subset f(\overline{A})$.

   Deuxième méthode. D'après D'après les questions 3 et 7 de l'exercice 37 on a $f(A\cup\overline{A})=f(A)\cup f(\overline{A})$ et $f(A\cap\overline{A})=f(A)\cap f(\overline{A})$. Donc, $f(E)=f(A)\cup f(\overline{A})$ et $f(\emptyset)=f(A)\cap f(\overline{A})$. Or $f(\emptyset)=\emptyset$ et, puisque f est surjective alors $f(E)=F$. Donc $f(A)\cup f(\overline{A})=F$ et $f(A)\cap f(\overline{A})=\emptyset$. En appliquant les questions 4 et 5 de l'exercice 28 on déduit que $f(\overline{A})\subset f(\overline{A})$ et $f(\overline{A})\subset f(\overline{A})$, donc $f(\overline{A})=f(\overline{A})$.

Exercice 39

Soit f une application d'un ensemble E dans un ensembles F , A une partie de E et B une partie de F .

1. Montrer que $A\subset f^{-1}(f(A))$. A-t-on égalité ?
2. Montrer que $f(f^{-1}(f(A)))=f(A)$.

3. Montrer que $f(f^{-1}(B)) \subset B$. A-t-on égalité ?
4. Montrer que $f^{-1}(f(f^{-1}(B))) = f^{-1}(B)$.
5. Montrer que $(\forall A \in P(E),\ f^{-1}(f(A)) = A) \Longleftrightarrow f$ est injective.
6. Montrer que $(\forall B \in P(F),\ f(f^{-1}(B)) = B) \Longleftrightarrow f$ est surjective.

Réponse 39

1. On sait que pour tout $x \in E$ on a $x \in f^{-1}(f(A)) \Leftrightarrow f(x) \in f(A)$. Or, pour tout $x \in A$ on a $f(x) \in f(A)$ et par suite $x \in f^{-1}(f(A))$. Donc $A \subset f^{-1}(f(A))$. En général on n'a pas d'égalité. En effet, les images des éléments de A par f peuvent avoir d'autres antécédents par f n'appartenant pas à A si jamais f n'est pas injective. Ainsi par exemple, si f est définie de $\mathbb{R}$ vers $\mathbb{R}$ par $f(x) = |x|$ pour tout $x \in \mathbb{R}$ et $A = \mathbb{R}_+$, alors $A \neq f^{-1}(f(A)) = \mathbb{R}$.
2. D'après la question précédente on a Pour tout $x \in E$ on a $A \subset f^{-1}(f(A))$. on en déduit que $f(A) \subset f(f^{-1}(f(A)))$. Soit maintenant $y \in f(f^{-1}(f(A)))$. Il existe donc un $x \in f^{-1}(f(A))$ tel que $f(x) = y$. Comme $x \in f^{-1}(f(A))$ alors $f(x) \in f(A)$; c'est à dire $y \in f(A)$. Ainsi $f(f^{-1}(f(A))) \subset f(A)$. Donc $f(f^{-1}(f(A))) = f(A)$.
3. Soit $y \in f(f^{-1}(B))$. Il existe donc un $x \in f^{-1}(B)$ tel que $f(x) = y$. Puisque $x \in f^{-1}(B)$ alors $y = f(x) \in B$. D'où $f(f^{-1}(B)) \subset B$. Pour l'égalité, il est clair que si B contient un élément qui n'admet pas un antécédent par f (ce qui suppose que f n'est pas surjective), alors $f(f^{-1}(B)) \neq B$. En effet, prenons par exemple comme précédemment l'application f définie de $\mathbb{R}$ vers $\mathbb{R}$ par $f(x) = |x|$ pour tout $x \in \mathbb{R}$, et $B = \mathbb{R}$. Dans ce cas on a $f(f^{-1}(B)) = f(\mathbb{R}) = \mathbb{R}^+ \neq B$. Ainsi, en général, on n'a pas égalité.
4. D'après la questions précédente on a $f(f^{-1}(B)) \subset B$. Ceci donne $f^{-1}(f(f^{-1}(B))) \subset (f^{-1}(B)$. Et d'après la question 1 du même exercice, en prenant $A = f^{-1}(B)$ on a $f^{-1}(B) \subset f^{-1}(f(f^{-1}(B)))$. D'où l'égalité : $f^{-1}(f(f^{-1}(B))) = f^{-1}(B)$.
5. — Supposons que :
$$\forall A \in P(E),\ f^{-1}(f(A)) = A.$$
Soit $x, y \in E$ tels que $f(x) = f(y)$. Posons $A = \{x\}$. On a $f(y) = f(x) \in f(A)$, donc $y \in f^{-1}(f(A))$. Or on a supposé que $f^{-1}(f(A)) = A$, donc $y \in A = \{x\}$ ce qui signifie que $x = y$. Ainsi f est injective.
— Supposons, par contraposée, qu'il existe une partie $A \subset E$ telle que $f^{-1}(f(A)) \neq A$. On sait que $A \subset f^{-1}(f(A))$, donc il existe $x \in f^{-1}(f(A))$ tel que $x \notin A$. Puisque $x \in f^{-1}(f(A))$ alors $f(x) \in f(A)$, et ceci montre qu'il existe $x' \in A$ tel que $f(x) = f(x')$. Il est clair que $x \neq x'$; car $x' \in A$ et $x \notin A$. f est alors non injective.

   Ceci achève la preuve.
6. $(\forall B \in P(F),\ f(f^{-1}(B)) = B) \Longleftrightarrow f$ est surjective.
— Supposons que :
$$\forall B \in P(F),\ f(f^{-1}(B)) = B.$$
Prenant $B = F$. Alors $f(f^{-1}(F)) = F$. Or, $f^{-1}(F) \subset E$ et par suite $f(f^{-1}(F)) \subset f(E)$. Ceci montre que $F \subset f(E)$. Ainsi f est surjective.
— Supposons que f est surjective et soit $B \in F$. On a déjà montré que $f(f^{-1}(B)) \subset B$. Soit $y \in B$. Comme f est surjective alors il existe $x \in E$ tel que $f(x) = y$. Ainsi, $f(x) \in B$ ce qui permet de dire que $x \in f^{-1}(B)$ puis $y = f(x) \in f(f^{-1}(B))$. Ainsi $f(f^{-1}(B)) = B$ ce qui achève la démonstration.

Exercice 40 Solution

Soit E un ensemble non vide et $A, B \in E$. On définit les applications : $f_A : \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ X & \longrightarrow & X \cap A \end{array}$, $g_A : \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ X & \longrightarrow & \end{array}$

et $f_{A,B} : \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \times \mathcal{P}(E) \\ X & \longrightarrow & (X \cap A, X \cap B) \end{array}$

1. Étude des fonctions f_A, $f_{A,B}$ et g_A.
   (a) Déterminer f_A et g_A lorsque $E = \{a, b\}$ et $A = \{a\}$ avec $a \neq b$.
   (b) Calculer les images de $\emptyset$, A et E par f_A et g_A.
   (c) Déterminer $f_A(\mathcal{P}(E))$ et $g_A(\mathcal{P}(E))$.
   (d) Les fonctions f_A, g_A et $f_{A,B}$ sont elles injectives, surjectives, bijectives ?
2. Quelques équations dans $\mathcal{P}(E)$.
   (a) Considérons dans $\mathcal{P}(E)$ l'équation $A \cap X = B$.
      i. Montrer que si $B \not\subseteq A$ alors cette équation n'admet pas de solution.
      ii. On suppose que $B \subseteq A$. Montrer alors que X est une solution de cette équation si et seulement si X est de la forme $X = B \cup Y$ où $Y \subset \overline{A}$.
      iii. Conclure.
   (b) Considérons dans $\mathcal{P}(E)$ l'équation $A \cup X = B$.
      Méthode 1 Raisonner de la même manière que précédemment pour résoudre l'équation $A \cup X = B$.
      Méthode 2 Déduire de la question 2(a)iii les solutions de l'équation $A \cup X = B$ en remarquant que pour tout $X \subset E$ on a $A \cup X = B \iff \overline{A} \cap \overline{X} = \overline{B}$.
   (c) Résoudre dans $\mathcal{P}(E)$ le système $\begin{cases} A \cap X = B \\ A \cup X = C \end{cases}$

Réponse 40

1. (a) Il est clair que $f_A(\emptyset) = f_A(\{b\}) = \emptyset$, $f_A(\{a\}) = f_A(\{a, b\}) = \{a\}$, $g_A(\emptyset) = g_A(\{a\}) = \{a\}$ et $g_A(\{b\}) = g_A(\{a, b\}) = \{a, b\}$.
   (b) $f_A(\emptyset) = \emptyset$, $f_A(A) = f_A(E) = g_A(A) = A$ et $g_A(E) = E$.
   (c) Pour tout $X \in \mathcal{P}(E)$ on a $f_A(X) = A \cap X \in \mathcal{P}(A)$, et réciproquement, si $X \in \mathcal{P}(A)$ alors $f_A(X) = A \cap X = X$. Donc $f_A(\mathcal{P}(E)) = \mathcal{P}(A)$. De la même manière, $g_A(\mathcal{P}(E))$ est l'ensemble des parties de E contenants A.
   (d) On a $f_A(A) = f_A(E) = A$, donc pour que f_A soit injective il faut que $A = E$. Cette condition étant aussi suffisante, on peut dire que f_A est injective si et seulement si $A = E$.
   Aussi, $f_A(\mathcal{P}(E)) = \mathcal{P}(A)$, donc f_A est surjective si et seulement si $A = E$.
   De la même façon il y a équivalence entre g_A est injective, g_A est est surjective, et $A = \emptyset$.
2. Quelques équations dans $\mathcal{P}(E)$.
   (a) i. Pour tout $X \subset E$ on a $A \cap X \subset A$. Donc si $A \cap X = B$ alors $B \subset A$. Finalement, si $B \not\subseteq A$ alors cette équation n'admet pas de solution.
      ii. On suppose que $B \subseteq A$ et on considère une partie X de E. On a $X = X \cap \left(A \cup \overline{A}\right) = (X \cap A) \cup Y$ avec $Y = X \cap \overline{A}$. IL est clair que $Y \subset \overline{A}$. Donc si $A \cap X = B$ alors $X = B \cup Y$, et réciproquement, si $X = B \cup Y$ où $Y \subset \overline{A}$ alors $A \cap X = A \cap (B \cup Y) = (A \cap B) \cup (A \cap Y)$. Comme $B \subset A$ alors $A \cap B = B$ et comme $Y \subset \overline{A}$ alors $A \cap Y = \emptyset$, donc $A \cap X = B$.
      Finalement, X est une solution de cette équation si et seulement si X est de la forme $X = B \cup Y$ où $Y \subset \overline{A}$.

iii. Conclusion : si $B \not\subseteq A$ alors cette équation n'admet pas de solution, et si $B \subseteq A$ alors l'ensemble de solutions est l'ensemble des parties X de E de la forme $X = B \cup Y$ où $Y \subset \overline{A}$.

(b) Considérons dans $\mathcal{P}(E)$ l'équation $A \cup X = B$.

Méthode 1 Soit X une solution de l'équation $A \cup X = B$. comme $A \subset A \cup X$ alors $A \subset B$. de là on peut déduire que si $A \not\subseteq B$ alors cette équation n'admet pas de solution. Supposons alors que $A \subset B$. Pour la même raison, si $A \cup X = B$ alors

$$X = X \cup \left(A \cap \overline{A}\right) = (X \cup A) \cap (X \cup \overline{A}) = B \cap Y$$

avec $Y = X \cup \overline{A} \supset \overline{A}$. Réciproquement, si $X = B \cap Y$ où $\overline{A} \subset Y$ alors $A \cup X = A \cup (B \cap Y) = (A \cup B) \cap (A \cup Y) = B \cap E = B$.
Conclusion : si $A \not\subseteq B$ alors cette équation n'admet pas de solution, et si $A \subset B$ alors l'ensemble de solutions est l'ensemble des parties X de E de la forme $X = B \cap Y$ où $\overline{A} \subset Y$.

Méthode 2
$$\begin{aligned} A \cup X = B &\iff \overline{A} \cap \overline{X} = \overline{B} \\ &\iff \overline{B} \subset \overline{A} \text{ et } \overline{X} = \overline{B} \cup Y \text{ où } Y \subset A \\ &\iff A \subset B \text{ et } X = B \cap \overline{Y} \text{ où } Y \subset A \\ &\iff A \subset B \text{ et } X = B \cap Y \text{ où } \overline{Y} \subset A \\ &\iff A \subset B \text{ et } X = B \cap Y \text{ où } \overline{A} \subset Y \end{aligned}$$

D'où le résultat.

(c) Une condition nécessaire pour que ce système admette une solution est que $B \subset A \subset C$. Supposons que cette condition est vérifiée. On a alors $A \cap X = B$ si et seulement si $X = B \cup Y$ où $Y \subset \overline{A}$. Dans ce cas
$$\begin{aligned} A \cup X = C &\iff A \cup Y = C \\ &\iff Y = C \cap Z \text{ où } \overline{A} \subset Z. \end{aligned}$$
Et comme $Y \subset \overline{A}$ alors $Y = Y \cap \overline{A} = \overline{A} \cap C \cap Z$ où $\overline{A} \subset Z$
Donc $Y = \overline{A} \cap C$ et par suite $X = B \cup (\overline{A} \cap C)$. Réciproquement, il est facile de vérifier que $B \cup (\overline{A} \cap C)$ est une solution du système.

2.4 Relation binaires

Exercice 41

Soit E un ensemble et f une application bijective de E dans E. Pour tout $n \in \mathbb{N}^\star$, on pose $f^n = f \circ f \circ \ldots \circ f$ (f répété n fois), $f^{-n} = (f^{-1})^n$ et $f^0 = id_E$. On définit dans E la relation $\mathcal{R}$ par :

$$\forall (x, y) \in E^2 \ , \ x \mathcal{R} y \Longleftrightarrow (\exists n \in \mathbb{Z} \ , \ y = f^n(x))$$

1. Démontrer que $\mathcal{R}$ est une relation d'équivalence sur E. (On admettra que $\forall (n, p) \in \mathbb{Z}^2$, $f^n o f^p = f^{n+p}$).
2. Montrer que si C est une classe d'équivalence modulo $\Re$, alors $f(C) = C$.
3. Démontrer quetoute partie X non vide de E telle que $f(X) = X$ est une réunion de classes d'équivalence pour $\mathcal{R}$.

Réponse 41

1. Soient $x, y, z \in E$.
   — On a bien $x = f^0(x)$, et donc $x \mathcal{R} x$. La relation est alors réflexive.
   — Supposons que $x \mathcal{R} y$. Il existe donc $n \in \mathbb{Z}$ tel que $y = f^n(x)$. En composant par f^{-1} on obtient $x = f^{-1}(y)$ ce qui donne $y \mathcal{R} x$. Donc la relation est symétrique.

— Supposons que $x\mathcal{R}y$ et $y\mathcal{R}z$. Il existe donc $m, n \in \mathbb{Z}$ tels que $y = f^m(x)$ et $z = f^n(y)$. Il s'ensuit que $z = f^n\left(f^m(x)\right) = f^{m+n}(x)$. Ainsi $x\mathcal{R}z$ et $\mathcal{R}$ est transitive.

Conclusion : $\mathcal{R}$ est une relation d'équivalence.

2. Soit C une une classe d'équivalence modulo $\mathcal{R}$. Soit $x \in C$. On a $x\mathcal{R}f^{-1}(x)$, donc $f^{-1}(x) \in C$ et par suit $x = f\left(f^{-1}(x)\right) x \in f(C)$. Ainsi $C \in f(C)$. Soit maintenant $y \in f(C)$. Il existe alors $x \in C$ tel que $f(x) = y$. Ainsi $x\mathcal{R}y$ puis $y \in C$ et ensuite $f(C) \subset C$. Finalement, $f(C) = C$.
3. Notons C_x, pour tout $x \in E$, la classe d'équivalence de x. Soit X une partie non vide de E telle que $f(X) = X$. Il suffit de montrer que :

$$X = \bigcup_{x \in X} C_x.$$

Soit $a \in X$. Comme $a \in C_a$ (car $x\mathcal{R}$), alors $a \in \bigcup_{x \in X} C_x$. Donc $X \subset \bigcup_{x \in X} C_x$. Réciproquement, soit $a \in \bigcup_{x \in X} C_x$. Il existe donc $x \in X$ tel que $x \in C_x$; c'est à dire $a\mathcal{R}x$. Il existe donc $n \in \mathbb{Z}$ tel que $a = f^n(x)$. Or f est bijective et $f(X) = X$, donc on peut montrer que $f^n(X) = X$. Ainsi $a \in X$ et on a $X = \bigcup_{x \in X} C_x$.

Exercice 42

Soit E un ensemble. Vérifier que la relation $\mathcal{R}$ définie dans P par :

$$A\mathcal{R}B \Longleftrightarrow A = B \text{ ou } A = \overline{B}$$

est une relation d'équivalence

Réponse 42

Soit A, B, C trois parties de E.

— On a $A\mathcal{R}A$ puisque $A = A$. Donc $\mathcal{R}$ est réflexive.

— Supposons que $A\mathcal{R}B$. Donc $A = B$ ou $A = \overline{B}$. Si $A = B$ alors $B = A$ puis $B\mathcal{A}$. Si $A = \overline{B}$ alors $\overline{A} = \overline{\overline{B}} = B$, ce qui implique que $B\mathcal{R}A$. Ainsi la relation est symétrique.

— Supposons que $A\mathcal{R}B$ et $B\mathcal{R}C$. Alors $A = B$ ou $A = \overline{B}$. Si $A = B$ alors $A\mathbb{C}$. Si $A = \overline{B}$ alors $B = \overline{A}$. On en déduit que $\overline{A} = C$ ou $\overline{A} = \overline{C}$, c'est à dire $\overline{A} = C$ ou $A = C$, donc $A\mathcal{R}C$. Ainsi $\mathcal{R}$ est transitive.

Donc $\mathcal{R}$ est une relation d'équivalence.

Exercice 43

On définit sur $\mathbb{R}$ la relation :

$$x\mathcal{R}y \Longleftrightarrow x^3 - y^3 = 3(x - y)$$

.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Déterminer, pour tout réel x, le cardinal de la classe d'équivalence de x.

Réponse 43

1. Soit $x, y, z \in \mathbb{R}$.
   - On a $x\mathcal{R}x$ puisque $x^3 - x^3 = 3(x - x) = 0$. Donc $\mathcal{R}$ est réflexive.
   - Supposons que $x\mathcal{R}y$. Donc $x^3 - y^3 = 3(x - y)$, ou encore $y^3 - x^3 = 3(y - x)$. Ainsi $y\mathcal{R}x$ et la relation est symétrique.
   - Supposons que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $x^3 - y^3 = 3(x - y)$ et $y^3 - z^3 = 3(y - z)$. En sommant ces deux identités on obtient $x^3 - z^3 = 3(x - z)$, donc $x\mathcal{R}z$ et la relation $\mathcal{R}$ est transitive.

   Donc $\mathcal{R}$ est une relation d'équivalence.
2. Soit $x \in \mathbb{R}$. Pour tout $y \in \mathbb{R}$ on a :

$$\begin{aligned} x\mathcal{R}y &\Leftrightarrow x^3 - y^3 = 3(x - y) \\ &\quad (x - y)\left(x^2 + xy + y^2 - 3\right) = 0 \\ &\quad x = y \text{ ou } x^2 + xy + y^2 - 3 = 0 \end{aligned}$$

   On est invité donc à résoudre dans $\mathbb{R}$ l'équation $x^2 + xy + y^2 - 3 = 0$ (d'inconnu y) . Le discriminant de cette équation est égal à $\Delta_x = x^2 - 4(x^2 - 3) = -3x^2 + 12$. Donc, $\Delta_x \geq 0 \Leftrightarrow |x| \leq 2$. Dans ce cas, l'équation admet deux solutions (qui peuvent être égales) $y_1 = \dfrac{-x - \sqrt{12 - 3x^2}}{2}$ et $y_2 = \dfrac{-x + \sqrt{12 - 3x^2}}{2}$. Notons que $y_1 = y_2$ si et seulement si $\Delta_x = 0$; c'est à dire si $x = \pm 2$. Notons aussi que x est solution de cette équation si et seulement si $3x^2 - 3 = 0$; c'est à dire si $x = \pm 1$ La classe d'équivalence de x est donc égale à

$$C(x) = \begin{cases} \{x\} & , \text{ si } |x| > 2 \\ \left\{x, \dfrac{-x - \sqrt{12 - 3x^2}}{2}, \dfrac{-x + \sqrt{12 - 3x^2}}{2}\right\} & , \text{ si } |x| \leq 2 \end{cases}$$

   Ainsi, le cardinal de la classe d'équivalence de x est égal à

$$\text{card}(C(x)) = \begin{cases} 1 & , \text{ si } |x| > 2 \\ 2 & , \text{ si } x = \pm 2 \text{ ou } x = \pm 1 \\ 3 & , \text{ sinon} \end{cases}$$

Exercice 44

Montrer que la relation $\Re$ définie dans $\mathbb{R}$ par :

$$x\Re y \Longleftrightarrow xe^y = ye^x$$

est une relation d'équivalence.

Réponse 44

Il clair que $x\mathcal{R}x$ est réflexive et symétrique. Montrons qu'elle est transitive. Pour cela, soit $x, y, z \in \mathbb{R}$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $xe^y = ye^x$ et $ye^z = ze^y$. Donc $xe^ye^z = ye^ze^x$ et par suite $xe^ye^z = ze^ye^x$ puis $xe^z = ze^x$; c'est à dire que $x\mathcal{R}z$. Donc $\mathcal{R}$ est transitive et par la suite c'est une relation d'équivalence.

Exercice 45

Étudier la relation $\Re$ défini dans $\mathbb{N}$ par :

$$x\Re y \Longleftrightarrow \exists n \in \mathbb{N}, y = x^n$$

Réponse 45

Il est façile de montrer que cette relation est réflexive et transitive. Montrons qu'elle est antisymétrique. Pour cela, considérons $x, y \in \mathbb{N}$ tels que $x\mathcal{R}y$ et $y\mathcal{R}x$. Il existe donc $m, n \in \mathbb{N}$ tels que $x = y^m$ et $y = x^n$. On en déduit que $x^{mn} = x$. Remarquons d'abord que si $x = 0$ alors, puisque $x = y^m$, on aura $y = 0$. Si $x \neq 0$ alors $x^{mn-1} = 1$ et par suite $x = 1$ ou $mn = 1$. Or, si $x = 1$ alors $y = 1$, et si $mn = 1$, comme $m, n \in \mathbb{N}$, alors $m = n = 1$ et par conséquent $x = y$. La relation est donc antisymétrique. Donc $\mathcal{R}$ est une relation d'ordre.

Exercice 46

Soit $(E, \leq)$ un ensemble ordonné .Pour tout $x \in E$ on définit la partie notée $\varphi(x)$ par :

$$\varphi(x) = \{t \in E \ / \ t \leq x\}$$

1. Démontrer que
$$\forall (x, y) \in E^2 \ , \ x \leq y \iff \varphi(x) \subset \varphi(y)$$
2. Démontrer que φ est une injection de E dans $\mathcal{P}(E)$.
3. φ est-ce une surjection ?
4. Réciproquement , Soit ϕ une injection de E dans $\mathcal{P}(E)$.On définit la relation $\Re$ par :
$$\forall (x, y) \in E^2 \ , \ x\Re y \iff \phi(x) \subset \phi(y)$$
Démontrer que $\Re$ est une relation d'ordre .

Réponse 46

1. Soit $(x, y) \in E^2$.
   (a) Supposons que $x \leq y$ .Soit $t \in \varphi(x)$ donc $t \leq x \leq y$ donc par définition de $\varphi(y)$ on a $t \in \varphi(y)$ et par suite $\varphi(x) \subset \varphi(y)$
   (b) Supposons que $\varphi(x) \subset \varphi(y)$ et montrons que $x \leq y$.On a $x \in \varphi(x)$ donc $x \in \varphi(y)$ et par suite $x \leq y$ d'où le résultat
2. Soit $(x, y) \in E^2$ tel que $\varphi(x) = \varphi(y)$, montrons que $x = y$ .On a $\varphi(x) \subset \varphi(y)$ *et* $\varphi(y) \subset \varphi(x)$ donc d'après la question précédente on a $x \leq y$ *et* $y \leq x$ d'où $x = y$ d'où le résultat .
3. D'après l'exercice 3 φ n'est pas surjective
4. Montrons que la relation ainsi définie est une relation d'ordre .
   (a) Soit $x \in E$ on a $\varphi(x) \subset \varphi(x)$ donc $x\Re x$ et par suite $\Re$ est réflexive
   (b) Soit $(x, y) \in E^2$ tel que $x \leq y$ et $y \leq x$, donc $\varphi(x) = \varphi(y)$ or φ est injective donc $x = y$, d'où $\Re$ est antisymétrique
   (c) Soit $(x, y, z) \in E^3$ tel que $x \leq y$ *et* $y \leq z$, donc $\varphi(x) \subset \varphi(y)$ *et* $\varphi(y) \subset \varphi(z)$ donc $\varphi(x) \subset \varphi(z)$ donc $x \leq z$ d'où $\Re$ est transitive et par suite $\Re$ est une relation d'ordre.

Exercice 47 Solution

On définit sur $\mathbb{R}^2$ la relation notée $\mathcal{R}$ par :

$$\forall x, x', y, y' \in \mathbb{R}, \quad (x, y)\mathcal{R}(x', y') \iff |x - x'| \leq y' - y.$$

1. Montrer qu'il s'agit d'une relation d'ordre.
2. Cet ordre est-il total ?

3. Représenter sur le plan $\mathbb{R}^2$ l'ensemble des majorants et l'ensemble des minorants d'un couple $(a,b) \in \mathbb{R}^2$.

Réponse 47

1. Soit $(x,y),\ \ (x',y')),\ \ (x'',y'') \in \mathbb{R}^2$.

   Réflexivité. On a $|x-x| = 0 \leq y-y = 0$, donc $(x,y)\mathcal{R}(x,y)$ et par suite la relation est réflexive.

   Antisymétrie. Supposons que $(x,y)\mathcal{R}(x',y')$ et $(x',y')\mathcal{R}(x,y)$. Alors $|x-x'| \leq y'-y$ et $|x'-x| \leq y-y'$. En sommant ces inégalités on obtient que $|x-x'| \leq 0$, et donc $x = x'$. Ainsi $0 \leq y'-y$ et $0 \leq y-y'$, ce qui entraine que $y = y'$. La relation est donc antisymétrique.

   Transitivité. Supposons que $(x,y)\mathcal{R}(x',y')$ et $(x',y')\mathcal{R}(x'',y'')$. Alors $|x-x'| \leq y'-y$ et $|x'-x''| \leq y''-y'$, et par conséquent $|x-x''| \leq |x-x'|+|x'-x''| \leq y'-y+y''-y' = y''-y$. D'où la transitivité.

   Conclusion : Il s'agit bien d'une relation d'ordre.

2. Les éléments $(0,0)$ et $(1,0)$ ne sont pas comparables ; c'est à dire que $(0,0)$ n'est pas en relation avec $(1,0)$ et $(1,0)$ n'est pas en relation avec $(0,0)$. Donc c'est un ordre partiel.

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

$$\begin{array}{rcl}(a,b)\mathcal{R}(x,y) & \iff & |x-a| \leq y-b \\ & \iff & b-y \leq x-a \leq y-b \\ & \iff & -x+a+b \leq y \text{ et } x-a+b \leq y\end{array}$$

   et

$$\begin{array}{rcl}(x,y)\mathcal{R}(a,b) & \iff & |x-a| \leq b-y \\ & \iff & y-b \leq x-a \leq b-y \\ & \iff & y \leq x-a+b \text{ et } y \leq -x+a+b\end{array}$$

   Donc le lieu géométrique des majorants du couple (a,b) est situé au dessus des droites d'équations $x-a+b = y$ et $-x+a+b = y$, et celui de ses minorants est situé au dessous des droites d'équations $x-a+b = y$ et $-x+a+b = y$.

Exercice 48 Solution

On définit sur $\mathbb{R}^2$, pour $n \in \mathbb{N}$, la relation notée $\mathcal{R}_n$ par :

$$\forall x,a,y,b \in \mathbb{R}, \quad (x,y)\mathcal{R}_n(a,b) \iff x^n+y^n = a^n+b^n.$$

1. Montrer qu'il s'agit d'une relation d'équivalence.
2. Dessiner sur le plan $\mathbb{R}^2$ la classe d'équivalence de $(1,1)$ pour $n = 1$ et $n = 2$.

Réponse 48

1. Soit $(a,b),\ \ (x,y)),\ \ (z,t) \in \mathbb{R}^2$ et $n \in \mathbb{N}$.

   Réflexivité. On a $x^n+y^n = x^n+y^n$, donc $(x,y)\mathcal{R}_n(x,y)$ et par suite la relation est réflexive.

   Symétrie.
$$\begin{array}{rcl}(x,y)\mathcal{R}_n(a,b) & \implies & x^n+y^n = a^n+b^n \\ & \implies & a^n+b^n = x^n+y^n \\ & \implies & (a,b)\mathcal{R}_n(x,y)\end{array}$$
   La relation est donc symétrique.

   Transitivité. Supposons que $(x,y)\mathcal{R}_n(a,b)$ et $(a,b)\mathcal{R}_n(z,t)$. Alors $x^n+y^n = a^n+b^n = z^n+t^n$ et la transitivité en découle.

Conclusion : Il s'agit bien d'une relation d'équivalence.

2. Pour tout $(x, y) \in \mathbb{R}^2$ on a $(x, y)\mathcal{R}_n(1, 1) \Longleftrightarrow x^n + y^n = 2$. Pour $n = 1$, le lieu géométrique de la classe d'équivalence de $(1, 1)$ il s'agit de la droite d'équation $x + y = 2$, et Pour $n = 2$ c'est le cercle d'équation $x^2 + y^2 = 2$, donc de centre l'origine du repère et de rayon $\sqrt{2}$.

Exercice 49

Soit $(E, \leq)$ un ensemble totalement ordonné et $f : E \longrightarrow E$ une application bijective de E vers E.. On dit qu'un élément $x \in E$ est strictement inférieur à un élément $y \in E$ et on écrit $x < y$ si $x \leq y$ et $x \neq y$. On suppose que f est strictement croissante ; c'est à dire :

$$\forall\, (x, y) \in E^2,\ x < y \Longrightarrow f\,(x) < f\,(y)$$

1. Montrer que f^{-1} est strictement croissante.
2. Montrer que si toute partie non vide de E admet un plus petit élément alors f est l'application identique.

Réponse 49

1. Soit $(x, y) \in E^2$ tels que $x < y$. Si $f^{-1}(x) \geq f^{-1}(y)$ alors, comme f est croissante, on aura $f(f^{-1}(x)) \geq f(f^{-1}(y))$, donc $x \geq y$, ce qui est faux. Donc $f^{-1}(x) < f^{-1}(y)$ et f^{-1} est strictement croissante.
2. Montrons d'abord que $\forall x \in E,\ x \leq f(x)$. Pour cela, Supposons qu'il existe au moins un élément $a \in E$ tel que $f(a) < a$. Ainsi l'ensemble $A = \{x \in E \ /\ f(x) < x\}$ est non vide, et par la suite il admet un plus petit élément b. Dans ce cas, puisque f est strictement croissante, $f(f(b)) < f(b)$ et par conséquent $f(b) \in A$. Ceci aboutit à une contradiction ; car $f(b) < b$ et $b = \min A$. Ainsi, $\forall x \in E,\ x \leq f(x)$. En appliquant ce résultat aussi à f^{-1}, qui est strictement croissante, nous déduisons que $\forall x \in E,\ x \leq f^{-1}(x)$, ce qui permet de déduire, en composant par f, que $\forall x \in E,\ f(x) \leq x$. Ainsi, $f(x) = x$ pour tout $x \in E$ et$f$ est l'application identique.

Chapitre 3

Arithmétique des entiers

3.1 Divisibilité, congruence

Exercice 50

1. Montrer que $671 \equiv 5 \ [6]$ et en déduire que $671^{800} - 1$ est divisible par 6.
2. Montrer que $2 \times 7^{2018} + 3 \times 5^{2018} - 5$ est divisible par 24.

Réponse 50

1. On a :
$$\begin{aligned} 671 &= 600 + 7.10 + 1 \\ &\equiv 0 + 10 + 1 \ [6] \\ &\equiv 5 \ [6] \end{aligned}$$
Comme $5 \equiv -1 \ [6]$, alors $671^{800} - 1 \equiv (-1)^{800} - 1 \equiv 0 \ [6]$, et par suite $671^{800} - 1$ est divisible par 6.
2. Puisque $7 \equiv 1 \ [3]$, $7 \equiv -1 \ [8]$ et $5^2 \equiv 1 \ [8]$ alors : $7^{2018} \equiv 1 \ [3]$ et $7^{2018} \equiv 5^{2018} \equiv 1 \ [8]$, et par suite $2 \times 7^{2018} + 3 \times 5^{2018} - 5 \equiv 0 \ [3]$ et $2 \times 7^{2018} + 3 \times 5^{2018} - 5 \equiv 2 + 3 - 5 \ [8] \equiv 0 \ [8]$. Ainsi, $2 \times 7^{2018} + 3 \times 5^{2018} - 5$ est divisible par 3 et 8, et comme $3 \wedge 8 = 1$, alors il est divisible par 24.

Exercice 51

Soit n est un entier naturel. Montrer que :

1. $n^3 - n$ est divisible par 3.
2. $n - 1$ divise $n^4 - 1$.
3. $n + 2$ divise $n^3 + 7n^2 + 16n + 12$.
4. $9n^2 - 6n - 1 + (-2)^n$ est divisible par 27.
5. $3^{2n+1} + 2^{6n+3}$ est divisible par 11.
6. n^2 divise $(n + 1)^n - 1$.
7. La somme des cubes de 3 entiers consécutifs est un multiple de 9.
8. $10^{9n+2} + 10^{6n+1} + 1$ est divisible par 111.

Réponse 51

1. On a soit $n \equiv 0 \ [3]$, soit $n \equiv 1 \ [3]$, soit $n \equiv 2 \ [3]$. Dans les trois cas on a $n^3 \equiv n \ [3]$, d'où $n^3 - n$ est divisible par 3
2. $n-1$ divise $n^4 - 1$.
3. Comme $n \equiv -2 \ [n+2]$ alors

$$\begin{aligned} n^3 + 7n^2 + 16n + 12 &\equiv (-2)^3 + 7.(-2)^2 + 16.(-2) + 12 \ [n+2] \\ &\equiv 0 \ [n+2] \end{aligned}$$

   $n+2$ divise $n^3 + 7n^2 + 16n + 12$.
4. En posant $A_n = 9n^2 - 6n - 1 + (-2)^n$ pour tout $n \in \mathbb{N}$ on a $A_{n+1} = 9n^2 + 18n - 6n - 2(-2)^n$ puis $A_{n+1} + 2A_n = 27n$. Une simple récurrence maintenant aboutit au résultat. $9n^2 - 6n - 1 + (-2)^n$ est divisible par 27
5. En effet :

$$\begin{aligned} 3^{2n+1} + 2^{6n+3} &\equiv 3^{2n+1} + 8^{2n+1} \ [11] \\ &\equiv 3^{2n+1} + (-3)^{2n+1} \ [11] \\ &\equiv 3^{2n+1} - 3^{2n+1} \ [11] \\ &\equiv 0 \ [11] \end{aligned}$$

   $3^{2n+1} + 2^{6n+3}$ est divisible par 11.
6. Pour $n = 0$ et $n = 1$ c'est évident, et pour $n \geq 2$ c'est on applique la formule du binôme de Newton :

$$\begin{aligned} (n+1)^n - 1 &= \sum_{k=1}^{n} \binom{n}{k} n^k \\ &= n^2 + \sum_{k=2}^{n} \binom{n}{k} n^k \\ &= n^2 \left(1 + \sum_{k=2}^{n} \binom{n}{k} n^{k-2} \right) \end{aligned}$$

   Ainsi n^2 divise $(n+1)^n - 1$
7. En posant $A_n = n^3 + (n+1)^3 + (n+2)^3$ pour tout $n \in \mathbb{N}$ alors

$$\begin{aligned} A_{n+1} - A_n &= (n+3)^3 - n^3 \\ &= 9n^2 + 27n + 27 \\ &\equiv 0 \quad [9]. \end{aligned}$$

   Puisque A_0 est divisible par 9, alors le résultat se découle par récurrence.
8. En remarquant que $10^2 \equiv -11 \ [111]$ alors $10^3 \equiv 1 \ [111]$ puis :

$$\begin{aligned} 10^{9n+2} + 10^{6n+1} + 1 &\equiv 10^2 . \left(10^3\right)^{3n} + 10. \left(10^3\right)^{2n} + 1 \ [111] \\ &\equiv -11 + 10 + 1 \ [111] \\ &\equiv 0 \ [111] \end{aligned}$$

   D'où le résultat.

Exercice 52

Soient $n, d \in \mathbb{N}$. Montrer que si d divise $13n + 1$ et $-26n + 4$ alors $d = 1$, $d = 2$, $d = 3$ ou $d = 6$.

Réponse 52

Si d divise $13n + 1$ et $-26n + 4$ alors d divise aussi $2(13n + 1) + (-26n + 4) = 6$. On en déduit que $d = 1$, $d = 2$, $d = 3$ ou $d = 6$.

Exercice 53

Trouver tous les entiers naturels n tels que $2n+3$ divise $3n+7$.

Réponse 53

Soit $n \in \mathbb{N}$ et supposons que $2n+3$ divise $3n+7$. Comme $3n+7 = (2n+3)+(n+4)$ alors $2n+3$ divise $n+4$, ce qui entraine que $2n+3 \leq n+4$ puis $n \leq 1$, c'est à dire que $n = 0$ où $n = 1$. Mais pour $n = 0$, la valeur $2n+3 = 3$ ne divise pas $3n+7 = 7$, alors que pour $n = 0$, la valeur $2n+3 = 5$ divise bien $3n+7 = 10$. Comme conclusion, $2n+3$ divise $3n+7$ si et seulement si $n = 1$.

Exercice 54

En remarquant que $10 \equiv -1$ [11], et en utilisant l'écriture décimal d'un entier, donner un critère de divisibilité par 11.

Réponse 54

Soit n un entier naturel dont l'écriture dans la base 10 est $n = a_d a_{d-1} \cdots a_0$. Donc, $n = 10^d a_d + 10^d d - 1 a_{d-1} + \cdots + 10a_1 + a_0$, et par suite, $n \equiv a_0 - a_1 + a_2 + \cdots + (-1)^d a_d$ [11]. On en déduit que n est divisible par 11 si et seulement si $a_0 - a_1 + a_2 + \cdots + (-1)^d a_d$ est divisible par 11.

Exercice 55

1. Soit $a \in \mathbb{Z}$. Montrer que le reste de la division euclidienne de a^2 par 8 est égal à $0, 1$ ou 4.
2. Soit $n \in \mathbb{N}$. Montrer que si 8 divise $n-7$, alors n ne peut pas être la somme de trois carrés d'entiers.

Réponse 55

1. Soit $a \in \mathbb{Z}$. Alors a est congru, modulo 8, à $0,\ \pm 1,\ \pm 2,\ \pm 3$ ou 4. D'où, a^2 est congru, modulo 8, à $0,\ 1$ ou 4, car $3^2 \equiv 1$ [8] ou $4^2 \equiv 0$ [8]. Ainsi, le reste de la division euclidienne de a^2 par 8 est égal à $0, 1$ ou 4.
2. Soit $n \in \mathbb{N}$, et supposons que n est la somme de de trois carrés d'entiers. Donc, d'après la première question, n est congru, , modulo 8, à l'une des valeurs suivante : $0+0+0 = 0,\ 0+0+1 = 1,\ 0+0+4 = 4,\ 0+1+1 = 2,\ 0+1+4 = 5,\ 0+4+4 = 8 \equiv 1$ [8], $1+1+1 = 3,\ 1+1+4 = 6,\ 1+4+4 = 9 \equiv 2$ [8], $4+4+4 = 12 \equiv 4$ [8]. Ainsi, le reste de la division Euclidienne de n par 8 est $0,\ 1,\ 2,\ 3,\ 4,\ 5$ ou 6. Dans tous les cas, 8 ne divise pas $n-7$, d'où le résultat.

Exercice 56

1. Quel est le reste dans la division euclidienne de $451 \times 6^{43} - 912$ par 7.
2. Quel est le chiffre des unités dans l'écriture décimal de 7^{98}.

Réponse 56

1. On a :

$$\begin{aligned} 451 \times 6^{43} - 912 &= (4.10^2 + 5.10 + 1) \times 6^{43} - 9.10^2 - 10 - 2 \\ &\equiv (4.3^2 - 2.3 + 1) \times (-1)^{43} - 2.3^2 - 3 - 2 \ \ [7] \\ &\equiv (4.2 + 1 + 1) \times 1 - 4 - 3 - 2 \ \ [7] \\ &\equiv (1 + 1 + 1) - 2 \ \ [7] \\ &\equiv 1 \ \ [7] \end{aligned}$$

Donc, le reste dans la division euclidienne de $451 \times 6^{43} - 912$ par 7 est égal à 1.

2. On a :
$$\begin{aligned} 7^{98} &\equiv (-3)^{98} \ [10] \\ &\equiv 9^{49} \ [10] \\ &\equiv (-1)^{49} \ [10] \\ &\equiv -1 \ [10] \\ &\equiv 9 \ [10] \end{aligned}$$
Ainsi, le chiffre des unités dans l'écriture décimal de 7^{98} es 9.

Exercice 57

On pose : $A_n = 10^{9n} + 2 \times 10^{6n} + 2 \times 10^{3n} + 1$ pour tout $n \in \mathbb{N}$.

1. Déterminer le reste de la division de A_n par 111.
2. Montrer que si n est impair alors A_n est divisible par 7, 11 et 13.
3. Montrer que si n est pair alors A_n a le même reste dans les divisions par 7, par 11 et par 13.
4. Trouver, suivant les valeurs de n, le reste de la division de A_n par 1001.

Réponse 57

1. En remarquant que $10^3 = 9.111 + 1 \equiv 1 \ [111]$, on déduit que $A_n \equiv 6 \ [111]$, c'est à dire que le reste de la division de A_n par 111 est égal à 6.
2. Remarquons que
$$\begin{aligned} 10^3 &= 10^3 \\ &\equiv 2^3 \ [7] \\ &\equiv -1 \ [7], \end{aligned}$$
et de la même manière on a $10^3 \equiv -1 \ [11]$, et $10^3 \equiv -1 \ [13]$. Ainsi, si n est impair, en posant $k = 7$, 11 ou 13 alors
$$\begin{aligned} A_n &\equiv -1 + 2 - 2 + 1 \ [k] \\ &\equiv 0 \ [k]. \end{aligned}$$
et par suite A_n est divisible par 7, 11 et 13.
3. Supposons que n est pair. En appliquant la même remarque que précédemment, en posant $k = 7$, 11 ou 13 on a
$$\begin{aligned} A_n &\equiv 1 + 2 + 2 + 1 \ [k] \\ &\equiv 6 \ [k]. \end{aligned}$$
Donc, le reste dans les divisions par 7, par 11 et par 13 est égal à 6.
4. On a
$$\begin{aligned} A_n &\equiv (-1)^{3n} + 2 \times (-1)^{2n} + 2(-1)^n + 1 \ [1001] \\ &\equiv (-1)^n + 2 + (-1)^n + 1 \ [1001] \\ &\equiv 2(-1)^n + 3 \ [1001]. \end{aligned}$$
Ainsi, le reste de la division de A_n par 1001 est égal à 5 si n est pair, et il est égal à 1 si n est pair

---

Exercice 58

On pose $S_n = 2^n + 3^n + 4^n + 5^n$ pour tout $n \in \mathbb{N}$ pour tout $n \in \mathbb{N}$.

1. Vérifier que le nombre 7 divise les nombres 2^6-1, 3^6-1, 4^6-1 et 5^6-1.
2. Démontrer que $S_{n+6}-S_n$ est divisible par 7 pour tout $n\in\mathbb{N}$.
3. Montrer que si r est le reste de la division Euclidienne de n par 6, alors $S_n\equiv S_r[7]$.
4. Trouver les valeurs de n pour lesquelles S_n est divisible par 7.
5. On pose : $T_n=100^n+101^n+102^n+103^n$.
6. Démontrer que : $S_n\equiv T_n[7]$, puis en déduis les valeurs de n pour lesquelles T_n est divisible par 7.

Réponse 58

1. En effet, $2^6\equiv 8^2\equiv 1\ [7]$, $4^6\equiv(2^6)^2\equiv 1\ [7]$, $3^6\equiv 9^3\equiv 2^3\equiv 1\ [7]$ et $5^6\equiv(-2)^6\equiv 2^6\equiv 1\ [7]$. Donc, 7 divise les nombres 2^6-1, 3^6-1, 4^6-1 et 5^6-1.
2. Car pour tout $n\in\mathbb{N}$ on a ; $S_{n+6}-S_n=2^n(2^6-1)+3^n(3^6-1)+4^n(4^6-1)+5^n(5^6-1)$.
3. Soit r est le reste de la division Euclidienne de n par 6. On peut écrire alors n sous la forme $n=6n+r$. Ainsi,
$$\begin{aligned} S_n=2^n2^r+3^n3^r+4^n4^r+5^n5^r & \\ & 2^r+3^r+4^r+5^r, \text{ d'après la question (1)}\\ & \equiv S_r[7]\end{aligned}$$
4. Remarquons d'abord que $2\equiv -5\ [7]$ et $3\equiv -4\ [7]$. Donc, si n est impair alors $S_n\equiv 0\ [7]$. Supposons que n est pair. Dans ce cas, son reste, n, dans la division Euclidienne par 6 est égal à 0, 2 ou 4. Or $S_0=4$, $S_2\equiv 2(4+9)\equiv -2\ [7]$ $S_4\equiv 2(4^2+9^2)\equiv -2\ [7]$. Comme conclusion, S_n est divisible par 7, si et seulement si n est impair.
5. Sachant que 100, 101, 102 et 103 sont congrus respectivement, modulo 7, à 2, 3, 4 et 5, alors $S_n\equiv T_n[7]$ et, par suite, T_n est divisible par 7 si et seulement si n est impair.

Exercice 59

Trouver les restes des divisions euclidiennes de 3286^{374} par 10, 371^{238} par 5, 76^{748} par 12, $3^{3n+2}+2^{n+4}$ par 5, et $1+2^n+3^n+4^n$ par 4.

Réponse 59

On a
$$\begin{aligned} 3286^{374} &\equiv 6^{374}\ [10]\\ &\equiv 6\ [10],\end{aligned}$$
car, par une simple récurrence, $\forall n\in\mathbb{N}^*,\ \ 6^n\equiv 6\ [10]$. Donc le reste de la divisions euclidienne de 3286^{374} par 10 est 6.
Et on a
$$\begin{aligned} 371^{238} &\equiv 1^{238}\ [5]\\ &\equiv 1\ [5].\end{aligned}$$
Donc le reste de la divisions euclidienne de 371^{238} par 5, est 1.
De même,
$$\begin{aligned} 76^{748} &\equiv 4^{748}\ [12]\\ &\equiv 4\ [12],\end{aligned}$$
car, par une simple récurrence, $\forall n\in\mathbb{N}^*,\ \ 4^n\equiv 4\ [10]$. Donc le reste de la divisions euclidienne de 76^{748} par 12 est 4.
Aussi
$$\begin{aligned} 3^{3n+2}+2^{n+4} &\equiv (-2)^{3n+2}+2^{n+4}\ [5]\\ &\equiv (-2)^{3n}.4+2^n.16\ [5]\\ &\equiv -(-8)^n+2^n\ [5]\\ &\equiv -2^n+2^n\ [5]\\ &\equiv 0\ [5]\end{aligned}$$

Donc le reste de la divisions euclidienne de $3^{3n+2}+2^{n+4}$ par 5, est 0.
Et

$$\begin{aligned} 1+2^n+3^n+4^n &\equiv 1+2^n+(-1)^n+4^n \ \ [4] \\ &\equiv \begin{cases} 2 \ \ [4], \text{ si } n \geq 2 \text{ et pair} \\ 0 \ \ [4], \text{ si } n \geq 2 \text{ et impair} \\ 0 \ \ [4], \text{ si } n = 0 \\ 2 \ \ [4], \text{ si } n = 1. \end{cases} \end{aligned}$$

Donc le reste de la divisions euclidienne de $1+2^n+3^n+4^n$ par 4 est égal à 0 si $n=0$, ou si ($n \geq 2$ et impair), et il est égal à 1 si $n=0$, ou si ($n \geq 2$ et pair) .

Exercice 60

Soit p un nombre premier. Donner la classe modulo p du coefficient $\binom{p-1}{k}$ pour tout $k \in [\![0, p-1]\!]$

Réponse 60

Pour $k=0$ et $k=1$ on a $\binom{p-1}{k} \equiv (-1)^k \ \ [p]$. Supposons que ce résultat reste vrais pour un $k \in [\![0, p-2]\!]$. On a

$$\begin{aligned} (k+1)\binom{p-1}{k+1} &= (p-k-1)\binom{p-1}{k} \\ &\equiv (-k-1)\binom{p-1}{k} \ \ [p] \\ &\equiv (-1)^{k+1}(k+1) \ \ [p] \end{aligned}$$

Et comme $1 \leq k+1 \leq p-1$ alors $p \wedge (k+1) = 1$ puis $\binom{p-1}{k+1} \equiv (-1)^{k+1} \ \ [p]$, ce qui achève la preuve

---

3.2 pgcd, ppcm, nombres premiers entre eux

Exercice 61

Calculer $\text{pgcd}(n!+1, (n+1)!+1)$.

Réponse 61

Soit $d = \text{pgcd}(n!+1, (n+1)!+1)$. Alors d divise $n!+1$ et $(n+1)!+1$, puis aussi $(n+1)(n!+1) - ((n+1)!+1) = n$ et enfin aussi $n!+1-(n-1)!n = 1$. Donc $d=1$

Exercice 62

Calculer $\text{pgcd}\,(11a+5b, 13a+6b)$ et $\text{pgcd}\left(a^3-b^3, a^2-b^2\right)$ sachant que a et b sont deux entiers premiers entre eux.

Réponse 62

On a

$$\text{pgcd}\left(a^3-b^3, a^2-b^2\right) = |a-b|\delta$$

avec

$$\delta = (a+b) \wedge \left(a^2+ab+b^3\right)$$

Or, puisque $a^2+ab+b^2 = (a+b)(a+b)+ab$ alors $\delta = (a+b)\wedge(ab)$. Donc δ divise $a^2 = a(a+b)-ab$ et divise $b^2 = b(a+b)-ab$. Mais $a \wedge b = 1$, donc $a^2 \wedge b^2 = 1$ et par la suite $\delta = 1$. Conclusion :

$$\text{pgcd}\left(a^3-b^3, a^2-b^2\right) = |a-b|.$$

Exercice 63

Calculer $(a+b)\wedge a$, $a^n \wedge b^n$, $a^2 \wedge b^2 \wedge ab$ pour $(a,b) \in \mathbb{Z}^2$.

Réponse 63

Posons $a = da'$ et $b = db'$ avec $d = a \wedge b$ et $a' \wedge b' = 1$.

- Il est facile de voir que les diviseurs communs de a et b sont les mêmes diviseurs communs de a et $a+b$, donc $(a+b)\wedge a = a \wedge b$.
- On a $a^n \wedge b^n = d^n\left((a')^n \wedge (b')^n\right) = d^n$. Donc, $a^n \wedge b^n = (a \wedge b)^n$.
- On a $a^2 \wedge b^2 \wedge ab = d^2\left((a')^2 \wedge (b')^2 \wedge a'b'\right) = (a \wedge b)^2$

Exercice 64

Pour quelles valeurs de $n \in \mathbb{N}$, $\dfrac{n^3+n}{2n+1}$ est-il irréductible dans $\mathbb{Q}$?

Réponse 64

Soit d un diviseur premier commun de $n^3+n = n(n^2+1)$ et $2n+1$. Alors d divise n ou n^2+1. Or $n \wedge (2n+1) = 1$, et d divise $2n+1$, donc d ne divise pas n, mais il divise plutôt n^2+1. On en déduit que d divise aussi $2(n^2+1)-n(2n+1) = 2-n$, puis $2(2-n)+(2n+1) = 5$. Ainsi, $\dfrac{n^3+n}{2n+1}$ est réductible dans $\mathbb{Q}$ si, et seulement si, n^3+n et $2n+1$ sont divisibles par 5. Or, $2n+1 \equiv 0 \ \ [5]$ si et seulement si $4n \equiv -2 \ \ [5]$, si et seulement si $n \equiv 2 \ \ [5]$. Et dans ce cas, on a $n^3+n \equiv 0 \ \ [5]$. Finalement, pour tout $n \in \mathbb{N}$, $\dfrac{n^3+n}{2n+1}$ est irréductible dans $\mathbb{Q}$ si et seulement si $n \equiv 2 \ \ [5]$.

Exercice 65

Soient $a, b, p, q, s, r \in \mathbb{Z}$ tels que : $ps-qr = 1$. On pose $A = pa+qb$, $B = ra+sb$. Montrer que $a \wedge b = A \wedge B$.

Réponse 65

Il est clair que tout diviseur commun de a et b est aussi diviseur commun de A et B. Soit d un diviseur commun de A et B. Alors d divise aussi $rA-pB = (qr-ps)b = -b$ et $sA-qB = (ps-qr)a = a$. Ainsi, $a \wedge b = A \wedge B$.

Exercice 66

Soient $a, b, c, d \in \mathbb{Z}^*$. Montrer que si $a \wedge b = c \wedge d = 1$ alors $(ac) \wedge (bd) = (a \wedge d)\,(b \wedge c)$

Réponse 66

Posons $\delta_1 = a \wedge d$ et $\delta_2 = b \wedge c$. On peut écrire alors $a = \delta_1 a'$, $d = \delta_1 d'$, $b = \delta_2 b'$ et $c = \delta_2 c'$ avec $a' \wedge d' = b' \wedge c' = 1$. On a alors :

$$(ac) \wedge (bd) = \delta_1.\delta_2\left[(a'c') \wedge (b'd')\right]$$

Or, comme $a' \wedge b' = 1$ alors $a' \wedge b' = 1$, et puisque $a' \wedge d' = 1$ alors $a' \wedge (b'd') = 1$. De la même manière $c' \wedge (b'd') = 1$, et par suite $a'c' \wedge (b'd') = 1$. Ainsi

$$(ac) \wedge (bd) = \delta_1.\delta_2 = (a \wedge d)\,(b \wedge c)$$

Exercice 67

Montrer que $\text{ppcm}(1, 2, \cdots, 2n) = \text{ppcm}(n+1, n+2, \cdots, 2n)$.

Réponse 67

Il suffit de montrer que $1, 2, \cdots, 2n$ et $n+1, n+2, \cdots, 2n$ ont le mêmes multiples communs. En effet, d'une part, il est clair que tout multiple commun de $1, 2, \cdots, 2n$ est aussi un multiple commun de $n+1, n+2, \cdots, 2n$, car $\{n+1, n+2, \cdots, 2n\} \subset \{1, 2, \cdots, 2n\}$. D'autre part, soit m est un multiple commun de $n+1, n+2, \cdots, 2n$, et montrons que c'est un multiple commun de $1, 2, \cdots, 2n$. Pour cela, il suffit de montrer que c'est un multiple commun de $1, 2, \cdots, n$. Pour ce faire, considérons $d \in [\![1, n]\!]$, et posons $n = dq + r$ la division de n par d. Il s'ensuit que $n + (d - r)$ est un multiple de d, et comme m est un multiple de $n + (d - r)$, alors m est un multiple de d et par suite m est un multiple commun de $1, 2, \cdots, 2n$. Comme conséquence : $\text{ppcm}(1, 2, \cdots, 2n) = \text{ppcm}(n+1, n+2, \cdots, 2n)$.

Exercice 68

Soit $n \geq 2$ un entier naturel et $a_1, a_2, ..., a_n \in \mathbb{N}$. Posons

$$N = \prod_{k=1}^{n} a_k, \quad m = ppcm(a_1, a_2, ..., a_n) \text{ et } d = pgcd(a_1, a_2, ..., a_n)$$

Posons aussi $b_i = \dfrac{N}{a_i}$ pour tout $1 \leq i \leq n$, et

$$m' = ppcm(b_1, b_2, ..., b_n) \text{ et } d' = pgcd(b_1, b_2, ..., b_n).$$

Montrer que $N = md' = m'd$.

Réponse 68

Posons, pour tout $i \in [\![1, n]\!]$, $a_i = da'_i$ et $b_i = d'b'_i$, où $a'_1, \cdots, a'_n$ et $b'_1, \cdots, b'_n$ sont des entiers naturel tels que $pgcd(a'_1, \cdots, a'_n) = pgcd(b'_1, \cdots, b'_n) = 1$. D'après le théorème du Bézout, il existe des entiers $u_1, \cdots, u_n$ et $v_1, \cdots, v_n$ tels que $\sum_{i=1}^{n} u_i a'_1 = \sum_{i=1}^{n} v_i b'_1 = 1$.

— Remarquons que pour tout $j \in [\![1, n]\!]$ on a $\dfrac{N}{d} = a'_i b_i$, donc $\dfrac{N}{d}$ est un multiple commun de $b_1, b_2, \cdots, b_n$. Soit maintenant k un autre multiple commun de $b_1, b_2, ..., b_n$, et posons $k = k_i b_i$ pour tout $i \in [\![1, n]\!]$. On a alors

$$k = \sum_{i=1}^{n} u_i a'_i k = \sum_{i=1}^{n} u_i a'_i k_i b_i = \frac{N}{d} \sum_{i=1}^{n} u_i k_i.$$

Ainsi, $\dfrac{N}{d}$ est un multiple commun de k, ce qui montre que $\dfrac{N}{d} = ppcm(b_1, b_2, \cdots, b_n)$, ou encore, que $N = dm'$.

— On raisonne de la même manière. pour tout $j \in [\![1,n]\!]$ on a $\dfrac{N}{d'} = a_i b'_i$, donc $\dfrac{N}{d}$ est un multiple commun de $a_1, a_2, \cdots, a_n$. Soit maintenant k un autre multiple commun de $a_1, a_2, \cdots, a_n$, et posons $k = k_i a_i$ pour tout $i \in [\![1,n]\!]$. On a alors

$$k = \sum_{i=1}^{n} v_i b'_i k = \sum_{i=1}^{n} v_i b'_i k_i a_i = \frac{N}{d'} \sum_{i=1}^{n} v_i k_i$$

et par suite, $\dfrac{N}{d}$ est un multiple commun de k, puis que $\dfrac{N}{d} = ppcm(a_1, \cdots, a_n)$, et finalement $N = d'm$.

Remarque : On pourrait aussi montrer ce résultat en écrivant les a_i sous forme de produit de facteurs premiers ; $a_i = \prod_{j=1}^{s} p_j^{\alpha_{i,j}}$. On écrit donc les écriture sous forme de produit de facteurs premiers des nombres b_i, N, d, d', m et m', puis on se ramène à montrer une égalité dans $\mathbb{N}$ ne contenant que les opérations : la somme, le maximum et le minimum d'entiers naturels, facile à démontrer.

Exercice 69 *Les nombres de Mersenne*

Pour $n \in \mathbb{N}^*$, on pose $M_n = 2^n - 1$. Soient n et p deux entiers naturels non nuls tels que $p > n$, et soient q et r le quotient et le reste, respectivement, de la division euclidienne de p par n.

1. En supposons que $r \neq 0$, déterminer l'entier naturel Q tel que : $M_p = QM_n + M_r$. En déduire le quotient et le reste de la division euclidienne de M_p par M_n.
2. En effectuant les divisions successives de p par n d'une part, et de M_p par M_n d'autre part, montrer que : $M_n \wedge M_p = M_{n \wedge p}$.

Réponse 69

1. On a $p = nq + r$, donc,

$$\begin{aligned} M_p &= 2^p - 1 \\ &= (2^n)^q 2^r - 1 \\ &= (M_n + 1)^q \, 2^r - 1 \\ &= -1 + \sum_{k=0}^{q} \binom{q}{k} M_n^k 2^r \\ &= -1 + 2^r + \sum_{k=1}^{q} \binom{q}{k} M_n^k 2^r \\ &= QM_n + M_r \end{aligned}$$

avec $Q = \sum_{k=1}^{q} \binom{q}{k} M_n^{k-1} 2^r$. Comme $0 \leq r < n$, alors $2^0 - 1 \leq 2^r - 1 < 2^n - 1$, c'est à dire $0 \leq M_r < M_n$. Donc, le quotient et le reste de la division euclidienne de M_p par M_n sont A et M_r.

2. D'après la question précédente, si on note $r_1, \cdots, r_s$ les restes des divisions successives de p par n, r_1 étant le dernier reste non nul, alors $M_{r_1}, \cdots, M_{r_s}$ sont les restes des divisions successives de M_p par M_n, et M_{r_s} étant le dernier reste non nul. On en déduit que $M_n \wedge M_p = M_{r_s} = M_{n \wedge p}$.

Exercice 70 *Une application de l'algorithme d'Euclide*

Soient a, b deux entiers de $\mathbb{N}$ avec $a > b$ et $d = pgcd(a, b)$

1. Montrer que si c est divisible par a et b, alors cd est divisible par ab.
2. Soit $n \in \mathbb{N}^*$. Montrer à l'aide de l'algorithme d'Euclide que :
   $pgcd(n^a - 1, n^b - 1) = n^d - 1$.
3. En déduire que si a et b sont premiers entre eux, alors $(m^a - 1)(m^b - 1)$ divise $(m^{ab} - 1)(m - 1)$.

Réponse 70

1. Comme a et b divisent c alors d divisent c. Posons $a = da'$ et $b = db'$ et $c = dc'$. On a alors $a' \wedge b' = 1$ et a', b' divisent c'. Donc $a'b'$ divise c', puis $ab = d^2a'b'$ divise cd
2. Soit r le reste de la division Euclidienne de a par b et posons $a = kb + r$. Alors

$$\begin{aligned} n^a - 1 &= (n^b)^k.n^r - 1 \\ &\equiv n^r - 1 \quad [n^b - 1] \end{aligned}$$

   Donc $n^r - 1$ est le reste de la division Euclidienne de $n^a - 1$ par $n^b - 1$. Comme d est le dernier reste non nul dans l'algorithme d'Euclide appliqué à a et b, alors $n^d - 1$ est le dernier reste non nul dans l'algorithme d'Euclide appliqué à $n^a - 1$ et $n^b - 1$, ce qui montre que $n \in \mathbb{N}*$. Montrer à l'aide de l'algorithme $pgcd(n^a - 1, n^b - 1) = n^d - 1$.
3. D'après (2), $(m^a - 1) \wedge (m^b - 1) = (m - 1)$. D'autre part, $m^{ab} - 1$ est divisible par $m^a - 1$ et $m^b - 1$. On applique alors (1) pour conclure que $(m^a - 1)(m^b - 1)$ divise $(m^{ab} - 1)(m - 1)$.

Exercice 71 *Propriétés arithmétiques de la suite de Fibonacci*

Soit (u_n) la suite définie par ses deux premiers termes $u_0 = 0, u_1 = 1$, et par la relation de récurrence $u_{n+1} = u_n + u_{n-1}$.

1. Montrer que pour tout $n \geqslant 1$, u_n et u_{n-1} sont premiers entre eux.
2. Montrer que pour tout $n \geqslant 1$, on a $u_{n-1}.u_{n+1} - (u_n)^2 = (-1)^n$, puis que pour tout couple (m, n) d'entiers naturels tels que $m \geqslant n$, on a $u_{m-n} = (-1)^n(u_m.u_{n+1} - u_{m+1}.u_n)$.
3. En déduire que le $pgcd$ de u_m et de u_n est u_d, où $d = pgcd(m, n)$.

Réponse 71

1. Car $u_{n+1} \wedge u_n = u_n \wedge u_{n-1}$ et $u_1 \wedge u_0 = 1$.
   C'est aussi par l'algorithme d'Euclide ; car u_{n-1} est le reste de la division Euclidienne de u_{n+1} par u_n, le dernier reste non nul étant $u_1 = 1$.
2. $$\begin{aligned} u_{n-1}.u_{n+1} - (u_n)^2 + u_n.u_{n+2} - (u_{n+1})^2 &= u_{n+1}(u_{n-1} - u_{n+2}) + u_n(u_{n+2} - u_n) \\ &= -u_{n+1}u_n + u_nu_{n+1} \\ &= 0 \end{aligned}$$ Donc,

   $\big(u_{n-1}.u_{n+1} - (u_n)^2\big)$ est une suite géométrique de raison -1 de premier terme $u_0.u_2 - (u_1)^2 = -1$, donc $u_{n-1}.u_{n+1} - (u_n)^2 = (-1)^n$.
   Pour la deuxième identité, on raisonne par récurrence sur n. Pour $n = 0$ le résultat est évident. Supposons que pour un certain n on a

$$\forall m \geq n, \quad u_{m-n} = (-1)^n(u_m.u_{n+1} - u_{m+1}.u_n).$$

Soi $m \geq n+1$. Alors

$$\begin{aligned} u_{m-(n+1)} &= u_{(m-1)-n} \\ &= (-1)^n(u_{m-1}.u_{n+1} - u_m.u_n) \\ &= (-1)^n\left((u_{m+1} - u_m).u_{n+1} - u_m.(u_{n+2} - u_{n+1})\right) \\ &= (-1)^n\left(u_{m+1}.u_{n+1} - u_m.u_{n+2}\right) \\ &= (-1)^{n+1}\left(u_m.u_{n+2} - u_{m+1}.u_{n+1}\right) \end{aligned}$$

Le résultat est donc vérifié pour $n+1$. Fin de la récurrence.

3. On montre d'abord que u_n divise u_{kn} par récurrence sur k. C'est évident pour $k=0$ et $k=1$. Supposons qu'il l'est pour k. On a $u_n = u_{(k+1)n-kn} = (-1)^{kn}(u_{(k+1)n}.u_{kn+1} - u_{..}.u_{kn})$. Donc u_n divise $u_{(k+1)n}.u_{kn+1}$. Et comme u_n divise u_{kn} et $u_{kn} \wedge u_{kn+1} = 1$, alors $u_n \wedge u_{kn+1} = 1$ et u_n divise $u_{(k+1)n}$.
Maintenant, soit $d = m \wedge n$ et $\delta = u_m \wedge u_n$. Donc u_d divise u_m et u_n, puis divise aussi $\delta = u_m \wedge u_n$. On peut supposer que $d = km - k'n$ avec $k, k' \in \mathbb{N}$. Il s'ensuit que $u_d = (-1)^n(u_{km}.u_{..} - u_{..}.u_{k'n})$ et il est on en déduit que δ divise u_d. Conclusion $u_{m\wedge n} = u_m \wedge u_n$.

Exercice 72 *Théorème d'Euler*

1. Soit n un entier ≥ 2 et soit a un entier premier avec n. Montrer que

$$a^{\varphi(n)} \equiv 1\ [n]$$

où φ est l'indicatrice d'Euler, c'est à dire

$$\varphi(n) = \text{Card}\ \ \{\in [\![1, n]\!]\ :\ k \wedge n = 1\} = \text{Card}\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right).$$

Ind : Considérer l'application

$$\begin{array}{rccc} f & :\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right) & \longrightarrow & \mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right) \\ & \overline{m} & \longmapsto & \overline{a}.\overline{m} \end{array}$$

2. Déduire *le petit théorème de Fermat* : Pour tout entier premier p et tout entier a non divisible par p on a :

$$a^{p-1} \equiv 1\ [p]$$

3. Application : Montrer que pour tout $m, n \in \mathbb{N}$ $mn(m^{60} - n^{60}) \equiv 0\ \ [56786730]$

Réponse 72

1. Il est facile de voir que f est bijective. Donc, $\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right) = \{\overline{a}.\overline{m}\ \ :\ \ \overline{m} \in \mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right)\}$, et par suite $\displaystyle\prod_{\overline{m}\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} \overline{m} = \prod_{\overline{m}\in\mathcal{U}(\mathbb{Z}/n\mathbb{Z})} \overline{a}.\overline{m}$. Après simplification, on obtient $\overline{a}^{\varphi(n)} = \overline{1}$, d'où le résultat.
2. Car, dans ce cas, $\varphi(p) = p-1$ et $p \wedge a = 1$.
3. Soit p est diviseur de 60 et $p+1$ es un nombre premier, et posons $k = \dfrac{60}{p}$ on a :
   - Si m ou n est divisible par $p+1$, alors il en est de même pour $mn(m^{60} - n^{60})$.
   - Sinon, alors $m^{60} = (m^p)^k \equiv 1\ [p]$, et de même $n^{60} \equiv 1\ [p+1]$, puis $mn(m^{60} - n^{60})$ est divisible par $p+1$.

   Ainsi, dans tous les cas, $mn(m^{60} - n^{60})$ est divisible par $p+1$. En appliquant ce résultat à $p \in \{1, 2, 4, 6, 10, 12, 30, 60\}$, on conclut que $mn(m^{60} - n^{60})$ est divisible par $2, 3, 5, 7, 11, 13, 31$ et 61, puis par leur produit : 56786730

Exercice 73

Soit n un entier ≥ 2, et $D(n)$ l'ensemble de ses diviseurs dans $\mathbb{N}$.

1. Montrer que l'application

$$\begin{array}{rccc} \delta: & \{1,2,...,n\} & \longrightarrow & D(n) \\ & a & \longmapsto & a \wedge n \end{array}$$

est surjective.

2. Pour tout $d \in D(n)$ on pose $A_d = \{a \in \mathbb{N} \quad : \quad 1 \leq a \leq n \text{ et } a \wedge n = d\}$. Montrer que $\text{card}(A_d) = \varphi\left(\frac{n}{d}\right)$, où φ est l'indicatrice d'Euler.
3. Déduire la formule d'Euler-Gauss : $\sum_{d \in D(n)} \varphi(d) = n$.

Réponse 73

1. Pour tout $d \in D(n)$ on a $d \in \{1, 2, \cdots, n\}$ et $\delta(d) = d$, donc δ est surjective.
2. Soit $d \in D(n)$ et posons $n' = \frac{n}{d}$. Pour tout $a \in\in \{1, 2, \cdots, n\}$, on $a \wedge n = d$ si, et seulement si a s'écrit sous la forme : $a = da'$, avec $1 \leq a' \leq n'$ et $a' \wedge n' = 1$. On en déduit $\text{card}(A_d) = \varphi(n') = \varphi\left(\frac{n}{d}\right)$.
3. Puisque δ est surjective, et $A_d = \varphi^{-1}\{d\}$ pour tout $d \in D(n)$, alors la famille $(A_d)_{d \in D(n)}$ est une partition de l'ensemble $d \in \{1, 2, \cdots, n\}$, et par conséquent :

$$\sum_{d \in D(n)} \varphi(d) = n.$$

3.3 Résolutions d'équations et systèmes

Exercice 74

Déterminer les solutions dentiers (x, y) des systèmes :

1. $\begin{cases} \text{pgcd}(x, y) = 5 \\ \text{ppcm}(x, y) = 24 \end{cases}$.
2. $\begin{cases} \text{pgcd}(x, y) = 5 \\ \text{ppcm}(x, y) = 25 \end{cases}$.

Réponse 74

1. L'ensemble de solutions est vide car 5 ne divise pas 24.
2. En posant $x = 5x'$ et $y = 5y'$ avec $x', y' \in \mathbb{Z}$ et $x' \wedge y' = 1$ on se à résoudre l'équation $x' \vee y' = 5$, qui est équivalente à $x'.y' = 5$, à son tour équivalent à $(x', y') \in \{(1, 5), (-1, -5), (5, 1), (-5, -1)\}$. L'ensemble de solutions est alors :

$$\mathcal{S} = \{(5, 25), (-5, -25), (25, 5), (-25, -5)\}.$$

Exercice 75

Résoudre dans $\mathbb{N}^2$ l'équation suivante :

$$\begin{cases} x \vee y = 72 \\ x \wedge y = x - y \end{cases}, \begin{cases} x \wedge y = 16 \\ x + y = 320 \end{cases}, \begin{cases} (3x + 5y)(x + 2y) = 1276 \\ xy = 2(x \vee y) \end{cases}$$

Réponse 75

1. En posant $\delta = x \wedge y$, $x = \delta x'$ et $y = \delta y'$ le système devient

$$\begin{cases} \delta x' y' = 72 \\ x' - y' = 1 \end{cases}$$

Ainsi y' et x' sont deux diviseurs successifs de 72. Les valeurs possibles sont :

$$\begin{array}{lll} y' = 1, & x' = 2, & \delta = 36 \\ y' = 2, & x' = 3, & \delta = 12 \\ y' = 3, & x' = 4, & \delta = 6 \\ y' = 8, & x' = 9, & \delta = 1 \end{array}$$

Donc l'ensemble de solutions est

$$\Big\{(72, 36), (36, 24), (24, 18), (9, 8)\Big\}$$

2. En posant $x = 16x'$ et $y = 16y'$ le système devient

$$\begin{cases} x' \wedge y' = 1 \\ x' + y' = 20 \end{cases} \tag{3.1}$$

Remarquons que si (x', y') est une solution de ce système, alors tout diviseur commun de 20 et x' (resp : y') est aussi diviseur commun de y' (resp : x'), et donc égal à1. Donc, 2 et 5 ne divise ni x' ni y'. Les solutions (x', y') du système (3.1), avec $x' \leq y'$, sont $(1, 19)$, $(3, 17)$, $(7, 13)$, $(9, 11)$. En multipliant ces couples par 16, et en tenant compte que x et y jouent des rôles symétriques dans notre système de départ, on déduit l'ensemble de solutions est :

$$\Big\{(16, 304),\ (48, 272),\ (112, 208),\ (144, 304),\ (304, 16),\ (272, 48),\ (208, 112),\ (304, 144)\Big\}.$$

3. Le système est équivalent à

$$\begin{cases} (3x + 5y)(x + 2y) = 1276 \\ x \wedge y = 2 \end{cases}$$

4. En posant $x = 2x'$ et $y = 2y'$ le système devient

$$\begin{cases} x' \wedge y' = 1 \\ (3x' + 5y')(x' + 2y') = 319 = 11 \times 29 \end{cases} \tag{3.2}$$

. Remarquant que $3x' + 5y' \geq x' + 2y'$, et que si $x' + 2y' = 1$ alors $x' = 1$ et $y' = 0$ et par la suite (x', y') n'est pas solution de ()3.2, on déduit que

$$(3.2) \quad \Leftrightarrow \begin{cases} x' + 2y' = 11 \\ 3x' + 5y' = 29 \end{cases}$$
$$\Leftrightarrow \begin{cases} y' = 4 \\ x' = 3 \end{cases}$$

L'ensemble de solutions est donc :

$$\Big\{(6, 8)\Big\}.$$

Exercice 76

Résoudre dans $\mathbb{N}^2$ les équations suivantes :

1. $x^2 - y^2 = 21$.
2. $3x^2 + xy - 11 = 0$.

Réponse 76

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

$$\begin{aligned} x^2 - y^2 = 21 &\iff (x + y)(x - y) = 21 \\ &\iff \begin{cases} x - y = 1 \\ x + y = 21 \end{cases} \text{ ou } \begin{cases} x - y = 3 \\ x + y = 7 \end{cases} \\ &\quad \text{ou } \begin{cases} x - y = 7 \\ x + y = 3 \end{cases} \text{ ou } \begin{cases} x - y = 21 \\ x + y = 1 \end{cases} \\ &\iff \begin{cases} 2x = 22 \\ 2y = 20 \end{cases} \text{ ou } \begin{cases} 2x = 10 \\ 2y = 4 \end{cases} \\ &\quad \text{ou } \begin{cases} 2x - y = 10 \\ 2y = -4 \end{cases} \text{ ou } \begin{cases} 2x = 10 \\ 2y = -20 \end{cases} \\ &\iff \begin{cases} x = 11 \\ y = 10 \end{cases} \text{ ou } \begin{cases} x = 5 \\ y = 2 \end{cases} \end{aligned}$$

. L'ensemble de solutions est donc $\big\{(11, 10), (5, 2)\big\}$

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

$$\begin{aligned} 3x^2 + xy - 11 = 0 &\iff x(3x + y) = 11 \\ &\quad (x = 11 \text{ et } 3x + y = 1) \text{ ou } (x = 1 \text{ et } 3x + y = 11) \\ &\quad x = 1 \text{ et } 3x + y = 11 \\ &\quad x = 1 \text{ et } y = 9 \end{aligned}$$

.

L'ensemble de solutions est $\big\{(1, 9)\big\}$.

Exercice 77

Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

1. $2x + 3y = 1$.
2. $6x + 10y = 1$.
3. $6x + 10y = 2$.

Réponse 77

1. Une solution triviale de cette équation est $(-1, 1)$ et $2 \wedge 3 = 1$. Donc, l'ensemble de solutions est $\{(-1 - 3k, 1 + 2k) \quad : \quad k \in \mathbb{Z}\}$.
2. Cette équation n'admet pas de solution car, sinon, d'après le théorème de Bézout, on aura $6 \wedge 10 = 1$.
3. Pour tout $x, y \in \mathbb{Z}$ on a $6x + 10y = 2 \Leftrightarrow 3x + 5y = 1$. On remarque que le couple $(2, -1)$est une solution particulière de cette équation, et $5 \wedge 3 = 1$, donc, l'ensemble de solutions est $\{(2 - 5k, -1 + 3k) \quad : \quad k \in \mathbb{Z}\}$.

Exercice 78

Résoudre dans $\mathbb{Z}^3$ l'équation :

$$2x + 3y + 5z = 1$$

Réponse 78

Soit $(x, y, z) \in \mathbb{Z}^3$. Supposons que $2x + 3y + 5z = 1$. Alors $2(x + z) + 3(y + z) = 1$ puis $2(x + z + 1) + 3(y + z - 1) = 0$. Il existe alors $k \in \mathbb{Z}$ tel que $x + z + 1 = 3k$ et $y + z - 1 = 2k$; c'est à dire que $x = 3k - z - 1$ et $y = 2k - z + 1$. Réciproquement, pour tous $z, k \in \mathbb{Z}$, le triplet $(3k - z - 1, 2k - z + 1, z)$ est solution de notre équation. Ainsi l'ensemble de solutions est

$$\left\{(3k - z - 1, 2k - z + 1, z) \quad : \quad (k, z) \in \mathbb{Z}^2\right\}.$$

Exercice 79

Résoudre dans $\mathbb{Z}^3$ l'équation :

$$x^2 + y^2 + z^2 = x^2 y^2$$

Réponse 79

Posons $d = x \wedge y \wedge z$. Donc, x, y, z s'écrivent $x = dx_1, y = dy_1, z = dz_1$ où x_1, y_1, z_1 sont des entiers tels que $x_1 \wedge y_1 \wedge z_1 = 1$. Si $d = 0$ alors $x = y = z = 0$ et $(0, 0, 0)$ est bien une solution de l'équation. Si $d \neq 0$, l'équation devient $x_1^2 + y_1^2 + z_1^2 = d^2 x_1^2 y_1^2$. Remarquant que, dans $\mathbb{Z}/4\mathbb{Z}$, les carrés sont seulement $\overline{0}$ et $\overline{1}$, et que si $x_1^2 \equiv 0 \ [4]$ ou $y_1^2 \equiv 0 \ [4]$ alors $d^2 x_1^2 y_1^2 \equiv 0 \ [4]$. Ainsi, forcément x_1^2, y_1^2 et z_1^2 sont tous équivaut à 0 modulo 4. Mais ceci contredit la relation $x_1 \wedge y_1 \wedge z_1 = 1$. Comme conséquence, $(0, 0, 0)$ est l'unique solution de l'équation.

Exercice 80

Résoudre dans $\mathbb{Z}^3$ le système :

$$\begin{cases} 2x + 5y - 11z = 1 \\ \\ x - 12y + 7z = 2 \end{cases}$$

Réponse 80

On a

$$\begin{cases} 2x + 5y - 11z = 1 \\ \\ x - 12y + 7z = 2 \end{cases} \iff \begin{cases} -29y - +25z = 3 \\ \\ x - 12y + 7z = 2 \end{cases}$$

et l'équation $-29y - +25z = 3$ est facile à résoudre. En effet, si $-29y - +25z = 3$ alors $-4z \equiv 3 \ [29]$ puis $z \equiv 21 \ [29]$, ou encore $z \equiv -8 \ [29]$. Dans ce cas z est de la forme $z = 29k - 8$. Ainsi, (x, y, z) est solution de l'équation si et seulement si $y = 25k - t$ et $x = 2 + 12y - 7z$.

Exercice 81

Résoudre dans $\mathbb{Z}$ l'équation suivante :

$$\begin{cases} x \equiv 3 \ [5] \\ x \equiv 2 \ [7] \end{cases}$$

Réponse 81

Soit $x \in \mathbb{Z}$. Supposons que : $x \equiv 3 \ [5]$ et $x \equiv 2 \ [7]$. Donc il existe $k \in \mathbb{Z}$, tel que : $x = 3 + 5k$.

$$\begin{aligned} x = 3 + 5k &\implies 3 + 5k \equiv 2 \ [7] \\ &\implies 5k \equiv -1 \ [7] \\ &\implies 15k \equiv -3 \ [7] \\ &\implies k \equiv -3 \ [7] \end{aligned}$$

Donc il existe $k' \in \mathbb{Z}$ tel que $k = -3 + 7k'$, et par la suite :

$$x = 3 + 5(-3 + 7k') = -12 + 35k'.$$

Réciproquement, pour tout $k' \in \mathbb{Z}$ on a : $-12 + 35k' \equiv 3[5]$ et $-12 + 35k' \equiv 2 \ [7]$.

Conclusion : $S = \Big\{ -12 + 35k \quad : \quad k' \in \mathbb{Z} \Big\}$

Exercice 82

Trouver tous les entiers n tels que $1 \leq n \leq 105$, et les restes des divisions euclidiennes de n par $3, 5$ et 7 sont $1, 2$ et 3 respectivement.

Réponse 82

Il s'agit de déterminer les entiers n tels que

$$\begin{cases} n \equiv 3 \ [7] \\ n \equiv 2 \ [5] \\ n \equiv 1 \ [3] \end{cases}$$

Si $n \equiv 3 \ [7]$ alors n est de la forme $n = 7k_1 + 3$ avec $k_1 \in \mathbb{N}$. Dans ce cas, $n \equiv 1 \ [3]$ si et seulement si $k_1 \equiv 1 \ [3]$; c'est dire k_1 est de la forme $k_1 = 3k_2 + 1$ avec $k_2 \in \mathbb{N}$, donc $n = 21k_2 + 10$. On répète le même raisonnement et on trouve que n est de la forme $n = 105k_3 + 52$. Sachant que $1 \leq n \leq 105$, alors $n = 52$.

Exercice 83

On considére dans$\mathbb{Z}^3$ une solution du le système suivant :

$$\begin{cases} x^2 + y^2 = z^2 \\ x \wedge y \wedge z = 1 \end{cases} \tag{3.3}$$

1. Résoudre dans $\mathbb{Z}/4\mathbb{Z}$ l'équation en x : $x^2 = \bar{k}$ avec $k \in \mathbb{Z}$.
2. Montrer que si (x, y, z) une solution du système 3.3, alors z est impair, et l'un des entiers, x et y, est impair, et l'autre est pair.
3. On suppose que $(x, y, z) \in \mathbb{Z}^3$ est une solution de 3.3, et que y est pair.
   (a) calculer $(z + y) \wedge (z - y)$.
   (b) Démontrer que, si $z \in \mathbb{N}$, alors on peut écrire $z + z = u^2$, $z - y = v^2$ avec $u, v \in \mathbb{Z}$ tels que $u \wedge v = 1$, u et v étant impairs.
4. Déterminer toutes les solutions de 3.3.
5. Déterminer toutes les solutions telles que $0 < x < 20$, $0 < y < 20$ et $0 < z < 20$.
6. Résoudre dans $\mathbb{Z}^3$ l'équation $x^2 + y^2 = z^2$.
7. Soit $(x, y, z) \in \mathbb{N}^*$ une solution telle que $xyz \neq 0$. Montrer que $\dfrac{xyz}{x + y + z} \in \mathbb{N}$.

Réponse 83

1. Les carrés de $\mathbb{Z}/4\mathbb{Z}$ sont $\bar{0} = \bar{0}^2 = \bar{2}^2, \bar{1} = \bar{1}^2 = \bar{3}^2$. Donc, cette équation n'admet pas de solution si $\bar{k} = 2$ ou $\bar{k} = 3$. Sinon, l'ensemble de solution est $\{k + 4l, k + 2 + 4l \quad : \quad l \in \mathbb{Z}\}$.
2. En passant modulo 4, alors, d'après la première question, le triplet $(\bar{x}^2, \bar{y}^2, \bar{z}^2) \in \{(\bar{0}, \bar{0}, \bar{0}), (\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{1})\}$. Sachant que $x \wedge y \wedge z = 1$, alors x, y, z ne peuvent pas être simultanément pairs, et par la suite, $(\bar{x}^2, \bar{y}^2, \bar{z}^2) \in \{(\bar{0}, \bar{1}, \bar{1}), (\bar{1}, \bar{0}, \bar{1})\}$. Ceci montre bien que z est impair ainsi que l'un des entiers x ou y, l'autre étant pair.
3. (a) Si d est un diviseur commun de $z + y$ et $z - y$, alors d est un diviseur commun de $2z = (z+y)+(z-y)$ et $2y = (z+y)-(z-y)$. Et comme $y+z$ et $z-y$ sont impairs, alors d en est de même, et par suite d est un diviseur commun de y et z. Ainsi, puis que (x, y, z)est une solution du système 3.3, alors d divise aussi x^2. Si on suppose de plus que d est premier, alors d divise aussi x, ce qui est contradictoire puisque $x \wedge y \wedge z = 1$. Donc $(y + z) \wedge (z - y) = 1$.
   (b) On peut écrire x^2 sous la forme $x^2 = \prod_{i=1}^{s} p_i^{2m_i}$, où $s \in \mathbb{N}^*$, $p_1, \cdots, p_s$ sont des nombres premiers deux à deux distincts et $m_1, \cdots, m_s \in \mathbb{N}$. Remarquons que $y + z \geq 0$ et $y - z \geq 0$. Comme $x^2 = z^2 - y^2 = (y + z)(y - z)$, et $(y + z) \wedge (y - z) = 1$, alors les décomposition de $y + z$ et $z - y$ en facteurs premiers n'ont pas de facteurs premiers communs. Ainsi, $y + z$ et $y - z$ sont de la forme $y + z = \prod_{i \in I} p_i^{2m_i}$, et $y - z = \prod_{i \in J} p_i^{2m_i}$ où (I, J) est une partition de $[\![1, s]\!]$, et le produit sur l'ensemble vide est supposé égal à 1. Il suffit de prendre donc $u = \prod_{i \in I} p_i^{m_i}$ et $v = \prod_{i \in J} p_i^{m_i}$.
4. D'après la question précédente, si $(x, y, z) \in \mathbb{Z}^3$ est une solution du système 3.3, y étant pair et $z \geq 0$, alors on peut écrire $y + z = u^2$, et $z - y = v^2$ avec $u, v \in \mathbb{Z}$ impairs vérifiant $u \wedge v = 1$, et donc $z = \dfrac{u^2 + v^2}{2}$, $y = \dfrac{u^2 - v^2}{2}$ puis $x = uv$. La réciproquement étant facile, on en déduit que l'ensemble de solution est :
$$\left\{ \left(uv, \frac{u^2 - v^2}{2}, \pm\frac{u^2 + v^2}{2} \right), \left(\frac{u^2 - v^2}{2}, uv, \pm\frac{u^2 + v^2}{2} \right) \quad : \quad u, v \in \mathbb{Z} \text{ impairs et } u \wedge v = 1 \right\}.$$
5. Si $(x, y, z) \in \mathbb{Z}^3$ est une solution du système 3.3 avec $0 < x < 20$, $0 < y < 20$ et $0 < z < 20$, alors z est de la forme $\frac{u^2+v^2}{2}$, où $u, v \in \mathbb{N}$ sont impairs et vérifiant $u \wedge v = 1$, et l'un des entiers x ou y est égal à uv et l'autre est égal à $\frac{u^2-v^2}{2}$. Les hypothèses imposées entrainent que $1 \leq u < v \leq 5$. Les couples (u, v) possibles sont donc $(1, 3)$, $(1, 5)$ et $(3, 5)$. Les solutions demandées sont alors : $(3, 4, 5)$, $(5, 12, 13)$, $(15, 8, 17)$, $(4, 3, 5)$, $(12, 5, 13)$, $(8, 15, 17)$.

6. En posant $x \wedge y \wedge z = d$, et en simplifiant par d^2 dans l'équation, on se ramène au cas précédent, et on déduit que l'ensemble de solutions est :

$$\left\{ \left(duv, d\frac{u^2-v^2}{2}, \pm d\frac{u^2+v^2}{2} \right), \left(\frac{u^2-v^2}{2}, uv, \pm\frac{u^2+v^2}{2} \right) \ : \ d \in \mathbb{N}, u, v \in \mathbb{Z} \text{ impairs et } u \wedge v = 1 \right\}.$$

7. D'après l'expression des solutions obtenus dans les questions précédentes, $\dfrac{xyz}{x+y+z}$ est de la forme $\dfrac{xyz}{x+y+z} = \dfrac{uv(u^4-v^4)}{4uv+4u^2}$, où $u, v \in \mathbb{N}$ impairs et $v < u$. Ainsi, $\dfrac{xyz}{x+y+z} = \dfrac{v(u-v)(u^2+v^2)}{4} \in \mathbb{N}$, car $u-v$ et u^2+v^2 sont pairs, puisque u et v sont impairs.

3.4 Nombres premiers

Exercice 84 *Nombres de Fermat*

1. Prouver que pour tout $m \in \mathbb{N}$, si $2^m + 1$ est premier alors m est une puissance de 2. Pour $n \in \mathbf{N}$, on note $F_n = 2^{2^n} + 1$. F_n s'appelle le n-ème nombre de Fermat.
2. Montrer que $\forall (n,m) \in \mathbb{N}^2 \quad m \neq n \Rightarrow F_n \wedge F_m = 1$. En déduire que l'ensemble des nombres premiers est infini.
3. En observant que $641 = 5^4 + 2^4 = 1 + 5.2^7$, montrer que F_5 est divisible par 641. (La conjecture de Fermat ; tous les F_n sont premiers, est donc fausse).
4. Montrer que pour tout $n > 1$, F_n se termine par un 7 en écriture décimale. Prouver que si n est congru à 0 (resp. $1, 2, 3$) *modulo* 4, alors F_n se termine par 37 (resp. $97, 17, 57$).

Réponse 84

1. Supposons que m n'est pas une puissance de 2 ; donc elle est de la forme $m = 2^d(2k+1)$ avec $d, k \in \mathbb{N}$. Ainsi,

$$\begin{aligned} 2^m + 1 &= 1 + 2^{2^d(2k+1)} \\ &= 1 + \left(2^{2^d}\right)^{2k+1} \\ &= 1 - \left(-2^{2^d}\right)^{2k+1} \end{aligned}$$

   On en déduit que $2^m + 1$ est divisible par $1 + 2^{2^d}$; donc $2^m + 1$ n'est pas premier.

2. Soient $m, n \in \mathbb{N}$ avec $n < m$ et $d = F_n \wedge F_m$. Alors

$$\begin{aligned} F_m &= 1 + \left(2^{2^n}\right)^{2^{m-n}} \\ &= 1 + (F_n - 1)^l \text{ avec } l = 2^{m-n} \\ &= 2 + \sum_{k=1}^{l} (-1)^{l-k} \binom{l}{k} F_n^k \end{aligned}$$

   Donc d divise 2, et comme F_n est impair, alors $d = 1$. Soit p_n un diviseur premier quelconque de F_n, pour tout $n \in \mathbb{N}$. Comme les F_n sont premiers entre eux deux à deux, alors les p_n sont distincts deux à deux et alors l'ensemble des nombres premiers est infini.

3. Puisque $641 = 5^4 + 2^4 = 1 + 5.2^7$ alors :

$$\begin{aligned} F_5 \equiv 0 \ \ [641] &\iff 2^{32} \equiv 5.2^7 \ \ [641] \\ &\iff 2^{25} \equiv 5 \ \ [641] \\ &\iff 2^4.2^{21} \equiv 5 \ \ [641] \\ &\iff -5^4 2^{21} \equiv 5 \ \ [641] \\ &\iff -5^3 2^{21} \equiv 1 \ \ [641] \\ &\iff -5^3 2^{21} \equiv -52^7 \ \ [641] \\ &\iff 5^2 2^{14} \equiv 1 \ \ [641] \\ &\iff 5^2 2^{14} \equiv -52^7 \ \ [641] \\ &\iff 52^7 \equiv -1 \ \ [641] \end{aligned}$$

ce qui est vrai. Donc F_5 est divisible par 641.

4. On montre par récurrence que $F_n \equiv 7 \ \ [10]$. C'est vérifié pour $n = 2$, si c'est aussi le cas pour n alors

$$\begin{aligned} F_{n+1} &= (F_n - 1)2 + 1 \\ &\equiv 36^2 + 1 \ \ [10] \\ &\equiv 37 \ \ [10] \\ &\equiv 7 \ \ [10] \end{aligned}$$

On a déjà pour $n = 2$, $n \equiv 2 \ \ [4]$ et $F_2 \equiv 17 \ \ [100]$.
Or si $F_n \equiv 17 \ \ [100]$, alors $F_{n+1} \equiv 57 \ \ [100]$, $F_{n+2} \equiv 37 \ \ [100]$, $F_{n+3} \equiv 97 \ \ [100]$ et $F_{n+4} \equiv 17 \ \ [100]$. Donc, par récurrence $F_{4n} \equiv 17 \ \ [100]$ et $F_{4n+r} \equiv$ selon $r \ \ [100]$.

Exercice 85 *Théorème de Wilson*

Soit $p \in \mathbf{N} \setminus \{0, 1\}$. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \ [p]$

Réponse 85

Pour tout $k \in [\![1, p-1]\!]$ il existe un unique élément $k' \in [\![1, p-1]\!]$ tel que $kk' \equiv 1 \ \ [p]$. On notera $k' = f(k)$. On a facilement $f(k) = k \implies k = 1$ ou $k = p - 1$. Aussi, si on note $\Delta = \left\{k \in [\![1, p-1]\!] \ : \ k < f(k)\right\}$ et $\nabla = \left\{k \in [\![1, p-1]\!] \ : \ k > f(k)\right\}$ alors f réalise une bijection de Δ vers ∇. Donc :

$$\begin{aligned} (p-1)! &= (p-1) \times \left(\prod_{k \in \Delta} k\right) \times \left(\prod_{k \in \nabla} k\right) \\ &= (p-1) \times \left(\prod_{k \in \Delta} k\right) \times \left(\prod_{k \in \Delta} f(k)\right) \\ &= (p-1) \times \left(\prod_{k \in \Delta} k f(k)\right) \\ &\equiv -1 \ \ [p] \end{aligned}$$

Exercice 86 *Le petit théorème de Fermat*

1. Soit p un nombre premier. Montrer que pour tout entier p divise $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$, et en déduire le petit théorème de Fermat :

$$\forall n \in \mathbb{Z}, \quad n^p \equiv n \ \ [p]$$

2. **Application :** Montrer que pour tout $m, n \in \mathbb{N}$, le nombre $A = mn\left(m^{60} - n^{60}\right)$ est divisible par 56786730.

Réponse 86

1. Récurrence sur n
2. **Application :** Soient k, l deux entiers naturels tels que $60 = kl$. Remarquons d'abord que $m^{60} - n^{60}$ est divisible par $m^k - n^k$. Posons donc $m^{60} - n^{60} = \left(m^k - n^k\right) B$ avec $b \in \mathbb{N}$. Si de plus $k+1$ est un nombre premier alors :

$$\begin{aligned} A &= mn\left(m^{60} - n^{60}\right) \\ &= mn\left(m^k - n^k\right) B \\ &= \left(nm^{k+1} - mn^{k+1}\right) B \\ &\equiv (mn - mn)\, B \ \ [k+1] \\ &\equiv 0 \ \ [k+1] \end{aligned}$$

C'est à dire que $k+1$ divise A. Les diviseurs de 60 vérifiant cette propriété sont $1, 2, 4, 6, 10, 12, 30$ et 60. On en déduit que les nombres $2, 3, 5, 7, 11, 13, 31, 61$ divisent A. Étant premiers, leur produit, qui n'est autre que 56786730, divise A.

Exercice 87

Soit p un entier premier supérieur ou égal à 3. On considére sur $(\mathbb{Z}/p\mathbb{Z})^*$ la relation $\mathcal{R}$ définie par :

$$x\mathcal{R}y \Leftrightarrow x^2 = y^2 \text{ ou } x^2y^2 = 1$$

1. Montrer que $\mathcal{R}$ est d'équivalence.
2. Quelle est la classe $cl(x)$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$?
3. Montrer que card $(cl(x)) < 4 \Leftrightarrow x = 1$ ou $x = -1$ ou $x^2 = -1$.
4. Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1\ [4]$.

Réponse 87

1. Facile.
2. Soit $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$. Alors,

$$\begin{aligned} x^2 = y^2 &\Leftrightarrow (x-y)(x+y) = \overline{0} \\ &\Leftrightarrow x = y \text{ ou } x = -y, \text{ car, } p \text{ étant premier, } \mathbb{Z}/p\mathbb{Z} \text{ est un anneau intègre} \end{aligned}$$

et de la même manière,

$$\begin{aligned} x^2y^2 = 1 &\Leftrightarrow xy = 1 \text{ ou } xy = -1 \\ &\Leftrightarrow y = x^{-1} \text{ ou } y = -x^{-1} \end{aligned}$$

On en tire que $cl(x) = \{x, -x, x^{-1}, -x^{-1}\}$.

3. D'après l'expression de $cl(x)$, on a card $(cl(x)) < 4$ si et seulement si deux au moins parmi les éléments $x, -x, x^{-1}, -x^{-1}$ coïncident. Remarquons que $x \neq -x$, sinon, on aura $2.x = 0$, ce qui faut puisque p est un nombre premier différent de 2 et x est inversible dans l'anneau $\mathbb{Z}/p\mathbb{Z}$. Pour la même raison on a $x^{-1} \neq -x^{-1}$. D'où

$$\begin{aligned} card(cl(x)) < 4 &\Leftrightarrow x = x^{-1} \text{ ou } x = -x^{-1} \\ &\Leftrightarrow x^2 = 1 \text{ ou } x^2 = -1 \\ &\Leftrightarrow x = 1 \text{ ou } x = -1 \text{ ou } x^2 = -1 \end{aligned}$$

4. D'après la question précédente, les seules classes d'équivalences dont le cardinal n'est pas égale à 4 sont : celle de 1, qui est $\{1,-1\}$ et dont le cardinal est 2 car $p \neq 2$, et éventuellement, en cas d'existence, d'un élément a dont le carré est égal à -1, et qui sera $a, -a$, donc de cardinal égal à 2. Remarquons que si un tel élément a existe, les seuls éléments dont le carré est égal à -1 sont a et $-a$. Puisque les classes d'équivalence forment une partition de $(\mathbb{Z}/p\mathbb{Z})^*$, alors le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$, qui n'est autre que $p-1$, est la somme des cardinaux de ces classes d'équivalence. On en déduit que $p-1 \equiv 2 \ [4]$ lorsque -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, et $p-1 \equiv 0 \ [4]$ lorsque -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Donc, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \ [4]$.

Exercice 88

1. Montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$.
2. Montrer qu'il existe une infinité de nombres premiers de la forme $6k-1$.
3. Montrer qu'il existe une infinité de nombres premiers de la forme $3k+2$.

Réponse 88

1. Déjà, il existe au un tel nombre premier, par exemple 3. Supposons que cet ensemble est fini, et notons le A. Posons $N = 4\left(\prod_{p\in A} p\right) - 1$ de sorte que $N \equiv -1 \ [4]$, et que N n'admette pas de diviseur premier dans A. Remarquant que pour tout nombre premier p on a $p \equiv 1 \ [4]$ ou $p \equiv -1 \ [4]$. Donc tous les diviseurs premiers de N sont congrus à 1 modulo 4, et par suite, en décomposant N en facteurs premiers on a $N \equiv 1 \ [4]$, ce qui est faux. Conclusion : Il existe une infinité de nombres premiers de la forme $4k-1$.

Exercice 89 *Décomposition de $n!$*
Soient $n \geq 2$ et $p \in \mathcal{P}$.

1. On suppose $p > n$. Calculer $v_p(n!)$
2. Calculer $v_p(p!)$.
3. On suppose que $p < n$ et soit $m = \lfloor \frac{n}{p} \rfloor$ où $\lfloor . \rfloor$ désigne la partie entière d'un réel. Montrer que $v_p(n!) = m + v_p(m!)$.
4. En déduire que pour tout entier $n \geq 2$

$$v_p(n!) = \sum_{k=1}^{k=s} \lfloor \frac{n}{p^k} \rfloor$$

où s est le plus grand des entiers naturels qui vérifie $p^s \leq n$.

5. Exemple : Décomposer en produit de facteurs premiers 20!

Réponse 89

1. Si $p > n$ alors $v_p(n!) = 0$.
2. $v_p(p!) = 1$, car p ne divise aucun entier $k \in \{1, 2, \cdots, p-1\}$.

3. Pour tout $k \in [\![1, n]\!]$ on a $v_p(k) \neq 0$ si et seulement si k est de la forme $k = pk'$ avec $k' \in \mathbb{N}$ tel que $1 \leq k' \leq m$. Donc,

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{n} v_p(k) \\ &= \sum_{k=1}^{m} v_p(pk) \\ &= \sum_{k=1}^{m} (v_p(p) + v_p(k)) \\ &= \sum_{k=1}^{m} (1 + v_p(k)) \\ &= m + \sum_{k=1}^{m} v_p(k) \\ &= m + v_p(m!) \end{aligned}$$

4. On montre par récurrence sur i que, pour tout $i \in [\![1, s]\!]$, on a :

$$v_p(n!) = v_p(m_i!) + \sum_{k=1}^{i} \lfloor \frac{n}{p^k} \rfloor,$$

où $m_i = \lfloor \frac{n}{p^i} \rfloor$ Le cas $i = 1$ était l'objet de la question précédente. Supposons que le résultat est vérifié pour un certain i tel que $1 \leq i < s$, et calculons $v_p(m_i!)$. On a

$$\begin{aligned} v_p(m_i!) &= \sum_{k=1}^{m_i} v_p(k) \\ &= \sum_{1 \leq k \leq \frac{n}{p^i}} v_p(k) \\ &= \sum_{1 \leq k \leq \frac{n}{p^{i+1}}} v_p(pk) \\ &= \sum_{k=1}^{m_{i+1}} (v_p(p) + v_p(k)) \\ &= \sum_{k=1}^{m_{i+1}} (1 + v_p(k)) \\ &= m_{i+1} + \sum_{k=1}^{m_{i+1}} v_p(k) \\ &= m_{i+1} + v_p(m_{i+1}!) \end{aligned}$$

et par suite, $v_p(n!) = v_p(m_{i+1}!) + \sum_{k=1}^{i+1} \lfloor \frac{n}{p^k} \rfloor$. Ainsi, pour tout $i \in [\![1, s]\!]$, on a : $v_p(n!) = v_p(m_s!) + \sum_{k=1}^{s} \lfloor \frac{n}{p^k} \rfloor$. Or, comme $n < p^{s+1}$, alors $m_s \leq \frac{n}{p^s} < p$, et par suite $v_p(m_s!) = 0$. On en déduit que

$$v_p(n!) = \sum_{k=1}^{k=s} [\frac{n}{p^k}]$$

5. Les nombres premiers inférieurs à 20 sont : 2, 3, 5, 7, 11, 13, 17 et 19. Selon la formule précédente on a $v_2(20!) = 10 + 5 + 2 + 1 = 18$, $v_3(20!) = 6 + 2 = 8$, $v_5(20!) = 4$, $v_7(20!) = 2$, $v_{11}(20!) = 1$, $v_{13}(20!) = 1$, $v_{17}(20!) = 1$ et $v_{19}(20!) = 1$. Comme conséquence : $20 = 2^{18}.3^8.5^4.7^2.11.13.17.19$

Exercice 90

Le but de cette partie est la résolution dans $\mathbb{N}^* \times \mathbb{N}^*$ de l'équation

$$x^y = y^x \tag{E}$$

1. Soit (x, y) une solution de (E) tel que $x \geq 2$ et $y \geq 2$.
   (a) Montrer que $\mathcal{P}(x) = \mathcal{P}(y)$
   (b) Montrer que $\forall p \in \mathcal{P}(x) = \mathcal{P}(y), \qquad yv_p(x) = xv_p(y)$
   (c) En déduire que x divise y ou y divise x.
   (d) Montrer que pour tout $m, n \in \mathbb{N}^*$, tel que $m > 2$ et $n > 1$ on a : $n^{m-1} > m$.
   (e) Résoudre alors dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation $n^{m-1} = m$.
2. Résoudre (E).

Réponse 90

1. Soit (x, y) une solution de E tel que $x \geqslant 2$ et $y \geqslant 2$
   (a) Soit $p \in \mathcal{P}(x)$, alors p divise x^y, donc p divise y^x, or p est premier alors p divise y, donc $p \in \mathcal{P}(y)$, de même si $p \in \mathcal{P}(y)$ alors $p \in \mathcal{P}(x)$, d'où $\mathcal{P}(x) = \mathcal{P}(y)$
   (b) Soit $p \in \mathcal{P}(x)$, alors il existe $\beta \in \mathbb{N}^*$ tel que $x = p^{v_p(x)}\beta$ et $p \nmid \beta$, alors $x^y = p^{yv_p(x)}\beta^y$. D'autre part on a : $p \in \mathcal{P}(y)$, alors il existe $\gamma \in \mathbb{N}^*$ tel que $y = p^{v_p(y)}\gamma$ et $p \nmid \gamma$, alors $y^x = p^{xv_p(y)}\gamma^x$, donc $x^y = p^{xv_p(y)}\gamma^x$, donc $x^y = p^{yv_p(x)}\beta^y = p^{xv_p(y)}\gamma^x$, donc d'après l'unicité de décomposition en éléments premiers on a : $yv_p(x) = xv_p(y)$
   (c) Si $x = y$ alors (x, y) est solution de E et x divise y et y divise x.
   Supposons que $x \neq y$, supposons par exemple que $x < y$, comme $\mathcal{P}(x) = \mathcal{P}(y)$,alors pour montrer que x divise y il suffit de montrer que $v_p(x) < v_p(y)$.
   On a : $x < y$, donc $xv_p(y) < yv_p(y)$ or, $yv_p(x) = xv_p(y)$, donc : $x\frac{yv_p(x)}{x} < yv_p(y)$, or, $x \neq 0$ et $y \neq 0$, donc $v_p(x) < v_p(y)$, d'où x divise y. De même si $y < x$, on a y divise x. car x et y jouent des rôles similaires.
   (d) Soit $n > 1$, montrer par récurrence que pour tout $m > 2$ on a $n^{m-1} > m$.
   pour $m = 3$ on a $n > 1$, donc $n^2 > 3$, donc $n^{m-1} > m$.
   Soit $m > 2$, et supposons que : $n^{m-1} > m$, Montrons que $n^m > (m + 1)$.
   On a : $n^m = n^{m-1}n > mn$, car $n^{m-1} > m$ par hypothèse de récurrence, et comme $n > 1$, alors $nm > m + 1$ donc $n^m > m + 1$, d'où : $n^{m-1} > m$ pour tout $m > 2$.
   (e) Pour tout $m, n \in \mathbb{N}^*$, tel que $m > 2$ et $n > 1$ on a : $n^{m-1} > m$, donc les solutions de $n^{m-1} = m$, sont $(0 < m \leqslant 2$ et $n \in \mathbb{N}^*)$ ou $(m \in \mathbb{N}^*$ et $0 < n \leqslant 1)$, donc les solution sont (n, n) avec $n \in \mathbb{N}^*$.
2. Soit (x, y) une solution de E, alors on a : d'après $1-c)$ x divise y ou y divise x, supposons par exemple que x divise y alors, il existe $a \in \mathbb{N}^*$ te que $y = ax$, alors :

$$x^y = y^x \Rightarrow x^{ax} = (ax)^x \Rightarrow (x^x)^a = (a^x)(x^x) \Rightarrow (x^x)^{a-1} = (a^x) \Rightarrow (x^{a-1})^x = a^x$$

   Or $x > 0$, donc $x^{a-1} = a^x$, et d'après $1 - e)$ les solution de E sont (x, x) avec $x \in \mathbb{N}^*$

Exercice 91 *Croissance comparée des nombres premiers*

1. Prouver que tout entier $n > 6$ peut sécrire comme somme $a + b$ où a et b sont deux entiers premiers entre eux et strictement supérieur à strictement à 1. (distinguer n pair, puis n impair).
2. Soit $(p_n)_{n\geq 1}$ la suite strictement croissante des nombres premiers. Montrer que $p_1p_2 \cdots p_n \geqslant p_{n+1} + p_{n+2}$ pour tout $n \geqslant 3$.

3. Pour $n \in \mathbb{N}^*$, on pose q_n le plus petit nombre premier ne divisant pas n. Montrer que $\lim\limits_{n\to+\infty} \dfrac{q_n}{n} = 0$.

Réponse 91

1. — Premier cas : Si n est impair. Dans ce cas, on prend $a = n-2$ et $b = 2$. En effet, comme $b - a = 2$ et $a + b = n$ alors $a \wedge b$ divise 2 et n et par suite, puisque n est impair, $a \wedge b = 1$.
   — Deuxième cas : Supposons que n est pair et posons $n = 2k$ avec $k \in \mathbb{N}$. Là aussi on distingue deux cas.
      — Supposons que k est impair. On prend $a = k-2$ et $b = k+2$. Comme précédemment, puisque $b - a = 4$, alors $a \wedge b$ divise 4. Et puisque $a \wedge b$ divise aussi a, qui est impair, alors $a \wedge b = 1$.
      — Supposons que k est pair. On prend $a = k-1$ et $b = k+1$. Comme précédemment, $a \wedge b$ divise 2 et $a = k - 1$, et par suite $a \wedge b = 1$.
2. Soit $n \geq 3$. Remarquons que $p_2 \times p_3 \cdots \times p_n - 2 \geq 2$; car $p_2 = 3$ et $p_3 = 5$. Donc, $p_2 \times p_3 \cdots \times p_n - 2$ admet un diviseur premier q. Remarquons aussi que q est impair, car $p_2 \times p_3 \cdots \times p_- 2$ l'est, et que $q \notin \{p_2, p_3 \cdots, p_n\}$. Donc $p_{n+1} \leq q \leq p_2 \times p_3 \cdots \times p_n - 2 \leq p_1 \times p_2 \cdots \times p_n - 2$ et par suite $2 \leq p_1 \times p_2 \cdots \times p_n - p_{n+1}$. De la même manière, $p_1 \times p_2 \cdots \times p_n - p_{n+1}$ admet un diviseur premier r et $r \notin \{p_1, \cdots, p_{n+1}\}$. Ainsi $p_{n+2} \leq r \leq p_1 \times p_2 \cdots \times p_n - p_{n+1}$ et finalement $p_1 p_2 \cdots p_n \geqslant p_{n+1} + p_{n+2}$.
3. Supposons que non. Il existe donc $c > 0$ tel que, pour tout $n \in \mathbb{N}^*$, il existe $\varphi(n) \in \mathbb{N}^*$ vérifiant : $n \leq \varphi(n)$ et $\dfrac{q_{\varphi(n)}}{\varphi(n)} > c$. Soit $n \in \mathbb{N}^*$ de sorte que $cn > p_3$; et donc $p_3 < q_{\varphi(n)}$. Il existe alors $f(n) \in \mathbb{N}$ tel que $f(n) \geq 4$ tel que $q_{\varphi(n)} = p_{f(n)}$. Ainsi, $p_1, \ldots, p_{f(n)-1}$ divisent $\varphi(n)$, ce qui donne $p_1 \times p_2 \cdots \times p_{f(n)-1} \leq \varphi(n)$, puis $p_{f(n)-1} p_{f(n)} \leq \varphi(n)$ et ensuite $p_{f(n)-1} \leq \dfrac{\varphi(n)}{p_{f(n)}} \leq \dfrac{1}{c}$. Or, puisque $n \leq \varphi(n)$ et $q_{\varphi(n)} = p_{f(n)}$ alors $f(n) \to +\infty$ et par suite $p_{f(n)-1} \to +\infty$ ce qui est contradictoire. Par conséquent $\lim\limits_{n\to+\infty} \dfrac{q_n}{n} = 0$.

3.5 Systèmes de numération

Exercice 92

Démontrer qu'un entier écrit avec p chiffres en décimal nécessite au moins $(3p-2)$ chiffres et au plus $4p$ chiffres en système binaire.

Réponse 92

Remarquons d'abord que ce résultat est évident pour 0. Pour cela, considérons un entier naturel x à p chiffres en écriture décimale. Cela se traduit par $10^{p-1} \leq x < 10^p$. Pour répondre à la question, il suffit de montrer que $2^{3p-3} \leq x < 2^{4p}$, ce qui sera le cas si on démontre que $2^{3p-3} \leq 10^{p-1}$ et $10^p \leq 2^{4p}$. En effet,

$$\begin{aligned} 2^{3p-3} \leq 10^{p-1} &\Leftrightarrow 2^{2p-2} \leq 5^{p-1} \\ &\Leftrightarrow 4^{p-1} \leq 5^{p-1} \end{aligned}$$

et

$$\begin{aligned} 10^p \leq 2^{4p} &\Leftrightarrow 5^p \leq 2^{3p} \\ &\Leftrightarrow 5^p \leq 8^p \end{aligned}$$

ce qui est vrai. Donc, tout entier écrit avec p chiffres en décimal nécessite au moins $(3p-2)$ chiffres et au plus $4p$ chiffres en système binaire.

Exercice 93

Existe t-il un système de numération de base b dans lequel on puisse avoir une égalité de la forme :

$$\overline{xxx} \times \overline{xxx} = \overline{yyyyyy}$$

Réponse 93

Supposons que, dans un système de numération de base b, on a $\overline{xxx} \times \overline{xxx} = \overline{yyyyyy}$, avec bien entendu, $2 \leq b$, $1 \leq x < b$ et $1 \leq x < b$. Alors $x^2 \times \overline{111}^2 = y \times \overline{xxx} \times \overline{1001}$, et en simplifiant par $\overline{111}$ on obtient $x^2 \times \overline{111} = y \times \overline{1001}$, ce qui se traduit par $x^2 \times \left(1 + b + b^2\right) = y \times \left(1 + b^3\right)$. Donc, $1 + b + b^2$ divise $y \times \left(1 + b^3\right)$. Pour pouvoir appliquer le théorème Gauss, montrons que $(1 + b + b^2) \wedge (1 + b^3) = 1$. Soit donc d un diviseur commun de $1 + b + b^2$ et $\left(1 + b^3\right)$. Comme $1 + b + b^2$ divise $b^3 - 1$, alors d divise aussi $b^3 - 1$. Ainsi, d divise aussi $b^3 - 1$ et $b^3 + 1$, et donc aussi leur somme, c'est à dire que d divise 2. Or $1 + b + b^2$ est un nombre impair, car b et b^2 ont la même parité, donc 2 ne divise pas $1 + b + b^2$, et $d = 1$. On vient de montrer donc que, effectivement, $(1 + b + b^2) \wedge (1 + b^3) = 1$, d'où, appliquant le théorème Gauss, on déduit que $1+b+b^2$ divise y. Ceci est faux, car $1 \leq y < b < 1+b+b^2$. Comme conclusion, il n'existe aucun système de numération de base b dans lequel on pourra avoir une égalité de la forme :

$$\overline{xxx} \times \overline{xxx} = \overline{yyyyyy}.$$

Chapitre 4

Les polynômes

4.1 Divisibilité, racine d'un polynôme

Exercice 94

Justifier les divisibilités suivantes :

1. $\forall n \in \mathbb{N},\ \ X^2 \ / \ (X+1)^n - nX - 1$.
2. $\forall n \in \mathbb{N},\ \ (X-1)^3 \ / \ nX^{n+2} - (n+2)\,X^{n+1} + (n+2)\,X - n$.
3. $\left(X^2+X+1\right) \ / \ (X+1)^{6n+1} - X^{6n+1} - 1$.
4. $1 + X + X^2 \ / \ X^{3n} + X^{3p+1} + X^{3q+2}, \quad n, p, q \in \mathbb{N}$.

Réponse 94

On posera chaque fois P le polynôme concerné.

1. On a $P' = 0$ si $n = 0$, et $P' = n(X+1)^{n-1} - n$ sinon. Donc, $P(0) = P'(0) = 0$, d'où le résultat.
2. Car $P(1) = P'(1) = 0$
3. On a $X^2 + X + 1 = (X-j)(X-j^2)$, où $j = e^{2i\pi/3}$. De plus, Si w désigne j ou j^2 alors : $P(w) = (w+1)^{6n+1} - w^{6n+1} - 1 = \left(-w^2\right)^{6n+1} - w^{6n+1} - 1 = -w^2 - w - 1 = 0$, d'où le résultat.
4. Comme précédemment, on a $X^2 + X + 1 = (X-j)(X-j^2)$, où $j = e^{2i\pi/3}$, et si w désigne j ou j^2 alors : $P(w) = w^{3n} + w^{3p+1} + w^{3q+2} = 1 + w + w^2 = 0$, d'où le résultat.

Exercice 95

Donner une condition nécessaire et suffisante sur n pour que

$$1 + X + X^2 / X^{2n} + X^n + 1.$$

Réponse 95

On a $X^2 + X + 1 = (X-j)(X-j^2)$, où $j = e^{2i\pi/3}$. Donc,

$$1 + X + X^2 / X^{2n} + X^n + 1 \quad \Leftrightarrow \begin{cases} j^{2n} + j^n + 1 = 0 \\ j^{4n} + j^{2n} + 1 = 0 \end{cases}$$

$$\Leftrightarrow j^{2n} + j^n + 1 = 0$$
$$\Leftrightarrow j^n = j \text{ ou } j^n = j^2$$
$$\Leftrightarrow n \equiv 1 \ \ [3] \text{ ou } n \equiv 2 \ \ [3].$$

Exercice 96

Pour quelle valeurs de n le polynôme $(X+1)^n - X^n$ est divisible par par X^2+X+1.

Réponse 96

On a $X^2+X+1 = (X-j)(X-j^2)$, où $j = e^{2i\pi/3}$. Donc, $1+X+X^2/(X+1)^n - X^n$ si et seulement si j et j^2 sont des racines $(X+1)^n - X^n$. Or, si on désigne par w l'une des valeurs j ou j^2 alors :

$$\begin{aligned}(w+1)^n - w^n = 0 &\Leftrightarrow (-1)^n w^{2n} - w^n = 0\\ &\Leftrightarrow (-1)^n w^n = 1\\ &\Leftrightarrow n \equiv 0 \ \ [6],\end{aligned}$$

$$\text{car } \begin{cases} w^n = 1 \ si \equiv 0 \ \ [3] \\ w^n = w \ si \ \equiv 1 \ \ [3] \\ w^n = w^2 \ si \ \equiv 2 \ \ [3]. \end{cases}$$

Exercice 97

Donner une condition nécessaire et suffisante sur α et β pour que

$$X^2+2/X^4+X^3+\alpha X^2+\beta X+2.$$

Réponse 97

Une condition suffisante et nécessaire est que, toute racine x de X^2+2 dans $\mathbb{C}$, est une racine de $X^4+X^3+\alpha X^2+\beta X+2$. C'est à dire $4-2x-2\alpha+\beta x+2=0$, ou encore $(\beta-2)x = 2\alpha-6$. Sachant que les racines de X^2+2 sont $i\sqrt{2}$ et $-i\sqrt{2}$, alors ceci est équivalent à $\alpha = 3$ et $\beta = 2$.

Exercice 98

Montrer qu'il existe un unique polynôme P, que l'on déterminera, de degré inférieur à 3 tel que $(X-1)^2/P-1$ et $(X+1)^2/P+1$.

Réponse 98

Soit P un de degré inférieur à 3. Alors $(X-1)^2/P-1$ et $(X+1)^2/P+1$ si et seulement si $P(1)-1 = P(-1)+1 = P'(1) = P'(-1) = 0$.Or, $P(1)-1 = P(-1)+1 = 0$ si et seulement si 1 et -1 sont des racines du polynôme $P(X)-X$, c'est à dire que P est de la forme $P = (X^2-1)Q+X$, où Q est un polynôme tel que $\deg Q \leq 1$. Dans cas,

$$\begin{aligned}P'(1) = P'(-1) = 0 &\iff \begin{cases} 2Q(1)+1 = 0 \\ -2Q(-1)+1 = 0 \end{cases}\\ &\iff 1 \text{ et } -1 \text{ sont des racines du polynôme } 2Q(X)+X\\ &\iff Q(X) = \frac{-X}{2}\end{aligned}$$

Donc, $P = \dfrac{-X}{2}(X^2-1)Q+X$ est l'unique polynôme vérifiant $(X-1)^2/P-1$.

Exercice 99

Déterminer tous les polynômes de $\mathbb{K}[X]$ qui sont divisibles par leur polynômes dérivé.

Réponse 99

Remarquons que le polynôme nul est l'unique polynôme constant divisible par son polynôme dérivé, et tous les polynôme de degré 1 sont divisibles par leurs polynômes dérivés. Soit P un polynôme de $\mathbb{K}[X]$, de degré $n \geq 2$, divisible par son polynôme dérivé. Donc il existe $a \in \mathbb{K}$ et $\lambda \in \mathbb{K}$ tel que $P = \lambda(X-a)P'$. Comme $\deg P \geq 2$ alors $\deg P' \geq 1$, et par la suite P' admet au moins une racine dans $\mathbb{C}$. Soit α une racine complexe de P' de multiplicité égale à m, et supposons qu'elle est différente de a. On en déduit que α est aussi une racine de P, de multiplicité égale à m si on considère l'égalité $P = \lambda(X-a)P'$, mais de multiplicité égale à $m+1$ si on considère l'égalité $P(\alpha) = P'(\alpha) = \cdots = P^{(m)}(\alpha) = 0$, ce qui est contradictoire. Donc $\alpha = a$ et par suite $P = \lambda(X-a)^n$. La réciproque étant évidente, on en déduit que les polynômes de $\mathbb{K}[X]$ qui sont divisibles par leur polynômes dérivé sont ceux de la forme $\lambda(X-a)^n$ avec $\lambda \in \mathbb{K}$ et $n \geq 1$.

Exercice 100

Soit a, b, c trois éléments non nuls et distincts, du corps $\mathbb{K}$. Montrer que le polynôme $P = \dfrac{X(X-b)(X-c)}{a(a-b)(a-c)} + \dfrac{X(X-a)(X-b)}{c(c-a)(c-b)} + \dfrac{X(X-c)(X-a)}{b(b-c)(b-a)}$ peut s'écrire sous la forme $P = \alpha\,(X-a)\,(X-b)\,(X-c) + 1$ où α est une constante que l'on déterminera.

Réponse 100

En effet, a, b, c sont des racines du polynôme $P-1$ et $\deg P = 3$, donc, $P = \alpha\,(X-a)\,(X-b)\,(X-c)+1$ et $\alpha = \dfrac{1}{6}P^{(3)}$.

4.2 Division Euclidienne, pgcd et ppcm

Exercice 101

Determiner le reste de la division Euclidienne de

1. $X^8 - X^7 + X^4 - 1$ par $X^5 - 1$.
2. $X^n + a^n$ par $X^p + a^p$, où $n, p \in \mathbb{N}^*$ et $a \in \mathbb{C}$.

Réponse 101

1. On a
$$\begin{aligned} X^8 - X^7 + X^4 - 1 &= X^3(X^5-1) + X^3 - X^2(X^5-1) - X^2 + X^4 - 1 \\ &= (X^5-1)(X^3 - X^2) + X^4 - X^2 - 1. \end{aligned}$$

2. Si $n < p$ alors le quotient et le reste de la division Euclidienne de $X^n + a^n$ par $X^p + a^p$ sont respectivement 0 et $X^n + a^n$. Supposons donc que $p \leq n$, et posons $n = pq + r$ avec $q, r \in \mathbb{N}$, $q \geq 1$ et $r < p$. Alors
$$\begin{aligned} X^n + a^n &= X^r X^{pq} + a^n \\ &= X^r\,(X^p + a^p - a^p)^q + a^n \\ &= a^n + X^r \sum_{k=0}^{q} \binom{q}{k} (X^p + a^p)^k\,(-a^p)^{q-k} \\ &= a^n + (-a^p)^q + X^r \sum_{k=1}^{q} \binom{q}{k} (X^p + a^p)^k\,(-a^p)^{q-k} \\ &= a^n + (-a^p)^q + (X^p + a^p)\,X^r \sum_{k=1}^{q} \binom{q}{k} (X^p + a^p)^{k-1}\,(-a^p)^{q-k}. \end{aligned}$$

Exercice 102

Soient $(a,b) \in \mathbb{K}^2$ tel que $a \neq b$ et $P \in \mathbb{K}[X]$.

1. Exprimer le reste de la division euclidienne de P par $(X-a)(X-b)$ en fonction de $P(a)$ et $P(b)$.
2. Exprimer le reste de la division euclidienne de P par $(X-a)^2$ en fonction de $P(a)$ et $P'(a)$.

Réponse 102

1. Le reste de la division euclidienne de P par $(X-a)(X-b)$ est de la forme $P = (X-a)(X-b)Q + \alpha X + \beta$ avec $Q \in \mathbb{K}[X]$ et $\alpha, \beta \in \mathbb{K}$. Ainsi

$$\begin{cases} P(a) = a\alpha + \beta \\ P(b) = b\alpha + \beta \end{cases}$$

et par la suite

$$\begin{cases} \beta = \dfrac{aP(b) - bP(a)}{a-b} \\ \alpha = \dfrac{P(a) - P(b)}{a-b} \end{cases} .$$

2. D'après la formule de Taylor on a : $P = P(a) + P'(a)(X-a) + \sum_{k=2}^{n} \dfrac{P^{(k)}(a)}{k!} (X-a)^2$ où $n \geq \deg P$. Donc, le reste de la division euclidienne de P par $(X-a)^2$ est $P(a) + P'(a)(X-a)$.

Exercice 103

Soit $n, m \in \mathbb{N}^*$.

1. De la division euclidienne de n par m, déduire celle de $X^n - 1$ par $X^m - 1$.
2. Établir que $p\gcd(X^n - 1 \ , \ X^m - 1) = X^{n \wedge m} - 1$.

Réponse 103

1. La division euclidienne de n par m s'écrit : $n = md + r$ avec $1 \leq d$ et $0 \leq r < m$. Donc,

$$\begin{aligned} X^n - 1 &= X^{md+r} - 1 \\ &= X^r \left((X^m - 1) + 1 \right)^d - 1 \\ &= -1 + X^r \sum_{k=0}^{d} \binom{d}{k} (X^m - 1)^k. \end{aligned}$$

Si $d = 0$ alors $n = r < m$, et par suite $X^r - 1 = X^n - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^m - 1$. si $d \geq 1$ alors

$$\begin{aligned} X^n - 1 &= X^r - 1 + X^r \sum_{k=1}^{d} \binom{d}{k} (X^m - 1)^k \\ &= X^r - 1 + X^r \sum_{k=1}^{d} \binom{d}{k} (X^m - 1)^k. \end{aligned}$$

On en déduit que la division euclidienne de $X^n - 1$ par $X^m - 1$ est $X^r - 1$.

2. D'après la première question, on déduit que, si r est le dernier reste non nul dans l'algorithme d'Euclide du calcul du pcgd $n \wedge m$, alors $X^r - 1$ est le dernier reste non nul dans l'algorithme d'Euclide du calcul du pcgd $(X^m-1)\wedge(X^n-1)$. Ainsi, $pgcd(X^n-1, X^m-1) = X^{n\wedge m} - 1$.

Exercice 104

Soient $A, B, C \in \mathbb{K}[X]$ tels que $A \wedge B = 1$. Montrer que $A \wedge BC = A \wedge C$.

Réponse 104

D'une part, $A \wedge C$ est un diviseur commun de A et C, donc aussi de BC. Soit D un autre diviseur commun de A et BC. Dans ce cas, $D \wedge B$ divise D et B, et donc divise A et B. Et comme $A \wedge B = 1$, alors $D \wedge B = 1$. On applique alors le théorème de Gauss et on déduit que D divise C. Sachant qu'il divise A, alors il divise $A \wedge C$. Comme conclusion, $A \wedge BC = A \wedge C$.

Exercice 105

Soient $A, B \in \mathbb{K}[X]$ non nuls. Montrer que A et B sont premiers entre eux ssi $A + B$ et AB le sont

Réponse 105

Supposons que $A \wedge B = 1$, et soit $Q = (A+B)\wedge(AB)$. Alors Q divise AB, A^2+AB et B^2+AB, et par la suite Q divise A^2 et B^2, puis $A\wedge B^2$. Comme $A \wedge B = 1$, alors $A\wedge B^2 = 1$ et par conséquent $Q = 1$ et finalement $(A + B) \wedge (AB) = 1$. Réciproquement, si $D = A \wedge B$, il est clair que D divise AB et $A + B$, d'où $D = 1$ et le résultat en découle.

Exercice 106

1. Montrer que si deux polynômes a coefficients dans $\mathbb{K}$, ont une racine commune a, alors a est une racine de leur $PGCD$.
2. En déduire que si a est une racine multiple de P, alors a est une racine de $P \wedge P'$.
3. Soit $P \in \mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$. Montrer que P n'as que des racines simples dans $\mathbb{C}$.

Réponse 106

1. Soit P et Q deux polynômes a coefficients dans $\mathbb{K}$, et supposons que P et Q ont une racine commune a. Alors que $X - a$ divise P et Q dans $\mathbb{K}[X]$, et par la suite donc $X - a$ divise leur PGCD.
2. Si a est une racine multiple de P, alors a est une racine commune de P et P', et donc de leur PGCD aussi.
3. Supposons que P est un polynôme irréductible dans $\mathbb{Q}[X]$. Donc, $\deg P > 1$, et par la suite $1 \leq \deg P' < \deg P$. Ainsi, P ne divise pas P', et comme P est irréductible dans $\mathbb{Q}[X]$, alors $P \wedge P' = 1$ et par conséquent P et P' n'ont pas de racine commune dans $\mathbb{C}$.

Exercice 107

Soient $A, B \in \mathbb{K}[X]$ non constants et premiers entre eux. Montrer qu'il existe un couple unique $(U, V) \in \mathbb{K}[X]$ tel que $AU + BV = 1$, $d^\circ U < d^\circ B$ et $d^\circ V < d^\circ A$.

Réponse 107

D' après le théorème de Bézout, il existe $U_1, U_2 \in \mathbb{K}[X]$ tels que $AU_1 + BU_2 = 1$. La division Euclidienne de U_1 par B et de U_2 par A s'écrit $U_1 = PB+U$ et $U_2 = AQ+V$ avec $\deg U < \deg B$ et $\deg V < \deg A$. Donc, $AB(P+Q)+AU+BV = 1$, et on en déduit que $\deg AB + \deg(P+Q) = \deg(1-AU-BV) < \deg AB$, ce qui entraine que $P+Q = 0$, et finalement $AU-BV = 1$ comme demandé. Pour l'unicité, supposons qu'il existe deux couples de polynômes (U_1, V_1) et(U_2, V_2) tels que $AU_1 + BV_1 = AU_2 + BV_2 = 1$ avec $\deg U_i < \deg B$ et $\deg V_i < \deg A$, $i = 1, 2$. Dans ce cas, $A(U_1 - U_2) = B(V_2 - V_1)$, et en appliquant le théorème de Gauss on déduit que A divise $V_2 - V_1$. Comme $\deg V_2 - V_1 < \deg A$, alors $V_2 = V_1$, puis $U_2 = U_1$.

4.3 Décomposition en facteurs irréductibles

Exercice 108

Factoriser $(X+i)^n - (X-i)^n$ pour $n \in \mathbb{N}^*$.

Réponse 108

Posons $P = (X+i)^n - (X-i)^n$. Alors le degré de P est $\deg P = n-1$, et et son coefficient dominant est $2ni$. Si $n = 1$ alors $P = 2ni$. Supposons que ≥ 2. Dans ce cas, P admet $n-1$ racines dans $\mathbb{C}$. Remarquant que i n'est pas une racine du polynôme P, on a , pour tout $z \in \mathbb{C}$ on a :

$$\begin{aligned}
(z+i)^n - (z-i)^n &\Leftrightarrow z \neq i \text{ et } \frac{z+i}{z-i} = 1 \\
&\Leftrightarrow z \neq i \text{ et } \left(\frac{z+i}{z-i}\right)^n = 1 \\
&\Leftrightarrow z \neq i \text{ et } \exists k \in [\![0, n-1]\!] \ : \ \frac{z+i}{z-i} = e^{2ik\pi/n} \\
&\Leftrightarrow z \neq i \text{ et } \exists k \in [\![1, n-1]\!] \ : \ \frac{z+i}{z-i} = e^{2ik\pi/n} \\
&\Leftrightarrow \text{ et } \exists k \in [\![1, n-1]\!] \ : \ z\left(1 - e^{2ik\pi/n}\right) = -i - ie^{2ik\pi/n} \\
&\Leftrightarrow z \neq i \text{ et } \exists k \in [\![1, n-1]\!] \ : \ z = -i\frac{2\cos(k\pi/n)}{-2i\sin(k\pi/n)} \\
&\Leftrightarrow z \neq i \text{ et } \exists k \in [\![1, n-1]\!] \ : \ z = \operatorname{Cotan}(k\pi/n)
\end{aligned}$$

Donc, P admet $n-1$ racines distinctes deux à deux, et par suite :

$$P = 2ni \prod_{k=0}^{n-1} \left(X - \operatorname{Cotan}(k\pi/n)\right).$$

Conséquences :

- $\sum_{k=1}^{n-1} \operatorname{Cotan}(k\pi/n) = \sigma_1 = 0$
- $\prod_{k=1}^{n-1} \operatorname{Cotan}(k\pi/n) = \sigma_{n-1} = \dfrac{(-1)^{n-1}i^n - (-i)^{n-1}}{2ni} = \begin{cases} 0 \text{ si } n \text{ est pair} \\ \dfrac{i^{n-1}}{n} \text{ si } n \text{ est pair.} \end{cases}$

Exercice 109

1. Factoriser $X^n - 1$ sur $\mathbb{C}$.

2. En déduire la valeur de $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$.
3. Factoriser le polynôme $P = (1+X)^n - \cos(2na) + i\sin(2na)$, $a \in \mathbb{C}$.
4. En déduire la valeur de $\prod_{k=0}^{n-1} \sin\left(\frac{k\pi}{n} + \theta\right)$.

Réponse 109

1. On a : $X^n - 1 = \prod_{K=0}^{n-1} \left(X - \omega^k\right)$, avec $\omega = e^{\frac{2i\pi}{n}}$.
2. Posons $Q = \sum_{K=0}^{n-1} X^k$. On a alors $X^n - 1 = (X-1)Q$, et par intégrité de $\mathbb{C}[X]$, on a $Q = \prod_{k=1}^{n-1} \left(X - \omega^k\right)$ et la suite $Q(1) = n = \prod_{k=1}^{n-1} \left(1 - \omega^k\right)$. Or, pour tout $k \in [\![1, n-1]\!]$ on a $1 - e^{\frac{2ik\pi}{n}} = -2i\sin\left(\frac{k\pi}{n}\right)$, donc

$$n = \prod_{k=1}^{n-1} \left(-2i\sin\left(\frac{k\pi}{n}\right) e^{\frac{ik\pi}{n}}\right) = (-2i)^{n-1} e^{\frac{i\pi(n(n-1))}{2n}} \prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right).$$

Finalement

$$\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}.$$

3. On a $\cos(2na) + i\sin(2na) = e^{2ia}$, et pour tout $z \in \mathbb{C}$ on a :

$$\begin{aligned}
(1+z)^n = e^{2ina} &\Leftrightarrow \left(\frac{1+z}{e^{2ia}}\right)^n = 1 \\
&\Leftrightarrow \exists k \in [\![0, n-1]\!],\ \frac{1+z}{e^{2ia}} = e^{2i\frac{k\pi}{n}} \\
&\Leftrightarrow \exists k \in [\![0, n-1]\!],\ z = e^{2i(a+\frac{k\pi}{n})} - 1 \\
&\Leftrightarrow \exists k \in [\![0, n-1]\!],\ z = e^{i(a+\frac{k\pi}{n})}\left(e^{i(a+\frac{k\pi}{n})} - e^{-i(a+k\pi/n)}\right) \\
&\Leftrightarrow \exists k \in [\![0, n-1]\!],\ z = 2ie^{i(a+\frac{k\pi}{n})}\sin\left(a+\tfrac{k\pi}{n}\right)
\end{aligned}$$

Les racines complexes de P sont donc les nombres complexes de la forme $2ie^{i(a+\frac{k\pi}{n})}\sin\left(a+\frac{k\pi}{n}\right)$, avec $k \in [\![0, n-1]\!]$. Et comme P un polynôme unitaire, alors

$$P = \prod_{k=0}^{n-1} \left(X - 2ie^{i(a+\frac{k\pi}{n})}\sin\left(a+\frac{k\pi}{n}\right)\right).$$

4. En appliquant les relations entre coefficients et racines, ou en évaluons P en 0, on obtient : $1 - e^{2ina} = \prod_{k=0}^{n-1} -2ie^{i(a+\frac{k\pi}{n})}\sin\left(a+\frac{k\pi}{n}\right)$. Donc,

$$\begin{aligned}
-2i\sin(na)e^{ina} &= \prod_{k=0}^{n-1} -2ie^{i(a+\frac{k\pi}{n})}\sin\left(a+\tfrac{k\pi}{n}\right) \\
&= (-2i)^n e^{i(na+\frac{n-1\pi}{2})} \prod_{k=0}^{n-1} \sin\left(a+\tfrac{k\pi}{n}\right) \\
&= (-2i)^n e^{ina}.i^{n-1} \prod_{k=0}^{n-1} \sin\left(a+\tfrac{k\pi}{n}\right) \\
&= (-2)^n i(-1)^{n-1} e^{ina} \prod_{k=0}^{n-1} \sin\left(a+\tfrac{k\pi}{n}\right) \\
&= -2^n ie^{ina} \prod_{k=0}^{n-1} \sin\left(a+\tfrac{k\pi}{n}\right)
\end{aligned}$$

Ainsi

$$\prod_{k=0}^{n-1} \sin(a + \frac{k\pi}{n}) = \frac{\sin(na)}{2^{n-1}}.$$

Exercice 110

Soit $a \in]0, \pi[$ et $n \in \mathbb{N}^*$. Factoriser dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme

$$X^{2n} - 2\cos a.X^n + 1$$

Réponse 110

Il est facile de voir que $X^2 - 2\cos a.X + 1 = \left(X - e^{ia}\right)\left(X - e^{-ia}\right)$ et par la suite :

$$\begin{aligned} X^{2n} - 2\cos a.X^n + 1 &= \left(X^n - e^{ia}\right)\left(X^n - e^{-ia}\right) \\ &= \prod_{k=0}^{n-1} \left(X - e^{i\frac{a+2k\pi}{n}}\right) \prod_{k=0}^{n-1} \left(X - e^{-i\frac{a+2k\pi}{n}}\right) \\ &= \prod_{k=0}^{n-1} \left(X^2 - 2\cos\tfrac{a+2k\pi}{n} + 1\right) \end{aligned}$$

Exercice 111

Soit $P \in \mathbb{R}[X]$. Montrer que si $P(x) > 0$, pour tout $x \in \mathbb{R}$, alors il existe $(A, B) \in (\mathbb{R}[X])^2$ tels que $P = A^2 + B^2$.

Réponse 111

D'après les hypothèses, la décomposition de P en produit de facteurs irréductibles dans $\mathbb{R}[X]$ est : $P = \gamma \prod_{k=1}^{r} \left(X^2 + a_k X + b_k\right)^{\alpha_k}$, avec $r \in \mathbb{N}^*$, $\gamma > 0$ et $a_k^2 - 4b_k < 0$ pour tout $k \in [\![1, r]\!]$. D'autre part, pour tout $k \in [\![1, r]\!]$, il existe $\beta_k \in \mathbb{C}/\mathbb{R}$ tel que $X^2 + a_k X + b_k = (X - \beta_k)(X - \overline{\beta})$,d'où

$$P = \gamma \prod_{k=1}^{r} (X - \beta_k)^{\alpha_k} \prod_{k=1}^{r} \left(X - \overline{\beta_k}\right)^{\alpha_k}.$$

Par ailleurs, on peut écrire $\prod_{k=1}^{r} (X - \beta_k)^{\alpha_k} = A + iB$, avec un certain $(A, B) \in \mathbb{R}[X]^2$. Ainsi, $\prod_{k=1}^{r} \left(X - \overline{\beta_k}\right)^{\alpha_k} = A - iB$ ce qui entraine que :

$$P = (\sqrt{\gamma}A)^2 + (\sqrt{\gamma}B)^2.$$

4.4 Racine d'un polynôme et multiplicité d'une racine

Exercice 112

Soit P un polynôme à coefficients réels et de degré supérieur ou égale à 1 .

1. Montrer que si P admet une racine α complexe non réelle de multiplicité m, alors $\overline{\alpha}$ est aussi une racine de multiplicité m de P.
2. Montrer, à l'aide d'une méthode algébrique, que tout polynôme à coefficients réels de degré impaire admet au moins une racine réelle.

Réponse 112

1. Associons à tout polynôme $P = \sum_{k=0}^{n} a_k X^k$, son polynôme conjugué $\overline{P}$ défini par : $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$. Il est clair alors que si $P \in \mathbb{R}[X]$ alors $\overline{P} = P$, et que L'application $P \longmapsto \overline{P}$ est un automorphisme du $\mathbb{R}$-algèbre $\mathbb{C}[X]$. Supposons maintenant que P est un polynôme à coefficients réels admettant une racine complexe non réelle noté α de multiplicité $m \geq 1$. Il existe alors $Q \in \mathbb{C}[X]$ tel que $P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$. Et comme $P \in \mathbb{R}[X]$, alors $P = \overline{P} = (X-\overline{\alpha})^m . \overline{Q}$, ce qui montre alors que $\overline{\alpha}$ est une racine de P de multiplicité au moins égale à m. Or $\overline{Q}(\overline{\alpha}) = \overline{Q(\alpha)} \neq 0$, donc $\overline{\alpha}$ est une racine de P de multiplicité égale à m.
2. Supposons que P est un polynôme à coefficients réels de degré impaire, qui n'admet aucune racine réelle. D'après la première question, P s'écrit : $P = \gamma \prod_{k=1}^{n} (X-\alpha_k)^{\beta_k} (X-\overline{\alpha}_k)^{\beta_k}$, où $\gamma, \alpha_k \in \mathbb{C}$ et $\beta_k \in \mathbb{N}$. Or ceci montre que P est de degrés pair, ce qui donne le résultat.

Exercice 113

Soit $c \in \mathbb{Q}[X]$ un nombre rationnel tel que $\sqrt{c} \notin \mathbb{Q}$.

1. Montrer que pour tout $a, b \in \mathbb{Q}[X]$ on a : $a + b\sqrt{c} = 0 \Leftrightarrow a = b = 0$, puis en déduire que $a + b\sqrt{c} = 0 \Leftrightarrow a - b\sqrt{c} = 0$, et que pour tout $a, b, a', b' \in \mathbb{Q}[X]$ on a : $a + b\sqrt{c} = a' + b'\sqrt{c} \Leftrightarrow (a = a' \text{ et } b = b')$.
2. Montrer que l'ensemble $\mathbb{Q}[\sqrt{c}] = \{a + b\sqrt{c} \ : \ a, b \in \mathbb{Q}\}$ est un sous corps de $\mathbb{R}$.
3. Établir que l'application

$$\begin{array}{rccc} \Phi : & \mathbb{Q}[\sqrt{c}] & \longrightarrow & \mathbb{Q}[\sqrt{c}] \\ & a + b\sqrt{c} & \longmapsto & a - b\sqrt{c} \end{array}$$

est bien définie, et est un morphisme de corps.

4. Soit $P \in \mathbb{Q}[X]$ un polynôme non nul, et a , $b \in \mathbb{Q}$. Montrer que si $a + b\sqrt{c}$ est une racine de P de multiplicité m, alors $a - b\sqrt{c}$ est aussi une racine de P de même ordre de multiplicité.

Réponse 113

1. Soit Soit $a, b \in \mathbb{Q}[X]$ tels que $a + b\sqrt{c} = 0$. Si $b \neq 0$, alors $\sqrt{c} = \dfrac{-a}{b} \in \mathbb{Q}$, ce qui est faux. Donc $b = 0$ et par la suite $a = -b\sqrt{c} = 0$. La réciproque étant évidente, on alors $a + b\sqrt{c} = 0 \Leftrightarrow a = b = 0$. Ainsi,

$$\begin{array}{rl} a - b\sqrt{c} = 0 & \Leftrightarrow a = -b = 0 \\ & \Leftrightarrow a = -b = 0 \\ & a + b\sqrt{c} = 0, \end{array}$$

et pour tout $a, b, a', b' \in \mathbb{Q}[X]$ on a :

$$\begin{array}{rl} a + b\sqrt{c} = a' + b'\sqrt{c} & \Leftrightarrow (a - a') + (b - b')\sqrt{c} = 0 \\ & \Leftrightarrow a = a' \text{ et } b = b'. \end{array}$$

2. On a
   - $1 = 1 + 0 \times \sqrt{c} \in \mathbb{Q}[\sqrt{c}]$,
   - pour tout $a, b, a', b' \in \mathbb{Q}[X]$:
     - $(a + b\sqrt{c}) - (a' + b'\sqrt{c}) = (a - a') + (b - b')\sqrt{c} \in \mathbb{Q}[\sqrt{c}]$,
     - $(a + b\sqrt{c}) \times (a' + b'\sqrt{c}) = (aa' + bb'c) + (a'b + ab')\sqrt{c} \in \mathbb{Q}[\sqrt{c}]$,
     - si de plus $a + b\sqrt{c} \neq 0$, alors d'après la première question on a $a - b\sqrt{c} \neq 0$, et on peut écrire alors $\dfrac{1}{a + b\sqrt{c}} = \dfrac{a - b\sqrt{c}}{(a + b\sqrt{c}) \times (a - b\sqrt{c})} = \dfrac{a}{a^2 - b^2c} - \dfrac{b\sqrt{c}}{a^2 - b^2c} \in \mathbb{Q}[\sqrt{c}]$

   D'où, $\mathbb{Q}[\sqrt{c}] = \{a + b\sqrt{c} \ : \ a, b \in \mathbb{Q}\}$ est un sous corps de $\mathbb{R}$.
3. D'après la première question, tout élément de $\mathbb{Q}[\sqrt{c}]$ s'écrit de manière unique sous a forme $a+b\sqrt{c}$. Donc, puisque $a-b\sqrt{c} \in \mathbb{Q}[\sqrt{c}]$, l'application Φ est bien définie. De plus, un calcul simples montre que $\Phi(1) = 1$ et que, pour tout $x, y \in \mathbb{Q}[\sqrt{c}]$ on a $\Phi(x - y) = \Phi(x) - \Phi(y)$ et $\Phi(x \times y) = \Phi(x) \times \Phi(y)$, c'est à dire que Φ est un morphisme de corps.
4. Soit $a, b \in \mathbb{Q}$. Puisque Φ est un morphisme de corps alors $P(a - b\sqrt{c}) = P(\Phi(a + b\sqrt{c})) = \Phi(P(a+b\sqrt{c}))$ et $P(a-b\sqrt{c}) = P(\Phi(a+b\sqrt{c})) = \Phi(P(a+b\sqrt{c}))$. On en déduit que $a+b\sqrt{c}$ est une racine de P si et seulement si $a - b\sqrt{c}$ est une racine de P. Pour la même raison, pour tout $k \in \mathbb{N}$, $a + b\sqrt{c}$ est une racine de $P^{(k)}$ si et seulement si $a - b\sqrt{c}$ est une racine de $P^{(k)}$. Or, la multiplicité d'une racine x de P est $m(x) = \min\{k \in \mathbb{N} \ : \ P^{(k)}(x) \neq 0\}$, donc, , $a + b\sqrt{c}$ est une racine de P de multiplicité m si et seulement si $a - b\sqrt{c}$ est une racine de P de multiplicité m.

Exercice 114

Soit P un polynôme à coefficients réels de degré $n+1$, possédant $n+1$ racines réelles distinctes. Montrer que P' possède éxactement n racines réelles distinctes.

Réponse 114

Soit P un polynôme à coefficients réels de degré $n+1$, possédant $n+1$ racines réelles distinctes : $x_1, \cdots, x_{n+1}$. D'après le théorème de Rolle, pour chaque $i \in [\![1, n]\!]$, P' admet une racine $y_k \in]x_k, x_{k+1}[$. Ainsi, P' possède éxactement n racines réelles distinctes.

Exercice 115

Montrer que pour tout $n \in \mathbb{N}$ tel que $n \geq 2$ le polynôme :

$$P_n = 1 + \frac{1}{1!}X + \frac{1}{2!}X^2 + \ldots + \frac{1}{n!}X^n$$

n'ont que des racines simples dans $\mathbb{C}$

Réponse 115

Remarquons que $P = P' + \frac{X^n}{n!}$. Donc, si P_n admet une racine z complexes multiple, on a aura $P(z) = P'(z) = 0$ et par la suite $z = 0$. Or $P(0) = 1$, donc P n'admet que des racines complexes simples.

Exercice 116

Soit P un polynôme non constant à coefficients réels dont toutes ses racines sont réelles.

1. Montrer que les racines de P' sont réelles.
2. En déduire que :$\forall a \in \mathbb{R}^*$ les racines de $P^2 + a^2$ sont simples.

Réponse 116

1. Notons $a_1, \ldots, a_r$ les racines (deux à deux distinctes) de P, $m_1, \ldots, m_r$ leurs multiplicités respectives. et $n = \deg P$. Ainsi, $\deg P = \sum_{k=1}^{r} m_k$, et $a_1, \ldots, a_r$ sont des racines distinctes deux a deux de P' de multiplicités respectives $m_1 - 1, \ldots, m_r - 1$ (éventuellement nuls). D'autre part, si on suppose que $a_1 < a_2 < \ldots < a_r$, par application du théorème de Rolle on déduit que pour tout $k \in [\![1, r-1]\!]$, il existe $b_k \in]a_k, a_{k+1}[$ tel que $P'(b_k) = 0$. Le nombre des racines réelles de P' est donc supérieur ou égal à : $\sum_{k=1}^{r} (m_k -) + r - 1 = n - 1$. Comme $\deg P' = n - 1$, on conclut alors que P' est scindé dans $\mathbb{R}$.
2. Soit a un réel non nul et posons $Q = P^2 + a^2$. Il est clair que Q n'a pas de racines réelles. Soit alors z une racine de Q. Comme $Q' = 2PP'$, $P(z) \neq 0$ et $P'(z) \neq 0$ alors $Q'(z) \neq 0$, ce qui veut dire que Q n'a que des racines complexes non réelles simples.

Exercice 117

1. Soit $P = \sum_{k=0}^{n} a_k X^k$, $n \geq 1$, un polynôme à coefficients dans $\mathbb{Z}$. On suppose que P admet une racine rationnelle dont la forme réduite est $\frac{p}{q}$.
   (a) Montrer que p/a_0 et q/a_n.
   (b) Montrer qu'il existe un polynôme Q à coefficients entiers tel que $P = (qX - p)\, Q$.
   (c) En déduire que $p - q$ divise $P(1)$ et que $p + q$ divise $P(-1)$.
2. **Application :**
   (a) Montrer $P = X^3 - X^2 - X - 1$ n'a pas de racine rationnelle.
   (b) Factoriser dans $\mathbb{R}[X]$ le polynôme $P = 72X^4 - 306X^3 + 469X^2 - 306X + 72$.

Réponse 117

1. (a) Puisque $\frac{p}{q}$ est une racine de P alors $\sum_{k=0}^{n} a_k \frac{p^k}{q^k} = 0$. En multipliant par q^n on obtient $\sum_{k=0}^{n} a_k p^k q^{n-k} = 0$. Et comme p divise $\sum_{k=1}^{n} a_k p^k q^{n-k}$ et q divise $\sum_{k=0}^{n-1} a_k p^k q^{n-k}$ alors p divise $a_0 q^n$ et q divise $a_n p^n$. Or, $p \wedge q = 1$, donc aussi $p \wedge q^n = p^n \wedge q = 1$, et le théorème de Gauss permet de conclure que p/a_0 et q/a_n.
   (b) On va montrer le résulta par récurrence sur n.
   — Si $n = 0$, alors P est un polynôme constant. Comme il admet une racine, alors c'est le polynôme nul, et par la suite $P = (qX - p)\, Q$, où Q est le polynôme nul.
   — Supposons que ce résultat reste vrai jusqu'un certain n, et que, maintenant, $P = \sum_{k=0}^{n+1} a_k X^k$. D'après la première question, il existe $a'_{n+1} \in \mathbb{Q}$ tel que $a_{n+1} = q a'_{n+1}$. Posons $L = P - (qX - p) a'_{n+1} X^n$. Alors L est à coefficients rationnels, $\deg L \leq n$ et $\frac{p}{q}$ est une racine de L. Donc, d'après l'hypothèse de récurrence, il existe un polynôme Q à coefficients entiers tel que $L = (qX - p)\, Q$, ce qui donne $P = (qX - p)\left(Q + a'_{n+1} X^n\right)$, et le résultat est établi.
   (c) Selon la question précédente, il existe un polynôme Q à coefficients entiers tel que $P = (qX - p)\, Q$. Il en découle que $P(1) = (q - p)\, Q(1)$ et $P(-1) = (q + p)\, Q(-1)$, puis que $p - q$ divise $P(1)$ et $p + q$ divise $P(-1)$.

2. **Application :**

(a) Supposons que le polynôme $P = X^3 - X^2 - X - 1$ admet une racine rationnelle dont la forme réduite est $\frac{p}{q}$. Alors, p et q divisent 1, ce qui signifie que $p = \pm 1$ et $q = 1$, et par conséquent $\frac{p}{q} = \pm 1$. Or, ni 1 ni -1 ne sont des racine de P, comme conséquence, P n'a pas de racine rationnelle.

(b) Supposons P admet une racine rationnelle dont la forme réduite est $\frac{p}{q}$. Alors, p et q divisent $72 = 3^2 \times 2^3$. Et comme p et q sont premiers entre eux, alors on a l'une des deux éventualités :

— L'un d'entre eux est de la forme $\pm 2^i$, et l'autre de la forme $\pm 3^j$, avec $0 \leq i \leq 3$ et $0 \leq j \leq 2$ et, bien entendu $q \geq 1$,

— l'un d'entre eux est égal à ± 72, et l'autre est égal à ± 1, avec $0 \leq i \leq 3$ et $0 \leq j \leq 2$ et, bien entendu $q \geq 1$.

D'autre part, $p - q$ divise 1, donc les valeurs possibles pour le couple (p, q) sont : $(1, 2)$, $(2, 1)$, $(2, 3)$, $(3, 2)$, $(4, 3)$, $(3, 4)$, $(8, 9)$ et $(9, 8)$. Mais, sachant que $p + q$ divise $1225 = 5^2 \times 7^2$, alors les valeurs possibles sont : $(2, 3)$, $(3, 2)$, $(4, 3)$, $(3, 4)$. Il ne nous reste maintenant qu'à vérifier si ces valeurs répondent bien à la question, ce qui est facile. En effet, les racines de notre polynôme sont $\frac{2}{3}$, $\frac{3}{2}$, $\frac{3}{4}$, $\frac{4}{3}$, et par suite :

$$P = (2X - 3)(3X - 2)(4X - 3)(3X - 4)$$

4.5 Relations entre coefficients et racines d'un polynôme scindé

Exercice 118

Résoudre $x^3 - 8x^2 + 23x - 28$ sachant que la somme de deux racines est égale à la troisième.

Réponse 118

Soit $a, b \in \mathbb{C}$ tels que $a \neq b$. D'après les relations entre coefficients et racines d'un polynôme, on déduit que le polynôme P admet $a, b, a + b$ comme racines si et seulement si

$$\begin{cases} 2a + 2b = 8 \\ ab + a^2 + ab + ab + b^2 = 23 \\ a^2 b + b^2 a = 28. \end{cases} \tag{4.1}$$

Or,

$$
\begin{aligned}
(4.1) \quad &\Leftrightarrow \begin{cases} 2a+2b=8 \\ ab+a^2+ab+ab+b^2=23 \\ a^2b+b^2a=28 \end{cases} \\
&\Leftrightarrow \begin{cases} a+b=4 \\ a^2+b^2=2 \\ ab=7 \end{cases} \\
&\Leftrightarrow \begin{cases} a+b=4 \\ a^2+b^2-2ab=-12 \\ ab=7 \end{cases} \\
&\Leftrightarrow \begin{cases} a+b=4 \\ (a-b)^2=-12 \\ ab=7 \end{cases} \\
&\Leftrightarrow \begin{cases} a+b=4 \\ a-b=2i\sqrt{3} \\ ab=7 \end{cases} \\
&\Leftrightarrow \begin{cases} 2+i\epsilon\sqrt{3} \quad \text{avec } \epsilon=\pm 1 \\ b=\overline{a} \end{cases}
\end{aligned}
$$

Ainsi, les solutions de cette équation sont $2+i\sqrt{3}$, $2-i\sqrt{3}$ et 4.

Exercice 119

Donner une condition nécessaire et suffisante sur $\alpha \in \mathbb{C}$ pour que le polynôme $P = X^3 - 7X + \alpha$ admette une racine qui soit le double d'une autre. Résoudre dans ce cas l'équation $P(x) = 0$.

Réponse 119

Soit $a, b \in \mathbb{C}$ tels que $a \neq b$. D'après les relations entre coefficients et racines d'un polynôme, on déduit que le polynôme P admet $a, 2a$ et b comme racines si et seulement si

$$
\begin{cases} 3a+b=0 \\ 2a^2+3ab=-7 \\ 2a^2b=-\alpha. \end{cases} \tag{4.2}
$$

Or,

$$
\begin{aligned}
(4.2) \quad &\Leftrightarrow \begin{cases} b=-3a \\ 2a^2-9a^2=-7 \\ -6a^3=-\alpha \end{cases} \\
&\Leftrightarrow \begin{cases} b=-3a \\ a=\pm 1 \\ \alpha=6a \end{cases}
\end{aligned}
$$

Donc, le polynôme $P = X^3 - 7X + \alpha$ admet une racine qui soit le double d'une autre si, et seulement si, $\alpha = 6$ ou $\alpha = -6$. Dans le premier cas, les racines de P sont $1, 2$ et -3, dans le second, ce sont $-1, -2$ et 3.

Exercice 120

1. Donner une condition nécessaire et suffisante sur $q \in \mathbb{C}$ pour que le polynôme $P = X^3 - 3X + q$ ait une racine double, puis résoudre l'équation $P(x) = 0$.
2. De manière générale, donner une condition nécessaire et suffisante sur p et q pour que le polynôme $X^3 + pX + q$ ait une racine double.

Réponse 120

1. Soit $a, b \in \mathbb{C}$ tels que $a \neq b$. Le polynôme P admet a et b comme racines, avec a comme racine double, si et seulement si

$$\begin{cases} 2a + b = 0 \\ a^2 + 2ab = -3 \\ a^2 b = -q. \end{cases} \tag{4.3}$$

Or,

$$(4.3) \quad \Leftrightarrow \begin{cases} b = -2a \\ a^2 - 4a^2 = -3 \\ -2a^3 = -q \end{cases} \Leftrightarrow \begin{cases} b = -2a \\ a = \pm 1 \\ q = 2a \end{cases}$$

Donc, le polynôme P admet une racine double si, et seulement si, $q = 2$ ou $q = -2$. Dans le premier cas, les racines de P sont 1 et -2, dans le second, ce sont -1 et 2.

2. Soit $a, b \in \mathbb{C}$ tels que $a \neq b$. Le polynôme P admet a et b comme racines, avec a comme racine double, si et seulement si

$$\begin{cases} 2a + b = 0 \\ a^2 + 2ab = p \\ a^2 b = -q. \end{cases} \tag{4.4}$$

Or,

$$(4.4) \quad \Leftrightarrow \begin{cases} b = -2a \\ a^2 - 4a^2 = p \\ -2a^3 = q \end{cases} \Leftrightarrow \begin{cases} b = -2a \\ p = -3a^2 \\ q = 2a^3 \end{cases}$$

Remarquons alors que si c'est le cas, alors $p \neq 0$ et $q \neq 0$; sinon, on aura $a = b = 0$. Dans ce cas, P ait une racine double si et seulement $\dfrac{q}{2}$ admet une racine cubique qui est égale une racine carrée de $\dfrac{-p}{3}$. Cette racine commune ne peut être que $\frac{\frac{q}{2}}{\frac{-p}{3}} = \dfrac{-3q}{2p}$, donc ceci équivalent à la condition

$$\begin{cases} \dfrac{q}{2} = \dfrac{-27q^3}{8p^3} \\ \dfrac{-p}{3} = \dfrac{9q^2}{4p^2}, \end{cases} \tag{4.5}$$

à son tour équivalent à $4p^3 = -27q^2$. Dans ce cas, les racines sont : $a = \dfrac{-3q}{2p}$, qui est une racine double, et $b = \dfrac{3q}{p}$, qui est une racine simple.

Exercice 121

En utilisant les relations entre les coefficients d'un polynôme et ses racines, et en admettant les formules $x^2+y^2+z^2 = \sigma_1^2 - 2\sigma_2$ et $x^3+y^3+z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$ pour tout $x, y, z \in \mathbb{K}$, où σ_1, σ_2 et σ_3 sont les polynômes symétriques élémentaires de x, y, z, c'est à dire $\sigma_1 = x + y + z, \sigma_2 = xy + yz + zx$ et $\sigma_3 = xyz$, résoudre dans $\mathbb{K}^3$ les systèmes suivants :

1. $x + y + z = xy + yz + zx = xyz = 1$.
2. $x + y + z = \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = -\dfrac{xyz}{4} = 1$.
3. $x + y + z = \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = \dfrac{1}{9}(x^2 + y^2 + z^2) = 1$.
4. $x + y + z = \dfrac{x^2 + y^2 + z^2}{7} = \dfrac{x^3 + y^3 + z^3}{10} = 2$.

Réponse 121

1. $x + y + z = -xy - yz - zx = -xyz = 1$ si et seulement si x, y, z sont les racines du polynôme $X^3 - X^2 + X - 1$. Or $X^3 - X^2 - X + 1 = (X - 1)^2(X + 1)$, donc, l'ensemble de solutions est $\{(1, 2, -2), (1, -2, 2), (1, 1, -1), (1, -1, 1), (-1, 1, 1)\}$.
2. $x + y + z = \dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = -\dfrac{xyz}{4} = 1$ si et seulement si
$$\begin{cases} \sigma_1 = 1 \\ \sigma_2 = -4 \\ \sigma_3 = -4, \end{cases}$$
si et seulement si x, y, z sont les racines du polynôme $X^3 - X^2 - 4X + 4$. Or, il est clair que $X^3 - X^2 - 4X + 4 = (X - 1)(X - 2)(X + 2)$, donc, l'ensemble de solutions est $\{(1, 2, -2), (1, -2, 2), (2, 1, -2), (2, -2, 1), (-2, 1, 2), (-2, 2, 1)\}$.
3. $x+y+z = \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} = \dfrac{1}{9}(x^2+y^2+z^2) = 1$ si et seulement si $\sigma_1 = \dfrac{\sigma_2}{\sigma_3} = \dfrac{1}{9}(\sigma_1^2 - 2\sigma_2) = 1$ si et seulement si $\sigma_1 = 1$ et $\sigma_2 = \sigma_3 = -4$, si et seulement si x, y, z sont les racines du polynôme $X^3 - X^2 - 4X + 4$. Or, il est clair que $X^3 - X^2 - 4X + 4 = (X - 1)(X - 2)(X + 2)$, donc, l'ensemble de solutions est $\{(1, 2, -2), (1, -2, 2), (2, 1, -2), (2, -2, 1), (-2, 1, 2), (-2, 2, 1)\}$.
4. $x + y + z = \dfrac{x^2 + y^2 + z^2}{7} = \dfrac{x^3 + y^3 + z^3}{10} = 2$ si et seulement si
$$\begin{cases} \sigma_1 = 2 \\ \sigma_2 = -5 \\ \sigma_3 = -6, \end{cases}$$
si et seulement si x, y, z sont les racines du polynôme $X^3 - 2X^2 - 5X + 6$. Or, il est clair que $X^3 - 2X^2 - 5X + 6 = X^3 - X^2 - X^2 + X - 6X + 6 = (X - 1)(X + 2(X - 3)$, donc, l'ensemble de solutions est $\{(1, 3, -2), (1, -2, 3), (-2, 1, 3), (-2, 3, 1), (3, 1, -2), (3, -2, 1)\}$.

4.6 Equations dans $\mathbb{K}[X]$

Exercice 122

Résoudre dans $\mathbb{K}[X]^2$ l'équation $Q^2 = XP^2$, d'inconnue $(P, Q) \in \mathbb{K}[X]^2$.

Réponse 122

Étant donné deux polynomes P et Q on a :

$$\begin{aligned} Q^2 = XP^2 &\Rightarrow \deg Q = 1 + 2\deg P \\ &\Rightarrow P = Q = 0 \end{aligned}$$

Réciproquement, le couple $(0, 0)$ est une solution de l'équation $Q^2 = XP^2$, donc, l'ensemble de solutions de cette équation est le singleton $\{(0, 0)\}$.

Exercice 123

Trouver tous les polynômes P de $\mathbb{C}[x]$ vérifiant

$$P(X^2) = P(X)P(X + 1) \ (*)$$

Réponse 123

Soit P un polynôme à coefficients dans $\mathbb{C}$.

- Si P est constant alors $P(X^2) = P(X)P(X + 1)$ si et seulement si $P^2 = P$, ce qui est équivalent à dire que $P = 0$ ou $P = 1$.
- Supposons P n'est pas constant. D'après le théorème de *Gauss*, P admet au moins une racine dans $\mathbb{C}$. Soit α une telle racine. Si P est une solution de l'équation $*$, alors α^{2^n} et $(\alpha - 1)^{2^n}$ l'est aussi pour tout $n \in \mathbb{N}^*$. Comme P n(admet pas une infinité de racines, alors $\alpha = 0$, $\alpha = 1$ ou $|\alpha| = |\alpha - 1| = 0$. Si $|\alpha| = |\alpha - 1| = 0$ alors α est sur le cercle unité, et sur la médiatrice du segment dont les extrémités sont 0 et 1. Dans ce cas, $\alpha = -j$ ou $\alpha = -\bar{j}$, où $j = e^{2i\pi/3}$, et par la suite j^2 est aussi une racine de P, ce qui est contradictoire, puisqu'on viens de montrer que les seules racines possibles sont $0, 1, -j$ et $-\bar{j}$. Ainsi, les seules racines possibles sont 0 et 1 ou $-\bar{j}$, et par conséquent P est de la forme $P = \gamma X^a(X - 1)^b$, avec $\gamma, a, b \in \mathbb{C}$ et $\gamma \neq 0$. Réciproquement, un simple calcul qu'un tel polynôme est une solution de l'équation $*$ si et seulement si $\gamma = 1$ et $a = b$, c'est à dire que est de la forme $P = X^a(X - 1)^a$.

Exercice 124

Résoudre dans $\mathbb{K}[X]$ les équations suivantes :

1. $(P')^2 = 4P$,
2. $\left(X^2 + 1\right) P'' - 6P = 0$.

Réponse 124

1. — Si P est constant alors P est solution de cette équation si et seulement si $P = 0$.
   — Supposons que P est solution de cette équation et que $\deg P = n \geq 1$. Dans ce cas $2(n-1) = n$, et donc $n = 2$. De plus, si α est une racine de P alors $P'(\alpha) = 0$, ce qui signifie que α est une racine double de P, et alors P est de la forme $P = \gamma(X - \alpha)^2$, où $\alpha, \gamma \in \mathbb{K}$ avec $\gamma \neq 0$. Réciproquement, en choisissant P ainsi on a :

   $$\begin{aligned} (P')^2 = 4P &\iff \gamma^2(X - \alpha)^2 = \gamma(X - \alpha)^2 \\ &\iff \gamma = 1 \end{aligned}$$

   Conclusion : l'ensemble de solutions est $S = \{0, (X - \alpha)^2 \ : \ \alpha \in \mathbb{K}\}$.
2. — Si $\deg P \leq 1$ est constant alors P est solution de cette équation si et seulement si $P = 0$.

— Supposons que P est solution de cette équation et que $\deg P = n \geq 2$. Dans ce cas $n(n-1)\gamma = 6\gamma$, où γ est le coefficient dominant de P, et donc $n = 3$. Et comme X^2+1 divise P, alors P est de la forme $P = (X^2+1)(aX+b)$, où $a, b \in \mathbb{K}$ avec $a \neq 0$. Réciproquement, en choisissant P ainsi on a : $\left(X^2+1\right)P'' - 6P = 0 \iff b = 0$. Conclusion : l'ensemble de solutions est $S = \{aX^3 + aX \ : \ a \in \mathbb{K}\}$.

Exercice 125

Montrer que pour tout $n \in \mathbb{N}$, il existe un unique $P_n \in \mathbb{K}[X]$ tel que $P_n - P_n' = X^n$. Exprimer les coefficients de à l'aide de nombres factoriels.

Réponse 125

Soit $n \in \mathbb{N}$, et supposons qu'il existe un polynôme $P_n \in \mathbb{K}[X]$ tel que $P_n - P_n' = X^n$. Dans ce cas, pour tout $k \in [\![0, n]\!]$, on a : $P_n^{(k)} - P_n^{(k+1)} = \dfrac{n!}{(n-k)!}X^{n-k}$. Ainsi, $\sum\limits_{k=0}^{n} P_n^{(k)} - P_n^{(k+1)} = \sum\limits_{k=0}^{n} \dfrac{n!}{(n-k)!}X^{n-k}$, et finalement $P_n = \sum\limits_{k=0}^{n} \dfrac{n!}{(n-k)!}X^{n-k} = \sum\limits_{k=0}^{n} \dfrac{n!}{(k)!}X^{k}$. Réciproquent,

---

4.7 Divers

Exercice 126

Soit $P \in \mathbb{K}[X]$. Montrer que $P(X+1) = \sum\limits_{n=0}^{N} \dfrac{1}{n!}P^{(n)}(X)$, avec $N > d^\circ P$.

Réponse 126

Pour tout $x \in \mathbb{K}$, la formule de Taylor s'écrit : $P(X+x) = \sum\limits_{n=0}^{N} \dfrac{X^n}{n!}\widetilde{P}^{(n)}(x)$. Par substitution, on obtient $\widetilde{P}(1+x) = \sum\limits_{n=0}^{N} \dfrac{1}{n!}\widetilde{P}^{(n)}(x)$. Sachant que de deux polynômes ayant la même fonction polynomiale sont égaux, on conclut que $P(X+1) = \sum\limits_{n=0}^{N} \dfrac{1}{n!}P^{(n)}(X)$.

Exercice 127 *Polynôme d'intérpolation de Lagrange*

Soit $(x_k)_{0\leq k\leq n}$ une famille de n complexes distincts deux à deux. On définit la familles $(L_k)_{0\leq k\leq n}$ des polynômes d'interpolation de Lagrange associée à la famille $(x_k)_{0\leq k\leq n}$ par :

$$L_i = \prod_{k=0, k\neq l}^{n} \frac{(X - x_j)}{x_i - x_j}$$

1. Montrer que
$$\forall (i,j) \in [\![0,n]\!]^2 \quad , \quad L_i(x_j) = \delta_{i,j}.$$
2. Montrer que tout polynôme $P \in \mathbb{C}_n[X]$ s'écrit de manière unique sous la forme $P = \sum\limits_{k=0}^{n} \alpha_k L_k$, où les α_k sont des nombres complexes que l'on déterminera en fonction de P. Que peut-on déduire ?
3. En déduire que, pour toute famille $(y_k)_{0\leq k\leq n}$ de nombres complexes, il existe un unique polynôme $P \in \mathbb{C}_n[X]$ de degré inférieur ou égal à n tel que $P(x_k) = y_k$ pour tout $k \in [\![0,n]\!]$. On déterminera l'expression de P.

4. Soit P un polynôme non nul à coefficients dans $\mathbb{C}$ tel que $P(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{N}$. Montrer que $P \in \mathbb{Q}[X]$. Plus précisement , si $d = deg(P)$, montrer que $d!P \in \mathbb{Z}$

Réponse 127

1. facile à vérifier
2. Soit $P \in \mathbb{C}_n[X]$. Supposons que P s'écrit sous la forme : $P = \sum_{k=0}^{n} \alpha_k L_k$, où $\alpha_0, \cdots, \alpha_n \in \mathbb{C}$. Il en découle que, pour tout $j \in [\![0, n]\!]$, on a $P(x_j) = \sum_{i=0}^{n} \alpha_i L_i(x_j) = \alpha_j$. D'autre part, si on pose $Q = P - \sum_{k=0}^{n} P(x_k) L_k$, on vérifie facilement que Q est un polynôme de degré inférieur ou égal à n, et admet $x_0, \cdots, x_n$ comme racines. Donc $Q = 0$, et par suite, effectivement, $P = \sum_{k=0}^{n1} P(x_k) L_k$. Comme conséquence, on déduit que la famille $(L_k)_{0 \leq k \leq n}$ est une base de l'espace vectoriel $(\mathbb{C}_n[X], +, .)$.
3. Soit $P \in \mathbb{C}_n[X]$. D'après la question précédente, $P = \sum_{k=0}^{n} P(x_k) L_k$. Ainsi, $P(x_k) = y_k$ pour tout $k \in [\![0, n]\!]$ si et seulement si $P = \sum_{k=0}^{n} y_k L_k$, d'où le résultat.
4. Considérons la famille des polynômes de Lagrange $(L_i)_{0 \leq i \leq d}$, associe à la famille des $(1, 2, \ldots, d)$, avec $d = \deg P$. D'après la question précédente on a $P = \sum_{i=0}^{d} P(i) L_i$. Remarquons que pour tout $i\, [\![0, d]\!]$, $L_i \in \mathbb{Q}[X]$, et que $d!L_i \in \mathbb{Z}[X]$, donc $P \in \mathbb{Q}[X]$ et $d!P \in \mathbb{Z}[X]$.

Exercice 128 *polynômes de Legendre*

Pour tout $n \in \mathbb{N}$, on introduit la famille des polynômes de Legendre P_n par

$$P_n(x) = \frac{1}{2^n.n!} \frac{d^n}{dx^n} \left(\left(x^2 - 1\right)^n \right)$$

1. Voir la solution Déterminer le degré et le coefficient dominant de P_n.
2. Voir la solution En commençant par dériver deux fois $\left(x^2 - 1\right)^{n+1}$, établir que pour tout $n \geq 1$, $P'_{n+1} = (2n + 1)P_n + P'_{n-1}$.

Réponse 128

1. Revenir à la question D'après la formule de Leibniz on a :

$$\begin{aligned} P_n(x) &= \frac{1}{2^n.n!}\frac{d^n}{dx^n}\left(\left(x^2-1\right)^n\right) \\ &= \frac{1}{2^n.n!}\frac{d^n}{dx^n}\left((x-1)^n(x+1)^n\right) \\ &= \frac{1}{2^n.n!}\sum_{k=0}^{n}\binom{n}{k}\frac{d^k}{dx^k}\left((x-1)^n\right)\frac{d^{n-k}}{dx^{n-k}}\left((x+1)^n\right) \\ &= \frac{1}{2^n.n!}\sum_{k=0}^{n}\binom{n}{k}\frac{n!}{(n-k)!}\frac{n!}{k!}(x-1)^{n-k}(x+1)^k \\ &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}^2(x-1)^{n-k}(x+1)^k \end{aligned}$$

Ceci montre que P_n est un polynôme de degrés inférieur ou égal à n, car les fonctions $x \mapsto (x-1)^{n-k}(x+1)^k$ sont des polynômes de degrés égaux à n. D'autre part, le coefficient de P_n de rang n est $\gamma(P_n) = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}^2$, qui est non nul. Ainsi, P_n est un polynôme de degrés n et de coefficient dominant $\gamma(P_n) = \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}^2$.

2. Revenir à la question Soit $n \geq 1$. Alors

$$\begin{aligned} P'_{n+1}(x) &= \frac{1}{2^{n+1}.(n+1)!}\frac{d^{n+2}}{dx^{n+2}}\left(\left(x^2-1\right)^{n+1}\right) \\ &= \frac{1}{2^{n+1}.(n+1)!}\frac{d^n}{dx^n}\left(2x(n+1)\left(x^2-1\right)^n\right) \\ &= d\tfrac{1}{2^{n+1}.(n+1)!}\frac{d^n}{dx^n}\left(2(n+1)\left(x^2-1\right)^n + 4n(n+1)x^2\left(x^2-1\right)^{n-1}\right) \\ &= \frac{1}{2^{n+1}.(n+1)!}\frac{d^n}{dx^n}\left(2(n+1)(2n+1)\left(x^2-1\right)^n + 4n(n+1)\left(x^2-1\right)^{n-1}\right) \\ &= (2n+1)\frac{1}{2^n.n!}\frac{d^n}{dx^n}\left(\left(x^2-1\right)^n\right) + \frac{1}{2^{n-1}.n-1!}\frac{d^n}{dx^n}\left(\left(x^2-1\right)^{n-1}\right) \\ &= (2n+1)P_n + P'_{n-1} \end{aligned}$$

Exercice 129 *Polynômes de Fibonacci*

Soit (P_n) la suite de polynômes définie par $P_0 = 0, P_1 = 1$ et $P_{n+2} = XP_{n+1} - P_n$.

1. Montrer que pour tout $n \in \mathbb{N}$, $P_{n+1}^2 = P_{n+2}P_n + 1$.
2. En déduire que pour tout $n \in \mathbb{N}$, P_n et P_{n+1} sont premiers entre eux.
3. Montrer que pour tout $n \in \mathbb{N}^*$ et $m \in \mathbb{N}$, $P_{n+m} = P_nP_{m+1} - P_{n-1}P_m$.
4. Établir que pour tout $n \in \mathbb{N}$ et $m \in \mathbb{N}$, $P_{n+m} \wedge P_n = P_m \wedge P_n$.
5. En déduire que $P_m \wedge P_n = P_n \wedge P_r$ où r est le reste de la division euclidienne de m par n puis que que $P_m \wedge P_n = P_{m\wedge n}$.

Réponse 129

1. Le résultat est bien vérifié pour $n = 0$. Supposons qu'il l'est pour un certain $n \geq 0$. Ainsi,

$$\begin{aligned} P_{n+2}P_n &= XP_{n+1}P_n - P_n^2 \\ &= P_{n+1}(P_{n+1} + P_{n-1}) - P_{n+1}P_{n-1} - 1 \\ &= P_{n+1}^2 + P_{n+1}P_{n-1}) - P_{n+1}P_{n-1} - 1 \\ &= P_{n+1}^2 - 1, \end{aligned}$$

   d'où le résultat :

$$\forall n \in \mathbb{N}, \quad P_{n+1}^2 = P_{n+2}P_n + 1.$$

2. C'est une application directe du théorème de Bézout, puisque $P_{n+1}^2 - P_{n+2}P_n = 1$.
3. Le résultat est évident pour n quelconque et $m = 0$. Supposons que pour un certain $m \geq 0$, le résultat reste vrai pour tout $n \geq 1$. Donc, pour tout $n \in \mathbb{N}^*$ on a :

$$\begin{aligned} P_{n+(m+1)} &= P_{(n+1)+m} \\ &= P_{n+1}P_{m+1} - P_nP_m \\ &= (XP_n - P_{n-1})P_{m+1} - P_nP_m \\ &= XP_{m+1}P_n - P_{n-1}P_{m+1} - P_nP_m \\ &= (XP_{m+1} - P_m)P_n - P_{n-1}P_{m+1} \\ &= P_nP_{m+2} - P_{n-1}P_{m+1} \end{aligned}$$

   Donc, le résultat est vrai pour $m + 1$, et par suite :

$$\forall n \in \mathbb{N}^*, \quad \forall m \in \mathbb{N}, \quad P_{n+m} = P_nP_{m+1} - P_{n-1}P_m.$$

4. Remarquons que le résultat est évident pour $n = 0$, et supposons dans la suite que $n \neq 0$. Il est clair, d'après la formule précédente, que tout diviseur commun de P_m et P_n est un diviseur aussi de P_{n+m}, donc c'est un diviseur commun de P_{n+m} et P_n. Réciproquement, soit d un un diviseur commun de P_{n+m} et P_n. Toujours d'après la formule précédente, d est un diviseur aussi de $P_{n-1}P_m$. D'autre part, comme d divise P_n et $P_n \wedge P_{n-1} = 1$, alors $d \wedge P_{n-1} = 1$. Ainsi, d'après le théorème de Gauss, d divise P_m, et donc c'est diviseur commun de P_m et P_n. Comme conséquence, $P_{n+m} \wedge P_n = P_m \wedge P_n$.
5. La division Euclidienne de m par n s'écrit : $m = nd+r$. En appliquant l'identité précédente d fois on obtient :

$$P_m \wedge P_n = P_{nd+r} \wedge P_n = P_{n(d-1)+r} \wedge P_n = P_{n(d-2)+r} \wedge P_n = \cdots = P_r \wedge P_n.$$

6. Posons $r_1, \cdots r_s, 0$ les restes des divisions Euclidiennes dans l'algorithme d'Euclide pour le calcul du pgcd de m et n, r_s étant le dernier reste non nul. Donc, $m \wedge n = r_s$, et d'après la question précédente on a

$$P_m \wedge P_n = P_n \wedge P_{r_1} = P_{r_1} \wedge P_{r_2} = \cdots = P_{r_s} \wedge P_0 = P_{r_s} \wedge 0 = P_{r_s} = P_{m \wedge n}.$$

Exercice 130

Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Posons $P_n(X) = \dfrac{1}{n!}X^n(a - bX)^n$. Montrer que P_n, ainsi que toute ses dérivées, prend des valeurs entières en 0 et $\dfrac{a}{b}$.

Réponse 130

Posons $A = X^n$ et $B = (a - bX)^n$ et soit $k \in \mathbb{N}$. D'après la formule de Leibnitz on a :

$$P_n^{(k)}(X) = \frac{1}{n!}\sum_{i=0}^{k}\binom{k}{i}A^{(i)}B^{(k-i)} = \frac{1}{n!}\sum_{i=0}^{k}\binom{k}{i}A^{(k-i)}B^{(i)}.$$

Ainsi, il suffit de montrer que, pour tout $i, j \in \mathbb{N}$, $\frac{1}{n!}\binom{i+j}{i} A^{(i)}B^{(j)}$ prend des valeurs entières en 0 et $\frac{a}{b}$. Or, si $i > n$, ou $i > n$, alors $A^{(i)}B^{(j)} = 0$. Aussi, tenant compte de la multiplicité des racines, si $i < n$, alors $A^{(i)}(0) = 0$, et si $j < n$, alors $B^{(j)}(\frac{a}{b}) = 0$. De plus, pour $i = n$ et $j \leq n$ on a :

$$\frac{1}{n!}\binom{n+j}{n} A^{(n)}(0).B^{(j)}(0) = \binom{n+j}{n}\binom{n}{j} j!a^{2n-k}(-b)^{n-j} \in \mathbb{Z}.$$

De la même manière, pour $j = n$ et $i \leq n$ on a :

$$\begin{aligned}\frac{1}{n!}\binom{n+i}{n} A^{(i)}(\frac{a}{b}).B^{(n)}(\frac{a}{b}) &= \binom{n+i}{n}\binom{n}{i} i!(\frac{a}{b})^{n-i}(-b)^n \\ &= \binom{n+i}{n}\binom{n}{i} i!a^{n-i}b^i \in \mathbb{Z}\end{aligned}$$

d'où le résultat.

Exercice 131 *Contenu des produits de polynômes et divisibilité*

Soient $P(X), Q(X) \in \mathbb{Z}[X]$. On définit le **contenu** d'un polynôme $P(X)$, noté $\mathrm{C}(P(X))$, comme étant le plus grand commun diviseur (pgcd) des coefficients de $P(X)$. On dit qu'un polynôme de $\mathbb{Z}[X]$ est primitif si ses coefficients sont premiers entre eux dans l'ensemble, i.e., $\mathrm{C}(P(X)) = 1$.

1. **Lemme de Gauss sur le contenu des produits** :
   (a) Montrez que si le produit de deux polynômes primitifs est également un polynôme primitif.
   (b) En déduire que, pour tout $P(X), Q(X) \in \mathbb{Z}[X]$, on a :
   $$\mathrm{C}(P(X)Q(X)) = \mathrm{C}(P(X)) \cdot \mathrm{C}(Q(X)).$$
2. **Application à la divisibilité et à l'irréductibilité dans** $\mathbb{Z}[X]$ Soit $P(X), Q(X) \in \mathbb{Z}[X]$.
   (a) Soit $Q(X) \in \mathbb{Z}[X]$ et $L(X) \in \mathbb{Q}[X]$. Montrer que si
   $$P(X) = Q(X)L(X).$$
   alors $L \in \mathbb{Z}[X]$.
   (b) En déduire que P est irréductible dans $\mathbb{Z}[X]$ si et seulement si il l'est dans $\mathbb{Q}[X]$.

Réponse 131

1. (a) Soit $P(X), Q(X) \in \mathbb{Z}[X]$ deux polynômes primitifs, et posons $P = \sum_{k=0}^{m} a_k X^k$ et $P = \sum_{k=0}^{n} abkX^k$. Soit p un nombre premier. Comme $\bigwedge_{0\leq k\leq m} a_k = \bigwedge_{0\leq k\leq n} b_k = 1$, alors il existe $k \in [\![0, m]\!]$ et $l \in [\![0, n]\!]$ de sorte que p ne divise ni a_k ni b_l. On choit k et l comme étant les plus petits entiers à vérifier cette propriété. Pour montrer que PQ est primitif, il suffit de montrer que p ne divise pas tous ses coefficients. Plus précisément, on va montrer qu'il ne divise pas le coefficient de X^{k+l}, c'est à dire que p ne divise pas $\sum_{\substack{0\leq i\leq m\\ 0\leq j\leq n\\ i+j=k+l}} a_i b_j$. Or, pour tout $i \in [\![0, m]\!]$ et $j \in [\![0, n]\!]$ tels que $i+j = k+l$ on a, soit $i \leq i$, soit $j \leq l$. De plus, si $i < k$ alors p/a_i, et si $j < l$ alors p/b_j, donc, dans les deux cas $p/a_i b_j$. Et comme p est un nombre premier qui ne divise ni a_k ni

b_l, alors p ne divise pas $a_k b_l$, et par la suite p ne divise pas aussi $\sum_{\substack{0\leq i\leq m\\ 0\leq j\leq n\\ i+j=k+l}} a_i b_j$, et le résultat est établi.

(b) Soit $P(X), Q(X) \in \mathbb{Z}[X]$. En factorisant par leur contenus, on peut écrire $P = \mathrm{C}(P)A$ et $Q = \mathrm{C}(Q)B$, où A, B sont des polynômes primitifs . Ainsi, $PQ = \mathrm{C}(P)\mathrm{C}(Q)AB$, et par suite :

$$\mathrm{C}(PQ) = \mathrm{C}\left(\mathrm{C}(P)\mathrm{C}(Q)AB\right) = \mathrm{C}(P)\mathrm{C}(Q)\mathrm{C}\left(AB\right) = \mathrm{C}(P)\mathrm{C}(Q)$$

2. **Application à la divisibilité dans** $\mathbb{Z}[X]$:

(a) Soit $P(X), Q(X) \in \mathbb{Z}[X]$ et $L(X) \in \mathbb{Q}[X]$ tels que $P(X) = Q(X)L(X)$. On peut multiplier L par un entier naturel a de sorte que $aL(X) \in \mathbb{Z}[X]$. Dans ce cas,

$$\mathrm{C}(aP) = \mathrm{C}\left(Q(aL)\right) = \mathrm{C}(Q)\mathrm{C}(aL) = \mathrm{C}(aL)$$

Ceci montrer que a divise $\mathrm{C}(aL)$, puis que $L \in \mathbb{Z}[X]$.

(b) Le sens réciproque est évident. Montrons donc le sens direct par contraposé. Pour cela, supposons que P est réductible dans $\mathbb{Q}[X]$, et montrons qu'il l'est dans $\mathbb{Z}[X]$. Il existe dans ce cas $L(X), Q(X) \in \mathbb{Q}[X]$ tels que $P(X) = Q(X)L(X)$ avec $1 \deg Q < \deg P$. On peut multiplier L par un entier naturel a, et Q par un entier naturel b de sorte que $aL(X) \in \mathbb{Z}[X]$ et $bQ(X) \in \mathbb{Z}[X]$. On peut ainsi écrire $abP(X) = cA(X)B(X)$, où $c \in \mathbb{N}$, et A, B sont deux polynômes à coefficients dans $\mathbb{Z}$ et primitifs tels que avec $1 \deg A < \deg P$. Ainsi, ab divise c, et on a alors $P(X) = \dfrac{c}{ab}A(X)B(X)$, ce qui montre que P est réductible dans $\mathbb{Z}[X]$.

Exercice 132 *Le critère d'Eisenstein*

Soit P un polynôme à coefficients dans $\mathbb{Z}$ défini par :

$$P(x) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

1. On suppose qu'il existe un nombre premier p tel que :
   — $p \mid a_i$ pour tout $i \in \{0, 1, \ldots, n-1\}$,
   — $p \nmid a_n$,
   — $p^2 \nmid a_0$.

   Montrez que, dans ce cas, le polynôme P est irréductible sur $\mathbb{Q}$, c'est-à-dire qu'il ne peut pas être écrit comme le produit de deux polynômes non constants à coefficients rationnels.
2. Vérifiez si le polynôme suivant est irréductible sur $\mathbb{Q}$ en utilisant le critère d'Eisenstein :

$$Q = X^4 + 5X^3 + 10X^2 + 15X + 25.$$

Réponse 132

1. Supposons que P soit réductible sur $\mathbb{Q}$. D'après l'exercice 131, P est aussi réductible sur $\mathbb{Z}$, et par la suite il existe deux polynômes A et B dans $\mathbb{Z}[x]$, de degrés respectifs d_A et d_B (avec $d_A, d_B \geq 1$ et $d_A + d_B = n$), tels que

$$P = AB.$$

Pour la suite, on utilisera deux méthodes, la première est élémentaires, la seconde se fait par réduction à $\mathbb{Z}/p\mathbb{Z}[X]$.

— *Première méthodes :* Posons $A = \sum_{k=0}^{r} c_k X^k$ et $B = \sum_{k=0}^{s} d_k X^k$. Donc $a_0 = c_0 d_0$, et comme $p \mid a_0$, alors $p \mid c_0$ ou $p \mid d_0$. Supposons que $p \mid c_0$. Dans ce cas, puisque $p^2 \nmid a_0$, alors $p \nmid d_0$. Maintenant, il est facile de montrer par récurrence sur k, que $p \mid c_k$, pour tout $k \in [\![0, r]\!]$, ce qui entraine que $p \mid a_n$, car $a_n = c_r d_s$, ce qui est faux par hypothèse.

— *Première méthodes :* En passant modulo p, on aura dans $\mathbb{Z}/p\mathbb{Z}[X]$ l'identité $\overline{P} = \overline{A} \times \overline{B}$.

Et comme, $p \mid a_i$ pour $i = 0, \ldots, n-1$, donc $\overline{P} = \overline{a_n} X^n \pmod{p}$. Puisque $p \nmid a_n$, alors p ne divise pas les coefficients dominants de A et B, et il s'ensuit que $\deg \overline{A}, \deg \overline{B} \geq 1$. Et de l'égalité, $\overline{a_n} X^n = \overline{A} \times \overline{B}$, on déduit que X divise $\overline{A}$ et $\overline{B}$. d'où, p divise les coefficients constants de A et B, et par suite, p^2 divise le produit des coefficients constants de A et B. Or, ce produit est égal à a_0, ce qui contredit l'hypothèse $p^2 \nmid a_0$. Conclusion : P est irréductible sur $\mathbb{Q}$.

2. Remarquons que le nombre $p = 5$ vérifie les hypothèses du critère d'Eisenstein, donc, le polynôme Q est irréductible sur $\mathbb{Q}$.

Exercice 133

Soit P un polynôme non constant à coéfficients entiers. Montrer que pour tout $n_0 \in \mathbb{N}$, il existe $n \geqslant n_0$ tel que $P(n)$ n'est pas un nombre premier

Réponse 133

Cela revient à montrer qu'il existe une infinité d'entiers naturels n pour lesquels $P(n)$ n'est pas un nombre premier.

— Premier cas : Supposons que $\deg P = 1$, donc de la forme $p = aX + b$, où $a, b \in \mathbb{N}$ avec $a \neq 0$. Soit p un nombre premier qui ne divise pas a. Il existe alors $a' \in \mathbb{N}$ tel que $a \cdot a' \equiv 1 \pmod{p}$, et il en découle que :

$$\forall \in \mathbb{N}, \quad an + b \equiv 0 \pmod{p} \Leftrightarrow n \equiv -b \cdot a' \pmod{p}.$$

Ainsi, $P(n)$ n'est pas un nombre premier, pour tout entiers naturels n de la forme $n = kp - ba'$ avec $k \in \mathbb{N}$.

— Deuxième cas : Supposons que $\deg P > 1$, et soit z une racine complexe de P. Une telle racine existe par le théorème de *Gauss*. Remarquons que l'ensemble

$$\{n \in \mathbb{N}^* \ : \ \exists A \in \mathbb{Q}[X] \text{ et } A(z) = 0\}$$

est une partie non vide de $\mathbb{N}$, contenant $\deg P$. Donc, elle admet un plus petit élément d. Considérons alors un polynôme non constant $Q \in \mathbb{Q}[X]$ annulant z de degré minimal, i.e., $\deg Q = d$. En multipliant Q par un entier naturel bien choisi, on peut supposer que $Q \in \mathbb{Z}[X]$ primitif, c'est à dire que ses coefficients sont premiers entre eux. Maintenant, effectuons la division Euclidienne dans $\mathbb{Q}[X]$ du polynôme $L = P \circ (P + X)$ par Q. Elle s'écrit : $L = QA + R$ avec $\deg R < \deg Q$. Or, il est facile de voir que $R(z) = 0$, ce qui permet de conclure que $R = 0$, sinon, on aboutira à une contradiction avec la définition de Q. Ainsi, $L = QA$, et en appliquant l'exercice 131, on déduit que $A \in \mathbb{Z}[X]$. D'autre part, il est clair que $1 \leq \deg Q \leq \deg P < \deg L$, et donc aussi $1 \leq \deg A < \deg L$. Il s'ensuit que $2 \leq A(n)$ et $2 \leq Q(n)$ à partir d'un certain rang, ce qui entraine que $L(n)$, qui n'est autre que $P\,(n + P(n))$, n'est pas un nombre premier. Pour conclure, il suffit d'avoir $\lim n + P(n) = +\infty$, ce qui est possible en remplaçant P par $-P$ dans le cas échéant.

Exercice 134

Soit $\alpha \in \mathbb{C}$. On dit que α est algébrique sur $\mathbb{Q}$, s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $\widetilde{P}(\alpha) = 0$. On suppose que α est algébrique.

1. Montrer que l'ensemble $I(\alpha) = \left\{P \in \mathbb{Q}[X] : \ \widetilde{P}(\alpha) = 0\right\}$ est un idéal de $\mathbb{Q}[X]$, c'est à dire un sous groupe de $\mathbb{Q}[X]$ tel que pour tous $P \in I(\alpha)$ et $P \in \mathbb{Q}[X]$, on a $PQ \in I(\alpha)$.
2. En déduire qu'il existe un unique $\pi_\alpha \in I(\alpha)$ tel que $I(\alpha) = \{\pi_\alpha P : \ P \in \mathbb{Q}[X]\}$. π_α s'appelle le polynôme minimal α dans $\mathbb{Q}$
3. Montrer que π_α est irréductible dans $\mathbb{Q}[X]$, et que α est une racine simple de π_α.

Réponse 134

1. En effet, $I_\alpha \neq \emptyset$, car il contient le polynôme nul. De plus, pour tous polynôme $P, Q \in I(\alpha)$ et $L \in \mathbb{Q}[X]$, on a $\widetilde{(PL - Q)}(\alpha) = 0$, donc $PL - Q \in I_\alpha$, et par suite $I(\alpha)$ est un idéal de $\mathbb{Q}[X]$.
2. Car c'est un idéal non nul de $P\mathbb{Q}[X]$.
3. Supposons que π_α se factorise sous la forme $\pi_\alpha = AB$, avec $A, B \in \mathbb{Q}[X]$. On en déduit que $\widetilde{A}(\alpha) = 0$ ou $\widetilde{B}(\alpha) = 0$. Supposons par exemple que $\widetilde{A}(\alpha) = 0$. Donc, $A \in I(\alpha)$, et par suite π_α divise A. Et comme A divise π_α, alors A et π_α sont associés, ce qui implique que π_α est irréductible dans $\mathbb{Q}[X]$. Supposons maintenant que α est une racine multiple de π_α. Ceci veut dire que $\widetilde{\pi'_\alpha}(\alpha) = 0$, et par suite $\pi'_\alpha \in I(\alpha)$, puis π_α divise π'_α, ce qui est contradictoire, car $0 \leq \deg \pi'_\alpha < \deg \pi_\alpha$.

Chapitre 5

Les fractions rationnelles

5.1 Généralité

Exercice 135

Soit $F \in \mathbb{K}(X)$. Montrer que $\deg F' \leq \deg F - 1$, avec égalité si et seulement si $\deg F \neq 0$. Montrer, de plus, que pour tout entier $n \geq 2$, il existe une fraction rationnelle telle que $\deg F = 0$ et $\deg F' = -n$.

Réponse 135

— Supposons que $\deg F < 0$. Si $F = 0$ alors il est clair que $\deg(F') = \deg(F) - 1 = -\infty$. Supposons de plus, que $F \neq 0$. Alors F s'écrit sous la forme $F = \dfrac{P}{Q}$, où P, Q sont deux polynômes non nuls tels que $\deg P < \deg Q$. Ainsi, $\deg(F) = \deg(P) - \deg(Q)$, et

$$\deg(F') = \deg\left(\frac{P'Q - PQ'}{Q^2}\right) = \deg\left(P'Q - PQ'\right) - 2\deg\left(Q\right).$$

Or, il est facile de montrer que $P'Q - PQ'$ est un polynôme de degré $\deg P + \deg Q - 1$, dont le coefficient dominant est $\mathrm{dom}(P)\mathrm{dom}(P)\left(\deg P - \deg Q\right) \neq 0$, où $\mathrm{dom}(P)$ et $\mathrm{dom}(Q)$ désignent les coefficients dominants de P et Q. On en déduit que

$$\deg F' = \deg F - 1.$$

— Supposons que $\deg F \geq 0$, et posons F sous la forme $F = E + G$, où E est la partie entière de F, et G est une fraction rationnelle de degré strictement négatif. Alors, $F' = E' + G'$, $\deg F = \deg E$ et

$$\deg F' = \begin{cases} \deg E' \text{ , si } E' \neq 0 \\ \deg G' \text{ , si } E' = 0 \end{cases}.$$

Donc,

— Si $E' = 0$, ce qui revient à dire que $\deg F = \deg E = 0$, alors

$$\deg F' = \deg G' = \deg G - 1 < \deg F - 1,$$

— Si $E' > 0$, ce qui revient à dire que $\deg F = \deg E > 0$, alors

$$\deg F' = \deg E' = \deg E - 1 = \deg F - 1.$$

Comme conclusion, $\deg F' \leq \deg F - 1$, avec égalité si et seulement si $\deg F \neq 0$. De plus, pour tout entier $n \geq 2$, en prenant $F = 1 + \dfrac{1}{X^{n-1}}$ on a $\deg F = 0$ et $\deg F' = -n$.

Exercice 136

1. Démontrer qu'il n'existe pas de fraction rationnelle F tel que $F^2 = X$.
2. Démontrer qu'il n'existe pas de fraction rationnelle F tel que $F' = \dfrac{1}{X}$.

Réponse 136

1. La fraction rationnelle nulle nul n'est pas solution de notre équation, et si F est une fraction rationnelle non nulle telle que $F^2 = X$, alors $\deg(F^2) = 2\deg(F)$. Or, $\deg(X) = 1$, et l'équation $2n = 1$ n'a pas de solutions dans $\mathbb{Z}$.
2. Soit F une fraction rationnelle telle que $F' = \dfrac{1}{X}$.
   - **Première méthode :** On sait que F s'écrit de manière unique sous la forme $F = E + G$, avec E est la partie entière de F, et G est une fraction rationnelle de degré strictement négatif. D'après l'exercice 135 on a $\deg G' < \deg G$. D'autre part, après dérivation, on déduit que $E' = 0$ et $G' = \dfrac{1}{X}$, et par suite $\deg G' = -1$. D'où, $-1 = \deg G' < \deg G < 0$, ce qui est impossible.
   - **Deuxième méthode :** Il est facile de remarque que 0 est un pôle de F. Sa partie polaire s'écrit sous la forme $\sum_{k=1}^{m} \dfrac{a_k}{X^k}$, où $m \in \mathbb{N}^*$ et $a_1, \cdots, a_m \in \mathbb{K}$ non tous nuls. On en déduit que 0 est un pôle de F' de partie polaire égale à $\sum_{k=1}^{m} \dfrac{-ka_k}{X^{k+1}}$. Or, d'après ce l'égalité $F' = \dfrac{1}{X}$, 0 est un pôle de F' de partie polaire égale à $\dfrac{1}{X}$, d'où la contradiction.

   Conclusion : Il n'existe donc pas de fraction rationnelle F telle que $F' = 1/X$.

Exercice 137

Existe-t-il une fraction rationnelle F telle que

$$F(X)^2 = (X^2+1)^3 ?$$

Réponse 137

Écrivons $F(X) = \frac{P(X)}{Q(X)}$ avec P et Q deux polynômes premiers entre eux, et Q unitaire. La condition $F(X)^2 = (X^2+1)^3$ devient

$$P^2 = (X^2+1)^3 Q^2.$$

Ainsi, Q^2 divise P^2. D'où $Q^2 = 1$, puisque P^2 et Q^2 sont premiers entre eux. Donc $Q = 1$ (ou -1). Ainsi, $F = P$ est un polynôme et $P^2 = (X^2+1)^3$.

En particulier, P^2 est de degré 6, donc P doit être de degré 3. Écrivons $P = aX^3 + bX^2 + cX + d$, et développons l'identité $P^2 = (X^2+1)^3$:

$$X^6+3X^4+3X^2+1 = a^2X^6+2abX^5+(2ac+b^2)X^4+(2ad+2bc)X^3+(2bd+c^2)X^2+2cdX+d^2.$$

On identifie les coefficients : pour le coefficient de X^6, on a $a = \pm 1$; pour le coefficient de X^5, on a $b = 0$; pour le coefficient constant, on a $d = \pm 1$; pour le coefficient de X, on a $c = 0$. Mais alors, le coefficient de X^3 doit vérifier $2ad + 2bc = 0$, ce qui est faux.

Ainsi, aucun polynôme ne vérifie l'équation $P^2 = (X^2+1)^3$, et par le raisonnement du début, aucune fraction non plus.

Exercice 138

Déterminer un supplémentaire de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$.

Réponse 138

On sait que toute fraction rationnelle s'écrit de manière unique comme la somme d'un polynôme, qui est sa partie entière, et une fraction rationnelle de degré strictement négatif. L'ensemble des fractions rationnelles de degrés strictement négatifs étant un sous espace vectoriel de $\mathbb{K}(X)$, alors c'est un supplémentaire de $\mathbb{K}[X]$ dans $\mathbb{K}(X)$.

Exercice 139

Soit $F \in \mathbb{K}(X)$ une fraction rationnelle non nulle de représentant irréductible $\dfrac{P}{Q}$. Montrer que F est paire si, et seulement si, P et Q sont tous deux pairs, ou tous deux impairs.

Réponse 139

Supposons que F est paire. Donc, $P(-x)Q(x) = Q(-x)P(x)$, et d'après le théorème de Gauss, $P(x)$ divise $P(-x)$ et $Q(x)$ divise $Q(-x)$. Comme $\deg P = \deg P(-x)$ et $\deg Q = \deg Q(-x)$, alors les polynômes P, $P(-x)$, ainsi que Q, $Q(-x)$ sont associés, c'est à dire qu'on a $P(-x) = \alpha P(x)$ et $Q(-x) = \beta Q(x)$ pour certain $\alpha, \beta \in \mathbb{K}^*$. Ainsi, $\alpha P(x)Q(x) = \beta Q(x)P(x)$ et, par identification des coefficients dominants, on a $\alpha = \pm 1$ et $\alpha = \pm 1$. Et puisque $F \neq 0$, alors $\alpha = \beta = \pm$, et le résultat en découle.

Exercice 140

Soit F une fraction rationnelle de $\mathbb{R}(X)$ telle que $F(n) \in \mathbb{Q}$ pour une infinité d'entiers $n \in \mathbb{N}$. On veut démontrer que $F \in \mathbb{Q}(X)$.

On note $\omega(R) = \deg(P) + \deg(Q)$.

1. Démontrer le résultat si F est de la forme $F = \dfrac{P}{Q}$ avec $\deg(P) + \deg(Q) \leq 0$.
2. Soit $d \geq 0$. On suppose que le résultat est vrai pour toute fraction rationnelle de la forme $\dfrac{P}{Q} \in \mathbb{R}(X)$ tel que $\deg(P) + \deg(Q) \leq d$, et supposons que F est de la forme $F = \dfrac{P}{Q}$ tel que $\deg(P) + \deg(Q) = d + 1$.
   (a) Justifier l'existence d'un entier $m \in \mathbb{N}$ tel que $Q(m) \neq 0$ et $F(m) \in \mathbb{Q}$. Dans toute la suite, m désigne cet entier.
   (b) Montrer qu'il existe un polynôme $P_0 \in \mathbb{R}[X]$ tel que
   $$P(X)Q(m) - Q(X)P(m) = (X - m)P_0,$$
   et que $\deg(P_0) < \max(\deg(P), \deg(Q))$.
   (c) On supposer dans cette question que $\deg(P) \geq \deg(Q)$, et on pose $G = \dfrac{P_0}{Q(m)Q}$. Exprimer G en fonction de F, et en déduire que $\dfrac{P_0}{Q(m)Q} \in \mathbb{Q}(X)$, puis que $F \in \mathbb{Q}(X)$.
   (d) En déduire que $F \in \mathbb{Q}(X)$.
3. Conclure.

Réponse 140

1. Si $\deg(P)+\deg(Q)\leq 0$, alors F est le quotient de deux réels, et donc F est réel r. Mais, par hypothèse, $F(n)\in\mathbb{Q}$ pour une infinité d'entiers $n\in\mathbb{N}$, donc $F=r\in\mathbb{Q}$.
2. (a) Comme Q est non nul, alors il admet au plus un nombre fini de racines, et comme $F(n)\in\mathbb{Q}$ pour une infinité d'entiers $n\in\mathbb{N}$, alors il existe 'un entier $m\in\mathbb{N}$ tel que $Q(m)\neq 0$ et $F(m)\in\mathbb{Q}$.
   (b) Considérons S le polynôme $S(X)=P(X)Q(m)-Q(X)P(m)$. Alors, $\deg(S)\leq\max(\deg(P),\deg(Q))$. De plus, $S(m)=0$. Ainsi, S se factorise en $S(X)=(X-m)P_0(X)$ avec $\deg(P_0)<\max(\deg(P),\deg(Q))$.
   (c) Il est clair que $G=\dfrac{1}{X-m}\left(F-\dfrac{P(m)}{Q(m)}\right)$. On en déduit que, pour tout entier $n\neq m$ tel que $F(m)\in\mathbb{Q}$, on a $G(m)\in\mathbb{Q}$. D'autre part, puisque $\deg(P_0)<\deg(P)$, alors $\deg(P_0)+\deg(Q(m)Q)<\deg(P)+\deg(Q)=d+1$. Donc, d'après l'hypothèse de récurrence, $G\in\mathbb{Q}[X]$. Et comme $F=(X-n)G+\frac{P(m)}{Q(m)}$, alors $F\in\mathbb{Q}[X]$.
   (d) D'après ce qui précède, si $\deg(P)\geq\deg(Q)$ alors $F\in\mathbb{Q}[X]$. Si $\deg(P)<\deg(Q)$, alors le résultat précédent s'applique $\dfrac{1}{F}$, qui vérifie les mêmes hypothèses que F, et donc $\dfrac{1}{F}\in\mathbb{Q}[X]$ puis $F\in\mathbb{Q}[X]$. Donc, dans tout les cas, $F\in\mathbb{Q}[X]$.
3. D'après le principe de récurrence, Si F une fraction rationnelle de $\mathbb{R}(X)$ telle que $F(n)\in\mathbb{Q}$ pour une infinité d'entiers $n\in\mathbb{N}$, alors $F\in\mathbb{Q}(X)$.

Exercice 141

Soient p et q deux entiers naturels premiers entre eux. Déterminer les racines et les pôles de $\dfrac{X^p-1}{X^q-1}$, en précisant leur ordre de multiplicité.

Réponse 141

Les racines de X^p-1 (resp. X^q-1) sont les racines p-ièmes de l'unité (resp. q-ièmes) et elles sont toutes simples. Soit ω une racine de X^p-1 et de X^q-1. Alors $\omega^p=\omega^q=1$. Mais, puisque p et q sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers $u,v\in\mathbb{Z}$ tels que $pu+qv=1$. Alors

$$\omega=\omega^{pu+qv}=(\omega^p)^u(\omega^q)^v=1.$$

Donc, les racines de la fraction rationnelle sont simples, et ce sont les racines p-ièmes de l'unité autre que 1, et ses pôles sont aussi simples et ce sont les racines q-ièmes de l'unité, autre que 1.

Exercice 142

Soit $F=\dfrac{P}{Q}$ une fraction rationnelle écrite sous forme irréductible. On suppose qu'il existe une fraction rationnelle G telle que

$$G\left(\frac{P(X)}{Q(X)}\right)=X.$$

1. Si $G=\dfrac{a_nX^n+\cdots+a_1X+a_0}{b_nX^n+\cdots+b_1X+b_0}$, montrer que P divise (a_0-b_0X) et que Q divise (a_n-b_nX).
2. En déduire que $F=\dfrac{P}{Q}$ est de la forme $F(X)=\dfrac{aX+b}{cX+d}$.

3. Pour $Y = \dfrac{aX+b}{cX+d}$, exprimer X en fonction de Y. En déduire l'expression de G.

Réponse 142

1. Posons $G = \frac{A}{B}$ et $F = \frac{P}{Q}$ (avec A, B, P, Q des polynômes). On réécrit l'identité $G(F(X)) = X$ sous la forme
$$A(F(X)) = XB(F(X)).$$
Posons $n = \max(\deg A, \deg B)$. Alors $n \geq 1$ car sinon, A et B seraient constants et $G\left(\frac{P}{Q}\right) = X$ aussi.
On a donc $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{n} b_k X^k$, où $(a_n, b_n) \neq (0,0)$, et l'identité devient
$$\sum_{k=0}^{n} a_k \left(\frac{P}{Q}\right)^k = X \sum_{k=0}^{n} b_k \left(\frac{P}{Q}\right)^k.$$
En multipliant par Q^n, cela donne
$$\sum_{k=0}^{n} a_k P^k Q^{n-k} = \sum_{k=0}^{n} b_k X P^k Q^{n-k}.$$
Donc
$$(a_0 - b_0 X)Q^n + \left(\cdots + (a_k - b_k X)P^k Q^{n-k} + \cdots\right) + (a_n - b_n X)P^n = 0,$$
où les termes dans la parenthèse centrale sont tous divisibles par P et par Q. Comme Q divise aussi le premier terme, alors Q divise $(a_n - b_n X)P^n$.
D'après le lemme de Gauss, puisque P et Q sont premiers entre eux, alors Q divise $(a_n - b_n X)$. De même, P divise tous les termes de la parenthèse centrale et le dernier, donc P divise aussi $(a_0 - b_0 X)Q^n$, donc P divise $(a_0 - b_0 X)$.
2. Supposons de plus qu'on a écrit $G = \frac{A}{B}$ sous forme irréductible, c'est-à-dire avec $\gcd(A, B) = 1$. Vu que a_n et b_n ne sont pas tous les deux nuls, alors $a_n - b_n X$ n'est pas le polynôme nul. Comme Q divise $a_n - b_n X$, alors nécessairement Q est de degré au plus 1 ; on écrit $Q(X) = cX + d$.
Par ailleurs, $a_0 - b_0 X$ n'est pas non plus le polynôme nul, car sinon on aurait $a_0 = b_0 = 0$ et donc A et B seraient tous les deux sans terme constant, donc divisibles par X (ce qui est impossible puisqu'ils sont premiers entre eux). Donc P est aussi de degré au plus 1, et on écrit $P(X) = aX + b$. Conclusion :
$$F(X) = \frac{aX+b}{cX+d}.$$
Notez que a et b ne sont pas tous les deux nuls en même temps (de même pour c et d).
3. Si $Y = \frac{aX+b}{cX+d}$ avec $(a, b) \neq (0, 0)$, alors
$$X = \frac{-dY - b}{cY - a}.$$
Autrement dit, si on note $\phi(X) = \frac{aX+b}{cX+d}$, alors sa bijection réciproque est
$$\phi^{-1}(Y) = \frac{-dY - b}{cY - a}.$$
Nous avons prouvé que
$$G\left(\frac{aX+b}{cX+d}\right) = X.$$

Cette identité s'écrit $G(\phi(X)) = X$. Appliquée en $X = \phi^{-1}(Y)$, elle devient $G(\phi(\phi^{-1}(Y))) = \phi^{-1}(Y)$, c'est-à-dire $G(Y) = \phi^{-1}(Y)$. Ainsi,

$$G(Y) = \frac{-dY - b}{cY - a}.$$

5.2 Décomposition en éléments simples

Exercice 143

Décomposer sur $\mathbb{R}$ les fractions rationnelles suivantes :

1. $\dfrac{X^2 + 2X + 5}{X^2 - 3X + 2}$
2. $\dfrac{X^2 + 3X + 1}{(X-1)^2(X-2)}$
3. $\dfrac{1}{X^4 - 1}$.

Réponse 143

1. posons $P(X) = X^2 + 2X + 5$, $Q(X) = X^2 - 3X + 2$, $Q'(X) = 2X - 3$. On a $X^2 + 2X + 5 = 1(X^2 - 3X + 2) + 5X + 3$ et $X^2 - 3X + 2 = (X-1)(X-2)$. La décomposition en éléments simples s'écrit sous la forme :

$$\frac{X^2 + 2X + 5}{X^2 - 3X + 2} = 1 + \frac{a}{X-1} + \frac{b}{X-2}.$$

avec $a, b \in \mathbb{R}$. Ainsi, $a = \frac{P(1)}{Q'(1)} = \frac{8}{-1} = -8$ et $b = \frac{P(2)}{Q'(2)} = \frac{13}{1} = 13$, et finalement :

$$\frac{X^2 + 2X + 5}{X^2 - 3X + 2} = 1 - \frac{8}{X-1} + \frac{13}{X-2}.$$

2. — Puisque le degré du dénominateur est strictement supérieur au degré du numérateur, la partie entière est nulle.
   — On a donc
   $$\frac{X^2 + 3X + 1}{(X-1)^2(X-2)} = \frac{a}{X-2} + \frac{b}{X-1} + \frac{c}{(X-1)^2}.$$
   — Calculons a. On pose $P(X) = X^2 + 3X + 1$, $Q(X) = (X-1)^2(X-2)$, $Q'(X) = 2(X-1)(X-2) + (X-1)^2$ et
   $$a = \frac{P(2)}{Q'(2)} = \frac{11}{1} = 11.$$
   — Calculons c. On multiplie par $(X-1)^2$ et on évalue en $X = 1$.
   $$\begin{aligned} \frac{X^2 + 3X + 1}{X-2} &= \frac{11(X-1)^2}{X-2} + b(X-1) + c \\ \frac{5}{-1} &= c \implies c = -5. \end{aligned}$$
   On a donc
   $$\frac{X^2 + 3X + 1}{(X-1)^2(X-2)} = \frac{11}{X-2} + \frac{b}{X-1} + \frac{-5}{(X-1)^2}.$$

— Pour calculer b, on multiplie par X et on fait tendre X vers l'infini.

$$\frac{X(X^2+3X+1)}{(X-1)^2(X-2)} = \frac{11X}{X-2} + \frac{bX}{X-1} + \frac{-5X}{(X-1)^2}.$$

Quand $X \to +\infty$,

$$1 = 11 + b + 0 \implies b = -10.$$

Conclusion :

$$\frac{X^2+3X+1}{(X-1)^2(X-2)} = \frac{11}{X-2} - \frac{10}{X-1} - \frac{5}{(X-1)^2}.$$

3. — La partie entière est nulle.

— On factorise le dénominateur :

$$X^4 - 1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1).$$

— On écrit

$$\frac{1}{X^4-1} = \frac{a}{X-1} + \frac{b}{X+1} + \frac{cX+d}{X^2+1}.$$

— On pose $P(X) = 1$, $Q(X) = X^4 - 1$ de sorte que $Q'(X) = 4X^3$ et

$$a = \frac{P(1)}{Q'(1)} = \frac{1}{4}$$

$$b = \frac{P(-1)}{Q'(-1)} = \frac{-1}{4}.$$

— Pour calculer c et d, on effectue d'abord la décomposition en éléments neutres sur $\mathbb{C}$ et on regroupe les termes conjugués.

— Décomposons la fraction rationnelle sur $\mathbb{C}$.

$$X^4 - 1 = (X-1)(X+1)(X^2+1) = (X-1)(X+1)(X-i)(X+i).$$

On écrit

$$\frac{1}{X^4-1} = \frac{a}{X-1} + \frac{b}{X+1} + \frac{e}{X-i} + \frac{f}{X+i}.$$

On pose $P(X) = 1$, $Q(X) = X^4 - 1$, $Q'(X) = 4X^3$. On a déjà vu $a = 1/4$, $b = -1/4$ et on a

$$e = \frac{P(i)}{Q'(i)} = \frac{1}{4i^3} = \frac{1}{-4i} = \frac{i}{4}$$

$$f = \frac{P(i)}{Q'(-i)} = \frac{1}{4(-i)^3} = \frac{1}{4i} = \frac{-i}{4}.$$

Ainsi,

$$\frac{1}{X^4-1} = \frac{1/4}{X-1} - \frac{1/4}{X+1} + \frac{i/4}{X-i} - \frac{i/4}{X+i}.$$

— On termine en passant de $\mathbb{C}$ à $\mathbb{R}$.

$$\begin{aligned}
\frac{1}{X^4-1} &= \frac{1/4}{X-1} - \frac{1/4}{X+1} + \frac{i/4}{X-i} - \frac{i/4}{X+i} \\
&= \frac{1/4}{X-1} - \frac{1/4}{X+1} + \frac{1}{4} \cdot \frac{i(X+i) - i(X-i)}{(X-i)(X+i)} \\
&= \frac{1/4}{X-1} - \frac{1/4}{X+1} + \frac{1}{4} \cdot \frac{-2}{X^2+1} \\
&= \frac{1/4}{X-1} - \frac{1/4}{X+1} - \frac{1/2}{X^2+1}.
\end{aligned}$$

Exercice 144

Décomposer en éléments simples les fractions rationnelles suivantes :

1. $\dfrac{1}{X^3 - X}$ **2.** $\dfrac{X^3}{(X-1)(X-2)(X-3)}$

Réponse 144

1. La partie entière est nulle, et le dénominateur se factorise en $X(X-1)(X+1)$. Multipliant par X et faisant $X = 0$, on trouve la partie polaire relativement à $X-0$, et ainsi de suite... On trouve finalement
$$\frac{1}{X^3 - X} = \frac{-1}{X} + \frac{1/2}{X-1} + \frac{1/2}{X+1}.$$
2. En appliquant exactement la même méthode, on trouve que la décomposition en éléments simples est
$$1 + \frac{1}{2(X-1)} - \frac{8}{X-2} + \frac{27}{2(X-3)}.$$

Exercice 145

Décomposer en éléments simples les fractions rationnelles suivantes :

1. $\dfrac{2X^2+1}{(X^2-1)^2}$ **2.** $\dfrac{X^3+1}{(X-1)^3}$

Réponse 145

1. Le dénominateur se factorise en $(X^2-1)^2 = (X-1)^2(X+1)^2$. Il faut donc étudier la partie polaire relative à $+1$ et à -1. Commençons par étudier la partie polaire relative à -1. La fraction rationnelle s'écrit sous la forme
$$\frac{2X^2+1}{(X-1)^2(X+1)^2} = \frac{\lambda_1}{X+1} + \frac{\lambda_2}{(X+1)^2} + G(X),$$
où $G(X) = \frac{\mu_1}{X-1} + \frac{\mu_2}{(X-1)^2}$ est une fraction rationnelle dont -1 n'est pas un pôle. Multipliant cette égalité par $(X+1)^2$ et faisant $X = -1$, on trouve $\lambda_2 = 3/4$. On calcule ensuite
$$\frac{2X^2+1}{(X-1)^2(X+1)^2} - \frac{3/4}{(X+1)^2} = \frac{(5X+1)/4}{(X+1)(X-1)^2} = \frac{\lambda_1}{X+1} + G(X).$$
On multiplie cette fois par $X+1$, et on fait $X = -1$, et on trouve $\lambda_1 = -1/4$. Pour étudier la partie polaire relative à 1, on peut procéder de la même façon ou simplement remarquer que la fraction rationnelle est paire. On en déduit que
$$\frac{2X^2+1}{(X-1)^2(X+1)^2} = \frac{-1/4}{X+1} + \frac{3/4}{(X+1)^2} + \frac{1/4}{X-1} + \frac{3/4}{(X-1)^2}.$$
2. La partie entière de cette fraction rationnelle est égale à 1, et on a
$$\frac{X^3+1}{(X-1)^3} = 1 + \frac{3X^2-3X+2}{(X-1)^3} = 1 + \frac{a}{(X-1)^3} + \frac{b}{(X-1)^2} + \frac{c}{X-1}.$$

Pour trouver a, on multiplie par $(X-1)^3$ et on fait $X=1$. On trouve

$$a = 2.$$

Pour trouver b, on soustrait $\frac{2}{(X-1)^3}$, et on trouve

$$\begin{aligned}\frac{3X^2-3X+2}{(X-1)^3} - \frac{2}{(X-1)^3} &= \frac{3X}{(X-1)^2} \\ &= \frac{b}{(X-1)^2} + \frac{c}{X-1}.\end{aligned}$$

Multipliant par $(X-1)^2$ et faisant $X=1$, on trouve

$$b = 3.$$

Finalement, on retranche encore $\frac{3}{(X-1)^2}$ de sorte que

$$\begin{aligned}\frac{3X}{(X-1)^2} - \frac{3}{(X-1)^2} &= \frac{3}{X-1} \\ &= \frac{c}{X-1}.\end{aligned}$$

On a donc $c=3$. Finalement, la décomposition en éléments simples recherché est

$$1 + \frac{2}{(X-1)^3} + \frac{3}{(X-1)^2} + \frac{3}{X-1}.$$

Exercice 146

Décomposer en éléments simples sur $\mathbb{R}$ la fraction rationnelle suivante :

$$\frac{X^4+1}{(X+1)^2(X^2+1)}$$

Réponse 146

On commence par réaliser la décomposition en éléments simples sur $\mathbb{C}$. Les pôles sont -1 (double), i et $-i$. La fraction rationnelle étant à coefficients réels, les parties polaires sont conjuguées. On a donc

$$\frac{X^4+1}{(X+1)^2(X^2+1)} = 1 + \frac{a}{(X+1)^2} + \frac{b}{X+1} + \frac{c}{X-i} + \frac{\bar{c}}{X+i}.$$

Multipliant par $X-i$ et faisant $X=i$, on trouve

$$c = \frac{i^4+1}{(i+i)(i+1)^2} = -\frac{1}{2}.$$

De même, on a

$$a = \frac{1+1}{1+1} = 1.$$

En retranchant $\frac{1}{(X+1)^2}$, on trouve

$$\frac{X^4-X^2}{(X+1)^2(X^2+1)} = \frac{X^2(X-1)}{(X+1)(X^2+1)} = 1 + \frac{b}{X+1} + \frac{c}{X-i} + \frac{\bar{c}}{X+i}.$$

Multipliant par $X+1$ et faisant $X=-1$, on trouve

$$b=-1.$$

Finalement,

$$\frac{X^4+1}{(X+1)^2(X^2+1)}=1+\frac{1}{(X+1)^2}-\frac{1}{X+1}-\frac{1/2}{X-i}-\frac{1/2}{X+i}.$$

Finalement, en regroupant les deux derniers termes, on trouve la décomposition sur $\mathbb{R}$:

$$\frac{X^4+1}{(X+1)^2(X^2+1)}=1+\frac{1}{(X+1)^2}-\frac{1}{X+1}-\frac{X}{X^2+1}.$$

Exercice 147

Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$, par identification des coefficients.

1. $F=\frac{X}{X^2-4}$
2. $G=\frac{X}{3-3X^2+X-4(X-1)}$
3. $H=\frac{2X^3+X^2-X+1}{X^2-2X+1}$
4. $K=\frac{X+1}{X^4+1}$

Réponse 147

1. $F=\frac{X}{X^2-4}$. Commençons par factoriser le dénominateur :

   $$X^2-4=(X-2)(X+2),$$

   d'où une décomposition en éléments simples du type

   $$F=\frac{a}{X-2}+\frac{b}{X+2}.$$

   En réduisant au même dénominateur, il vient

   $$\frac{X}{X^2-4}=\frac{(a+b)X+2(a-b)}{X^2-4},$$

   et en identifiant les coefficients, on obtient le système :

   $$\begin{cases}a+b=1,\\2(a-b)=0.\end{cases}$$

   Ainsi $a=b=\frac{1}{2}$ et

   $$\frac{X}{X^2-4}=\frac{1}{2(X-2)}+\frac{1}{2(X+2)}.$$

2. $G=\frac{X^3-3X^2+X-4}{X-1}$. Lorsque le degré du numérateur (ici 3) est supérieur ou égal au degré du dénominateur (ici 1), il faut effectuer la division euclidienne du numérateur par le dénominateur pour faire apparaître la partie polynomiale (ou partie entière). Ici, la division euclidienne s'écrit :

   $$X^3-3X^2+X-4=(X-1)(X^2-2X-1)-5.$$

   Ainsi, en divisant les deux membres par $X-1$, on obtient :

   $$\frac{X^3-3X^2+X-4}{X-1}=X^2-2X-1-\frac{5}{X-1}.$$

   La fraction est alors déjà décomposée en éléments simples.

3. $H = \frac{2X^3+X^2-X+1}{X^2-2X+1}$. Commençons par faire la division euclidienne du numérateur par le dénominateur :

$$2X^3 + X^2 - X + 1 = (X^2 - 2X + 1)(2X + 5) + (7X - 4),$$

ce qui donne :

$$H = 2X + 5 + \frac{7X - 4}{X^2 - 2X + 1}.$$

Il reste à décomposer en éléments simples la fraction rationnelle $H_1 = \frac{7X-4}{X^2-2X+1}$. Puisque le dénominateur se factorise en $(X-1)^2$, elle sera de la forme :

$$H_1 = \frac{a}{(X-1)^2} + \frac{b}{X-1}.$$

En réduisant au même dénominateur, il vient :

$$\frac{7X - 4}{X^2 - 2X + 1} = \frac{bX + a - b}{X^2 - 2X + 1},$$

et en identifiant les coefficients, on obtient $b = 7$ et $a = 3$. Finalement,

$$\frac{2X^3 + X^2 - X + 1}{X^2 - 2X + 1} = 2X + 5 + \frac{3}{(X-1)^2} + \frac{7}{X-1}.$$

4. $K = \frac{X+1}{X^4+1}$. Ici, il n'y a pas de partie polynomiale puisque le degré du numérateur est strictement inférieur au degré du dénominateur. Le dénominateur admet quatre racines complexes $e^{i\pi/4}$, $e^{3i\pi/4}$, $e^{5i\pi/4} = e^{-3i\pi/4}$ et $e^{7i\pi/4} = e^{-i\pi/4}$.
En regroupant les racines complexes conjuguées, on obtient sa factorisation sur $\mathbb{R}$:

$$X^4 + 1 = (X - e^{i\pi/4})(X - e^{-i\pi/4})(X - e^{3i\pi/4})(X - e^{-3i\pi/4}),$$

ce qui donne :

$$X^4 + 1 = \left(X^2 - 2\cos\frac{\pi}{4}X + 1\right)\left(X^2 - 2\cos\frac{3\pi}{4}X + 1\right),$$

ou encore :

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

Puisque les deux facteurs $(X^2 - \sqrt{2}X + 1)$ et $(X^2 + \sqrt{2}X + 1)$ sont irréductibles sur $\mathbb{R}$, la décomposition en éléments simples de K est de la forme :

$$K = \frac{aX + b}{X^2 - \sqrt{2}X + 1} + \frac{cX + d}{X^2 + \sqrt{2}X + 1}.$$

En réduisant au même dénominateur et en identifiant les coefficients avec ceux de $K = \frac{X+1}{X^4+1}$, on obtient le système :

$$\begin{cases} a + c = 0, \\ \sqrt{2}a + b - \sqrt{2}c + d = 0, \\ a + \sqrt{2}b + c - \sqrt{2}d = 1, \\ b + d = 1. \end{cases}$$

En résolvant, on obtient :

$$a = -\frac{\sqrt{2}}{4}, \quad c = \frac{\sqrt{2}}{4}, \quad b = \frac{2 + \sqrt{2}}{4}, \quad d = \frac{2 - \sqrt{2}}{4}.$$

Ainsi :

$$\frac{X+1}{X^4+1} = \frac{-\frac{\sqrt{2}}{4}X + \frac{2+\sqrt{2}}{4}}{X^2 - \sqrt{2}X + 1} + \frac{\frac{\sqrt{2}}{4}X + \frac{2-\sqrt{2}}{4}}{X^2 + \sqrt{2}X + 1}.$$

Exercice 148

Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$, en raisonnant par substitution pour obtenir les coefficients.

1. $F = \frac{X^5+X^4+1}{X^3-X}$
2. $G = \frac{X^3+X+1}{(X-1)^3(X+1)}$
3. $H = \frac{X}{(X^2+1)(X^2+4)}$
4. $K = \frac{2X^4+X^3+3X^2-6X+1}{2X^3-X^2}$

Réponse 148

1. Pour obtenir la partie polynomiale, on effectue une division euclidienne :

$$X^5 + X^4 + 1 = (X^3 - X)(X^2 + X + 1) + X^2 + X + 1.$$

Cela donne :

$$F = X^2 + X + 1 + F_1, \quad \text{où} \quad F_1 = \frac{X^2 + X + 1}{X^3 - X}.$$

Puisque $X^3-X = X(X-1)(X+1)$, la décomposition en éléments simples est de la forme :

$$F_1 = \frac{X^2 + X + 1}{X(X-1)(X+1)} = \frac{a}{X} + \frac{b}{X-1} + \frac{c}{X+1}.$$

Pour obtenir a :

— Multiplions l'égalité par X :

$$\frac{X(X^2 + X + 1)}{X(X-1)(X+1)} = a + \frac{bX}{X-1} + \frac{cX}{X+1}.$$

— En remplaçant X par 0, on obtient $-1 = a$, donc $a = -1$.

Pour b :

— Multiplions par $X-1$ et remplaçons X par 1 : $b = \frac{3}{2}$.

Pour c :

— Multiplions par $X+1$ et remplaçons X par -1 : $c = \frac{1}{2}$.

Ainsi :

$$F = X^2 + X + 1 - \frac{1}{X} + \frac{1}{2(X+1)} + \frac{3}{2(X-1)}.$$

2. La partie polynomiale est nulle. La décomposition en éléments simples est de la forme :

$$G = \frac{a}{(X-1)^3} + \frac{b}{(X-1)^2} + \frac{c}{X-1} + \frac{d}{X+1}.$$

Pour a :

— Multiplions les deux membres par $(X-1)^3$, simplifions, et remplaçons X par 1 :

$$a = \frac{3}{2}.$$

Pour d :

— Multiplions par $X+1$, simplifions, et remplaçons X par -1 :

$$d = \frac{1}{8}.$$

Pour c :

— Multiplions par X et considérons la limite quand $X \to +\infty$: $c = \frac{7}{8}$.

Pour b :

— En remplaçant X par 0 : $b = \frac{5}{4}$.

Ainsi :

$$G = \frac{\frac{3}{2}}{(X-1)^3} + \frac{\frac{5}{4}}{(X-1)^2} + \frac{\frac{7}{8}}{X-1} + \frac{\frac{1}{8}}{X+1}.$$

3. Puisque X^2+1 et X^2+4 sont irréductibles sur $\mathbb{R}$, la décomposition en éléments simples est de la forme :

$$H = \frac{aX+b}{X^2+1} + \frac{cX+d}{X^2+4}.$$

En remplaçant X par 0, on obtient $b + \frac{1}{4}d = 0$. En multipliant par X et passant à la limite $X \to +\infty$, on a $a+c=0$. Enfin, en évaluant pour $X=1$ et $X=-1$, on obtient $b=d=0$, $a=\frac{1}{3}$, $c=-\frac{1}{3}$. Ainsi :

$$H = \frac{\frac{1}{3}X}{X^2+1} - \frac{\frac{1}{3}X}{X^2+4}.$$

4. Pour la partie polynomiale, effectuons la division euclidienne :

$$2X^4 + X^3 + 3X^2 - 6X + 1 = (2X^3 - X^2)(X+1) + (4X^2 - 6X + 1).$$

Cela donne :

$$K = X + 1 + K_1, \quad \text{où} \quad K_1 = \frac{4X^2 - 6X + 1}{2X^3 - X^2}.$$

En factorisant $2X^3 - X^2 = 2X^2(X - \frac{1}{2})$, la décomposition est :

$$K_1 = \frac{a}{X^2} + \frac{b}{X} + \frac{c}{X - \frac{1}{2}}.$$

On trouve $a=-1$, $b=4$, et $c=-2$. Ainsi :

$$K = X + 1 - \frac{1}{X^2} + \frac{4}{X} - \frac{2}{X - \frac{1}{2}}.$$

Exercice 149

Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$.

1. **À l'aide de divisions euclidiennes successives :**

$$F = \frac{4X^6 - 2X^5 + 11X^4 - X^3 + 11X^2 + 2X + 3}{X(X^2+1)^3}$$

2. **À l'aide d'une division selon les puissances croissantes :**

$$G = \frac{4X^4 - 10X^3 + 8X^2 - 4X + 1}{X^3(X-1)^2}$$

3. **Idem pour :**

$$H = \frac{X^4 + 2X^2 + 1}{X^5 - X^3}$$

4. **À l'aide du changement d'indéterminée $X = Y + 1$:**

$$K = \frac{X^5 + X^4 + 1}{X(X-1)^4}$$

Réponse 149

1.

$$F = \frac{4X^6 - 2X^5 + 11X^4 - X^3 + 11X^2 + 2X + 3}{X(X^2+1)^3}.$$

(a) La décomposition en éléments simples de F est de la forme

$$F = \frac{a}{X} + \frac{bX + c}{(X^2+1)^3} + \frac{dX + e}{(X^2+1)^2} + \frac{fX + g}{X^2 + 1}.$$

Il est difficile d'obtenir les coefficients par substitution.

(b) Pour trouver a, on multiplie F par X, puis on remplace X par 0, ce qui donne $a = 3$.

(c) On fait la soustraction $F_1 = F - \frac{a}{X}$. La fraction F_1 doit se simplifier par X. On trouve :

$$F_1 = \frac{X^5 - 2X^4 + 2X^3 - X^2 + 2X + 2}{(X^2+1)^3}.$$

(d) La décomposition se poursuit par divisions euclidiennes successives. Tout d'abord, on divise le numérateur $X^5 - 2X^4 + 2X^3 - X^2 + 2X + 2$ par $X^2 + 1$:

$$X^5 - 2X^4 + 2X^3 - X^2 + 2X + 2 = (X^2+1)(X^3 - 2X^2 + X + 1) + (X + 1).$$

Puis on divise à nouveau le quotient obtenu par $X^2 + 1$:

$$X^5 - 2X^4 + 2X^3 - X^2 + 2X + 2 = (X^2+1)\big((X^2+1)(X-2) + 3\big) + (X + 1).$$

En divisant cette identité par $(X^2+1)^3$, on obtient :

$$F_1 = \frac{X+1}{(X^2+1)^3} + \frac{3}{(X^2+1)^2} + \frac{X-2}{X^2+1}.$$

Ainsi, on a :

$$F = \frac{3}{X} + \frac{X+1}{(X^2+1)^3} + \frac{3}{(X^2+1)^2} + \frac{X-2}{X^2+1}.$$

2.

$$G = \frac{4X^4 - 10X^3 + 8X^2 - 4X + 1}{X^3(X-1)^2}.$$

La décomposition en éléments simples de G est de la forme :

$$G = \frac{a}{X^3} + \frac{b}{X^2} + \frac{c}{X} + \frac{d}{(X-1)^2} + \frac{e}{X-1}.$$

En effectuant la division suivant les puissances croissantes (ordre 2), on calcule :

$$1 - 4X + 8X^2 - 10X^3 + 4X^4 = (1 - 2X + X^2)(1 - 2X + 3X^2) + (-2X^3 + X^4).$$

En divisant par $X^3(X-1)^2$, on trouve :

$$G = \frac{1}{X^3} - \frac{2}{X^2} + \frac{3}{X} + \frac{X-2}{(X-1)^2}.$$

3.
$$H = \frac{X^4 + 2X^2 + 1}{X^5 - X^3} = \frac{X^4 + 2X^2 + 1}{X^3(X-1)(X+1)}.$$

La décomposition est de la forme :

$$H = \frac{a}{X^3} + \frac{b}{X^2} + \frac{c}{X} + \frac{d}{X-1} + \frac{e}{X+1}.$$

En effectuant la division selon les puissances croissantes, on obtient :

$$H = -\frac{1}{X^3} - \frac{3}{X} + \frac{2}{X-1} + \frac{2}{X+1}.$$

4.
$$K = \frac{X^5 + X^4 + 1}{X(X-1)^4}.$$

Puisque le degré du numérateur est supérieur ou égal à celui du dénominateur, il y a une partie polynomiale. On trouve :

$$K = 1 + \frac{1}{X} + \frac{3}{(X-1)^4} + \frac{6}{(X-1)^3} + \frac{10}{(X-1)^2} + \frac{4}{X-1}.$$

Exercice 150

1. Décomposer les fractions suivantes en éléments simples sur $\mathbb{C}$
   (a) $\dfrac{(3-2i)X - 5 + 3i}{X^2 + iX + 2}$
   (b) $\dfrac{X+i}{X^2+i}$
   (c) $\dfrac{2X}{(X+i)^2}$
2. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$, puis sur $\mathbb{C}$
   (a) $\dfrac{X^5 + X + 1}{X^4 - 1}$
   (b) $\dfrac{X^2 - 3}{(X^2+1)(X^2+4)}$
   (c) $\dfrac{X^2+1}{X^4+1}$

Réponse 150

1. (a)
$$\frac{(3-2i)X - 5 + 3i}{X^2 + iX + 2} = \frac{2+i}{X-i} + \frac{1-3i}{X+2i}.$$

   (b)
$$\frac{X+i}{X^2+i} = \frac{2 - \dfrac{\sqrt{2}}{4} + \dfrac{\sqrt{2}}{4}i}{X - \dfrac{\sqrt{2} - \sqrt{2}i}{2}} + \frac{2 + \dfrac{\sqrt{2}}{4} - \dfrac{\sqrt{2}}{4}i}{X + \dfrac{\sqrt{2} - \sqrt{2}i}{2}}.$$

(c)
$$\frac{X}{(X+i)^2} = \frac{1}{X+i} + \frac{-i}{(X+i)^2}.$$

2. (a)
$$\frac{X^5+X+1}{X^4-1} = X + \frac{\frac{3}{4}}{X-1} + \frac{\frac{1}{4}}{X+1} - \frac{X+\frac{1}{2}}{X^2+1}.$$
$$= X + \frac{\frac{3}{4}}{X-1} + \frac{\frac{1}{4}}{X+1} + \frac{-\frac{1}{2}+\frac{1}{4}i}{X-i} + \frac{-\frac{1}{2}-\frac{1}{4}i}{X+i}.$$

(b)
$$\frac{X^2-3}{(X^2+1)(X^2+4)} = -\frac{\frac{4}{3}}{X^2+1} + \frac{\frac{7}{3}}{X^2+4}.$$
$$= \frac{\frac{2}{3}i}{X-i} + \frac{-\frac{2}{3}i}{X+i} + \frac{-\frac{7}{12}i}{X-2i} + \frac{\frac{7}{12}i}{X+2i}.$$

(c)
$$\frac{X^2+1}{X^4+1} = \frac{\frac{1}{2}}{X^2-\sqrt{2}X+1} + \frac{\frac{1}{2}}{X^2+\sqrt{2}X+1}.$$
$$= \frac{-\frac{\sqrt{2}}{4}i}{X-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i} + \frac{\frac{\sqrt{2}}{4}i}{X-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i} + \frac{\frac{\sqrt{2}}{4}i}{X+\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i} + \frac{-\frac{\sqrt{2}}{4}i}{X+\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i}.$$

Exercice 151

Décomposer en éléments simples les fractions rationnelles suivantes :

1. $\dfrac{1}{X^n-1}$ **2.** $\dfrac{X^{n-1}}{X^n-1}$

Réponse 151

1. Les pôles de $1/(X^n-1)$ sont les racines n-ièmes de l'unité, c'est-à-dire les complexes $x_k = e^{2ik\pi/n}$, $k = 0, \ldots, n-1$. Chaque pôle est simple, la partie polaire correspondante est donc de la forme $\frac{c_k}{X-x_k}$ avec $c_k = \frac{1}{P'(x_k)} = \frac{1}{nx_k^{n-1}}$. Or, $x_k^{n-1} = \frac{x_k^n}{x_k} = \frac{1}{x_k} = e^{-2ik\pi/n}$. La décomposition en éléments simples recherché vaut donc
$$\frac{1}{X^n-1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{e^{2ik\pi/n}}{X-e^{2ik\pi/n}}.$$

2. Les racines de X^n-1 sont les complexes $\omega_k = e^{2ik\pi/n}$, $0 \le k \le n-1$. La fraction rationnelle admet donc n pôles, qui sont tous simples. Sa décomposition en éléments simples a pour forme
$$\frac{X^{n-1}}{X^n-1} = \sum_{k=0}^{n-1} \frac{\alpha_k}{X-\omega_k}$$
avec $\alpha_k = \frac{\omega_k^{n-1}}{n\omega_k^{n-1}} = \frac{1}{n}$. La décomposition en éléments simples est
$$\frac{X^{n-1}}{X^n-1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{1}{X-e^{2ik\pi/n}}.$$

Exercice 152

Décomposer en éléments simples les fractions rationnelles suivantes :

$$\textbf{1.}\quad \frac{X^m}{(X-1)^n} \qquad \textbf{2.}\quad \frac{1}{X(X+1)\cdots(X+n)}$$

Réponse 152

1. On écrit $X = (X-1)+1$ et on utilise la formule du binôme. Il vient

$$X^m = \big((X-1)+1\big)^m = \sum_{k=0}^{m} \binom{m}{k} (X-1)^k.$$

On distingue alors deux cas pour l'écriture de la décomposition en éléments simples : si $m \geq n$, alors

$$\frac{X^m}{(X-1)^n} = \sum_{k=n}^{m} \binom{m}{k} (X-1)^{k-n} + \sum_{k=0}^{n-1} \frac{\binom{m}{k}}{(X-1)^{n-k}},$$

le premier terme étant la partie entière et le second la partie polaire. Si $m \leq n$, alors on écrit simplement

$$\frac{X^m}{(X-1)^n} = \sum_{k=0}^{m} \frac{\binom{m}{k}}{(X-1)^{n-k}}.$$

2. On peut écrire

$$\frac{1}{X(X+1)\cdots(X+n)} = \sum_{k=0}^{n} \frac{a_k}{X+k}.$$

Reste à déterminer a_k pour $k = 0, \ldots, n$. Le plus simple ici, comme le dénominateur est déjà factorisé, est de multiplier par $X+k$ et de faire tendre X vers $-k$. On obtient alors

$$a_k = \frac{1}{(-k)(-k+1)\cdots(-k+(k-1))(-k+(k+1))\cdots(-k+n)} = \frac{(-1)^k}{k!(n-k)!}.$$

Exercice 153

Décomposer en éléments simples la fraction rationnelle suivante :

$$\frac{1}{(X-1)(X^n-1)}.$$

Réponse 153

La fraction admet 1 comme pôle double et $\omega_k = e^{2i\pi k/n}$, $k = 1, \ldots, n-1$ comme pôles simples. On commence par calculer le coefficient devant $(X-1)^2$. On écrit que la fraction est égale à

$$\frac{1}{(X-1)^2(1+X+\cdots+X^{n-1})} = \frac{\lambda}{(X-1)^2} + Q(X),$$

où 1 n'est pas pôle double de Q. Multipliant par $(X-1)^2$ et faisant tendre X vers 1, on en déduit que $\lambda = \frac{1}{n}$. Le coefficient devant $\frac{1}{X-\omega_k}$ est lui obtenu en dérivant le dénominateur, et en remplaçant par ω_k. On trouve :

$$\frac{1}{\omega_k^n - 1 + (\omega_k - 1)n\omega_k^{n-1}} = \frac{\omega_k}{n(\omega_k - 1)}.$$

Enfin, pour calculer le terme en $\frac{1}{X-1}$, on écrit que

$$\frac{1}{(X-1)^2(1+X+\cdots+X^{n-1})} - \frac{1/n}{(X-1)^2} = \frac{\mu}{(X-1)} + R(X),$$

où 1 n'est plus un pôle de R. On a alors

$$\begin{aligned}
&\frac{1}{(X-1)^2(1+X+\cdots+X^{n-1})} - \frac{1/n}{(X-1)^2} \\
&\qquad = \frac{n-(1+X+\cdots+X^{n-1})}{n(X-1)^2(1+X+\cdots+X^{n-1})} \\
&\qquad = -\frac{(X-1)+(X^2-1)+\cdots+(X^{n-1}-1)}{n(X-1)^2(1+X+\cdots+X^{n-1})} \\
&= -\frac{1+(1+X)+(1+X+X^2)+\cdots+(1+X+\cdots+X^{n-2})}{n(X-1)(1+X+\cdots+X^{n-1})}.
\end{aligned}$$

Multipliant par $X-1$ et faisant $X=1$, on trouve

$$\mu = -\frac{1+2+\cdots+n-1}{n^2} = \frac{1-n}{2n}.$$

Finalement, la décomposition en éléments simples de la fraction rationnelle est donc :

$$\frac{1-n}{2n(X-1)} + \frac{1}{n(X-1)^2} + \sum_{k=1}^{n-1} \frac{\omega_k}{n(\omega_k-1)} \frac{1}{X-\omega_k}.$$

Exercice 154

Soit $n \in \mathbb{N}^*$ et $P(X) = c(X-a_1)\cdots(X-a_n)$ (où les a_i sont des nombres complexes et où $c \neq 0$).

1. Exprimer à l'aide de P et de ses dérivées les sommes suivantes :

$$\sum_{k=1}^{n} \frac{1}{X-a_k}, \quad \sum_{k=1}^{n} \frac{1}{(X-a_k)^2}, \quad \sum_{1\leq k,\ell\leq n,\ k\neq\ell} \frac{1}{(X-a_k)(X-a_\ell)}.$$

2. Montrer que si z est racine de P' mais pas de P, alors il existe $\lambda_1, \ldots, \lambda_n$ des réels positifs ou nuls tels que

$$\sum_{k=1}^{n} \lambda_k = 1 \quad \text{et} \quad z = \sum_{k=1}^{n} \lambda_k a_k.$$

   Si toutes les racines de P sont réelles, que peut-on en déduire sur les racines de P' ?

Réponse 154

1. (a) Puisque $P(X) = c(X-a_1)\cdots(X-a_n)$:

$$P'(X) = c(X-a_2)\cdots(X-a_n) + c(X-a_1)(X-a_3)\cdots(X-a_n) + \cdots$$

$$+c(X-a_1)\cdots(X-a_{k-1})(X-a_{k+1})\cdots(X-a_n) + \cdots + c(X-a_1)\cdots(X-a_{n-1}).$$

La dérivée est donc la somme des termes de la forme :

$$\frac{c(X-a_1)\cdots(X-a_n)}{X-a_k} = \frac{P(X)}{X-a_k}.$$

Ainsi,

$$P'(X) = \frac{P(X)}{X-a_1} + \cdots + \frac{P(X)}{X-a_k} + \cdots + \frac{P(X)}{X-a_n}.$$

Donc :

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{X-a_k}.$$

(b) Puisque $\sum_{k=1}^{n} \frac{1}{(X-a_k)^2}$ est la dérivée de $-\sum_{k=1}^{n} \frac{1}{X-a_k}$, on obtient par dérivation de $-\frac{P'}{P}$:

$$\frac{P'^2 - PP''}{P^2} = \sum_{k=1}^{n} \frac{1}{(X-a_k)^2}.$$

(c) On a remarqué que la dérivée de P' est la somme de facteurs $c(X-a_1)\cdots(X-a_n)$ avec un des facteurs en moins, donc de la forme :

$$\frac{c(X-a_1)\cdots(X-a_n)}{X-a_k} = \frac{P}{X-a_k}.$$

De même, P'' est la somme de facteurs $c(X-a_1)\cdots(X-a_n)$ avec deux facteurs en moins, c'est-à-dire de la forme :

$$\frac{c(X-a_1)\cdots(X-a_n)}{(X-a_k)(X-a_\ell)} = \frac{P}{(X-a_k)(X-a_\ell)}.$$

Ainsi,

$$P'' = \sum_{1\le k,\ell\le n,\ k\neq\ell} \frac{P}{(X-a_k)(X-a_\ell)},$$

donc

$$\frac{P''}{P} = \sum_{1\le k,\ell\le n,\ k\neq\ell} \frac{1}{(X-a_k)(X-a_\ell)}.$$

2. On applique l'identité $\frac{P'(X)}{P(X)} = \sum_{k=1}^{n} \frac{1}{X-a_k}$ en z avec les hypothèses $P(z) \neq 0$ et $P'(z) = 0$. On en déduit

$$\sum_{k=1}^{n} \frac{1}{z-a_k} = 0.$$

L'expression conjuguée est aussi nulle :

$$\sum_{k=1}^{n} \frac{z-a_k}{|z-a_k|^2} = 0.$$

Posons $\mu_k = \frac{1}{|z-a_k|^2}$. Alors

$$\sum_{k=1}^{n} \mu_k(z-a_k) = 0,$$

donc

$$\sum_{k=1}^{n} \mu_k z = \sum_{k=1}^{n} \mu_k a_k.$$

Posons $\lambda_k = \frac{\mu_k}{\sum_{k=1}^{n} \mu_k}$, alors :

— Les λ_k sont des réels positifs.
— $\sum_{k=1}^{n} \lambda_k = 1$.
— Et $z = \sum_{k=1}^{n} \lambda_k a_k$.

En particulier, si les a_k sont tous des nombres réels, alors z est aussi un nombre réel. On vient de prouver que si un polynôme P a toutes ses racines réelles, alors P' a aussi toutes ses racines réelles.

On a même plus : si on ordonne les racines réelles de P en $a_1 \leq a_2 \leq \cdots \leq a_n$, alors une racine z de P' est réelle et vérifie $a_1 \leq z \leq a_n$.

Plus généralement, l'interprétation géométrique de ce que l'on vient de prouver s'appelle le théorème de Gauss-Lucas :

« Les racines de P' sont dans l'enveloppe convexe des racines (réelles ou complexes) de P. »

5.3 Applications

Exercice 155

Déterminer une primitive des fonctions suivantes :

1. $x \mapsto \dfrac{1}{1-x^2}$ sur $]1, +\infty[$ **2**. $x \mapsto \dfrac{x}{x^3 - 7x + 6}$ sur $]2, +\infty[$.

Réponse 155

1. On peut factoriser $1 - X^2$ en $(1-X)(1+X)$ et on sait qu'il existe des réels a et b de sorte que

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

Notons $Q(X) = 1 - X^2$, de sorte que $Q'(X) = -2X$. On a $a = 1/Q'(1) = -1/2$ et $b = 1/Q'(-1) = 1/2$. Ainsi,

$$\frac{1}{1-X^2} = \frac{-1/2}{X-1} + \frac{1/2}{X+1}.$$

Ainsi, une primitive de $x \mapsto \frac{1}{1-x^2}$ sur $]1, +\infty[$ est la fonction

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

2. On peut factoriser $X^3 - 7X + 6$ en $(X+3)(X-1)(X-2)$ (pour cela, on remarque auparavant que 1 est racine évidente par exemple). On en déduit qu'il existe trois réels a, b et c tels que

$$\frac{X}{X^3 - 7X + 6} = \frac{a}{X+3} + \frac{b}{X-1} + \frac{c}{X-2}.$$

Posons $P(X) = X$ et $Q(X) = X^3 - 7X + 6$, de sorte que $Q'(X) = 3X^2 - 7$. Alors on a

$$a = \frac{P(-3)}{Q'(-3)} = -\frac{3}{20},\ b = \frac{P(1)}{Q'(1)} = -\frac{1}{4},\ c = \frac{P(2)}{Q(2)} = \frac{2}{5}.$$

On a donc

$$\frac{x}{x^3-7x+6} = -\frac{3}{20(x+3)} - \frac{1}{4(x-1)} + \frac{2}{5(x-2)}.$$

Une primitive de cette fonction sur $]2,+\infty[$ est donc donnée par

$$x \mapsto -\frac{3}{20}\ln(x+3) - \frac{1}{4}\ln(x-1) + \frac{2}{5}\ln(x-2).$$

Exercice 156

Soit $f(x) = \frac{5x^2+21x+22}{(x-1)(x+3)^2}$, $x \in]1,+\infty[$.

1. Décomposer en éléments simples la fraction rationnelle

$$\frac{5X^2+21X+22}{(X-1)(X+3)^2}$$

en éléments simples.

2. En déduire la primitive de f sur $]1,+\infty[$ qui s'annule en 2.

Réponse 156

1. On écrit la décomposition a priori :

$$\frac{5X^2+21X+22}{(X-1)(X+3)^2} = \frac{a}{X-1} + \frac{b}{X+3} + \frac{c}{(X+3)^2}.$$

Pour déterminer a, on multiplie par $X-1$ et on fait tendre X vers 1 : on trouve

$$a = \frac{5+21+22}{4^2} = \frac{48}{16} = 3.$$

Pour déterminer c, on multiplie par $(X+3)^2$ et on trouve

$$c = \frac{45-63+22}{-4} = -1.$$

Pour déterminer b, on multiplie par X et on fait tendre X vers $+\infty$. On a donc

$$\frac{3X}{X-1} + \frac{bX}{X+3} - \frac{X}{(X+3)^2} = \frac{5X^3+21X^2+22X}{(X-1)(X+3)^2}.$$

En faisant tendre X vers $+\infty$, on obtient

$$3+b=5 \iff b=2.$$

2. On a donc obtenu, pour $x>1$,

$$f(x) = \frac{3}{x-1} + \frac{2}{x+3} - \frac{1}{(x+3)^2}.$$

On intègre chacun des éléments simples de la décomposition précédente, en tenant compte du fait que l'on travaille sur l'intervalle $]1,+\infty[$. Les primitives de f sur cet intervalle sont donc les fonctions

$$F(x) = 3\ln(x-1) + 2\ln(x+3) + \frac{1}{x+3} + d.$$

La primitive qui s'annule en 2 et celle pour laquelle d vérifie l'équation

$$3\ln(1) + 2\ln 5 + \frac{1}{5} + d = 0.$$

La primitive de f sur l'intervalle $]1, +\infty[$ qui s'annule en 2 est donc la fonction F définie par

$$F(x) = 3\ln(x-1) + 2\ln(x+3) + \frac{1}{x+3} - 2\ln 5 - \frac{1}{5}.$$

Exercice 157

Pour $x > 0$, on pose

$$f(x) = \frac{x^4 + x^3 + 4x^2 + 2x + 2}{x^3 + x}.$$

1. Décomposer en éléments simples la fraction rationnelle

$$\frac{X^4 + X^3 + 4X^2 + 2X + 2}{X^3 + X}.$$

2. En déduire la valeur de $\int_1^2 f(x)dx$.

Réponse 157

1. On commence par effectuer la division euclidienne de $X^4+X^3+4X^2+2X+2$ par X^3+X. On trouve que le quotient vaut $X+1$ et le reste vaut $3X2+X+2$. On a donc

$$\begin{aligned}\frac{X^4 + X^3 + 4X^2 + 2X + 2}{X^3 + X} &= X + 1 + \frac{3X^2 + X + 2}{X^3 + X} \\ &= X + 1 + \frac{3X^2 + X + 2}{X(X-i)(X+i)} \\ &= X + 1 + \frac{a}{X} + \frac{b}{X-i} + \frac{\bar{b}}{X+i}.\end{aligned}$$

Posons $P(X) = 3X^2 + X + 2$ et $Q(X) = X^3 + X$. Alors $a = P(0)/Q'(0) = 2$, $b = P(i)/Q'(i) = \frac{1}{2} - \frac{i}{2}$. On obtient

$$\begin{aligned}\frac{X^4 + X^3 + 4X^2 + 2X + 2}{X^3 + X} &= X + 1 + \frac{2}{X} + \frac{1}{2}\frac{1-i}{X-i} + \frac{1}{2}\frac{1+i}{X+i} \\ &= X + 1 + \frac{2}{X} + \frac{X+1}{X^2+1}.\end{aligned}$$

2. On calcule l'intégrale en cherchant une primitive de chacun des termes précédents. On écrit encore

$$\frac{X+1}{X^2+1} = \frac{X}{X^2+1} + \frac{1}{X^2+1}.$$

On obtient donc

$$\begin{aligned}\int_1^2 f(x)dx &= \left[\frac{x^2}{2} + x + 2\ln(x) + \frac{1}{2}\ln(x^2+1) + \arctan(x)\right]_1^2 \\ &= \frac{5}{2} + \frac{3}{2}\ln(2) + \frac{1}{2}\ln(5) + \arctan(2) - \frac{\pi}{4}.\end{aligned}$$

Exercice 158

Soit $n \geq 1$. Déterminer la dérivée n-ème de la fonction suivante :

$$f(x) = \frac{1}{x^2 - 3x + 2}.$$

Réponse 158

On va commencer par décomposer en éléments simples la fraction rationnelle

$$\frac{1}{X^2 - 3X + 2}.$$

On peut factoriser $X^2 - 3X + 2$ en $(X-1)(X-2)$. On a donc

$$\frac{1}{X^2 - 3X + 2} = \frac{a}{X-1} + \frac{b}{X-2}.$$

Notons $P(X) = X^2 - 3X + 2$ de sorte que $P'(X) = 2X - 3$. Alors $a = \frac{1}{P'(1)} = -1$ et $b = \frac{1}{P'(2)} = 1$. Ainsi, on a

$$f(x) = \frac{1}{x-2} - \frac{1}{x-1}.$$

D'autre part, il est facile de voir (par exemple par récurrence) que la dérivée n-ème de $x \mapsto \frac{1}{x}$ est $x \mapsto \frac{(-1)^n n!}{x^{n+1}}$. On en déduit finalement que

$$f^{(n)}(x) = \frac{(-1)^n n!}{(x-2)^{n+1}} - \frac{(-1)^n n!}{(x-1)^{n+1}}.$$

Exercice 159

1. Décomposer en éléments simples la fraction rationnelle $\dfrac{1}{X(X+1)(X+2)}$.
2. En déduire la limite de la suite (S_n) suivante : $S_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)}$.

Réponse 159

1. On sait que la fraction rationnelle admet une décomposition en éléments simples de la forme

   $$\frac{a}{X} + \frac{b}{X+1} + \frac{c}{X+2}.$$

   Par les techniques usuelles (identification, multiplication par X et faire $X = 0$,...), on trouve

   $$\frac{1}{X(X+1)(X+2)} = \frac{1/2}{X} - \frac{1}{X+1} + \frac{1/2}{X+2}.$$

2. Utilisant la décomposition en éléments simples précédente, il vient

   $$\begin{aligned} S_n &= \sum_{k=1}^{n} \frac{1/2}{k} - \sum_{k=1}^{n} \frac{1}{k+1} + \sum_{k=1}^{n} \frac{1/2}{k+2} \\ &= \sum_{k=1}^{n} \frac{1/2}{k} - \sum_{k=2}^{n+1} \frac{1}{k} + \sum_{k=3}^{n+2} \frac{1/2}{k} \\ &= \frac{1}{2} + \frac{1}{4} - \frac{1}{2} - \frac{1}{n+1} + \frac{1/2}{n+1} + \frac{1/2}{n+2}. \end{aligned}$$

On en déduit immédiatement que (S_n) converge vers $\frac{1}{4}$.

Exercice 160

Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geq 1$ possédant n racines distinctes $x_1, \ldots, x_n$ non-nulles.

1. Décomposer en éléments simples la fraction rationnelle $\dfrac{1}{XP(X)}$.
2. En déduire que $\displaystyle\sum_{k=1}^{n} \frac{1}{x_k P'(x_k)} = \frac{-1}{P(0)}$.

Réponse 160

1. On écrit la forme à priori de la décomposition en éléments simples qui est ici

$$\frac{1}{XP(X)} = \frac{\alpha_0}{X} + \sum_{k=1}^{n} \frac{\alpha_k}{X - x_k}.$$

On calcule α_0 en multipliant tout par X et en faisant tendre X vers 0, et on trouve $\alpha_0 = \frac{1}{P(0)}$. Pour $k \geq 1$, on multiplie tout par $X - x_k$ et on fait tendre X vers x_k. On trouve cette fois

$$\alpha_k = \lim_{x \to x_k} \frac{x - x_k}{x_k P(x)} = \lim_{x \to x_k} \frac{x - x_k}{x_k (P(x) - P(x_k))} = \frac{1}{x_k P'(x_k)}.$$

La décomposition en éléments simples est donc

$$\frac{1}{XP(X)} = \sum_{k=1}^{n} \frac{1}{x_k P'(x_k)} \times \frac{1}{X - x_k} + \frac{1}{P(0)} \times \frac{1}{X}.$$

2. On va multiplier par X cette fraction rationnelle, et on va étudier sa limite en $+\infty$. On trouve d'une part

$$\lim_{x \to +\infty} \frac{x}{xP(x)} = 0$$

et d'autre part

$$\lim_{x \to +\infty} \sum_{k=1}^{n} \frac{1}{x_k P'(x_k)} \times \frac{x}{x - x_k} + \frac{1}{P(0)} \times \frac{x}{x} = \sum_{k=1}^{n} \frac{1}{x_k P'(x_k)} + \frac{1}{P(0)}.$$

Identifiant ces deux égalités, on trouve le résultat voulu !

Exercice 161

Soit $n \geq 1$, $a_0, \ldots, a_n, b_0, \ldots, b_n$ des réels et P le polynôme trigonométrique défini par

$$P(x) = \sum_{k=0}^{n} \big(a_k \cos(kx) + b_k \sin(kx)\big).$$

Démontrer que P admet au plus $2n$ racines dans $[0, 2\pi[$.

Réponse 161

D'après les formules d'Euler, on a

$$\begin{aligned} P(x) &= \sum_{k=0}^{n} \left(\frac{a_k}{2}(e^{ikx} + e^{-ikx}) + \frac{b_k}{2i}(e^{ikx} - e^{-ikx}) \right) \\ &= \sum_{k=0}^{n} \left(\frac{a_k}{2} \left((e^{ix})^k + \frac{1}{(e^{ix})^k} \right) + \frac{b_k}{2i} \left((e^{ix})^k - \frac{1}{(e^{ix})^k} \right) \right). \end{aligned}$$

Ceci incite à considérer la fraction rationnelle

$$R(X) = \sum_{k=0}^{n} \left(\frac{a_k}{2} \left(X^k + \frac{1}{X^k} \right) + \frac{b_k}{2i} \left(X^k - \frac{1}{X^k} \right) \right)$$

de sorte que

$$P(x) = R(e^{ix}).$$

R peut s'écrire $R = A/B$ où $\deg(A) \leq 2n$. Ainsi, R admet au plus $2n$ racines. L'application $[0; 2\pi[\to \mathbb{C}$, $x \mapsto e^{ix}$ étant injective, des racines distinctes de P dans $[0; 2\pi[$ donnent des racines distinctes de P. Donc P admet au plus $2n$ racines dans $[0, 2\pi[$.

Exercice 162

Soit $P(X) = \prod_{k=1}^{n}(X - x_k) \in \mathbb{R}_n[X]$ un polynôme scindé à racines simples de degré $n \geq 2$.

1. Décomposer en éléments simples $\dfrac{1}{p}$.
2. En déduire la valeur de $\sum_{k=1}^{n} \frac{1}{P'(x_k)}$.

Réponse 162

1. Les racines de P étant simples, on a

$$P(X) = \sum_{k=1}^{n} \frac{\lambda_k}{X - x_k}.$$

De plus, pour tout $k = 1, \ldots, n$,

$$\lambda_k = \lim_{x \to x_k} \frac{x - x_k}{P(x)} = \frac{1}{P'(x_k)}.$$

2. Multipliant par X, on a pour tout $x \in \mathbb{R}$,

$$\frac{x}{P(x)} = \sum_{k=1}^{n} \frac{1}{P'(x_k)} \times \frac{x}{x - x_k}.$$

Faisons tendre x vers $+\infty$. Puisque $\deg(P) \geq 2$, on obtient

$$\sum_{k=1}^{n} \frac{1}{P'(x_k)} = 0.$$

Exercice 163

Décomposer en éléments simples la fraction $\frac{P'}{P}$, où P est un polynôme de $\mathbb{C}[X]$.

Réponse 163

On va étudier séparément les parties polaires relatives à chaque racine. Soit donc a une racine de P, de multiplicité m. Alors on peut factoriser P en $P(X) = (X-a)^m Q(X)$, soit en dérivant $P'(X) = m(X-a)^{m-1}Q(X) + (X-a)^m Q'(X)$. On trouve alors

$$\frac{P'(X)}{P(X)} = \frac{m}{X-a} + \frac{Q'(X)}{Q(X)}.$$

Or, a n'est pas racine de Q, donc Q'/Q n'admet pas a pour pôle et $\frac{m}{X-a}$ est la partie polaire de P'/P relative à a. En résumé, si $P(X) = \lambda(X-a_1)^{m_1}\dots(X-a_p)^{m_p}$, alors on trouve

$$\frac{P'}{P} = \sum_{i=1}^{p} \frac{m_i}{X-a_i}.$$

Si $P'|P$, alors $P(X) = \lambda(X-a)P'$ (car $\deg P' = \deg P - 1$) et $P'/P = \frac{1/\lambda}{X-a}$. Par unicité de la décomposition en éléments simples et le résultat de la question précédente, ceci entraîne que a est l'unique racine de P, et donc que $P(X) = \lambda(X-a)^m$. Réciproquement, les polynômes de cette forme sont tels que $P'|P$.

Exercice 164

Soit $P \in \mathbb{C}_n[X]$ admettant n racines simples $\alpha_1, \dots, \alpha_n$. Soient $A_1, \dots, A_n$ les points du plan complexe d'affixe respectives $\alpha_1, \dots, \alpha_n$.

1. Décomposer la fraction rationnelle P'/P en éléments simples.
2. Soit β une racine de P', et soit B son image dans le plan complexe. Déduire de la question précédente que
$$\sum_{j=1}^{n} \frac{1}{\beta - \alpha_j} = 0.$$
3. En déduire que B est un barycentre de la famille de points $(A_1, \dots, A_n)$, avec des coefficients positifs. Interpréter géométriquement cette propriété.

Réponse 164

1. On va étudier séparément les parties polaires relatives à chaque racine. On peut factoriser P en $P(X) = (X-\alpha_j)Q(X)$, soit en dérivant $P'(X) = Q(X) + (X-\alpha_j)Q'(X)$. On trouve alors
$$\frac{P'(X)}{P(X)} = \frac{1}{X-\alpha_j} + \frac{Q'(X)}{Q(X)}.$$
Or, α_j n'est pas racine de Q, donc Q'/Q n'admet pas α_j pour pôle et $\frac{1}{X-\alpha_j}$ est la partie polaire de P'/P relative à a. En résumé, la décomposition en éléments simples recherchée est
$$\frac{P'}{P} = \sum_{j=1}^{p} \frac{1}{X-\alpha_j}.$$
2. Il suffit d'évaluer l'équation précédente en β.

3. On multiplie par la quantité conjuguée et on trouve

$$\sum_{j=1}^{n} \frac{\bar{\beta} - \bar{\alpha}_j}{|\beta - \alpha_j|^2} = 0.$$

Prenant le conjugué de cette expression, on trouve :

$$\left(\sum_{j=1}^{n} \frac{1}{|\beta - \alpha_j|^2} \right) \beta = \sum_{j=1}^{n} \frac{1}{|\beta - \alpha_j|^2} \alpha_j,$$

ce qui correspond bien au résultat souhaité. On vient donc de prouver que toute racine de P' est dans l'enveloppe convexe des racines de P. Ce résultat s'appelle le théorème de Lucas, il est aussi valide si les racines de P ne sont pas simples. La preuve est similaire, si ce n'est que la décomposition en éléments simples de P'/P est plus difficile à obtenir.

Exercice 165

On pose $Q_0 = (X-1)(X-2)^2$, $Q_1 = X(X-2)^2$ et $Q_2 = X(X-1)$. À l'aide de la décomposition en éléments simples de $\dfrac{1}{X(X-1)(X-2)^2}$, trouver des polynômes A_0, A_1, A_2 tels que

$$A_0 Q_0 + A_1 Q_1 + A_2 Q_2 = 1.$$

Que peut-on en déduire sur Q_1, Q_2 et Q_3 ?

Réponse 165

La décomposition en éléments simples s'écrit :

$$\frac{1}{X(X-1)(X-2)^2} = -\frac{1}{4X} + \frac{1}{X-1} + \frac{1}{2(X-2)^2} - \frac{3}{4(X-2)}.$$

En multipliant cette identité par le dénominateur $X(X-1)(X-2)^2$, il vient :

$$1 = -\frac{1}{4} Q_0 + Q_1 + \left(\frac{1}{2} - \frac{3}{4}(X-2) \right) Q_2.$$

Ainsi, $A_0 = -\dfrac{1}{4}$, $A_1 = 1$, et $A_2 = 2 - \dfrac{3}{4}X$ conviennent.

On a obtenu une relation de Bézout entre Q_1, Q_2, et Q_3, qui prouve que ces trois polynômes sont premiers entre eux :

$$\operatorname{pgcd}(Q_1, Q_2, Q_3) = 1.$$

Exercice 166

Soit $T_n(x) = \cos(n \arccos(x))$ pour $x \in [-1, 1]$.

1. (a) Montrer que pour tout $\theta \in [0, \pi]$, $T_n(\cos\theta) = \cos(n\theta)$.
   (b) Calculer T_0 et T_1.
   (c) Montrer la relation de récurrence

$$T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x), \quad \text{pour tout } n \geq 0.$$

(d) En déduire que T_n est une fonction polynomiale de degré n.

2. Soit $P(X) = \lambda(X - a_1)\cdots(X - a_n)$ un polynôme, où les a_k sont deux à deux distincts et $\lambda \neq 0$. Montrer que
$$\frac{1}{P(X)} = \sum_{k=1}^{n} \frac{1}{P'(a_k)} \frac{1}{X - a_k}.$$

3. Décomposer $\dfrac{1}{T_n}$ en éléments simples.

Réponse 166

1. (a) Si on pose $x = \cos\theta$, alors l'égalité $T_n(x) = \cos(n \arccos(x))$ devient $T_n(\cos\theta) = \cos(n\theta)$, car $\arccos(\cos\theta) = \theta$ pour $\theta \in [0, \pi]$.

(b)
$$T_0(x) = 1, \quad T_1(x) = x.$$

(c) En écrivant $(n+2)\theta = (n+1)\theta + \theta$ et $n\theta = (n+1)\theta - \theta$, on obtient :
$$\cos((n+2)\theta) = \cos((n+1)\theta)\cos\theta - \sin((n+1)\theta)\sin\theta,$$
$$\cos(n\theta) = \cos((n+1)\theta)\cos\theta + \sin((n+1)\theta)\sin\theta.$$
Lorsque l'on fait la somme de ces deux égalités, on obtient :
$$\cos((n+2)\theta) + \cos(n\theta) = 2\cos((n+1)\theta)\cos\theta.$$
Avec $x = \cos\theta$, cela donne :
$$T_{n+2}(x) + T_n(x) = 2xT_{n+1}(x).$$

(d) T_0 et T_1 étant des polynômes, alors, par récurrence, $T_n(x)$ est un polynôme. De plus, toujours par la formule de récurrence, il est facile de voir que le degré de $T_n(x)$ est n.

2. Puisque les racines de $P = \lambda(X - a_1)\cdots(X - a_n)$ sont deux à deux distinctes, la décomposition en éléments simples de $\dfrac{1}{P}$ est de la forme :
$$\frac{1}{P} = \frac{c_1}{X - a_1} + \cdots + \frac{c_n}{X - a_n}.$$
Expliquons comment calculer le coefficient c_1. On multiplie la fraction $\dfrac{1}{P}$ par $(X - a_1)$, ce qui donne :
$$\frac{X - a_1}{P} = c_1 + c_2\frac{X - a_1}{X - a_2} + \cdots + c_n\frac{X - a_1}{X - a_n},$$
et
$$\frac{X - a_1}{P} = \frac{1}{\lambda(X - a_2)\cdots(X - a_n)}.$$
En évaluant ces égalités en $X = a_1$, on obtient :
$$c_1 = \frac{1}{\lambda(a_1 - a_2)\cdots(a_1 - a_n)} = \frac{1}{\lambda\prod_{j\neq 1}(a_1 - a_j)}.$$
De même, le coefficient c_k s'obtient en multipliant $\dfrac{1}{P}$ par $(X - a_k)$, puis en remplaçant X par a_k, ce qui donne :
$$c_k = \frac{1}{\lambda\prod_{j\neq k}(a_k - a_j)}.$$

Or, la dérivée de P est :

$$P'(X) = \lambda \sum_{k=1}^{n} \prod_{j \neq k} (X - a_j).$$

En particulier :

$$P'(a_k) = \lambda \prod_{j \neq k} (a_k - a_j).$$

On a donc prouvé que :

$$c_k = \frac{1}{P'(a_k)}.$$

Ainsi, la décomposition en éléments simples de $\dfrac{1}{P}$ est :

$$\frac{1}{P(X)} = \sum_{k=1}^{n} \frac{1}{P'(a_k)} \frac{1}{X - a_k}.$$

3. (a) Cherchons d'abord les racines de $T_n(x)$. Soit $x \in [-1, 1]$:

$$T_n(x) = 0 \iff \cos(n \arccos(x)) = 0 \iff n \arccos(x) \equiv \frac{\pi}{2} \pmod{\pi}.$$

Cela revient à dire qu'il existe $k \in \mathbb{Z}$ tel que :

$$\arccos(x) = \frac{\pi}{2n} + \frac{k\pi}{n}.$$

Comme par définition $\arccos(x) \in [0, \pi]$, les entiers k possibles sont $k = 0, \ldots, n-1$. Ainsi :

$$\arccos(x) = \frac{\pi}{2n} + \frac{k\pi}{n} \iff x = \cos\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right).$$

Posons donc $\omega_k = \cos\left(\frac{(2k+1)\pi}{2n}\right)$ pour $k = 0, \ldots, n-1$. Les ω_k sont les racines de T_n. Finalement :

$$T_n(x) = \lambda \prod_{k=0}^{n-1} (x - \omega_k).$$

(b) On sait que la décomposition en éléments simples de $\dfrac{1}{T_n(x)}$ s'écrit :

$$\frac{1}{T_n(X)} = \sum_{k=0}^{n-1} \frac{1}{T_n'(\omega_k)} \frac{1}{X - \omega_k}.$$

En partant de $T_n(x) = \cos(n \arccos(x))$, on calcule :

$$T_n'(x) = n \frac{\sqrt{1 - x^2}}{\sin(n \arccos(x))}.$$

En utilisant que $\sin(n \arccos(\omega_k)) = \sin\left(\frac{\pi}{2} + k\pi\right) = (-1)^k$ et que $\sqrt{1 - \cos^2\theta} = \sin\theta$ pour $\theta \in [0, \pi]$, on trouve :

$$T_n'(\omega_k) = n(-1)^k \sin\left(\frac{(2k+1)\pi}{2n}\right).$$

Ainsi :

$$\frac{1}{T_n(X)} = \sum_{k=0}^{n-1} \frac{(-1)^k}{n \sin\left(\frac{(2k+1)\pi}{2n}\right)} \frac{1}{X - \omega_k}.$$