Chapter 3

Modules and Vector Spaces

3.1 Definitions and Examples

Modules are a generalization of the vector spaces of linear algebra in which the "scalars" are allowed to be from an arbitrary ring, rather than a field. This rather modest weakening of the axioms is quite far reaching, including, for example, the theory of rings and ideals and the theory of abelian groups as special cases.

(1.1) Definition. *Let R be an arbitrary ring with identity (not necessarily commutative).*

(1) *A* **left R-module** *(or* **left module over** R*) is an abelian group M together with a scalar multiplication map*

$$\cdot : R \times M \to M$$

that satisfy the following axioms (as is customary we will write am in place of $\cdot(a, m)$ for the scalar multiplication of $m \in M$ by $a \in R$). In these axioms, a, b are arbitrary elements of R and m, n are arbitrary elements of M.

($\mathrm{a_l}$) $a(m + n) = am + an$.
($\mathrm{b_l}$) $(a + b)m = am + bm$.
($\mathrm{c_l}$) $(ab)m = a(bm)$.
($\mathrm{d_l}$) $1m = m$.

(2) *A* **right R-module** *(or* **right module over** R*) is an abelian group M together with a scalar multiplication map*

$$\cdot : M \times R \to M$$

that satisfy the following axioms (again a, b are arbitrary elements of R and m, n are arbitrary elements of M).

($\mathrm{a_r}$) $(m + n)a = ma + na$.
($\mathrm{b_r}$) $m(a + b) = ma + mb$.

$(\mathrm{c_r})m(ab) = (ma)b.$
$(\mathrm{d_r})m1 = m.$

(1.2) *Remarks.*

(1) If R is a commutative ring then any left R-module also has the structure of a right R-module by defining $mr = rm$. The only axiom that requires a check is axiom $(\mathrm{c_r})$. But

$$m(ab) = (ab)m = (ba)m = b(am) = b(ma) = (ma)b.$$

(2) More generally, if the ring R has an antiautomorphism (that is, an additive homomorphism $\phi : R \to R$ such that $\phi(ab) = \phi(b)\phi(a)$) then any left R-module has the structure of a right R-module by defining $ma = \phi(a)m$. Again, the only axiom that needs checking is axiom $(\mathrm{c_r})$:

$$\begin{aligned}(ma)b &= \phi(b)(ma)\\ &= \phi(b)(\phi(a)m)\\ &= (\phi(b)\phi(a))m\\ &= \phi(ab)m\\ &= m(ab).\end{aligned}$$

An example of this situation occurs for the group ring $R(G)$ where R is a ring with identity and G is a group (see Example 2.1.10 (15)). In this case the antiautomorphism is given by

$$\phi\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} a_g g^{-1}.$$

We leave it as an exercise to check that $\phi : R(G) \to R(G)$ is an antiautomorphism. Thus any left $R(G)$-module M is automatically a right $R(G)$-module.

(3) Let R be an arbitrary ring and let R^{op} ("op" for opposite) be the ring whose elements are the elements of R, whose addition agrees with that of R, but whose multiplication $\cdot$ is given by $a \cdot b = ba$ (where the multiplication on the right-hand side of this equation is that of R). Then any left R-module is naturally a right R^{op}-module (and vice-versa). In fact, if M is a left R-module, define a right multiplication of elements of R^{op} (which are the same as elements of R) on M by $m\cdot a = am$. As in Remark 1.2 (1), the only axiom that requires checking is axiom (c_r). But

$$m \cdot (a \cdot b) = (a \cdot b)m = (ba)m = b(am) = b(m \cdot a) = (m \cdot a) \cdot b.$$

The theories of left R-modules and right R-modules are entirely parallel, and so, to avoid doing everything twice, we must choose to work on

one side or the other. Thus, we shall work primarily with left R-modules unless explicitly indicated otherwise and we will define an R**-module** (or module over R) to be a left R-module. (Of course, if R is commutative, Remark 1.2 (1) shows there is no difference between left and right R-modules.) Applications of module theory to the theory of group representations will, however, necessitate the use of both left and right modules over noncommutative rings. Before presenting a collection of examples some more notation will be introduced.

(1.3) Definition. *Let R be a ring and let M, N be R-modules. A function $f : M \to N$ is an* R**-module homomorphism** *if*

(1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ *for all* $m_1, m_2 \in M$, *and*
(2) $f(am) = af(m)$ *for all* $a \in R$ *and* $m \in M$.

The set of all R-module homomorphisms from M to N will be denoted $\mathrm{Hom}_R(M, N)$. In case $M = N$ we will usually write $\mathrm{End}_R(M)$ rather than $\mathrm{Hom}_R(M, M)$; elements of $\mathrm{End}_R(M)$ are called **endomorphisms**. If $f \in \mathrm{End}_R(M)$ is invertible, then it is called an **automorphism** of M. The group of all R-module automorphisms of M is denoted $\mathrm{Aut}_R(M)$ ($\mathrm{Aut}(M)$ if R is implicit). If $f \in \mathrm{Hom}_R(M, N)$ then we define $\mathrm{Ker}(f) \subseteq M$ and $\mathrm{Im}(f) \subseteq N$ to be the kernel and image of f considered as an abelian group homomorphism.

(1.4) Definition.

(1) *Let F be a field. Then an F-module V is called a* **vector space** *over F.*
(2) *If V and W are vector spaces over the field F then a* **linear transformation** *from V to W is an F-module homomorphism from V to W.*

(1.5) Examples.

(1) Let G be any abelian group and let $g \in G$. If $n \in \mathbf{Z}$ then define the scalar multiplication ng by

$$ng = \begin{cases} g + \cdots + g & (n \text{ terms}) \text{ if } n > 0, \\ 0 & \text{if } n = 0, \\ (-g) + \cdots + (-g) & (-n \text{ terms}) \text{ if } n < 0. \end{cases}$$

Using this scalar multiplication G is a $\mathbf{Z}$-module. Furthermore, if G and H are abelian groups and $f : G \to H$ is a group homomorphism, then f is also a $\mathbf{Z}$-module homomorphism since (if $n > 0$)

$$f(ng) = f(g + \cdots + g) = f(g) + \cdots + f(g) = nf(g)$$

and $f(-g) = -f(g)$.

(2) Let R be an arbitrary ring. Then R^n is both a left and a right R-module via the scalar multiplications

$$a(b_1, \ldots, b_n) = (ab_1, \ldots, ab_n)$$

and

$$(b_1, \ldots, b_n)a = (b_1a, \ldots, b_na).$$

(3) Let R be an arbitrary ring. Then the set of matrices $M_{m,n}(R)$ is both a left and a right R-module via left and right scalar multiplication of matrices, i.e.,

$$\mathrm{ent}_{ij}(aA) = a\ \mathrm{ent}_{ij}(A)$$

and

$$\mathrm{ent}_{ij}(Aa) = (\mathrm{ent}_{ij}(A))a.$$

(4) As a generalization of the above example, the matrix multiplication maps

$$\begin{aligned} M_m(R) \times M_{m,n}(R) &\longrightarrow M_{m,n}(R) \\ (A,\, B) &\longmapsto AB \end{aligned}$$

and

$$\begin{aligned} M_{m,n}(R) \times M_n(R) &\longrightarrow M_{m,n}(R) \\ (A,\, B) &\longmapsto AB \end{aligned}$$

make $M_{m,n}(R)$ into a left $M_m(R)$-module and a right $M_n(R)$-module.

(5) If R is a ring then a left ideal $I \subseteq R$ is a left R-module, while a right ideal $J \subseteq R$ is a right R-module. In both cases the scalar multiplication is just the multiplication of the ring R.

(6) If R is a ring and $I \subseteq R$ is an ideal then the quotient ring R/I is both a left R-module and a right R-module via the multiplication maps

$$\begin{aligned} R \times R/I &\longrightarrow R/I \\ (a,\, b + I) &\longmapsto ab + I \end{aligned}$$

and

$$\begin{aligned} R/I \times R &\longrightarrow R/I \\ (a + I,\, b) &\longmapsto ab + I. \end{aligned}$$

(7) M is defined to be an **R-algebra** if M is both an R-module and a ring, with the ring addition being the same as the module addition, and the multiplication on M and the scalar multiplication by R satisfying the following identity: For every $r \in R$, m_1, $m_2 \in M$,

$$r(m_1m_2) = (rm_1)m_2 = m_1(rm_2). \tag{1.1}$$

For example, every ring is a $\mathbf{Z}$-algebra, and if R is a commutative ring, then R is an R-algebra. Let R and S be rings and let $\phi : R \to S$ be a ring homomorphism with $\mathrm{Im}(\phi) \subseteq C(S) = \{a \in S : ab = ba$ for all $b \in S\}$, the center of S. If M is an S-module, then M is also an R-module using the scalar multiplication $am = (\phi(a))m$ for all $a \in R$ and $m \in M$. Since S itself is an S-module, it follows that S is an R-module, and moreover, since $\mathrm{Im}(\phi) \subseteq C(S)$, we conclude that S is an R-algebra. As particular cases of this construction, if R is a commutative ring, then the polynomial ring $R[X]$ and the matrix ring $M_n(R)$ are both R-algebras.

(8) If M and N are R-modules then $\mathrm{Hom}_R(M, N)$ is an abelian group via the operation $(f + g)(m) = f(m) + g(m)$. However, if we try to make $\mathrm{Hom}_R(M, N)$ into an R-module in the natural way by defining af by the formula $(af)(m) = a(f(m))$ we find that the function af need not be an R-module homomorphism unless R is a commutative ring. To see this, note that

$$(af)(rm) = a(f(rm)) = a(r(f(m))) = arf(m).$$

This last expression is equal to $r(af)(m) = raf(m)$ if R is a commutative ring, but not necessarily otherwise. Thus, if R is a commutative ring, then we may consider $\mathrm{Hom}_R(M, N)$ as an R-module for all M, N, while if R is not commutative then $\mathrm{Hom}_R(M, N)$ is only an abelian group. Since $\mathrm{End}_R(M)$ is also a ring using composition of R-module homomorphisms as the multiplication, and since there is a ring homomorphism $\phi : R \to \mathrm{End}_R(M)$ defined by $\phi(a) = a\,1_M$ where 1_M denotes the identity homomorphism of M, it follows from Example 1.5 (7) that $\mathrm{End}_R(M)$ is an R-algebra if R is a commutative ring.

(9) If G is an abelian group, then $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, G) \cong G$. To see this, define $\Phi : \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, G) \to G$ by $\Phi(f) = f(1)$. We leave it as an exercise to check that Φ is an isomorphism of $\mathbf{Z}$-modules.

(10) Generalizing Example 1.5 (9), if M is an R-module then

$$\mathrm{Hom}_R(R, M) \cong M$$

as $\mathbf{Z}$-modules via the map $\Phi : \mathrm{Hom}_R(R, M) \to M$ where $\Phi(f) = f(1)$.

(11) Let R be a commutative ring, let M be an R-module, and let $S \subset \mathrm{End}_R(M)$ be a subring. (Recall from Example 1.5 (8) that $\mathrm{End}_R(M)$ is a ring, in fact, an R algebra.) Then M is an S-module by means of the scalar multiplication map $S \times M \to M$ defined by $(f, m) \mapsto f(m)$.

(12) As an important special case of Example 1.5 (11), let $T \in \mathrm{End}_R(M)$ and define a ring homomorphism $\phi : R[X] \to \mathrm{End}_R(M)$ by sending X to T and $a \in R$ to $a1_M$. (See the polynomial substitution theorem (Theorem 2.4.1).) Thus, if

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

then

$$\phi(f(X)) = a_0 1_M + a_1 T + \cdots + a_n T^n.$$

We will denote $\phi(f(X))$ by the symbol $f(T)$ and we let $\mathrm{Im}(\phi) = R[T]$. That is, $R[T]$ is the subring of $\mathrm{End}_R(M)$ consisting of "polynomials" in T. Then M is an $R[T]$ module by means of the multiplication

$$f(T)m = f(T)(m).$$

Using the homomorphism $\phi : R[X] \to R[T]$ we see that M is an $R[X]$-module using the scalar multiplication

$$f(X)m = f(T)(m).$$

This example is an extremely important one. It provides the basis for applying the theory of modules over principal ideal domains to the study of linear transformations; it will be developed fully in Section 4.4.

(13) We will present a concrete example of the situation presented in Example 1.5 (12). Let F be a field and define a linear transformation $T : F^2 \to F^2$ by $T(u_1, u_2) = (u_2, 0)$. Then $T^2 = 0$, so if $f(X) = a_0 + a_1 X + \cdots + a_m X^m \in F[X]$, it follows that $f(T) = a_0 1_{F^2} + a_1 T$. Therefore the scalar multiplication $f(X)u$ for $u \in F^2$ is given by

$$\begin{aligned} f(X) \cdot (u_1, u_2) &= f(T)(u_1, u_2) \\ &= (a_0 1_{F^2} + a_1 T)(u_1, u_2) \\ &= (a_0 u_1 + a_1 u_2, a_0 u_2). \end{aligned}$$

3.2 Submodules and Quotient Modules

Let R be a ring and M an R-module. A subset $N \subseteq M$ is said to be a **submodule** (or **R-submodule**) of M if N is a subgroup of the additive group of M that is also an R-module using the scalar multiplication on M. What this means, of course, is that N is a submodule of M if it is a subgroup of M that is closed under scalar multiplication. These conditions can be expressed as follows.

(2.1) Lemma. *If M is an R-module and N is a nonempty subset of M, then N is an R-submodule of M if and only if $am_1 + bm_2 \in N$ for all $m_1, m_2 \in N$ and $a, b \in R$.*

Proof. Exercise. □

If F is a field and V is a vector space over F, then an F-submodule of V is called a **linear subspace** of V.

(2.2) Examples.

(1) If R is any ring then the R-submodules of the R-module R are precisely the left ideals of the ring R.
(2) If G is any abelian group then G is a $\mathbf{Z}$-module and the $\mathbf{Z}$-submodules of G are just the subgroups of G.
(3) Let $f : M \to N$ be an R-module homomorphism. Then $\mathrm{Ker}(f) \subseteq M$ and $\mathrm{Im}(f) \subseteq N$ are R-submodules (exercise).
(4) Continuing with Example 1.5 (12), let V be a vector space over a field F and let $T \in \mathrm{End}_F(V)$ be a fixed linear transformation. Let V_T denote V with the $F[X]$-module structure determined by the linear transformation T. Then a subset $W \subseteq V$ is an $F[X]$-submodule of the module V_T if and only if W is a linear subspace of V and $T(W) \subseteq W$, i.e., W must be a T**-invariant subspace** of V. To see this, note that $X \cdot w = T(w)$, and if $a \in F$, then $a \cdot w = aw$—that is to say, the action of the constant polynomial $a \in F[X]$ on V is just ordinary scalar multiplication, while the action of the polynomial X on V is the action of T on V. Thus, an $F[X]$-submodule of V_T must be a T-invariant subspace of V. Conversely, if W is a linear subspace of V such that $T(W) \subseteq W$ then $T^m(W) \subseteq W$ for all $m \geq 1$. Hence, if $f(X) \in F[X]$ and $w \in W$ then $f(X) \cdot w = f(T)(w) \in W$ so that W is closed under scalar multiplication and thus W is an $F[X]$-submodule of V.

(2.3) Lemma. *Let M be an R-module and let $\{N_\alpha\}_{\alpha \in A}$ be a family of submodules of M. Then $N = \bigcap_{\alpha \in A} N_\alpha$ is a submodule of M.*

Proof. Exercise. □

We now consider quotient modules and the noether isomorphism theorems. Let M be an R-module and let $N \subseteq M$ be a submodule. Then N is a subgroup of the abelian group M, so we can form the quotient group M/N. Define a scalar multiplication map on the abelian group M/N by $a(m + N) = am + N$ for all $a \in R$, $m + N \in M/N$. Since N is an R-submodule of M, this map is well defined. Indeed, if $m + N = m' + N$ then $m - m' \in N$ so that $am - am' = a(m - m') \in N$ so that $am + N = am' + N$. The resulting R-module M/N is called the quotient module of M with respect to the submodule N. The noether isomorphism theorems, which we have seen previously for groups and rings, then have direct analogues for R-modules.

(2.4) Theorem. (First isomorphism theorem) *Let M and N be modules over the ring R and let $f : M \to N$ be an R-module homomorphism. Then*

$M/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

Proof. Let $K = \operatorname{Ker}(f)$. From Theorem 1.3.10 we know that $\overline{f} : M/K \to \operatorname{Im}(f)$ defined by $\overline{f}(m+K) = f(m)$ is a well-defined isomorphism of abelian groups. It only remains to check that $\overline{f}$ is an R-module homomorphism. But $\overline{f}(a(m+K)) = \overline{f}(am+K) = f(am) = af(m) = a\overline{f}(m+K)$ for all $m \in M$ and $a \in R$, so we are done. □

(2.5) Theorem. (Second isomorphism theorem) *Let M be an R-module and let N and P be submodules. Then there is an isomorphism of R-modules*

$$(N+P)/P \cong N/(N \cap P).$$

Proof. Let $\pi : M \to M/P$ be the natural projection map and let π_0 be the restriction of π to N. Then π_0 is an R-module homomorphism with $\operatorname{Ker}(\pi_0) = N \cap P$ and $\operatorname{Im}(\pi_0) = (N+P)/P$. The result then follows from the first isomorphism theorem. □

(2.6) Theorem. (Third isomorphism theorem) *Let M be an R-module and let N and P be submodules of M with $P \subseteq N$. Then*

$$M/N \cong (M/P)/(N/P).$$

Proof. Define $f : M/P \to M/N$ by $f(m+P) = m+N$. This is a well-defined R-module homomorphism and

$$\operatorname{Ker}(f) = \{m+P : m+N = N\} = \{m+P : m \in N\} = N/P.$$

The result then follows from the first isomorphism theorem (Theorem 2.4). □

(2.7) Theorem. (Correspondence theorem) *Let M be an R-module, N a submodule, and $\pi : M \to M/N$ the natural projection map. Then the function $P \mapsto P/N$ defines a one-to-one correspondence between the set of all submodules of M that contain N and the set of all submodules of M/N.*

Proof. Exercise. □

(2.8) Definition. *If S is a subset of an R-module M then $\langle S \rangle$ will denote the intersection of all the submodules of M that contain S. This is called the* **submodule of M generated by S,** *while the elements of S are called* **generators** *of $\langle S \rangle$.*

Thus, $\langle S \rangle$ is a submodule of M that contains S and it is contained in every submodule of M that contains S, i.e., $\langle S \rangle$ is the smallest submodule of M containing S. If $S = \{x_1, \ldots, x_n\}$ we will usually write $\langle x_1, \ldots, x_n \rangle$

rather than $\langle\{x_1, \ldots, x_n\}\rangle$ for the submodule generated by S. There is the following simple description of $\langle S\rangle$.

(2.9) Lemma. *Let M be an R-module and let $S \subseteq M$.*

(1) *If $S = \emptyset$ then $\langle S\rangle = \{0\}$.*
(2) *If $S \neq \emptyset$ then*

$$\langle S\rangle = \left\{ \sum_{i=1}^{n} a_i s_i : n \in \mathbf{N},\ a_1, \ldots, a_n \in R,\ s_1, \ldots, s_n \in S \right\}.$$

Proof. Exercise. □

(2.10) Definition. *We say that the R-module M is* **finitely generated** *if $M = \langle S\rangle$ for some finite subset S of M. M is* **cyclic** *if $M = \langle m\rangle$ for some element $m \in M$. If M is finitely generated then let $\mu(M)$ denote the minimal number of generators of M. If M is not finitely generated, then we will define $\mu(M) = \infty$. We will call $\mu(M)$ the* **rank** *of M.*

(2.11) *Remarks.*

(1) We have $\mu(\{0\}) = 0$ by Lemma 2.9 (1), and $M \neq \{0\}$ is cyclic if and only if $\mu(M) = 1$.
(2) The concept of cyclic R-module generalizes the concept of cyclic group. Thus an abelian group G is cyclic (as an abelian group) if and only if it is a cyclic $\mathbf{Z}$-module.
(3) If R is a PID, then any R-submodule M of R is an ideal, so $\mu(M) = 1$.

If M is a finitely generated R-module and N is any submodule, then M/N is clearly finitely generated, and in fact, $\mu(M/N) \leq \mu(M)$ since the image in M/N of any generating set of M is a generating set of M/N. There is also the following result, which is frequently useful for constructing arguments using induction on $\mu(M)$.

(2.12) Proposition. *Suppose M is an R-module and N is a submodule. If N and M/N are finitely generated, then so is M and*

$$\mu(M) \leq \mu(N) + \mu(M/N).$$

Proof. Let $S = \{x_1, \ldots, x_k\} \subseteq N$ be a minimal generating set for N and if $\pi : M \to M/N$ is the natural projection map, choose $T = \{y_1, \ldots, y_\ell\} \subseteq M$ so that $\{\pi(y_1), \ldots, \pi(y_\ell)\}$ is a minimal generating set for M/N. We claim that $S \cup T$ generates M so that $\mu(M) \leq k + \ell = \mu(N) + \mu(M/N)$. To see this suppose that $x \in M$. Then $\pi(x) = a_1\pi(y_1) + \cdots + a_\ell\pi(y_\ell)$. Let $y =$

$a_1y_1+\cdots+a_\ell y_\ell \in \langle T\rangle$. Then $\pi(x-y)=0$ so that $x-y \in \mathrm{Ker}(\pi)=N=\langle S\rangle$. It follows that $x=(x-y)+y \in \langle S\cup T\rangle$, and the proof is complete. □

(2.13) Definition. *If $\{N_\alpha\}_{\alpha\in A}$ is a family of R-submodules of M, then the* **submodule generated by** *$\{N_\alpha\}_{\alpha\in A}$ is $\left\langle \bigcup_{\alpha\in A} N_\alpha\right\rangle$. This is just the set of all sums $n_{\alpha_1}+\cdots+n_{\alpha_k}$ where $n_{\alpha_i}\in N_{\alpha_i}$. Instead of $\left\langle \bigcup_{\alpha\in A} N_\alpha\right\rangle$, we will use the notation $\sum_{\alpha\in A} N_\alpha$; if the index set A is finite, e.g., $A=\{1,\ldots,m\}$, we will write $N_1+\cdots+N_m$ for the submodule generated by $N_1,\ldots,N_m$.*

(2.14) Definition. *If R is a ring, M is an R-module, and X is a subset of M, then the* **annihilator of** *X, denoted $\mathrm{Ann}(X)$, is defined by*

$$\mathrm{Ann}(X)=\{a\in R : ax=0 \text{ for all } x\in X\}.$$

It is easy to check that $\mathrm{Ann}(X)$ is a left ideal of R, and furthermore, if $X=N$ is a submodule of M, then $\mathrm{Ann}(N)$ is an ideal of R. If R is commutative and $N=\langle x\rangle$ is a cyclic submodule of M with generator x, then

$$\mathrm{Ann}(N)=\{a\in R : ax=0\}.$$

This fact is not true if the ring R is not commutative. As an example, let $R=M_n(\mathbf{R})=M$ and let $x=E_{11}$ be the matrix with a 1 in the 1 1 position and 0 elsewhere. It is a simple exercise to check that $\mathrm{Ann}(E_{11})$ consists of all matrices with first column 0, while $\mathrm{Ann}(\langle E_{11}\rangle)=\langle 0\rangle$.

If R is commutative and N is cyclic with generator x then we will usually write $\mathrm{Ann}(x)$ rather than $\mathrm{Ann}(\langle x\rangle)$. In this situation, the ideal $\mathrm{Ann}(x)$ is frequently called the **order ideal** of x. To see why, consider the example of an abelian group G and an element $g\in G$. Then G is a $\mathbf{Z}$-module and

$$\begin{aligned}\mathrm{Ann}(g)&=\{n\in\mathbf{Z} : ng=0\}\\ &=\langle p\rangle\end{aligned}$$

where $p=o(g)$ if $o(g)<\infty$ and $p=0$ if $\langle g\rangle$ is infinite cyclic.

Example. Let F be a field, V a vector space, $T\in \mathrm{End}_F(V)$ a linear transformation, and let V_T be the $F[X]$ module determined by T (Example 1.5 (12)). If $v\in V$ then

$$\mathrm{Ann}(v)=\{f(X)\in F[X] : f(T)(v)=0\}.$$

Note that this is a principal ideal $\langle g(X)\rangle$ since $F[X]$ is a PID.

(2.15) Proposition. *Let R be a ring and let $M=\langle m\rangle$ be a cyclic R-module. Then $M\cong R/\mathrm{Ann}(m)$.*

Proof. The function $f: R\to M$ defined by $f(a)=am$ is a surjective R-module homomorphism with $\mathrm{Ker}(f)=\mathrm{Ann}(m)$. The result follows by the first isomorphism theorem. □

(2.16) Corollary. *If F is a field and M is a nonzero cyclic F-module then $M \cong F$.*

Proof. A field has only the ideals $\{0\}$ and F, and $1 \cdot m = m \neq 0$ if $m \neq 0$ is a generator for M. Thus, $\mathrm{Ann}(m) \neq F$, so it must be $\{0\}$. □

If M is an R-module and $I \subseteq R$ is an ideal then we can define the product of I and M by

$$IM = \left\{ \sum_{i=1}^{n} a_i m_i : n \in \mathbf{N},\ a_i \in I,\ m_i \in M \right\}.$$

The set IM is easily checked to be a submodule of M. The product IM is a generalization of the concept of product of ideals. If R is commutative and $I \subseteq \mathrm{Ann}(M)$ then there is a map

$$R/I \times M \to M$$

defined by $(a + I)m = am$. To see that this map is well defined, suppose that $a + I = b + I$. Then $a - b \in I \subseteq \mathrm{Ann}(M)$ so that $(a - b)m = 0$, i.e., $am = bm$. Therefore, whenever an ideal $I \subseteq \mathrm{Ann}(M)$, M is also an R/I module. A particular case where this occurs is if $N = M/IM$ where I is any ideal of R. Then certainly $I \subseteq \mathrm{Ann}(N)$ so that M/IM is an R/I-module.

(2.17) Definition. *Let R be an integral domain and let M be an R-module. We say that an element $x \in M$ is a* **torsion element** *if $\mathrm{Ann}(x) \neq \{0\}$. Thus an element $x \in M$ is torsion if and only if there is an $a \neq 0 \in R$ such that $ax = 0$. Let M_τ be the set of torsion elements of M. M is said to be* **torsion-free** *if $M_\tau = \{0\}$, and M is a* **torsion module** *if $M = M_\tau$.*

(2.18) Proposition. *Let R be an integral domain and let M be an R-module.*

(1) *M_τ is a submodule of M, called the* **torsion submodule**.
(2) *M/M_τ is torsion-free.*

Proof. (1) Let $x, y \in M_\tau$ and let $c, d \in R$. There are $a \neq 0$, $b \neq 0 \in R$ such that $ax = 0$ and $by = 0$. Since R is an integral domain, $ab \neq 0$. Therefore, $ab(cx + dy) = bc(ax) + ad(by) = 0$ so that $cx + dy \in M_\tau$.

(2) Suppose that $a \neq 0 \in R$ and $a(x + M_\tau) = 0 \in (M/M_\tau)_\tau$. Then $ax \in M_\tau$, so there is a $b \neq 0 \in R$ with $(ba)x = b(ax) = 0$. Since $ba \neq 0$, it follows that $x \in M_\tau$, i.e., $x + M_\tau = 0 \in M/M_\tau$. □

(2.19) Examples.

(1) If G is an abelian group then the torsion $\mathbf{Z}$-submodule of G is the set of all elements of G of finite order. Thus, $G = G_\tau$ means that every element of G is of finite order. In particular, any finite abelian

group is torsion. The converse is not true. For a concrete example, take $G = \mathbf{Q}/\mathbf{Z}$. Then $|G| = \infty$, but every element of $\mathbf{Q}/\mathbf{Z}$ has finite order since $q(p/q + \mathbf{Z}) = p + \mathbf{Z} = 0 \in \mathbf{Q}/\mathbf{Z}$. Thus $(\mathbf{Q}/\mathbf{Z})_\tau = \mathbf{Q}/\mathbf{Z}$.

(2) An abelian group is torsion-free if it has no elements of finite order other than 0. As an example, take $G = \mathbf{Z}^n$ for any natural number n. Another useful example to keep in mind is the additive group $\mathbf{Q}$.

(3) Let $V = F^2$ and consider the linear transformation $T : F^2 \to F^2$ defined by $T(u_1, u_2) = (u_2, 0)$. See Example 1.5 (13). Then the $F[X]$ module V_T determined by T is a torsion module. In fact $\mathrm{Ann}(V_T) = \langle X^2 \rangle$. To see this, note that $T^2 = 0$, so $X^2 \cdot u = 0$ for all $u \in V$. Thus, $\langle X^2 \rangle \subseteq \mathrm{Ann}(V_T)$. The only ideals of $F[X]$ properly containing $\langle X^2 \rangle$ are $\langle X \rangle$ and the whole ring $F[X]$, but $X \notin \mathrm{Ann}(V_T)$ since $X \cdot (0, 1) = (1, 0) \neq (0, 0)$. Therefore, $\mathrm{Ann}(V_T) = \langle X^2 \rangle$.

The following two observations are frequently useful; the proofs are left as exercises:

(2.20) Proposition. *Let R be an integral domain and let M be a finitely generated torsion R-module. Then* $\mathrm{Ann}(M) \neq (0)$. *In fact, if $M = \langle x_1, \ldots, x_n \rangle$ then*

$$\mathrm{Ann}(M) = \mathrm{Ann}(x_1) \cap \cdots \cap \mathrm{Ann}(x_n) \neq (0).$$

Proof. Exercise. □

(2.21) Proposition. *Let F be a field and let V be a vector space over F, i.e., an F-module. Then V is torsion-free.*

Proof. Exercise. □

3.3 Direct Sums, Exact Sequences, and Hom

Let $M_1, \ldots, M_n$ be a finite collection of R-modules. Then the cartesian product set $M_1 \times \cdots \times M_n$ can be made into an R-module by the operations

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

where the 0 element is, of course, $(0, \ldots, 0)$. The R-module thus constructed is called the **direct sum** of $M_1, \ldots, M_n$ and is denoted

$$M_1 \oplus \cdots \oplus M_n \quad \Big(\text{or} \quad \bigoplus_{i=1}^{n} M_i\Big).$$

The direct sum has an important homomorphism property, which, in fact, can be used to characterize direct sums. To describe this, suppose that $f_i : M_i \to N$ are R-module homomorphisms. Then there is a map

$$f : M_1 \oplus \cdots \oplus M_n \to N$$

defined by

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} f_i(x_i).$$

We leave it as an exercise to check that f is an R-module homomorphism.

Now consider the question of when a module M is isomorphic to the direct sum of finitely many submodules. This result should be compared with Proposition 1.6.3 concerning internal direct products of groups.

(3.1) Theorem. *Let M be an R-module and let $M_1, \ldots, M_n$ be submodules of M such that*

(1) $M = M_1 + \cdots + M_n$, *and*
(2) *for* $1 \leq i \leq n$,

$$M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = 0.$$

Then

$$M \cong M_1 \oplus \cdots \oplus M_n.$$

Proof. Let $f_i : M_i \to M$ be the inclusion map, that is, $f_i(x) = x$ for all $x \in M_i$ and define

$$f : M_1 \oplus \cdots \oplus M_n \to M$$

by

$$f(x_1, \ldots, x_n) = x_1 + \cdots + x_n.$$

f is an R-module homomorphism and it follows from condition (1) that f is surjective. Now suppose that $(x_1, \ldots, x_n) \in \mathrm{Ker}(f)$. Then $x_1 + \cdots + x_n = 0$ so that for $1 \leq i \leq n$ we have

$$x_i = -(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n).$$

Therefore,

$$x_i \in M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = 0$$

so that $(x_1, \ldots, x_n) = 0$ and f is an isomorphism. □

Our primary emphasis will be on the finite direct sums of modules just constructed, but for the purpose of allowing for potentially infinite rank free modules, it is convenient to have available the concept of an arbitrary direct sum of R-modules. This is described as follows. Let $\{M_j\}_{j \in J}$ be

a family of R-modules indexed by the (possibly infinite) set J. Then the cartesian product set $\prod_{j\in J} M_j$ is the set of all the indexed sets of elements $(x_j)_{j\in J}$ where x_j is chosen from M_j. This set is made into an R-module by the coordinate-wise addition and scalar multiplication of elements. More precisely, we define

$$(x_j)_{j\in J} + (y_j)_{j\in J} = (x_j + y_j)_{j\in J}$$
$$a(x_j)_{j\in J} = (ax_j)_{j\in J}.$$

For each $k \in J$ there is an R-module homomorphism $\pi_k : \prod_{j\in J} \to M_k$ defined by $\pi_k((x_j)_{j\in J}) = x_j$, that is, π_k picks out the element of the indexed set $(x_j)_{j\in J}$ that is indexed by k. We define the **direct sum** of the indexed family $\{M_j\}_{j\in J}$ of R-modules to be the following submodule $\bigoplus_{j\in J} M_j$ of $\prod_{j\in J} M_j$:

$$\bigoplus_{j\in J} M_j = \{(x_j)_{j\in J} : x_j = 0 \text{ except for finitely many indices } j \in J\}.$$

It is easy to check that $\oplus_{j\in J} M_j$ is a submodule of $\prod_{j\in J} M_j$.

To get a feeling for the difference between direct sums and direct products when the index set is infinite, note that the polynomial ring $R[X]$, as an R-module (ignoring the multiplicative structure), is just a countable direct sum of copies of R, in fact, the n^{th} copy of R is indexed by the monomial X^n. However, the formal power series ring $R[[X]]$, as an R-module, is just a countable direct product of copies of R. Again, the n^{th} copy of R is indexed by the monomial X^n. Each element of the polynomial ring has only finitely many monomials with nonzero coefficients, while an element of the formal power series ring may have all coefficients nonzero.

The homomorphism property of the finite direct sum of R-modules extends in a natural way to arbitrary direct sums. That is, suppose that N is an arbitrary R-module and that for each $j \in J$ there is an R-module homomorphism $f_j : M_j \to N$. Then there is a map $f : \oplus_{j\in J} M_j \to N$ defined by $f((x_j)_{j\in J}) = \sum_{j\in J} f_j(x_j)$. Note that this sum can be considered as a well-defined finite sum since $x_j = 0$ except for finitely many indices $j \in J$. (Note that this construction does not work for infinite direct products.) We leave it as an exercise to check that f is an R-module homomorphism.

The characterization of when an R-module M is isomorphic to the direct sum of submodules is essentially the same as the characterization provided in Theorem 3.1. We state the result, but the verification is left as an exercise.

(3.2) Theorem. *Let M be an R-module and let $\{M_j\}_{j\in J}$ be a family of submodules such that*

(1) $M = \sum_{j\in J} M_j = \langle \bigcup_{j\in J} M_j \rangle$, *and*
(2) $M_k \bigcap \sum_{j\in J\setminus\{k\}} M_j = \{0\}$ *for every* $k \in J$.

Then

$$M \cong \bigoplus_{j \in J} M_j.$$

Proof. Exercise. □

(3.3) Definition. *If M is an R-module and $M_1 \subseteq M$ is a submodule, we say that M_1 is a* **direct summand** *of M, or is* **complemented** *in M, if there is a submodule $M_2 \subseteq M$ such that $M \cong M_1 \oplus M_2$.*

(3.4) Example. Let $R = \mathbf{Z}$ and $M = \mathbf{Z}_{p^2}$. If $M_1 = \langle p \rangle$ then M_1 is not complemented since M_1 is the only subgroup of M of order p, so condition (2) of Theorem 3.1 is impossible to satisfy.

The concept of exact sequences of R-modules and R-module homomorphisms and their relation to direct summands is a useful tool to have available in the study of modules. We start by defining exact sequences of R-modules.

(3.5) Definition. *Let R be a ring. A sequence of R-modules and R-module homomorphisms*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

is said to be **exact at** *M_i if $\operatorname{Im}(f_i) = \operatorname{Ker}(f_{i+1})$. The sequence is said to be* **exact** *if it is exact at each M_i.*

As particular cases of this definition note that

(1) $0 \longrightarrow M_1 \xrightarrow{f} M$ is exact if and only if f is injective,
(2) $M \xrightarrow{g} M_2 \longrightarrow 0$ is exact if and only if g is surjective, and
(3) the sequence

$$0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0 \tag{3.1}$$

is exact if and only if f is injective, g is surjective, and $\operatorname{Im}(f) = \operatorname{Ker}(g)$. Note that the first isomorphism theorem (Theorem 2.4) then shows that $M_2 \cong M/\operatorname{Im}(f)$. $M/\operatorname{Im}(f)$ is called the **cokernel** of f and it is denoted $\operatorname{Coker}(f)$.

(3.6) Definition.

(1) *The sequence* (3.1)*, if exact, is said to be a* **short exact sequence**.
(2) *The sequence* (3.1) *is said to be a* **split exact sequence** *(or just* **split***) if it is exact and if $\operatorname{Im}(f) = \operatorname{Ker}(g)$ is a direct summand of M.*

In the language of exact sequences, Proposition 2.12 can be stated as follows:

(3.7) Proposition. *Let* $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ *be a short exact sequence of* R*-modules. If* M_1 *and* M_2 *are finitely generated, then so is* M*, and moreover,*

$$\mu(M) \leq \mu(M_1) + \mu(M_2).$$

Proof. □

(3.8) Example. Let p and q be distinct primes. Then we have short exact sequences

$$0 \longrightarrow \mathbf{Z}_p \xrightarrow{\phi} \mathbf{Z}_{pq} \xrightarrow{\psi} \mathbf{Z}_q \longrightarrow 0 \tag{3.2}$$

and

$$0 \longrightarrow \mathbf{Z}_p \xrightarrow{f} \mathbf{Z}_{p^2} \xrightarrow{g} \mathbf{Z}_p \longrightarrow 0 \tag{3.3}$$

where $\phi(m) = qm \in \mathbf{Z}_{pq}$, $f(m) = pm \in \mathbf{Z}_{p^2}$, and ψ and g are the canonical projection maps. Exact sequence (3.2) is split exact while exact sequence (3.3) is not split exact. Both of these observations are easy consequences of the material on cyclic groups from Chapter 1; details are left as an exercise.

There is the following useful criterion for a short exact sequence to be split exact.

(3.9) Theorem. *If*

$$0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0 \tag{3.4}$$

is a short exact sequence of R*-modules, then the following are equivalent:*

(1) *There exists a homomorphism* $\alpha : M \to M_1$ *such that* $\alpha \circ f = 1_{M_1}$.
(2) *There exists a homomorphism* $\beta : M_2 \to M$ *such that* $g \circ \beta = 1_{M_2}$.
(3) *The sequence* (3.4) *is split exact and*

$$\begin{aligned} M &\cong \operatorname{Im}(f) \oplus \operatorname{Ker}(\alpha) \\ &\cong \operatorname{Ker}(g) \oplus \operatorname{Im}(\beta) \\ &\cong M_1 \oplus M_2. \end{aligned}$$

The homomorphisms α *and* β *are said to* **split** *the exact sequence* (3.4) *or be a* **splitting**.

Proof. Suppose that (1) is satisfied and let $x \in M$. Then

$$\alpha(x - f(\alpha(x))) = \alpha(x) - (\alpha \circ f)(\alpha(x)) = 0$$

since $\alpha \circ f = 1_{M_1}$. Therefore, $x - f(\alpha(x)) \in \mathrm{Ker}(\alpha)$ so that

$$M = \mathrm{Ker}(\alpha) + \mathrm{Im}(f).$$

Now suppose that $f(y) = x \in \mathrm{Ker}(\alpha) \cap \mathrm{Im}(f)$. Then

$$0 = \alpha(x) = \alpha(f(y)) = y,$$

and therefore, $x = f(y) = 0$. Theorem 3.1 then shows that

$$M \cong \mathrm{Im}(f) \oplus \mathrm{Ker}(\alpha).$$

Define $\beta : M_2 \to M$ by

$$\beta(u) = v - f(\alpha(v)) \tag{3.5}$$

where $g(v) = u$. Since g is surjective, there is such a $v \in M$, but it may be possible to write $u = g(v)$ for more than one choice of v. Therefore, we must verify that β is well defined. Suppose that $g(v) = u = g(v')$. Then $v - v' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ so that

$$\begin{aligned}(v - f(\alpha(v))) - (v' - f(\alpha(v'))) &= (v - v') + (f(\alpha(v') - f(\alpha(v))) \\ &\in \mathrm{Im}(f) \cap \mathrm{Ker}(\alpha) \\ &= \{0\}.\end{aligned}$$

We conclude that β is well defined. Since it is clear from the construction of β that $g \circ \beta = 1_{M_2}$, we have verified that (1) implies (2) and that $M \cong \mathrm{Im}(f) \oplus \mathrm{Ker}(\alpha)$, i.e., that (3) holds.

The proof that (2) implies (1) and (3) is similar and is left as an exercise.

Suppose that (3) holds, that is, $M \cong M_1 \oplus M_2$. Then the projection $\alpha : M \to M_1$ satisfies $\alpha \circ f = 1_{M_1}$, and the inclusion $\beta : M_2 \to M$ satisfies $g \circ \beta = 1_{M_2}$, so (1) and (2) hold. □

If M and N are R-modules, then the set $\mathrm{Hom}_R(M, N)$ of all R-module homomorphisms $f : M \to N$ is an abelian group under function addition. According to Example 1.5 (8), $\mathrm{Hom}_R(M, N)$ is also an R-module provided that R is a commutative ring. Recall that $\mathrm{End}_R(M) = \mathrm{Hom}_R(M)$ denotes the endomorphism ring of the R-module M, and the ring multiplication is composition of homomorphisms. Example 1.5 (8) shows that $\mathrm{End}_R(M)$ is an R-algebra if the ring R is commutative. Example 1.5 (10) shows that $\mathrm{Hom}_R(R, M) \cong M$ for any R-module M.

Now consider R-modules M, M_1, N, and N_1, and let $\phi : N \to N_1$, $\psi : M \to M_1$ be R-module homomorphisms. Then there are functions

$$\phi_* : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N_1)$$

and

$$\psi^* : \mathrm{Hom}_R(M_1, N) \to \mathrm{Hom}_R(M, N)$$

defined by

$$\phi_*(f) = \phi \circ f \qquad \text{for all} \quad f \in \mathrm{Hom}_R(M, N)$$

and

$$\psi^*(g) = g \circ \psi \qquad \text{for all} \quad g \in \mathrm{Hom}_R(M_1, N).$$

It is straightforward to check that $\phi_*(f+g) = \phi_*(f)+\phi_*(g)$ and $\psi^*(f+g) = \psi^*(f) + \psi^*(g)$ for appropriate f and g. That is, ϕ_* and ψ^* are homomorphisms of abelian groups, and if R is commutative, then they are also R-module homomorphisms.

Given a sequence of R-modules and R-module homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\phi_i} M_i \xrightarrow{\phi_{i+1}} M_{i+1} \longrightarrow \cdots \tag{3.6}$$

and an R-module N, then $\mathrm{Hom}_R(\ \ , N)$ and $\mathrm{Hom}_R(N, \ \ )$ produce two sequences of abelian groups (R-modules if R is commutative):

$$\cdots \longrightarrow \mathrm{Hom}_R(N, M_{i-1}) \xrightarrow{(\phi_i)_*} \mathrm{Hom}_R(N, M_i) \xrightarrow{(\phi_{i+1})_*} \mathrm{Hom}_R(N, M_{i+1}) \longrightarrow \cdots \tag{3.7}$$

and

$$\cdots \longleftarrow \mathrm{Hom}_R(M_{i-1}, N) \xleftarrow{(\phi_i)^*} \mathrm{Hom}_R(M_i, N) \xleftarrow{(\phi_{i+1})^*} \mathrm{Hom}_R(M_{i+1}, N) \longleftarrow \cdots. \tag{3.8}$$

A natural question is to what extent does exactness of sequence (3.6) imply exactness of sequences (3.7) and (3.8). One result along these lines is the following.

(3.10) Theorem. *Let*

$$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\psi} M_2 \tag{3.9}$$

be a sequence of R-modules and R-module homomorphisms. Then the sequence (3.9) *is exact if and only if the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(N, M_1) \xrightarrow{\phi_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, M_2) \tag{3.10}$$

is an exact sequence of $\mathbf{Z}$*-modules for all R-modules N.*

If

$$M_1 \xrightarrow{\phi} M \xrightarrow{\psi} M_2 \longrightarrow 0 \tag{3.11}$$

is a sequence of R-modules and R-module homomorphisms, then the sequence (3.11) *is exact if and only if the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M_2, N) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, N) \xrightarrow{\phi^*} \mathrm{Hom}_R(M_1, N) \tag{3.12}$$

is an exact sequence of $\mathbf{Z}$*-modules for all* R*-modules* N*.*

Proof. Assume that sequence (3.9) is exact and let N be an arbitrary R-module. Suppose that $f \in \mathrm{Hom}_R(N, M)$ and $\phi_*(f) = 0$. Then

$$0 = \phi \circ f(x) = \phi(f(x))$$

for all $x \in N$. But ϕ is injective, so $f(x) = 0$ for all $x \in N$. That is, $f = 0$, and hence, ϕ_* is injective.

Since $\psi \circ \phi = 0$ (because sequence (3.9) is exact at M), it follows that

$$\psi_*(\phi_*(f)) = \psi \circ \phi_*(f) = \psi \circ \phi \circ f = 0$$

for all $f \in \mathrm{Hom}_R(N, M)$. Thus $\mathrm{Im}(\phi_*) \subseteq \mathrm{Ker}(\psi_*)$. It remains to check the other inclusion. Suppose that $g \in \mathrm{Hom}_R(N, M)$ with $\psi_*(g) = 0$, i.e., $\psi(g(x)) = 0$ for all $x \in N$. Since $\mathrm{Ker}(\psi) = \mathrm{Im}(\phi)$, for each $x \in N$, we may write $g(x) = \phi(y)$ with $y \in M_1$. Since ϕ is injective, y is uniquely determined by the equation $g(x) = \phi(y)$. Thus it is possible to define a function $f : N \to M_1$ by $f(x) = y$ whenever $g(x) = \phi(y)$. We leave it as an exercise to check that f is an R-module homomorphism. Since $\phi_*(f) = g$, we conclude that $\mathrm{Ker}(\psi_*) = \mathrm{Im}(\phi_*)$ so that sequence (3.10) is exact.

Exactness of sequence (3.12) is a similar argument, which is left as an exercise.

Conversely, assume that sequence (3.10) is exact for all R-modules N. Then ϕ_* is injective for all R-modules N. Then letting $N = \mathrm{Ker}(\phi)$ and $\iota : N \to M_1$ be the inclusion, we see that $\phi_*(\iota) = \phi \circ \iota = 0$. Since $\phi_* : \mathrm{Hom}_R(N, M_1) \to \mathrm{Hom}_R(N, M)$ is injective, we see that $\iota = 0$, i.e., $N = \langle 0 \rangle$. Thus, ϕ is injective.

Now letting $N = M_1$ we see that

$$0 = (\psi_* \circ \phi_*)(1_{M_1}) = \psi \circ \phi.$$

Thus $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(\psi)$. Now let $N = \mathrm{Ker}(\psi)$ and let $\iota : N \to M$ be the inclusion. Since $\psi_*(\iota) = \psi \circ \iota = 0$, exactness of Equation (3.10) implies that $\iota = \phi_*(\alpha)$ for some $\alpha \in \mathrm{Hom}_R(N, M_1)$. Thus,

$$\mathrm{Im}(\phi) \supseteq \mathrm{Im}(\iota) = N = \mathrm{Ker}(\psi),$$

and we conclude that sequence (3.9) is exact.

Again, exactness of sequence (3.11) is left as an exercise. □

Note that, even if

$$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\psi} M_2 \longrightarrow 0$$

is a short exact sequence, the sequences (3.10) and (3.12) need not be short exact, i.e., neither ψ_* or ϕ^* need be surjective. Following are some examples to illustrate this.

(3.11) Example. Consider the following short exact sequence of $\mathbf{Z}$-modules:

$$0 \longrightarrow \mathbf{Z} \xrightarrow{\phi} \mathbf{Z} \xrightarrow{\psi} \mathbf{Z}_m \longrightarrow 0 \tag{3.13}$$

where $\phi(i) = mi$ and ψ is the canonical projection map. If $N = \mathbf{Z}_n$ then sequence (3.12) becomes

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}_n) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_n) \xrightarrow{\phi^*} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_n),$$

which, by Example 1.5 (10), becomes

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}_n) \longrightarrow \mathbf{Z}_n \xrightarrow{\phi^*} \mathbf{Z}_n$$

so that

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}_n) = \mathrm{Ker}(\phi^*).$$

Let $d = \gcd(m, n)$, and write $m = m'd$, $n = n'd$. Let $f \in \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}_n)$. Then, clearly, $\phi^*(f) = 0$ if and only if $\phi^*(f)(1) = 0$. But

$$\phi^*(f)(1) = f(m \cdot 1) = mf(1) = m'df(1).$$

Since m' is relatively prime to n, we have $m'df(1) = 0$ if and only if $df(1) = 0$, and this is true if and only if $f(1) \in n'\mathbf{Z}_n$. Hence, $\mathrm{Ker}(\phi^*) = n'\mathbf{Z}_n \cong \mathbf{Z}_d$, i.e.,

$$\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}_n) \cong \mathbf{Z}_d. \tag{3.14}$$

This example also shows that even if

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

is exact, the sequences (3.10) and (3.12) are not, in general, part of short exact sequences. For simplicity, take $m = n$. Then sequence (3.12) becomes

$$0 \longrightarrow \mathbf{Z}_n \longrightarrow \mathbf{Z}_n \xrightarrow{\phi^*} \mathbf{Z}_n \tag{3.15}$$

with $\phi^* = 0$ so that ϕ^* is not surjective, while sequence (3.10) becomes

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \mathbf{Z}) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \mathbf{Z}) \xrightarrow{\psi_*} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \mathbf{Z}_n). \tag{3.16}$$

Since $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \mathbf{Z}) = 0$ and $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \mathbf{Z}_n) \cong \mathbf{Z}_n$, sequence (3.16) becomes

$$0 \longrightarrow 0 \longrightarrow 0 \xrightarrow{\psi_*} \mathbf{Z}_n$$

and ψ_* is certainly not surjective.

These examples show that Theorem 3.10 is the best statement that can be made in complete generality concerning preservation of exactness under application of Hom_R. There is, however, the following criterion for the preservation of short exact sequences under Hom:

(3.12) Theorem. *Let N be an arbitrary R-module. If*

$$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\psi} M_2 \longrightarrow 0 \tag{3.17}$$

is a split short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(N, M_1) \xrightarrow{\phi_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, M_2) \longrightarrow 0 \tag{3.18}$$

and

$$0 \longrightarrow \mathrm{Hom}_R(M_2, N) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, N) \xrightarrow{\phi^*} \mathrm{Hom}_R(M_1, N) \longrightarrow 0 \tag{3.19}$$

are split short exact sequences of abelian groups (R-modules if R is commutative).

Proof. We will prove the split exactness of sequence (3.18); (3.19) is similar and it is left as an exercise. Given Theorem 3.10, it is only necessary to show that ψ_* is surjective and that there is a splitting for sequence (3.18). Let $\beta : M_2 \to M$ split the exact sequence (3.17) and let $f \in \mathrm{Hom}_R(N, M_2)$. Then

$$\begin{aligned} \psi_* \circ \beta_*(f) &= \psi_*(\beta \circ f) \\ &= (\psi \circ \beta) \circ f \\ &= (1_{M_2}) \circ f \\ &= \left(1_{\mathrm{Hom}_R(N,M_2)}\right)(f). \end{aligned}$$

Thus, $\psi_* \circ \beta_* = 1_{\mathrm{Hom}_R(N,M_2)}$ so that ψ_* is surjective and β_* is a splitting of exact sequence (3.18). □

(3.13) Corollary. *Let M_1, M_2, and N be R-modules. Then*

$$\mathrm{Hom}_R(N, M_1 \oplus M_2) \cong \mathrm{Hom}_R(N, M_1) \oplus \mathrm{Hom}_R(N, M_2) \tag{3.20}$$

and

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \cong \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N). \tag{3.21}$$

The isomorphisms are $\mathbf{Z}$-module isomorphisms (R-module isomorphisms if R is commutative).

Proof. Both isomorphisms follow by applying Theorems 3.12 and 3.9 to the split exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\iota} M_1 \oplus M_2 \xrightarrow{\pi} M_2 \longrightarrow 0$$

where $\iota(m) = (m, 0)$ is the canonical injection and $\pi(m_1, m_2) = m_2$ is the canonical projection. □

(3.14) *Remarks.*

(1) Notice that isomorphism (3.20) is given explicitly by

$$\Phi(f) = (\pi_1 \circ f,\, \pi_2 \circ f)$$

where $f \in \mathrm{Hom}_R(N,\, M_1 \oplus M_2)$ and $\pi_i(m_1,\, m_2) = m_i$ (for $i = 1,\, 2$); while isomorphism (3.21) is given explicitly by

$$\Psi(f) = (f \circ \iota_1,\, f \circ \iota_2)$$

where $f \in \mathrm{Hom}_R(M_1 \oplus M_2,\, N)$, $\iota_1 : M_1 \to M_1 \oplus M_2$ is given by $\iota_1(m) = (m,\, 0)$ and $\iota_2 : M_2 \to M_1 \oplus M_2$ is given by $\iota_2(m) = (0,\, m)$.

(2) Corollary 3.13 actually has a natural extension to arbitrary (not necessarily finite) direct sums. We conclude this section by stating this extension. The proof is left as an exercise for the reader.

(3.15) Proposition. *Let $\{M_i\}_{i\in I}$ and $\{N_j\}_{j\in J}$ be indexed families (not necessarily finite) of R-modules, and let $M = \oplus_{i\in I}$, $N = \oplus_{j\in J}$. Then*

$$\mathrm{Hom}_R(M,\, N) \cong \prod_{i\in I}\Big(\bigoplus_{j\in J} \mathrm{Hom}_R(M_i,\, N_j)\Big).$$

Proof. Exercise. □

3.4 Free Modules

(4.1) Definition. *Let R be a ring and let M be an R-module. A subset $S \subseteq M$ is said to be* R**-linearly dependent** *if there exist distinct $x_1,\, \ldots\, , x_n$ in S and elements $a_1,\, \ldots\, , a_n$ of R, not all of which are 0, such that*

$$a_1x_1 + \cdots + a_nx_n = 0.$$

A set that is not R-linearly dependent is said to be R**-linearly independent**.

When the ring R is implicit from the context, we will sometimes write linearly dependent (or just dependent) and linearly independent (or just independent) in place of the more cumbersome R-linearly dependent or R-linearly independent. In case S contains only finitely many elements $x_1, x_2,\, \ldots\, , x_n$, we will sometimes say that $x_1, x_2,\, \ldots\, , x_n$ are R-linearly dependent or R-linearly independent instead of saying that $S = \{x_1,\, \ldots\, , x_n\}$ is R-linearly dependent or R-linearly independent.

(4.2) *Remarks.*

(1) To say that $S \subseteq M$ is R-linearly independent means that whenever there is an equation

$$a_1x_1 + \cdots + a_nx_n = 0$$

where $x_1, \ldots, x_n$ are distinct elements of S and $a_1, \ldots, a_n$ are in R, then

$$a_1 = \cdots = a_n = 0.$$

(2) Any set S that contains a linearly dependent set is linearly dependent.
(3) Any subset of a linearly independent set S is linearly independent.
(4) Any set that contains 0 is linearly dependent since $1 \cdot 0 = 0$.
(5) A set $S \subseteq M$ is linearly independent if and only if every finite subset of S is linearly independent.

(4.3) Definition. *Let M be an R-module. A subset S of M is a* **basis** *of M if S generates M as an R-module and if S is R-linearly independent. That is, $S \subseteq M$ is a basis if and only if $M = \{0\}$, in which case $S = \emptyset$ is a basis, or $M \neq \{0\}$ and*

(1) *every $x \in M$ can be written as*

$$x = a_1x_1 + \cdots + a_nx_n$$

for some $x_1, \ldots, x_n \in S$ and $a_1, \ldots, a_n \in R$, and
(2) *whenever there is an equation*

$$a_1x_1 + \cdots + a_nx_n = 0$$

where $x_1, \ldots, x_n$ are distinct elements of S and $a_1, \ldots, a_n$ are in R, then

$$a_1 = \cdots = a_n = 0.$$

It is clear that conditions (1) and (2) in the definition of basis can be replaced by the single condition:

(1′) $S \subseteq M$ is a basis of $M \neq \{0\}$ if and only if every $x \in M$ can be written *uniquely* as

$$x = a_1x_1 + \cdots + a_nx_n$$

for $a_1, \ldots, a_n \in R$ and $x_1, \ldots, x_n \in S$.

(4.4) Definition. *An R-module M is a* **free R-module** *if it has a basis.*

(4.5) *Remark.* According to Theorem 3.2, to say that $S = \{x_j\}_{j \in J}$ is a basis of M is equivalent to M being the direct sum of the family $\{Rx_j\}_{j \in J}$

of submodules of M, where $\text{Ann}(x_j) = \{0\}$ for all $j \in J$. Moreover, if J is any index set, then $N = \oplus_{j\in J} R_j$, where $R_j = R$ for all $j \in J$, is a free R-module with basis $S = \{e_j\}_{j\in J}$, where $e_j \in N$ is defined by $e_j = (\delta_{jk})_{k\in J}$. Here, δ_{jk} is the kronecker delta function, i.e., $\delta_{jk} = 1 \in R$ whenever $j = k$ and $\delta_{jk} = 0 \in R$ otherwise. N is said to be **free on the index set** J.

(4.6) Examples.

(1) If R is a field then R-linear independence and R-linear dependence in a vector space V over R are the same concepts used in linear algebra.
(2) R^n is a free module with basis $S = \{e_1, \ldots, e_n\}$ where

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

with a 1 in the i^{th} position.
(3) $M_{m,n}(R)$ is a free R-module with basis

$$S = \{E_{ij} : 1 \le i \le m, 1 \le j \le n\}.$$

(4) The ring $R[X]$ is a free R-module with basis $\{X^n : n \in \mathbf{Z}^+\}$. As in Example 4.6 (2), $R[X]$ is also a free $R[X]$-module with basis $\{1\}$.
(5) If G is a finite abelian group then G is a $\mathbf{Z}$-module, but no nonempty subset of G is $\mathbf{Z}$-linearly independent. Indeed, if $g \in G$ then $|G| \cdot g = 0$ but $|G| \neq 0$. Therefore, finite abelian groups can never be free $\mathbf{Z}$-modules, except in the trivial case $G = \{0\}$ when $\emptyset$ is a basis.
(6) If R is a commutative ring and $I \subseteq R$ is an ideal, then I is an R-module. However, if I is not a principal ideal, then I is not free as an R-module. Indeed, no generating set of I can be linearly independent since the equation $(-a_2)a_1 + a_1a_2 = 0$ is valid for any $a_1, a_2 \in R$.
(7) If M_1 and M_2 are free R-modules with bases S_1 and S_2 respectively, then $M_1 \oplus M_2$ is a free R-module with basis $S_1' \cup S_2'$, where

$$S_1' = \{(x, 0) : x \in S_1\} \quad \text{and} \quad S_2' = \{(0, y) : y \in S_2\}.$$

(8) More generally, if $\{M_j\}_{j\in J}$ is a family of free R-modules and $S_j \subseteq M_j$ is a basis of M_j for each $j \in J$, then $M = \oplus_{j\in J} M_j$ is a free R-module and $S = \cup_{j\in J} S_j'$ is a basis of M, where $S_j' \subseteq M$ is defined by

$$S_j' = \{s_{j\alpha}' = (\delta_{jk} s_{j\alpha})_{k\in J} : s_{j\alpha} \in S_j\}.$$

Informally, S_j' consists of all elements of M that contain an element of S_j in the j^{th} component and 0 in all other components. This example incorporates both Example 4.6 (7) and Example 4.6 (2).

Example 4.6 (5) can be generalized to the following fact.

(4.7) Lemma. *Let M be an R-module where R is a commutative ring. Then an element $x \in M$ is R-independent if and only if* $\mathrm{Ann}(x) = \{0\}$. *In particular, an element $a \in R$ is an R-independent subset of the R-module R if and only if a is not a zero divisor.*

Proof. Exercise. □

(4.8) Proposition. *Let R be an integral domain and let M be a free R-module. Then M is torsion-free.*

Proof. Let M have a basis $S = \{x_j\}_{j\in J}$ and let $x \in M_\tau$. Then $ax = 0$ for some $a \neq 0 \in R$. Write $x = \sum_{j\in J} a_j x_j$. Then

$$0 = ax = \sum_{j\in J} (aa_j)x_j.$$

Since S is a basis of M, it follows that $aa_j = 0$ for all $j \in J$, and since $a \neq 0$ and R is an integral domain, we conclude that $a_j = 0$ for all $j \in J$. Therefore, $x = 0$, and hence, $M_\tau = \langle 0 \rangle$ so that M is torsion-free. □

The existence of a basis for an R-module M greatly facilitates the construction of R-module homomorphisms from M to another R-module N. In fact, there is the following important observation.

(4.9) Proposition. *Let M be a free R-module with basis S, let N be any R-module, and let $h : S \to N$ be any function. Then there is a unique $f \in \mathrm{Hom}_R(M, N)$ such that $f|_S = h$.*

Proof. Let $S = \{x_j\}_{j\in J}$. Then any $x \in M$ can be written uniquely as $x = \sum_{j\in J} a_j x_j$ where at most finitely many a_j are not 0. Define $f : M \to N$ by

$$f(x) = \sum_{j\in J} a_j h(x_j).$$

It is straightforward to check that $f \in \mathrm{Hom}_R(M, N)$ and that $f|_S = h$. □

Remark. The content of Proposition 4.9 is usually expressed as saying that the value of a homomorphism can be arbitrarily assigned on a basis.

(4.10) Corollary. *Suppose that M is a free R-module with basis $S = \{x_j\}_{j\in J}$. Then*

$$\mathrm{Hom}_R(M, N) \cong \prod_{j\in J} N_j$$

where $N_j = N$ for all $j \in J$.

Proof. Define $\Phi : \mathrm{Hom}_R(M, N) \to \prod_{j\in J} N_j$ by $\Phi(f) = (f(x_j))_{j\in J}$. Then Φ is an isomorphism of abelian groups (R-modules if R is commutative). □

(4.11) Theorem. *Let R be a commutative ring and let M and N be finitely generated free R-modules. Then $\mathrm{Hom}_R(M, N)$ is a finitely generated free R-module.*

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_m\}$ be a basis of M and $\mathcal{C} = \{w_1, \ldots, w_n\}$ a basis of N. Define $f_{ij} \in \mathrm{Hom}_R(M, N)$ for $1 \le i \le m$ and $1 \le j \le n$ by

$$f_{ij}(v_k) = \begin{cases} w_j & \text{if } k = i, \\ 0 & \text{if } k \neq i. \end{cases}$$

f_{ij} is a uniquely defined element of $\mathrm{Hom}_R(M, N)$ by Proposition 4.9.

We claim that $\{f_{ij} : 1 \le i \le m;\ \ 1 \le j \le n\}$ is a basis of $\mathrm{Hom}_R(M, N)$. To see this suppose that $f \in \mathrm{Hom}_R(M, N)$ and for $1 \le i \le m$ write

$$f(v_i) = a_{i1}w_1 + \cdots + a_{in}w_n.$$

Let

$$g = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_{ij}.$$

Then

$$g(v_k) = a_{k1}w_1 + \cdots + a_{kn}w_n = f(v_k)$$

for $1 \le k \le m$, so $g = f$ since the two homomorphisms agree on a basis of M. Thus, $\{f_{ij} : 1 \le i \le m;\ \ 1 \le j \le n\}$ generates $\mathrm{Hom}_R(M, N)$, and we leave it as an exercise to check that this set is linearly independent and, hence, a basis. □

(4.12) *Remarks.*

(1) A second (essentially equivalent) way to see the same thing is to write $M \cong \oplus_{i=1}^{m} R$ and $N \cong \oplus_{j=1}^{n} R$. Then, Corollary 3.13 shows that

$$\mathrm{Hom}_R(M, N) \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathrm{Hom}_R(R, R).$$

But any $f \in \mathrm{Hom}_R(R, R)$ can be written as $f = f(1) \cdot 1_R$. Thus $\mathrm{Hom}_R(R, R) \cong R$ so that

$$\mathrm{Hom}_R(M, N) \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} R.$$

(2) The hypothesis of finite generation of M and N is crucial for the validity of Theorem 4.11. For example, if $R = \mathbf{Z}$ and $M = \oplus_1^{\infty}\mathbf{Z}$ is the free $\mathbf{Z}$-module on the index set $\mathbf{N}$, then Corollary 4.10 shows that

$$\mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z}) \cong \prod_{1}^{\infty} \mathbf{Z}.$$

But the $\mathbf{Z}$-module $\prod_1^\infty \mathbf{Z}$ is not a free $\mathbf{Z}$-module. (For a proof of this fact (which uses cardinality arguments), see I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, (1968) p. 48.)

(4.13) Proposition. *Let M be a free R-module with basis $S = \{x_j\}_{j\in J}$. If I is an ideal of R, then IM is a submodule of M and the quotient module M/IM is an R/I-module. Let $\pi : M \to M/IM$ be the projection map. Then M/IM is a free R/I-module with basis $\pi(S) = \{\pi(x_j)\}_{j\in J}$.*

Proof. Exercise. □

(4.14) Proposition. *Every R-module M is the quotient of a free module and if M is finitely generated, then M is the quotient of a finitely generated free R-module. In fact, we may take $\mu(F) = \mu(M)$.*

Proof. Let $S = \{x_j\}_{j\in J}$ be a generating set for the R-module M and let $F = \oplus_{j\in J} R_j$ where $R_j = R$ be the free R-module on the index set J. Define the homomorphism $\psi : F \to M$ by

$$\psi((a_j)_{j\in J}) = \sum_{j\in J} a_j x_j.$$

Since S is a generating set for M, ψ is surjective and hence $M \cong F/\operatorname{Ker}(\psi)$. Note that if $|S| < \infty$ then F is finitely generated. (Note that every module has a generating set S since we may take $S = M$.) Since M is a quotient of F, we have $\mu(M) \le \mu(F)$. But F is free on the index set J (Remark 4.5), so $\mu(F) \le |J|$, and since J indexes a generating set of M, it follows that $\mu(F) \le \mu(M)$ if S is a minimal generating set of M. Hence we may take F with $\mu(F) = \mu(M)$. □

(4.15) Definition. *If M is an R-module then a short exact sequence*

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F is a free R-module is called a **free presentation** *of M.*

Thus, Proposition 4.14 states that every module has a free presentation.

(4.16) Proposition. *If F is a free R-module then every short exact sequence*

$$0 \longrightarrow M_1 \longrightarrow M \xrightarrow{f} F \longrightarrow 0$$

of R-modules is split exact.

Proof. Let $S = \{x_j\}_{j\in J}$ be a basis of the free module F. Since f is surjective, for each $j \in J$ there is an element $y_j \in M$ such that $f(y_j) = x_j$. Define $h : S \to M$ by $h(x_j) = y_j$. By Proposition 4.9, there is a unique $\beta \in$

$\mathrm{Hom}_R(F, M)$ such that $\beta|_S = h$. Since $f \circ \beta(x_j) = x_j = 1_F(x_j)$ for all $j \in J$, it follows that $f \circ \beta = 1_F$, and the result follows from Theorem 3.9. □

(4.17) Corollary.

(1) *Let M be an R-module and $N \subseteq M$ a submodule with M/N free. Then $M \cong N \oplus (M/N)$.*
(2) *If M is an R-module and F is a free R-module, then $M \cong \mathrm{Ker}(f) \oplus F$ for every surjective homomorphism $f : M \to F$.*

Proof. (1) Since M/N is free, the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

is split exact by Proposition 4.16 Therefore, $M \cong N \oplus (M/N)$ by Theorem 3.9.

(2) Take $N = \mathrm{Ker}(f)$ in part (1). □

(4.18) Corollary. *Let N be an arbitrary R-module and F a free R-module. If*

$$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\psi} F \longrightarrow 0 \tag{4.1}$$

is a short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(N, M_1) \xrightarrow{\phi_*} \mathrm{Hom}_R(N, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(N, F) \longrightarrow 0$$

is a (split) short exact sequence of abelian groups (R-modules if R is commutative).

Proof. By Proposition 4.16, the sequence (4.1) is split exact, so the corollary follows immediately from Theorem 3.12. □

(4.19) *Remark.* It is a theorem that any two bases of a free module over a commutative ring R have the same cardinality. This result is proved for finite-dimensional vector spaces by showing that any set of vectors of cardinality larger than that of a basis must be linearly dependent. The same procedure works for free modules over any commutative ring R, but it does require the theory of solvability of homogeneous linear equations over a commutative ring. However, the result can be proved for R a PID without the theory of solvability of homogeneous linear equations over R; we prove this result in Section 3.6. The result for general commutative rings then follows by an application of Proposition 4.13.

The question of existence of a basis of a module, that is, to ask if a given module is free, is a delicate question for a general commutative ring R. We have seen examples of $\mathbf{Z}$-modules, namely, finite abelian groups, which

are not free. We will conclude this section with the fact that all modules over division rings, in particular, vector spaces, are free modules. In Section 3.6 we will study in detail the theory of free modules over a PID.

(4.20) Theorem. *Let D be a division ring and let V be a D-module. Then V is a free D-module. In particular, every vector space V has a basis.*

Proof. The proof is an application of Zorn's lemma.

Let S be a generating set for V and let $B_0 \subseteq S$ be *any* linearly independent subset of S (we allow $B_0 = \emptyset$). Let $\mathcal{T}$ be the set of all linearly independent subsets of S containing B_0 and partially order $\mathcal{T}$ by inclusion. If $\{B_i\}$ is a chain in $\mathcal{T}$, then $\cup B_i$ is a linearly independent subset of S that contains B_0; thus, every chain in $\mathcal{T}$ has an upper bound. By Zorn's lemma, there is a maximal element in $\mathcal{T}$, so let B be a maximal linearly independent subset of S containing B_0. We claim that $S \subseteq \langle B \rangle$ so that $V = \langle S \rangle \subseteq \langle B \rangle$. Let $v \in S$. Then the maximality of B implies that $V \cup \{v\}$ is linearly dependent so that there is an equation

$$\sum_{i=1}^{m} a_i v_i + bv = 0$$

where $v_1, \ldots, v_m$ are distinct elements of B and $a_1, \ldots, a_m, b \in D$ are not all 0. If $b = 0$ it would follow that $\sum_{i=1}^{m} a_i v_i = 0$ with not all the scalars $a_i = 0$. But this contradicts the linear independence of B. Therefore, $b \neq 0$ and we conclude

$$v = b^{-1}(bv) = \sum_{i=1}^{m} (-b^{-1}a_i)v_i \in \langle B \rangle.$$

Therefore, $S \subseteq \langle B \rangle$, and as observed above, this implies that B is a basis of V. □

The proof of Theorem 4.20 actually proved more than the existence of a basis of V. Specifically, the following more precise result was proved.

(4.21) Theorem. *Let D be a division ring and let V be a D-module. If S spans V and $B_0 \subseteq S$ is a linearly independent subset, then there is a basis B of V such that $B_0 \subseteq B \subseteq S$.*

Proof. □

(4.22) Corollary. *Let D be a division ring, and let V be a D-module.*

(1) *Any linearly independent subset of V can be extended to a basis of V.*
(2) *A maximal linearly independent subset of V is a basis.*
(3) *A minimal generating set of V is a basis.*

Proof. Exercise. □

Notice that the above proof used the existence of inverses in the division ring D in a crucial way. We will return in Section 3.6 to study criteria that ensure that a module is free if the ring R is assumed to be a PID. Even when R is a PID, e.g., $R = \mathbf{Z}$, we have seen examples of R modules that are not free, so we will still be required to put restrictions on the module M to ensure that it is free.

3.5 Projective Modules

The property of free modules given in Proposition 4.16 is a very useful one, and it is worth investigating the class of those modules that satisfy this condition. Such modules are characterized in the following theorem.

(5.1) Theorem. *The following conditions on an R-module P are equivalent.*

(1) *Every short exact sequence of R-modules*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow P \longrightarrow 0$$

splits.

(2) *There is an R-module P' such that $P \oplus P'$ is a free R-module.*

(3) *For any R-module N and any surjective R-module homomorphism $\psi : M \to P$, the homomorphism*

$$\psi_* : \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N, P)$$

is surjective.

(4) *For any surjective R-module homomorphism $\phi : M \to N$, the homomorphism*

$$\phi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$$

is surjective.

Proof. (1) $\Rightarrow$ (2). Let $0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$ be a free presentation of P. Then this short exact sequence splits so that $F \cong P \oplus K$ by Theorem 3.9.

(2) $\Rightarrow$ (3). Suppose that $F = P \oplus P'$ is free. Given a surjective R-module homomorphism $\psi : M \to P$, let $\psi' = \psi \oplus 1_{P'} : M \oplus P' \to P \oplus P' = F$; this is also a surjective homomorphism, so there is an exact sequence

$$0 \longrightarrow \mathrm{Ker}(\psi') \longrightarrow M \oplus P' \xrightarrow{\psi'} F \longrightarrow 0.$$

Since F is free, Proposition 4.16 implies that this sequence is split exact; Theorem 3.12 then shows that

$$\psi'_* : \mathrm{Hom}_R(N, M \oplus P') \to \mathrm{Hom}_R(N, P \oplus P')$$

is a surjective homomorphism. Now let $f \in \mathrm{Hom}_R(N, P)$ be arbitrary and let $f' = \iota \circ f$, where $\iota : P \to P \oplus P'$ is the inclusion map. Then there is an $\widetilde{f} \in \mathrm{Hom}_R(N, M \oplus P')$ with $\psi'_*(\widetilde{f}) = f'$. Let $\pi : M \oplus P' \to M$ and $\pi' : P \oplus P' \to P$ be the projection maps. Note that $\pi' \circ \iota = 1_P$ and $\psi \circ \pi = \pi' \circ \psi'$. Then

$$\begin{aligned}\psi_*(\pi \circ \widetilde{f}) &= \psi \circ (\pi \circ \widetilde{f}) \\ &= \pi' \circ \psi' \circ \widetilde{f} \\ &= \pi' \circ f' \\ &= (\pi' \circ \iota) \circ f \\ &= f.\end{aligned}$$

Therefore, ψ_* is surjective.

(3) $\Rightarrow$ (4). Let $0 \longrightarrow K \longrightarrow F \xrightarrow{\psi} P \longrightarrow 0$ be a free presentation of P. By property (3), there is a $\beta \in \mathrm{Hom}_R(P, F)$ such that $\psi_*(\beta) = 1_P$, i.e., $\psi \circ \beta = 1_P$. Let $\phi : M \to N$ be any surjective R-module homomorphism and let $f \in \mathrm{Hom}_R(P, N)$. Then there is a commutative diagram of R-module homomorphisms

$$\begin{array}{ccccc} F & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow f & & \\ M & \xrightarrow{\phi} & N & \longrightarrow & 0 \end{array}$$

with exact rows. Let $S = \{x_j\}_{j \in J}$ be a basis of F. Since ϕ is surjective, we may choose $y_j \in M$ such that $\phi(y_j) = f \circ \psi(x_j)$ for all $j \in J$. By Proposition 4.9, there is an R-module homomorphism $g : F \to M$ such that $g(x_j) = y_j$ for all $j \in J$. Since $\phi \circ g(x_j) = \phi(y_j) = f \circ \psi(x_j)$, it follows that $\phi \circ g = f \circ \psi$. Define $\widetilde{f} \in \mathrm{Hom}_R(P, M)$ by $\widetilde{f} = g \circ \beta$ and observe that

$$\begin{aligned}\phi_*(\widetilde{f}) &= \phi \circ (g \circ \beta) \\ &= f \circ \psi \circ \beta \\ &= f \circ 1_P \\ &= f.\end{aligned}$$

Hence, $\phi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is surjective.

(4) $\Rightarrow$ (1). A short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \xrightarrow{\psi} P \longrightarrow 0,$$

in particular, includes a surjection $\psi : M \to P$. Now take $N = P$ in part (4). Thus,

$$\psi_* : \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, P)$$

is surjective. Choose $\beta : P \to M$ with $\psi_*(\beta) = 1_P$. Then β splits the short exact sequence and the result is proved. □

(5.2) Definition. *An R-module P satisfying any of the equivalent conditions of Theorem 5.1 is called* **projective**.

As noted before Theorem 5.1, projective modules are introduced as the class of modules possessing the property that free modules were shown to possess in Proposition 4.16. Therefore, we have the following fact:

(5.3) Proposition. *Free R-modules are projective.*

Proof. □

(5.4) Corollary. *Let R be an integral domain. If P is a projective R-module, then P is torsion-free.*

Proof. By Theorem 5.1 (2), P is a submodule of a free module F over R. According to Proposition 4.8, every free module over an integral domain is torsion-free, and every submodule of a torsion-free module is torsion-free. □

(5.5) Corollary. *An R-module P is a finitely generated projective R-module if and only if P is a direct summand of a finitely generated free R-module.*

Proof. Suppose that P is finitely generated and projective. By Proposition 4.14, there is a free presentation

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$$

such that F is free and $\mu(F) = \mu(P) < \infty$. By Theorem 5.1, P is a direct summand of F.

Conversely, assume that P is a direct summand of a finitely generated free R-module F. Then P is projective, and moreover, if $P \oplus P' \cong F$ then $F/P' \cong P$ so that P is finitely generated. □

(5.6) Examples.

(1) Every free module is projective.
(2) Suppose that m and n are relatively prime natural numbers. Then as abelian groups $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \oplus \mathbf{Z}_n$. It is easy to check that this isomorphism is also an isomorphism of $\mathbf{Z}_{mn}$-modules. Therefore, $\mathbf{Z}_m$ is a direct summand of a free $\mathbf{Z}_{mn}$-module, and hence it is a projective $\mathbf{Z}_{mn}$-module. However, $\mathbf{Z}_m$ is not a free $\mathbf{Z}_{mn}$ module since it has fewer than mn elements.
(3) Example 5.6 (2) shows that projective modules need not be free. We will present another example of this phenomenon in which the ring R is an integral domain so that simple cardinality arguments do not suffice. Let $R = \mathbf{Z}[\sqrt{-5}]$ and let I be the ideal $I = \langle 2, 1 + \sqrt{-5} \rangle = \langle a_1, a_2 \rangle$. It is easily shown that I is not a principal ideal, and hence by Example 4.6 (6), we see that I cannot be free as an R-module. We claim that I

is a projective R-module. To see this, let $b = 1 - \sqrt{-5} \in R$, let F be a free R-module with basis $\{s_1, s_2\}$, and let $\phi : F \to I$ be the R-module homomorphism defined by

$$\phi(r_1 s_1 + r_2 s_2) = r_1 a_1 + r_2 a_2.$$

Now define an R-module homomorphism $\alpha : I \to F$ by

$$\alpha(a) = -a s_1 + ((ab)/2) s_2.$$

Note that this makes sense because 2 divides ab for every $a \in I$. Now for $a \in I$,

$$\begin{aligned} \phi \circ \alpha(a) &= \phi(-a s_1 + ((ab)/2) s_2) \\ &= -a a_1 + ((ab)/2) a_2 \\ &= -a a_1 + a a_2 b/2 \\ &= -2a + 3a \\ &= a \end{aligned}$$

so that α is a splitting of the surjective map ϕ. Hence, $F \cong \mathrm{Ker}(\phi) \oplus I$ and by Theorem 5.1, I is a projective R-module.

Concerning the construction of new projective modules from old ones, there are the following two simple facts:

(5.7) Proposition. *Let $\{P_j\}_{j \in J}$ be a family of R-modules, and let $P = \oplus_{j \in J} P_j$. Then P is projective if and only if P_j is projective for each $j \in J$.*

Proof. Suppose that P is projective. Then by Theorem 5.1, there is an R-module P' such that $P \oplus P' = F$ is a free R-module. Then

$$F = P \oplus P' = \Big(\bigoplus_{j \in J} P_j \Big) \oplus P',$$

and hence, each P_j is also a direct summand of the free R-module F. Thus, P_j is projective.

Conversely, suppose that P_j is projective for every $j \in J$ and let P'_j be an R-module such that $P_j \oplus P'_j = F_j$ is free. Then

$$\begin{aligned} P \oplus \Big(\bigoplus_{j \in J} P'_j \Big) &\cong \bigoplus_{j \in J} (P_j \oplus P'_j) \\ &\cong \bigoplus_{j \in J} F_j. \end{aligned}$$

Since the direct sum of free modules is free (Example 4.6 (8)), it follows that P is a direct summand of a free module, and hence P is projective. □

(5.8) Proposition. *Let R be a commutative ring and let P and Q be finitely generated projective R-modules. Then* $\mathrm{Hom}_R(P, Q)$ *is a finitely generated projective R-module.*

Proof. Since P and Q are finitely generated projective R-modules, there are R-modules P' and Q' such that $P \oplus P'$ and $Q \oplus Q'$ are finitely generated free modules. Therefore, by Theorem 4.11, $\mathrm{Hom}_R(P \oplus P', Q \oplus Q')$ is a finitely generated free R-module. But

$$\begin{aligned}\mathrm{Hom}_R(P \oplus P', Q \oplus Q') \cong &\mathrm{Hom}_R(P, Q) \oplus \mathrm{Hom}_R(P, Q') \\ &\oplus \mathrm{Hom}_R(P', Q) \oplus \mathrm{Hom}_R(P', Q')\end{aligned}$$

so that $\mathrm{Hom}_R(P, Q)$ is a direct summand of a finitely generated free R-module, and therefore, it is projective and finitely generated by Corollary 5.5. □

Example 5.6 (3) was an example of an ideal in a ring R that was projective as an R-module, but not free. According to Example 4.6 (6), an ideal I in a ring R is free as an R-module if and only if the ideal is principal. It is a natural question to ask which ideals in a ring R are projective as R-modules. Since this turns out to be an important question in number theory, we will conclude our brief introduction to the theory of projective modules by answering this question for integral domains R.

(5.9) Definition. *Let R be an integral domain and let K be the quotient field of R. An ideal $I \subseteq R$ is said to be* **invertible** *if there are elements $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in K$ such that*

(5.1) $b_i I \subseteq R$ *for* $1 \leq i \leq n$, *and*
(5.2) $a_1 b_1 + \cdots + a_n b_n = 1$.

(5.10) Examples.

(1) If $I \subseteq R$ is the principal ideal $I = \langle a \rangle$ where $a \neq 0$, then I is an invertible ideal. Indeed, let $b = 1/a \in K$. Then any $x \in I$ is divisible by a in R so that $bx = (1/a)x \in R$, while $a(1/a) = 1$.
(2) Let $R = \mathbf{Z}[\sqrt{-5}]$ and let $I = \langle 2, 1 + \sqrt{-5} \rangle$. Then it is easily checked that I is not principal, but I is an invertible ideal. To see this, let $a_1 = 2$, $a_2 = 1 + \sqrt{-5}$, $b_1 = -1$, and $b_2 = (1 - \sqrt{-5})/2$. Then

$$a_1 b_1 + a_2 b_2 = -2 + 3 = 1.$$

Furthermore, $a_1 b_2$ and $a_2 b_2$ are in R, so it follows that $b_2 I \subseteq R$, and we conclude that I is an invertible ideal.

The following result characterizes which ideals in an integral domain R are projective modules. Note that the theorem is a generalization of Example 5.6 (3):

(5.11) Theorem. *Let R be an integral domain and let $I \subseteq R$ be an ideal. Then I is a projective R-module if and only if I is an invertible ideal.*

Proof. Suppose that I is invertible and choose $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n$ in the quotient field K of R so that Equations (5.1) and (5.2) are satisfied. Let $\phi : R^n \to I$ be defined by

$$\phi(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n,$$

and define $\beta : I \to R^n$ by

$$\beta(a) = (ab_1, \ldots, ab_n).$$

Note that $ab_i \in R$ for all i by Equation (5.1). Equation (5.2) shows that

$$\phi \circ \beta(a) = \sum_{i=1}^{n} a_i(ab_i) = a\left(\sum_{i=1}^{n} a_ib_i\right) = a$$

for every $a \in I$. Therefore $\phi \circ \beta = 1_P$ and Theorem 3.9 implies that I is a direct summand of the free R-module R^n, so I is a projective R-module.

Conversely, assume that the ideal $I \subseteq R$ is projective as an R-module. Then I is a direct summand of a free R-module F, so there are R-module homomorphisms $\phi : F \to I$ and $\beta : I \to F$ such that $\phi \circ \beta = 1_I$. Let $S = \{x_j\}_{j \in J}$ be a basis of F. Given $x \in I$, $\beta(x) \in F$ can be written uniquely as

$$\beta(x) = \sum_{j \in J} c_jx_j. \tag{5.3}$$

For each $j \in J$, let $\psi_j(x) = c_j$. This gives a function $\psi_j : I \to R$, which is easily checked to be an R-module homomorphism. If $a_j = \phi(x_j) \in I$, note that

(5.4) for each $x \in I$, $\psi_j(x) = 0$ except for at most finitely many $j \in J$;
(5.5) for each $x \in I$, Equation (5.3) shows that

$$x = \phi(\beta(x)) = \sum_{j \in J} \psi_j(x)a_j.$$

Given $x \neq 0 \in I$ and $j \in J$, define $b_j \in K$ (K is the quotient field of R) by

$$b_j = \frac{\psi_j(x)}{x}. \tag{5.6}$$

The element $b_j \in K$ depends on $j \in J$ but not on the element $x \neq 0 \in I$. To see this, suppose that $x' \neq 0 \in I$ is another element of I. Then

$$x'\psi_j(x) = \psi_j(x'x) = \psi_j(xx') = x\psi_j(x')$$

so that $\psi_j(x)/x = \psi_j(x')/x'$. Therefore, for each $j \in J$ we get a uniquely defined $b_j \in K$. By property (5.4), at most finitely many of the b_j are not 0. Label the nonzero b_j by $b_1, \ldots, b_n$. By property (5.5), if $x \neq 0 \in I$ then

$$x = \sum_{j=1}^{n} \psi_j(x) a_j = \sum_{j=1}^{n} (b_j x) a_j = x \left(\sum_{j=1}^{n} b_j a_j \right).$$

Cancelling $x \neq 0$ from this equation gives

$$a_1 b_1 + \cdots + a_n b_n = 1$$

where $a_1, \ldots, a_n \in I$ and $b_1 \cdots, b_n \in K$. It remains to check that $b_j I \subseteq R$ for $1 \leq j \leq n$. But if $x \neq 0 \in I$ then $b_j = \psi_j(x)/x$ so that $b_j x = \psi_j(x) \in R$. Therefore, I is an invertible ideal and the theorem is proved. □

(5.12) *Remark.* Integral domains in which every ideal is invertible are known as **Dedekind domains**, and they are important in number theory. For example, the ring of integers in any algebraic number field is a Dedekind domain.

3.6 Free Modules over a PID

In this section we will continue the study of free modules started in Section 3.4, with special emphasis upon theorems relating to conditions which ensure that a module over a PID R is free. As examples of the types of theorems to be considered, we will prove that all submodules of a free R-module are free and all finitely generated torsion-free R-modules are free, provided that the ring R is a PID. Both of these results are false without the assumption that R is a PID, as one can see very easily by considering an integral domain R that is not a PID, e.g., $R = \mathbf{Z}[X]$, and an ideal $I \subseteq R$ that is not principal, e.g., $\langle 2, X \rangle \subseteq \mathbf{Z}[X]$. Then I is a torsion-free submodule of R that is not free (see Example 4.6 (6)).

Our analysis of free modules over PIDs will also include an analysis of which elements in a free module M can be included in a basis and a criterion for when a linearly independent subset can be included in a basis. Again, these are basic results in the theory of finite-dimensional vector spaces, but the case of free modules over a PID provides extra subtleties that must be carefully analyzed.

We will conclude our treatment of free modules over PIDs with a fundamental result known as the invariant factor theorem for finite rank submodules of free modules over a PID R. This result is a far-reaching generalization of the freeness of submodules of free modules, and it is the basis

for the fundamental structure theorem for finitely generated modules over PIDs which will be developed in Section 3.7.

We start with the following definition:

(6.1) Definition. *Let M be a free R-module. Then the* **free rank** *of M, denoted* free-rank$_R(M)$*, is the minimal cardinality of a basis of M.*

Since we will not be concerned with the fine points of cardinal arithmetic, we shall not distinguish among infinite cardinals so that

$$\text{free-rank}_R(M) \in \mathbf{Z}^+ \cup \{\infty\}.$$

Since a basis is a generating set of M, we have the inequality $\mu(M) \leq$ free-rank$_R(M)$. We will see in Corollary 6.18 that for an arbitrary commutative ring R and for every free R-module, free-rank$_R(M) = \mu(M)$ and all bases of M have this cardinality.

(6.2) Theorem. *Let R be a* PID*, and let M be a free R-module. If $N \subseteq M$ is a submodule, then N is a free R-module, and*

$$\text{free-rank}_R(N) \leq \text{free-rank}_R(M).$$

Proof. Since $\langle 0 \rangle$ is free with basis $\emptyset$, we may assume that $N \neq \langle 0 \rangle$. Let $S = \{x_j\}_{j \in J}$ be a basis of M. For any subset $K \subseteq J$ let $M_K = \langle \{x_k\}_{k \in K} \rangle$ and let $N_K = N \cap M_K$. Let $\mathcal{T}$ be the set of all triples (K, K', f) where $K' \subseteq K \subseteq J$ and $f : K' \to N_K$ is a function such that $\{f(k)\}_{k \in K'}$ is a basis of N_K.

Claim. $\mathcal{T} \neq \emptyset$.

Since $N \neq \langle 0 \rangle$ there is an $x \neq 0 \in N$, so we may write $x = a_1 x_{j_1} + \cdots + a_k x_{j_k}$. Hence $x \in N_K$ where $K = \{j_1, \ldots, j_k\}$. Thus, there are finite subsets $K \subseteq J$ such that $N_K \neq \langle 0 \rangle$. Choose a finite set

$$K = \{j_1, \ldots, j_k\} \subseteq J$$

such that $N_K \neq \langle 0 \rangle$, but $N_{K'} = \langle 0 \rangle$ for all sets $K' \subseteq J$ with $|K'| < k$. Choose any nonzero $x \in N_K$ and write

$$x = a_1 x_{j_1} + \cdots + a_k x_{j_k}.$$

Let $d = \gcd\{a_1, \ldots, a_k\}$, and if $a_i = db_i$, let

$$x' = b_1 x_{j_1} + \cdots + b_k x_{j_k}.$$

Now consider $I = \{a \in R : ax' \in N\}$. Then I is an ideal, so $I = \langle a \rangle$ since R is a PID. Let $y = ax'$. We claim that $N_K = \langle y \rangle$ so that $\{y\}$ will be a basis of N_K. Let $z \neq 0 \in N_K$ be arbitrary. Then

$$z = c_1 x_{j_1} + \cdots + c_k x_{j_k}$$

and $c_i \neq 0$ since otherwise a linear combination of fewer than k elements of the basis S will be in N, which contradicts the choice of K. Since

$$ab_1 z - c_1 y = 0 \cdot x_{j_1} + \cdots + \alpha_k x_{j_k},$$

it follows that $ab_1 z - c_1 y \in N_K$ is a linear combination of fewer than k elements of the basis S, and hence we must have $ab_1 z - c_1 y = 0$. Dividing by a gives $b_1 z = c_1 x'$ so that $b_1 c_j = c_1 b_j$ for $1 \leq j \leq k$. But $\gcd\{b_1, \ldots, b_k\} = 1$, so we conclude that b_1 divides c_1, and hence $z = \widetilde{c}_1 x'$. From the definition of the ideal I, we conclude that a divides $\widetilde{c}_1$, i.e.,

$$z = c_1' a x' = c_1' y.$$

Therefore, we have shown that $\{y\}$ is a basis of N_K. Let $K' = \{j_1\}$ and define $f : K' \to N$ by $f(j_1) = y$. Then $(K, K', f) \in \mathcal{T}$ so that $\mathcal{T} \neq \emptyset$, as claimed.

Now define a partial order on $\mathcal{T}$ by setting $(K, K', f) \leq (L, L', g)$ if $K \subseteq L$, $K' \subseteq L'$, and $g|_{K'} = f$. If $\{(K_\alpha, K'_\alpha, f_\alpha)\}_{\alpha \in A} \subseteq \mathcal{T}$ is a chain, then $\left(\bigcup_{\alpha \in A} K_\alpha, \bigcup_{\alpha \in A} K_\alpha, F\right)$ where $F|_{K'_\alpha} = f_\alpha$ is an upper bound in $\mathcal{T}$ for the chain. Therefore, Zorn's lemma applies and there is a maximal element (K, K', f) of $\mathcal{T}$.

Claim. $K = J$.

Assuming the claim is true, it follows that $M_K = M$, $N_K = N \cap M_K = N$, and $\{f(k)\}_{k \in K'}$ is a basis of N. Thus, N is a free module (since it has a basis), and since S was an arbitrary basis of M, we conclude that N has a basis of cardinality $\leq \text{free-rank}_R(M)$, which is what we wished to prove.

It remains to verify the claim. Suppose that $K \neq J$ and choose $j \in J \setminus K$. Let $L = K \cup \{j\}$. If $N_K = N_L$ then $(K, K', f) \lneq (L, K', f)$, contradicting the maximality of (K, K', f) in $\mathcal{T}$. If

$$N_K \neq N_L = (M_K + \langle x_j \rangle) \cap N,$$

let

$$I = \{a \in R : ax_j + v \in N \text{ for some } v \in M_K\}.$$

I is an ideal of R and, since $N_K \neq N_L$, we must have $I \neq \langle 0 \rangle$. But R is a PID, so $I = \langle a \rangle$ for some $a \neq 0 \in R$. Thus there is a $w \in M_K$ such that $z = ax_j + w \in N$. Now let $L' = K' \cup \{j\}$ and define $f' : L' \to N_L$ by

$$f'(k) = \begin{cases} f(k) & \text{if } k \in K', \\ z & \text{if } k = j. \end{cases}$$

We need to show that $\{f'(k)\}_{k \in L'}$ is a basis of N_L. But if $x \in N_L$ then $x = bx_j + v$ for some $v \in M_K$. Thus, $b \in I$, so $b = ac$ for some $c \in R$, and hence,

$$x = acx_j + v = c(ax_j) + v = cz + (v - cw).$$

But $x - cz = v - cw \in M_K \cap N = N_K$ so that

$$x - cz = \sum_{k \in K'} b_k f(k)$$

where $b_k \in R$. Thus, $\{f(k)\}_{k \in L'}$ generates N_L.

Now suppose $\sum_{k \in L'} b_k f'(k) = 0$. Then

$$b_j z + \sum_{k \in K'} b_k f(k) = 0$$

so that

$$ab_j x_j + b_j w + \sum_{k \in K'} b_k f(k) = 0.$$

That is, $ab_j x_j \in M_K \cap \langle x_j \rangle = \langle 0 \rangle$, and since $S = \{x_\ell\}_{\ell \in J}$ is a basis of M, we must have $ab_j = 0$.

But $a \neq 0$, so $b_j = 0$. This implies that $\sum_{k \in K'} b_k f(k) = 0$. But $\{f(k)\}_{k \in K'}$ is a basis of N_K, so we must have $b_k = 0$ for all $k \in K'$. Thus $\{f'(k)\}_{k \in L'}$ is a basis of N_L. We conclude that $(K, K', f) \subsetneqq (L, L', f')$, which contradicts the maximality of (K, K', f). Therefore, the claim is verified, and the proof of the theorem is complete. □

(6.3) Corollary. *Let R be a* PID *and let P be a projective R-module. Then P is free.*

Proof. By Proposition 4.14, P has a free presentation

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0.$$

Since P is projective, this exact sequence splits and hence $F \cong P \oplus K$. Therefore, P is isomorphic to a submodule of F, and Theorem 6.2 then shows that P is free. □

(6.4) Corollary. *Let M be a finitely generated module over the* PID *R and let $N \subseteq M$ be a submodule. Then N is finitely generated and*

$$\mu(N) \leq \mu(M).$$

Proof. Let

$$0 \longrightarrow K \longrightarrow F \xrightarrow{\phi} M \longrightarrow 0$$

be a free presentation of M such that free-rank$(F) = \mu(M) < \infty$, and let $N_1 = \phi^{-1}(N)$. By Theorem 6.2, N_1 is free with

$$\mu(N_1) \leq \text{free-rank}(N_1) \leq \text{free-rank}(F) = \mu(M).$$

Since $N = \phi(N_1)$, we have $\mu(N) \leq \mu(N_1)$, and the result is proved. □

(6.5) *Remark.* The hypothesis that R be a PID in Theorem 6.2 and Corollaries 6.3 and 6.4 is crucial. For example, consider the ring $R = \mathbf{Z}[X]$ and let $M = R$ and $N = \langle 2, X\rangle$. Then M is a free R-module and N is a submodule of M that is not free (Example 4.6 (6)). Moreover, $R = \mathbf{Z}[\sqrt{-5}]$, $P = \langle 2, 1 + \sqrt{-5}\rangle$ gives an example of a projective R-module P that is not free (Example 5.6 (3)). Also note that $2 = \mu(N) > \mu(M) = 1$ and $2 = \mu(P) > 1 = \mu(R)$.

Recall that if M is a free module over an integral domain R, then M is torsion-free (Proposition 4.8). The converse of this statement is false even under the restriction that R be a PID. As an example, consider the $\mathbf{Z}$-module $\mathbf{Q}$. It is clear that $\mathbf{Q}$ is a torsion-free $\mathbf{Z}$-module, and it is a simple exercise to show that it is not free. There is, however, a converse if the module is assumed to be finitely generated (and the ring R is a PID).

(6.6) Theorem. *If R is a* PID *and M is a finitely generated torsion-free R-module, then M is free and*

$$\text{free-rank}_R(M) = \mu(M).$$

Proof. The proof is by induction on $\mu(M)$. If $\mu(M) = 1$ then M is cyclic with generator $\{x\}$. Since M is torsion-free, $\text{Ann}(x) = \{0\}$, so the set $\{x\}$ is linearly independent and, hence, is a basis of M.

Now suppose that $\mu(M) = k > 0$ and assume that the result is true for all finitely generated torsion-free R-modules M' with $\mu(M') < k$. Let $\{x_1, \ldots, x_k\}$ be a minimal generating set for M, and let

$$M_1 = \{x \in M : ax \in \langle x_1\rangle \qquad \text{for some } a \neq 0 \in R\}.$$

Then M/M_1 is generated by $\{x_2 + M_1, \ldots, x_k + M_1\}$ so that $\mu(M/M_1) = j \leq k - 1$. If $ax \in M_1$ for some $a \neq 0 \in R$, then from the definition of M_1, $b(ax) \in \langle x_1\rangle$ for some $b \neq 0$. Hence $x \in M_1$ and we conclude that M/M_1 is torsion-free. By the induction hypothesis, M/M_1 is free of free-rank j. Then Corollary 4.17 shows that $M \cong M_1 \oplus (M/M_1)$. We will show that M_1 is free of free-rank 1. It will then follow that

$$k = \mu(M) \leq \mu(M_1) + \mu(M/M_1) = 1 + j,$$

and since $j \leq k-1$, it will follow that $j = k-1$ and M is free of free-rank $= k$.

It remains to show that M_1 is free of rank 1. Note that if R is a field then $M_1 = R \cdot x_1$ and we are done. In the general case, M_1 is a submodule of M, so it is finitely generated by $\ell \leq k$ elements. Let $\{y_1, \ldots, y_\ell\}$ be a generating set for M_1 and suppose that $a_i y_i = b_i x_1$ with $a_i \neq 0$ for $1 \leq i \leq \ell$. Let $q_0 = a_1 \cdots a_\ell$.

Claim. *If $ax = bx_1$ with $a \neq 0$ then $a \mid bq_0$.*

To see this note that $x = \sum_{i=1}^{\ell} c_i y_i$ so that

$$\begin{aligned} q_0 x &= \sum_{i=1}^{\ell} c_i q_0 y_i \\ &= \sum_{i=1}^{\ell} c_i (q_0/a_i) a_i y_i \\ &= \sum_{i=1}^{\ell} c_i (q_0/a_i) b_i x_1 \\ &= \left(\sum_{i=1}^{\ell} c_i (q_0/a_i) b_i \right) x_1. \end{aligned}$$

Therefore.

$$bq_0 x_1 = aq_0 x = a \left(\sum_{i=1}^{\ell} c_i (q_0/a_i) b_i \right) x_1.$$

Since M_1 is torsion-free, it follows that

$$bq_0 = a \left(\sum_{i=1}^{\ell} c_i (q_0/a_i) b_i \right),$$

and the claim is proved.

Using this claim we can define a function $\phi : M_1 \to R$ by $\phi(x) = (bq_0)/a$ whenever $ax = bx_1$ for $a \neq 0$. We must show that ϕ is well defined. That is, if $ax = bx_1$ and $a'x = b'x$, then $(bq_0)/a = (b'q_0)/a'$. But $ax = bx_1$ and $a'x = b'x_1$ implies that $a'bx_1 = a'ax = ab'x_1$ so that $a'b = ab'$ because M is torsion-free. Thus $a'bq_0 = ab'q_0$ so that $(bq_0)/a = (b'q_0)/a'$ and ϕ is well defined. Furthermore, it is easy to see that ϕ is an R-module homomorphism so that $\mathrm{Im}(\phi)$ is an R-submodule of R, i.e., an ideal. Suppose that $\phi(x) = 0$. Then $ax = bx_1$ with $a \neq 0$ and $\phi(x) = (bq_0)/a = 0 \in R$. Since R is an integral domain, it follows that $b = 0$ and hence $ax = 0$. Since M is torsion-free we conclude that $x = 0$. Therefore, $\mathrm{Ker}(\phi) = \{0\}$ and

$$M_1 \cong \mathrm{Im}(\phi) = Rc.$$

Hence, M_1 is free of rank 1, and the proof is complete. □

(6.7) Corollary. *If M is a finitely generated module over a field F, then M is free.*

Proof. Every module over a field is torsion-free (Proposition 2.20). □

(6.8) *Remark.* We have already given an independent proof (based on Zorn's lemma) for Corollary 6.7, even without the finitely generated assumption (Theorem 4.20). We have included Corollary 6.7 here as an observation that

it follows as a special case of the general theory developed for torsion-free finitely generated modules over a PID.

(6.9) Corollary. *If M is a finitely generated module over a* PID *R, then $M \cong M_\tau \oplus (M/M_\tau)$.*

Proof. There is an exact sequence of R-modules

$$0 \longrightarrow M_\tau \longrightarrow M \longrightarrow M/M_\tau \longrightarrow 0.$$

Hence, M/M_τ is finitely generated and by Proposition 2.18, it is torsion-free, so Theorem 6.6 shows that M/M_τ is free. Then Corollary 4.17 shows that $M \cong M_\tau \oplus (M/M_\tau)$. □

The main point of Corollary 6.9 is that any finitely generated module over a PID can be written as a direct sum of its torsion submodule and a free submodule. Thus an analysis of these modules is reduced to studying the torsion submodule, once we have completed our analysis of free modules. We will now continue the analysis of free modules over a PID R by studying when an element in a free module can be included in a basis. As a corollary of this result we will be able to show that any two bases of a finitely generated free R-module (R a PID) have the same number of elements.

(6.10) Example. Let R be a PID and view R as an R-module. Then an element $a \in R$ forms a basis of R if and only if a is a unit. Thus if R is a field, then every nonzero element is a basis of the R-module R, while if $R = \mathbf{Z}$ then the only elements of $\mathbf{Z}$ that form a basis of $\mathbf{Z}$ are 1 and -1. As a somewhat more substantial example, consider the $\mathbf{Z}$-module $\mathbf{Z}^2$. Then the element $u = (2, 0) \in \mathbf{Z}^2$ cannot be extended to a basis of $\mathbf{Z}^2$ since if v is any element of $\mathbf{Z}^2$ with $\{u, v\}$ linearly independent, the equation

$$\alpha u + \beta v = (1, 0)$$

is easily seen to have no solution $\alpha, \beta \in \mathbf{Z}$. Therefore, some restriction on elements of an R-module that can be included in a basis is necessary. The above examples suggest the following definition.

(6.11) Definition. *Let M be an R-module. A torsion-free element $x \neq 0 \in M$ is said to be* **primitive** *if $x = ay$ for some $y \in M$ and $a \in R$ implies that a is a unit of R.*

(6.12) *Remarks.*

(1) If R is a field, then *every* nonzero $x \in M$ is primitive.
(2) The element $x \in R$ is a primitive element of the R-module R if and only if x is a unit.

(3) The element $(2, 0) \in \mathbf{Z}^2$ is not primitive since $(2, 0) = 2 \cdot (1, 0)$.
(4) If $R = \mathbf{Z}$ and $M = \mathbf{Q}$, then *no* element of M is primitive.

(6.13) Lemma. *Let R be a* PID *and let M be a free R-module with basis $S = \{x_j\}_{j\in J}$. If $x = \sum_{j\in J} a_j x_j \in M$, then x is primitive if and only if* $\gcd(\{a_j\}_{j\in J}) = 1$.

Proof. Let $d = \gcd(\{a_j\}_{j\in J})$. Then $x = d(\sum_{j\in J}(a_j/d)x_j)$, so if d is not a unit then x is not primitive. Conversely, if $d = 1$ and $x = ay$ then

$$\begin{aligned}\sum_{j\in J} a_j x_j &= x \\ &= ay \\ &= a\Big(\sum_{j\in J} b_j x_j\Big) \\ &= \sum_{j\in J} ab_j x_j.\end{aligned}$$

Since $S = \{x_j\}_{j\in J}$ is a basis, it follows that $a_j = ab_j$ for all $j \in J$. That is, a is a common divisor of the set $\{a_j\}_{j\in J}$ so that $a \mid d = 1$. Hence a is a unit and x is primitive. □

(6.14) Lemma. *Let R be a* PID *and let M be a finitely generated R-module. If $x \in M$ has $\mathrm{Ann}(x) = \langle 0\rangle$, then we may write $x = ax'$ where $a \in R$ and x' is primitive. (In particular, if M is not a torsion module, then M has a primitive element.)*

Proof. Let $x_0 = x$. If x_0 is primitive we are done. Otherwise, write $x_0 = a_1 x_1$ where $a_1 \in R$ is not a unit. Then $\langle x_0\rangle \subsetneqq \langle x_1\rangle$. To see this, it is certainly true that $\langle x_0\rangle \subseteq \langle x_1\rangle$. If the two submodules are equal then we may write $x_1 = bx_0$ so that $x_0 = a_1x_1 = a_1bx_0$, i.e., $(1 - a_1b) \in \mathrm{Ann}(x_0) = \langle 0\rangle$. Therefore, $1 = a_1b$ and a_1 is a unit, which contradicts the choice of a_1.

Now consider x_1. If x_1 is primitive, we are done. Otherwise, $x_1 = a_2x_2$ where a_2 is not a unit, and as above we conclude that $\langle x_1\rangle \subsetneqq \langle x_2\rangle$. Continuing in this way we obtain a chain of submodules

$$\langle x_0\rangle \subsetneqq \langle x_1\rangle \subsetneqq \langle x_2\rangle \subsetneqq \cdots. \tag{6.1}$$

Either this chain stops at some i, which means that x_i is primitive, or (6.1) is an infinite properly ascending chain of submodules of M. We claim that the latter possibility cannot occur. To see this, let $N = \bigcup_{i=1}^{\infty}\langle x_i\rangle$. Then N is a submodule of the finitely generated module M over the PID R so that N is also finitely generated by $\{y_1, \ldots, y_k\}$ (Corollary 6.5). Since $\langle x_0\rangle \subseteq \langle x_1\rangle \subseteq \cdots$, there is an i such that $\{y_1, \ldots, y_k\} \subseteq \langle x_i\rangle$. Thus $N = \langle x_i\rangle$ and hence $\langle x_i\rangle = \langle x_{i+1}\rangle = \cdots$, which contradicts having an infinite properly

ascending chain. Therefore, x_i is primitive for some i, and if we let $x' = x_i$ we conclude that $x = ax'$ where $a = a_1 a_2 \cdots a_i$. □

(6.15) *Remark.* Suppose that M is a free R-module, where R is a PID, and $x \in M$. Then $\mathrm{Ann}(x) = \langle 0 \rangle$, so $x = ax'$ where x' is a primitive element of M. If $S = \{x_j\}_{j \in J}$ is a basis of M, then we may write $x' = \sum_{j \in J} b_j x_j$ so that

$$x = ax' = \sum_{j \in J} a b_j x_j = \sum_{j \in J} c_j x_j.$$

Since $\gcd(\{b_j\}_{j \in J}) = 1$ (by Lemma 6.13) we see that $a = \gcd(\{c_j\}_{j \in J})$. The element $a \in R$, which is uniquely determined by x up to multiplication by a unit of R, is called the **content** of $x \in M$ and is denoted $c(x)$. (Compare with the concept of content of polynomials (Definition 2.6.3).) Thus, any $x \in M$ can be written

$$x = c(x) \cdot x' \tag{6.2}$$

where x' is primitive.

(6.16) Theorem. *Let R be a* PID *and let M be a free R-module with*

$$\mathrm{rank}(M) = k = \mu(M) = \text{free-rank}(M).$$

If $x \in M$ is primitive, then M has a basis of k elements containing x.

Proof. Assume first that $k < \infty$ and proceed by induction on k. Suppose $k = 1$ and let M have a basis $\{x_1\}$. Then $x = ax_1$ for some $a \in R$. Since x is primitive, it follows that a is a unit so that $\langle x \rangle = \langle x_1 \rangle = M$, hence $\{x\}$ is a basis of M.

The case $k = 2$ will be needed in the general induction step, so we present it separately. Thus suppose that M has a basis $\{x_1, x_2\}$ and let $x = rx_1 + sx_2$ where $r, s \in R$. Since x is primitive, $\gcd\{r, s\} = 1$, so we may write $ru + sv = 1$. Let $x_2' = -vx_1 + ux_2$. Then

$$x_1 = ux - sx_2'$$

and

$$x_2 = vx + rx_2'.$$

Hence, $\langle x, x_2' \rangle = M$. It remains to show that $\{x, x_2'\}$ is linearly independent. Suppose that $ax + bx_2' = 0$. Then

$$a(rx_1 + sx_2) + b(-vx_1 + ux_2) = 0.$$

Since $\{x_1, x_2\}$ is a basis of M, it follows that

$$ar - bv = 0$$

and

$$as + bu = 0.$$

Multiplying the first equation by u, multiplying the second by v, and adding shows that $a = 0$, while multiplying the first by $-s$, multiplying the second by r, and adding shows that $b = 0$. Hence, $\{x, x_2'\}$ is linearly independent and, therefore, a basis of M.

Now suppose that $\mu(M) = k > 2$ and that the result is true for all free R-modules of rank $< k$. By Theorem 6.6 there is a basis $\{x_1, \ldots, x_k\}$ of M. Let $x = \sum_{i=1}^{k} a_i x_i$. If $a_k = 0$ then $x \in M_1 = \langle x_1, \ldots, x_{k-1}\rangle$, so by induction there is a basis $\{x, x_2', \ldots, x_{k-1}'\}$ of M_1. Then $\{x, x_2', \ldots, x_{k-1}', x_k\}$ is a basis of M containing x. Now suppose that $a_k \neq 0$ and let $y = \sum_{i=1}^{k-1} a_i x_i$. If $y = 0$ then $x = a_k x_k$, and since x is primitive, it follows that a_k is a unit of R and $\{x_1, \ldots, x_{k-1}, x\}$ is a basis of M containing x in this case. If $y \neq 0$ then there is a primitive y' such that $y = by'$ for some $b \in R$. In particular, $y' \in M_1$ so that M_1 has a basis $\{y', x_2', \ldots, x_{k-1}'\}$ and hence M has a basis $\{y', x_2, \ldots, x_{k-1}', x_k\}$. But $x = a_k x_k + y = a_k x_k + by'$ and $\gcd(a_k, b) = 1$ since x is primitive. By the previous case ($k = 2$) we conclude that the submodule $\langle x_k, y'\rangle$ has a basis $\{x, y''\}$. Therefore, M has a basis $\{x, x_2', \ldots, x_{k-1}', y''\}$ and the argument is complete when $k = \mu(M) < \infty$.

If $k = \infty$ let $\{x_j\}_{j\in J}$ be a basis of M and let $x = \sum_{i=1}^{n} a_i x_{j_i}$ for some finite subset $I = \{j_1, \ldots, j_n\} \subseteq J$. If $N = \langle x_{j_1}, \ldots, x_{j_n}\rangle$ then x is a primitive element in the finitely generated module N, so the previous argument applies to show that there is a basis $\{x, x_2', \ldots, x_n'\}$ of N. Then $\{x, x_2', \ldots, x_n'\} \cup \{x_j\}_{j\in J\setminus I}$ is a basis of M containing x. □

(6.17) Corollary. *If M is a free module over a* PID *R, then* **every** *basis of M contains $\mu(M)$ elements.*

Proof. In case $\mu(M) < \infty$, the proof is by induction on $\mu(M)$. If $\mu(M) = 1$ then $M = \langle x\rangle$. If $\{x_1, x_2\} \subseteq M$ then $x_1 = a_1 x$ and and $x_2 = a_2 x$ so that $a_2 x_1 - a_1 x_2 = 0$, and we conclude that no subset of M with more than one element is linearly independent.

Now suppose that $\mu(M) = k > 1$ and assume the result is true for all free R-modules N with $\mu(N) < k$. Let $S = \{x_j\}_{j\in J} \subseteq M$ be any basis of M and choose $x \in S$. Since x is primitive (being an element of a basis), Theorem 6.16 applies to give a basis $\{x, y_2, \ldots, y_k\}$ of M with precisely $\mu(M) = k$ elements. Let $N = M/\langle x\rangle$ and let $\pi : M \to N$ be the projection map. It is clear that N is a free R-module with basis $\pi(S) \setminus \{\pi(x)\}$. By Proposition 2.12 it follows that $\mu(N) \geq k-1$, and since $\{\pi(y_2), \ldots, \pi(y_k)\}$ generates N, we conclude that $\mu(N) = k-1$. By induction, it follows that $|S| - 1 < \infty$ and $|S| - 1 = k - 1$, i.e., $|S| = k$, and the proof is complete in case $\mu(M) < \infty$.

In case $\mu(M) = \infty$, we are claiming that no basis of M can contain a finite number $k \in \mathbf{Z}^+$ of elements. This is proved by induction on k, the proof being similar to the case $\mu(M)$ finite, which we have just done. We leave the details to the reader. □

(6.18) Corollary. *Let R be any commutative ring with identity and let M be a free R-module. Then* **every** *basis of M contains $\mu(M)$ elements.*

Proof. Let I be any maximal ideal of R (recall that maximal ideals exist by Theorem 2.2.16). Since R is commutative, the quotient ring $R/I = K$ is a field (Theorem 2.2.18), and hence it is a PID. By Proposition 4.13, the quotient module M/IM is a finitely generated free K-module so that Corollary 6.17 applies to show that every basis of M/IM has $\mu(M/IM)$ elements. Let $S = \{x_j\}_{j\in J}$ be an arbitrary basis of the free R-module M and let $\pi : M \to M/IM$ be the projection map. According to Proposition 4.13, the set $\pi(S) = \{\pi(x_j)\}_{j\in J}$ is a basis of M/IM over K, and therefore,

$$\mu(M) \leq |J| = \mu(M/IM) \leq \mu(M).$$

Thus, $\mu(M) = |J|$, and the corollary is proved. □

(6.19) *Remarks.*

(1) If M is a free R-module over a commutative ring R, then we have proved that free-rank$(M) = \mu(M) =$ the number of elements in *any* basis of M. This common number we shall refer to simply as the **rank** of M, denoted $\text{rank}_R(M)$ or $\text{rank}(M)$ if the ring R is implicit. If R is a field we shall sometimes write $\dim_R(M)$ (the **dimension** of M over R) in place of $\text{rank}_R(M)$). Thus, a vector space M (over R) is finite dimensional if and only if $\dim_R(M) = \text{rank}_R(M) < \infty$.

(2) Corollary 6.18 is the invariance of rank theorem for finitely generated free modules over an arbitrary commutative ring R. The invariance of rank theorem is not valid for an arbitrary (possibly noncommutative) ring R. As an example, consider the $\mathbf{Z}$-module $M = \oplus_{n\in\mathbf{N}}\mathbf{Z}$, which is the direct sum of countably many copies of $\mathbf{Z}$. It is simple to check that $M \cong M \oplus M$. Thus, if we define $R = \text{End}_{\mathbf{Z}}(M)$, then R is a noncommutative ring, and Corollary 3.13 shows that

$$\begin{aligned} R &= \text{End}_{\mathbf{Z}}(M) \\ &= \text{Hom}_{\mathbf{Z}}(M, M) \\ &\cong \text{Hom}_{\mathbf{Z}}(M, M \oplus M) \\ &\cong \text{Hom}_{\mathbf{Z}}(M, M) \oplus \text{Hom}_{\mathbf{Z}}(M, M) \\ &\cong R \oplus R. \end{aligned}$$

The isomorphisms are isomorphisms of $\mathbf{Z}$-modules. We leave it as an exercise to check that the isomorphisms are also isomorphisms of R-modules, so that $R \cong R^2$, and hence, the invariance of rank does not hold for the ring R. There is, however, one important class of noncommutative rings for which the invariance of rank theorem holds, namely, division rings. This will be proved in Proposition 7.1.14.

(6.20) Corollary. *If M and N are free modules over a* PID *R, at least one of which is finitely generated, then $M \cong N$ if and only if* $\operatorname{rank}(M) = \operatorname{rank}(N)$.

Proof. If M and N are isomorphic, then $\mu(M) = \mu(N)$ so that $\operatorname{rank}(M) = \operatorname{rank}(N)$. Conversely, if $\operatorname{rank}(M) = \operatorname{rank}(N)$, then Proposition 4.9 gives a homomorphism $f : M \to N$, which takes a basis of M to a basis of N. It is easy to see that f must be an isomorphism. □

(6.21) *Remark.* One of the standard results concerning bases of finite-dimensional vector spaces is the statement that a subset $S = \{x_1, \ldots, x_n\}$ of a vector space V of dimension n is a basis provided that S is *either* a spanning set or linearly independent. Half of this result is valid in the current context of finitely generated free modules over a PID. The set $\{2\} \subseteq \mathbf{Z}$ is linearly independent, but it is not a basis of the rank 1 $\mathbf{Z}$-module $\mathbf{Z}$. There is, however, the following result.

(6.22) Proposition. *Let M be a finitely generated free R-module of* $\operatorname{rank} = k$ *where R is a* PID. *If $S = \{x_1, \ldots, x_k\}$ generates M, then S is a basis.*

Proof. Let $T = \{e_j\}_{j=1}^{k}$ be the standard basis of R^k. Then there is a homomorphism $\phi : R^k \to M$ determined by $\phi(e_j) = x_j$. Since $\langle S \rangle = M$, there is a short exact sequence

$$0 \longrightarrow K \longrightarrow R^k \xrightarrow{\phi} M \longrightarrow 0$$

where $K = \operatorname{Ker}(\phi)$. Since M is free, Corollary 4.16 gives $R^k \cong M \oplus K$, and according to Theorem 6.2, K is also free of finite rank. Therefore,

$$k = \operatorname{rank}(M) + \operatorname{rank}(K) = k + \operatorname{rank}(K)$$

and we conclude that $\operatorname{rank}(K) = 0$. Hence ϕ is an isomorphism and S is a basis. □

We will conclude this section with a substantial generalization of Theorem 6.2. This result is the crucial result needed for the structure theorem for finitely generated modules over a PID.

(6.23) Theorem. (Invariant factor theorem for submodules) *Let R be a* PID*, let M be a free R-module, and let $N \subseteq M$ be a submodule (which is automatically free by Theorem 6.2) of rank $n < \infty$. Then there is a basis S of M, a subset $\{x_1, \ldots, x_n\} \subseteq S$, and nonzero elements $s_1, \ldots, s_n \in R$ such that*

(6.3) $\{s_1 x_1, \ldots, s_n x_n\}$ *is a basis of N*

and

(6.4) $s_i \mid s_{i+1}$ *for* $1 \leq i \leq n-1$.

Proof. If $N = \langle 0 \rangle$, there is nothing to prove, so we may assume that $N \neq \langle 0 \rangle$ and proceed by induction on $n = \operatorname{rank}(N)$. If $n = 1$, then $N = \langle y \rangle$ and $\{y\}$ is a basis of N. By Lemma 6.14, we may write $y = c(y)x$ where $x \in M$ is a primitive element and $c(y) \in R$ is the content of y. By Theorem 6.16, there is a basis S of M containing the primitive element x. If we let $x_1 = x$ and $s_1 = c(y)$, then $s_1 x_1 = y$ is a basis of N, so condition (6.3) is satisfied; (6.4) is vacuous for $n = 1$. Therefore, the theorem is proved for $n = 1$.

Now assume that $n > 1$. By Lemma 6.14, each $y \in N$ can be written as $y = c(y) \cdot y'$ where $c(y) \in R$ is the content of y (Remark 6.15) and $y' \in M$ is primitive. Let

$$\mathcal{S} = \{\langle c(y) \rangle : y \in N\}.$$

This is a nonempty collection of ideals of R. Since R is Noetherian, Proposition 2.5.10 implies that there is a maximal element of $\mathcal{S}$. Let $\langle c(y) \rangle$ be such a maximal element. Thus, $y \in N$ and $y = c(y) \cdot x$, where $x \in M$ is primitive. Let $s_1 = c(y)$. Choose any basis T of M that contains x. This is possible by Theorem 6.16 since $x \in M$ is primitive. Let $x_1 = x$ and write $T = \{x_1\} \cup T' = \{x_1\} \cup \{x'_j\}_{j \in J'}$. Let $M_1 = \langle \{x'_j\}_{j \in J'} \rangle$ and let $N_1 = M_1 \cap N$.

Claim. $N = \langle s_1 x_1 \rangle \oplus N_1$.

To see this, note that $\langle s_1 x_1 \rangle \cap N_1 \subseteq \langle x_1 \rangle \cap M_1 = \langle 0 \rangle$ because T is a basis of M. Let $z \in N$. Then, with respect to the basis T, we may write

$$z = a_1 x_1 + \sum_{j \in J'} b_j x'_j. \tag{6.5}$$

Let $d = (s_1, a_1) = \gcd\{s_1, a_1\}$. Then we may write $d = us_1 + va_1$ where u, $v \in R$. If $w = uy + vz$, then Equation (6.5) shows that

$$\begin{aligned} w &= uy + vz \\ &= (us_1 + va_1)x_1 + \sum_{j \in J'} vb_j x'_j \\ &= dx_1 + \sum_{j \in J'} vb_j x'_j. \end{aligned}$$

Writing $w = c(w) \cdot w'$ where $c(w)$ is the content of w and $w' \in M$ is primitive, it follows from Lemma 6.13 that $c(w) \mid d$ (because $c(w)$ is the greatest common divisor of all coefficients of w when expressed as a linear combination of any basis of M). Thus we have a chain of ideals

$$\langle s_1 \rangle \subseteq \langle d \rangle \subseteq \langle c(w) \rangle,$$

and the maximality of $\langle s_1 \rangle$ in $\mathcal{S}$ shows that $\langle s_1 \rangle = \langle c(w) \rangle = \langle d \rangle$. In particular, $\langle s_1 \rangle = \langle d \rangle$ so that $s_1 \mid a_1$, and we conclude that

$$z = b_1(s_1 x_1) + \sum_{j \in J'} b_j x'_j.$$

That is, $z \in \langle s_1 x_1 \rangle + N_1$. Theorem 3.1 then shows that

$$N \cong \langle s_1 x_1 \rangle \oplus N_1,$$

and the claim is proved.

By Theorem 6.2, N_1 is a free R-module since it is a submodule of the free R-module M. Furthermore, by the claim we see that

$$\operatorname{rank}(N_1) = \operatorname{rank}(N) - 1 = n - 1.$$

Applying the induction hypothesis to the pair $N_1 \subseteq M_1$, we conclude that there is a basis S' of M_1 and a subset $\{x_2, \ldots, x_n\}$ of S', together with nonzero elements $s_2, \ldots, s_n$ of R, such that

$$\{s_2 x_2, \ldots, s_n x_n\} \qquad \text{is a basis of } N_1 \tag{6.6}$$

and

$$s_i \mid s_{i+1} \qquad \text{for} \quad 2 \le i \le n-1. \tag{6.7}$$

Let $S = S' \cup \{x_1\}$. Then the theorem is proved once we have shown that $s_1 \mid s_2$.

To verify that $s_1 \mid s_2$, consider the element $s_2 x_2 \in N_1 \subseteq N$ and let $z = s_1 x_1 + s_2 x_2 \in N$. When we write $z = c(z) \cdot z'$ where $z' \in M$ is primitive and $c(z) \in R$ is the content of z, Remark 6.15 shows that $c(z) = (s_1, s_2)$. Thus, $\langle s_1 \rangle \subseteq \langle c(z) \rangle$ and the maximality of $\langle s_1 \rangle$ in $\mathcal{S}$ shows that $\langle c(z) \rangle = \langle s_1 \rangle$, i.e., $s_1 \mid s_2$, and the proof of the theorem is complete. □

(6.24) Example. Let $N \subseteq \mathbf{Z}^2$ be the submodule generated by $y_1 = (2, 4)$, $y_2 = (2, -2)$, and $y_3 = (2, 10)$. Then $c(y_1) = c(y_2) = c(y_3) = 2$. Furthermore, 2 divides every component of any linear combination of y_1, y_2, and y_3, so the maximal content of any element of N is 2. Let $v_1 = (1, 2)$. Then $y_1 = 2v_1$. Extend v_1 to a basis of $\mathbf{Z}^2$ by taking $v_2 = (0, 1)$. Then

$$N_1 = N \cap \langle (0, 1) \rangle = \langle (0, 6) \rangle. \tag{6.8}$$

To see this note that every $z \in N_1$ can be written as

$$z = a_1 y_1 + a_2 y_2 + a_3 y_3$$

where $a_1, a_3, a_3 \in \mathbf{Z}$ satisfy the equation

$$2a_1 + 2a_2 + 2a_3 = 0.$$

Thus, $4a_1 = -4a_2 - 4a_3$, and considering the second coordinate of z, we see that $z = (z_1, z_2)$ where

$$z_2 = 4a_1 - 2a_2 + 10a_3 = -6a_2 + 6a_3 = 6(a_3 - a_2).$$

Therefore, $\{v_1, v_2\}$ is a basis of $\mathbf{Z}^2$, while $\{2v_1, 6v_2\}$ is a basis of N. To check, note that $y_1 = 2v_1$, $y_2 = 2v_1 - 6v_2$, and $y_3 = 2v_1 + 6v_2$.

(6.25) *Remark.* In Section 3.7, we will prove that the elements $\{s_1, \ldots, s_n\}$ are determined just by the rank n submodule N and not by the particular choice of a basis S of M. These elements are called the **invariant factors** of the submodule N in the free module M.

3.7 Finitely Generated Modules over PIDs

The invariant factor theorem for submodules (Theorem 6.24) gives a complete description of a submodule N of a finitely generated free R-module M over a PID R. Specifically, it states that a basis of M can be chosen so that the first $n = \text{rank}(N)$ elements of the basis, multiplied by elements of R, provide a basis of N. Note that this result is a substantial generalization of the result from vector space theory, which states that any basis of a subspace of a vector space can be extended to a basis of the ambient space. We will now complete the analysis of finitely generated R-modules (R a PID) by considering modules that need not be free. If the module M is not free, then, of course, it is not possible to find a basis, but we will still be able to express M as a finite direct sum of cyclic submodules; the cyclic submodules may, however, have nontrivial annihilator. The following result constitutes the fundamental structure theorem for finitely generated modules over principal ideal domains.

(7.1) Theorem. *Let $M \neq 0$ be a finitely generated module over the* PID *R. If $\mu(M) = n$, then M is isomorphic to a direct sum of cyclic submodules*

$$M \cong Rw_1 \oplus \cdots \oplus Rw_n$$

such that

$$R \neq \text{Ann}(w_1) \supseteq \text{Ann}(w_2) \supseteq \cdots \supseteq \text{Ann}(w_n) = \text{Ann}(M). \tag{7.1}$$

Moreover, for $1 \leq i < n$

$$\text{Ann}(w_i) = \text{Ann}\left(M/(Rw_{i+1} + \cdots + Rw_n)\right). \tag{7.2}$$

Proof. Since $\mu(M) = n$, let $\{v_1, \ldots, v_n\}$ be a generating set of M and define an R-module homomorphism $\phi : R^n \to M$ by

$$\phi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i v_i.$$

Let $K = \text{Ker}(\phi)$. Since K is a submodule of R^n, it follows from Theorem 6.2 that K is a free R-module of rank $m \leq n$. By Theorem 6.23, there is a basis $\{y_1, \ldots, y_n\}$ of R^n and nonzero elements $s_1, \ldots, s_m \in R$ such that

$$\{s_1y_1, \ldots, s_my_m\} \quad \text{is a basis for } K \tag{7.3}$$

and

$$s_i \mid s_{i+1} \quad \text{for} \quad 1 \leq i \leq m-1. \tag{7.4}$$

Let $w_i = \phi(y_i) \in M$ for $1 \leq i \leq n$. Then $\{w_1, \ldots, w_n\}$ generates M since ϕ is surjective and $\{y_1, \ldots, y_n\}$ is a basis of R^n. We claim that

$$M \cong Rw_1 \oplus \cdots \oplus Rw_n.$$

By the characterization of direct sum modules (Theorem 3.1), it is sufficient to check that if

$$a_1w_1 + \cdots + a_nw_n = 0 \tag{7.5}$$

where $a_i \in R$, then $a_iw_i = 0$ for all i. Thus suppose that Equation (7.5) is satisfied. Then

$$\begin{aligned} 0 &= a_1w_1 + \cdots + a_nw_n \\ &= a_1\phi(y_1) + \cdots + a_n\phi(y_n) \\ &= \phi(a_1y_1 + \cdots + a_ny_n) \end{aligned}$$

so that

$$a_1y_1 + \cdots + a_ny_n \in \operatorname{Ker}(\phi) = K = \langle s_1y_1, \ldots, s_my_m\rangle.$$

Therefore,

$$a_1y_1 + \cdots + a_ny_n = b_1s_1y_1 + \cdots + b_ms_my_m$$

for some $b_1, \ldots, b_m \in R$. But $\{y_1, \ldots, y_n\}$ is a basis of R^n, so we conclude that $a_i = b_is_i$ for $1 \leq i \leq m$ while $a_i = 0$ for $m+1 \leq i \leq n$. Thus,

$$a_iw_i = b_is_i\phi(y_i) = b_i\phi(s_iy_i) = 0$$

for $1 \leq i \leq m$ because $s_iy_i \in K = \operatorname{Ker}(\phi)$, while $a_iw_i = 0$ for $m+1 \leq i \leq n$ since $a_i = 0$ in this case. Hence

$$M \cong Rw_1 \oplus \cdots \oplus Rw_n.$$

Note that $\operatorname{Ann}(w_i) = \langle s_i\rangle$ for $1 \leq i \leq m$, and since $s_i \mid s_{i+1}$, it follows that

$$\operatorname{Ann}(w_1) \supseteq \operatorname{Ann}(w_2) \supseteq \cdots \supseteq \operatorname{Ann}(w_m),$$

while for $i > m$, since $\langle y_i\rangle \cap \operatorname{Ker}(\phi) = \langle 0\rangle$, it follows that $\operatorname{Ann}(w_i) = \langle 0\rangle$. Since $s_i \mid s_n$ for all i and since $\operatorname{Ann}(w_i) = \langle s_i\rangle$, we conclude that $s_nM = 0$. Hence, $\operatorname{Ann}(w_n) = \langle s_n\rangle = \operatorname{Ann}(M)$ and Equation (7.1) is satisfied. Since

$$M/(Rw_{i+1} + \cdots + Rw_n) \cong Rw_1 \oplus \cdots \oplus Rw_i,$$

Equation (7.2) follows from Equation (7.1). The proof is now completed by observing that $\operatorname{Ann}(w_i) \neq R$ for any i since, if $\operatorname{Ann}(w_i) = R$, then

$Rw_i = \langle 0 \rangle$, and hence, M could be generated by fewer than n elements. But $n = \mu(M)$, so this is impossible because $\mu(M)$ is the minimal number of generators of M. □

A natural question to ask is to what extent is the cyclic decomposition provided by Theorem 7.1 unique. Certainly, the factors themselves are not unique as one can see from the example

$$\begin{aligned} \mathbf{Z}^2 &\cong \mathbf{Z} \cdot (1,0) \oplus \mathbf{Z} \cdot (0,1) \\ &\cong \mathbf{Z} \cdot (1,0) \oplus \mathbf{Z} \cdot (1,1). \end{aligned}$$

More generally, if M is a free R-module of rank n, then any choice of basis $\{v_1, \ldots, v_n\}$ provides a cyclic decomposition

$$M \cong Rv_1 \oplus \cdots \oplus Rv_n$$

with $\operatorname{Ann}(v_i) = 0$ for all i. Therefore, there is no hope that the cyclic factors themselves are uniquely determined. What does turn out to be unique, however, is the chain of annihilator ideals

$$\operatorname{Ann}(w_1) \supseteq \cdots \supseteq \operatorname{Ann}(w_n)$$

where we require that $\operatorname{Ann}(w_i) \neq R$, which simply means that we do not allow copies of $\langle 0 \rangle$ in our direct sums of cyclic submodules. We reduce the uniqueness of the annihilator ideals to the case of finitely generated torsion R-modules by means of the following result. If M is an R-module, recall that the torsion submodule M_τ of M is defined by

$$M_\tau = \{x \in M : \operatorname{Ann}(x) \neq \langle 0 \rangle\}.$$

(7.2) Proposition. *If M and N are finitely generated modules over a* PID *R, then $M \cong N$ if and only if $M_\tau \cong N_\tau$ and* $\operatorname{rank} M/M_\tau = \operatorname{rank} N/N_\tau$.

Proof. Let $\phi : M \to N$ be an isomorphism. Then if $x \in M_\tau$, there is an $a \neq 0 \in R$ with $ax = 0$. Then $a\phi(x) = \phi(ax) = \phi(0) = 0$ so that $\phi(x) \in N_\tau$. Therefore, $\phi(M_\tau) \subseteq N_\tau$. Applying the same observation to ϕ^{-1} shows that $\phi(M_\tau) = N_\tau$. Thus, $\phi|_{M_\tau} : M_\tau \to N_\tau$ is an isomorphism; if $\pi : N \to N_\tau$ is the natural projection, it follows that $\operatorname{Ker}(\pi \circ \phi) = M_\tau$. The first isomorphism theorem then gives an isomorphism $M/M_\tau \cong N/N_\tau$. Since M/M_τ and N/N_τ are free R-modules of finite rank, they are isomorphic if and only if they have the same rank.

The converse follows from Corollary 6.20. □

Therefore, our analysis of finitely generated R-modules over a PID R is reduced to studying finitely generated torsion modules M; the uniqueness of the cyclic submodule decomposition of finitely generated torsion modules is the following result.

(7.3) Theorem. *Let M be a finitely generated torsion module over a* PID *R, and suppose that there are cyclic submodule decompositions*

$$M \cong Rw_1 \oplus \cdots \oplus Rw_k \tag{7.6}$$

and

$$M \cong Rz_1 \oplus \cdots \oplus Rz_r \tag{7.7}$$

where

$$\mathrm{Ann}(w_1) \supseteq \cdots \supseteq \mathrm{Ann}(w_k) \neq \langle 0\rangle \qquad \textit{with} \quad \mathrm{Ann}(w_1) \neq R \tag{7.8}$$

and

$$\mathrm{Ann}(z_1) \supseteq \cdots \supseteq \mathrm{Ann}(z_r) \neq \langle 0\rangle \qquad \textit{with} \quad \mathrm{Ann}(z_1) \neq R. \tag{7.9}$$

Then $k = r$ and $\mathrm{Ann}(w_i) = \mathrm{Ann}(z_i)$ for $1 \le i \le k$.

Proof. Note that $\mathrm{Ann}(M) = \mathrm{Ann}(w_k) = \mathrm{Ann}(z_r)$. Indeed,

$$\begin{aligned}\mathrm{Ann}(M) &= \mathrm{Ann}(Rw_1 + \cdots + Rw_k)\\ &= \mathrm{Ann}(w_1) \cap \cdots \cap \mathrm{Ann}(w_k)\\ &= \mathrm{Ann}(w_k)\end{aligned}$$

since $\mathrm{Ann}(w_1) \supseteq \cdots \supseteq \mathrm{Ann}(w_k)$. The equality $\mathrm{Ann}(M) = \mathrm{Ann}(z_r)$ is the same argument.

We will first show that $k = r$. Suppose without loss of generality that $k \ge r$. Choose a prime $p \in R$ such that $\langle p\rangle \supseteq \mathrm{Ann}(w_1)$, i.e., p divides the generator of $\mathrm{Ann}(w_1)$. Then $\langle p\rangle \supseteq \mathrm{Ann}(w_i)$ for all i. Since $p \in \mathrm{Ann}(M/pM)$, it follows that M/pM is an R/pR-module and Equations (7.6) and (7.7) imply

$$M/pM \cong Rw_1/(pRw_1) \oplus \cdots \oplus Rw_k/(pRw_k) \tag{7.10}$$

and

$$M/pM \cong Rz_1/(pRz_1) \oplus \cdots \oplus Rz_r/(pRz_r). \tag{7.11}$$

Suppose that $pRw_i = Rw_i$. Then we can write $apw_i = w_i$ for some $a \in R$. Hence, $ap - 1 \in \mathrm{Ann}(w_i) \subseteq \langle p\rangle$ by our choice of p, so $1 \in \langle p\rangle$, which contradicts the fact that p is a prime. Therefore, $pRw_i \neq Rw_i$ for all i and Equation (7.10) expresses the R/pR-module M/pM as a direct sum of cyclic R/pR-modules, none of which is $\langle 0\rangle$. Since R/pR is a field (in a PID prime ideals are maximal), all R/pR-modules are free, so we conclude that M/pM is free of rank k. Moreover, Equation (7.11) expresses M/pM as a direct sum of r cyclic submodules, so it follows that $k = \mu(M/pM) \le r$. Thus, $r = k$, and in particular, $Rz_i/(pRz_i) \neq 0$ since, otherwise, M/pM could be generated by fewer than k elements. Thus, $\langle p\rangle \supseteq \mathrm{Ann}(z_i)$ for all i; if not, then $\langle p\rangle + \mathrm{Ann}(z_i) = R$, so there are $a \in R$ and $c \in \mathrm{Ann}(z_i)$ such that $ap + c = 1$. Then $z_i = apz_i + cz_i = apz_i \in pRz_i$, so $Rz_i/(pRz_i) = 0$, and we just observed that $Rz_i/(pRz_i) \neq 0$.

We are now ready to complete the proof. We will work by induction on $\ell(\mathrm{Ann}(M))$ where, if $I = \langle a \rangle$ is an ideal of R, then $\ell(I)$ is the number of elements (counted with multiplicity) in a prime factorization of a. This number is well defined by the fundamental theorem of arithmetic for PIDs. Suppose that $\ell(\mathrm{Ann}(M)) = 1$. Then $\mathrm{Ann}(M) = \langle p \rangle$ where $p \in R$ is prime. Since $\mathrm{Ann}(M) = \mathrm{Ann}(w_k) = \mathrm{Ann}(z_k) = \langle p \rangle$ and since $\langle p \rangle$ is a maximal ideal, Equations (7.8) and (7.9) imply that $\mathrm{Ann}(w_i) = \langle p \rangle = \mathrm{Ann}(z_i)$ for all i, and the theorem is proved in the case $\ell(\mathrm{Ann}(M)) = 1$.

Now suppose the theorem is true for all finitely generated torsion R-modules N with $\ell(\mathrm{Ann}(N)) < \ell(\mathrm{Ann}(M))$, and consider the isomorphisms

$$pM \cong pRw_1 \oplus \cdots \oplus pRw_k \cong pRw_{s+1} \oplus \cdots \oplus pRw_k \tag{7.12}$$

and

$$pM \cong pRz_1 \oplus \cdots \oplus pRz_k \cong pRz_{t+1} \oplus \cdots \oplus pRz_k \tag{7.13}$$

where $\mathrm{Ann}(w_1) = \cdots = \mathrm{Ann}(w_s) = \mathrm{Ann}(z_1) = \cdots = \mathrm{Ann}(z_t) = \langle p \rangle$ and $\mathrm{Ann}(w_{s+1}) \neq \langle p \rangle$, $\mathrm{Ann}(z_{t+1}) \neq \langle p \rangle$ (s and t may be 0). Then $\mathrm{Ann}(pM) = \langle a/p \rangle$ where $\mathrm{Ann}(M) = \langle a \rangle$, so $\ell(\mathrm{Ann}(pM)) = \ell(\mathrm{Ann}(M)) - 1$. By induction we conclude that $k - s = k - t$, i.e., $s = t$, and $\mathrm{Ann}(pw_i) = \mathrm{Ann}(pz_i)$ for $s < i \leq k$. But $\mathrm{Ann}(pw_i) = \langle a_i/p \rangle$ where $\mathrm{Ann}(w_i) = \langle a_i \rangle$. Thus $\mathrm{Ann}(w_i) = \mathrm{Ann}(z_i)$ for all i and we are done. □

Since $Rw_i \cong R/\mathrm{Ann}(w_i)$ and since R/I and R/J are isomorphic R-modules if and only if $I = J$ (Exercise 10), we may rephrase our results as follows.

(7.4) Corollary. *Finitely generated modules over a* PID R *are in one-to-one correspondence with finite nonincreasing chains of ideals*

$$R \neq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n.$$

Such a chain of ideals corresponds to the module

$$M = R/I_1 \oplus \cdots \oplus R/I_n.$$

Note that $\mu(M) = n$ and if $I_{k+1} = \cdots = I_n = \langle 0 \rangle$ but $I_k \neq \langle 0 \rangle$, then

$$M \cong R/I_1 \oplus \cdots \oplus R/I_k \oplus R^{n-k}.$$

We will use the convention that the empty sequence of ideals ($n = 0$) corresponds to $M = \langle 0 \rangle$.

Proof. □

(7.5) Definition. *If M is a finitely generated torsion module over a* PID R *and $M \cong Rw_1 \oplus \cdots \oplus Rw_n$ with $\mathrm{Ann}(w_i) \supseteq \mathrm{Ann}(w_{i+1})$ $(1 \leq i \leq n-1)$ and $\mathrm{Ann}(w_i) \neq R$, then the chain of ideals $I_i = \mathrm{Ann}(w_i)$ is called the* **chain of invariant ideals of M.**

Using this language, we can express our results as follows:

(7.6) Corollary. *Two finitely generated torsion modules over a* PID *are isomorphic if and only if they have the same chain of invariant ideals.*

Proof. □

(7.7) *Remark.* In some cases the principal ideals $\mathrm{Ann}(w_j)$ have a preferred generator a_j. In this case the generators $\{a_j\}_{j=1}^n$ are called the **invariant factors of** M.

The common examples are $R = \mathbf{Z}$, in which case we choose $a_j > 0$ so that $a_j = |\mathbf{Z}/\operatorname{Ann}(w_j)|$, and $R = F[X]$, where we take monic polynomials as the preferred generators of ideals.

(7.8) Definition. *Let R be a* PID*, and let M be a finitely generated torsion R-module with chain of invariant ideals*

$$\langle s_1\rangle \supseteq \langle s_2\rangle \supseteq \cdots \supseteq \langle s_n\rangle.$$

We define $\mathrm{me}(M) = s_n$ *and* $\mathrm{co}(M) = s_1 \cdots s_n$.

Note that $\mathrm{me}(M)$ and $\mathrm{co}(M)$ are only defined up to multiplication by a unit, but in some cases ($R = \mathbf{Z}$ or $R = F[X]$) we have a preferred choice of generators of ideals. In these cases $\mathrm{me}(M)$ and $\mathrm{co}(M)$ are uniquely defined. Concerning the invariants $\mathrm{me}(M)$ and $\mathrm{co}(M)$, there is the following trivial but useful corollary of our structure theorems.

(7.9) Corollary. *Let M be a finitely generated torsion module over a* PID *R.*

(1) *If $a \in R$ with $aM = 0$, then* $\mathrm{me}(M) \mid a$.
(2) $\mathrm{me}(M)$ *divides* $\mathrm{co}(M)$.
(3) *If $p \in R$ is a prime dividing* $\mathrm{co}(M)$*, then p divides* $\mathrm{me}(M)$.

Proof. (1) Since $\mathrm{Ann}(M) = \langle s_n\rangle = \langle \mathrm{me}(M)\rangle$ by Theorem 7.1 and the defintion of $\mathrm{me}(M)$, it follows that if $aM = 0$, i.e., $a \in \mathrm{Ann}(M)$, then $\mathrm{me}(M) \mid a$.

(2) Clearly s_n divides $s_1 \cdots s_n$.

(3) Suppose that $p \mid s_1 \cdots s_n = \mathrm{co}(M)$. Then p divides some s_i, but $\langle s_i\rangle \supseteq \langle s_n\rangle$, so $s_i \mid s_n$. Hence, $p \mid s_n = \mathrm{me}(M)$. □

(7.10) *Remark.* There are, unfortunately, no standard names for these invariants. The notation we have chosen reflects the common terminology in the two cases $R = \mathbf{Z}$ and $R = F[X]$. In the case $R = \mathbf{Z}$, $\mathrm{me}(M)$ is the exponent and $\mathrm{co}(M)$ is the order of the finitely generated torsion $\mathbf{Z}$-module

(= finite abelian group) M. In the case $R = F[X]$ of applications to linear algebra to be considered in Chapter 4, $\mathrm{me}(V_T)$ will be the minimal polynomial and $\mathrm{co}(V_T)$ will be the characteristic polynomial of the linear transformation $T \in \mathrm{Hom}_F(V)$ where V is a finite-dimensional vector space over the field F and V_T is the $F[X]$-module determined by T (see Example 1.5 (12)).

There is another decomposition of a torsion R-module M into a direct sum of cyclic submodules which takes advantage of the prime factorization of any generator of $\mathrm{Ann}(M)$. To describe this decomposition we need the following definition.

(7.11) Definition. *Let M be a module over the* PID *R and let $p \in R$ be a prime. Define the* p**-component** *M_p of M by*

$$M_p = \{x \in M : \mathrm{Ann}(x) = \langle p^n \rangle \quad \text{for some} \quad n \in \mathbf{Z}^+\}.$$

If $M = M_p$, then M is said to be p**-primary**, *and M is* **primary** *if it is p-primary for some prime $p \in R$.*

It is a simple exercise to check that submodules, quotient modules, and direct sums of p-primary modules are p-primary (Exercise 54).

(7.12) Theorem. *If M is a finitely generated torsion module over a* PID *R, then M is a direct sum of primary submodules.*

Proof. Since M is a direct sum of cyclic submodules by Theorem 7.1, it is sufficient to assume that M is cyclic. Thus suppose that $M = \langle x \rangle$ and suppose that

$$\mathrm{Ann}(x) = \langle a \rangle = \langle p_1^{r_1} \cdots p_n^{r_n} \rangle$$

where $p_1, \ldots, p_n$ are the distinct prime divisors of a. Let $q_i = a/p_i^{r_i}$. Then $1 = (q_1, \ldots, q_n) = \gcd\{q_1, \ldots, q_n\}$, so there are $b_1, \ldots, b_n \in R$ such that

$$1 = b_1 q_1 + \cdots + b_n q_n. \tag{7.14}$$

Let $x_i = b_i q_i x$. Then Equation (7.14) implies that

$$x = x_1 + \cdots + x_n$$

so that

$$M = \langle x \rangle = \langle x_1 \rangle + \cdots + \langle x_n \rangle.$$

Suppose that $y \in \langle x_1 \rangle \cap (\langle x_2 \rangle + \cdots + \langle x_n \rangle)$. Then

$$y = c_1 x_1 = c_2 x_2 + \cdots + c_n x_n$$

and hence, $p_1^{r_1} y = c_1 b_1 p_1^{r_1} q_1 x = c_1 b_1 a x = 0$ and

$$q_1 y = c_2 \widetilde{q}_2 p_2^{r_2} x_2 + \cdots + c_n \widetilde{q}_n p_n^{r_n} x_n = 0,$$

where $\widetilde{q}_j = q_1/p_j^{r_j}$. Therefore, $\{p_1^{r_1}, q_1\} \subseteq \mathrm{Ann}(y)$, but $(p_1^{r_1}, q_1) = 1$ so that $\mathrm{Ann}(y) = R$. Therefore, $y = 0$. A similar calculation shows that

$$\langle x_i \rangle \cap \Big(\langle x_1 \rangle + \cdots + \widehat{\langle x_i \rangle} + \cdots + \langle x_n \rangle \Big) = \langle 0 \rangle,$$

so by Theorem 3.1, $M \cong \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$. □

Combining Theorems 7.1 and 7.12, we obtain the following result:

(7.13) Theorem. *Any finitely generated torsion module M over a* PID *R is a direct sum of primary cyclic submodules.*

Proof. Suppose $M \cong Rw_1 \oplus \cdots \oplus Rw_n$ as in Theorem 7.1. Then if $\mathrm{Ann}(w_i) = \langle s_i \rangle$, we have $s_i \mid s_{i+1}$ for $1 \le i \le n-1$ with $s_1 \neq 1$ and $s_n \neq 0$ (since M is torsion). Let $p_1, \ldots, p_k$ be the set of distinct nonassociate primes that occur as a prime divisor of some invariant factor of M. Then

$$\begin{aligned} s_1 &= u_1 p_1^{e_{11}} \cdots p_k^{e_{1k}} \\ &\vdots \\ s_n &= u_n p_1^{e_{n1}} \cdots p_k^{e_{nk}} \end{aligned}$$

where the divisibility conditions imply that

$$0 \le e_{1j} \le e_{2j} \le \cdots \le e_{nj} \qquad \text{for} \quad 1 \le j \le k.$$

Then the proof of Theorem 7.12 shows that M is the direct sum of cyclic submodules with annihilators $\{p_j^{e_{ij}} : e_{ij} > 0\}$, and the theorem is proved. □

(7.14) Definition. *The prime powers $\{p_j^{e_{ij}} : e_{ij} > 0,\ 1 \le j \le k\}$ are called the* **elementary divisors** *of M.*

(7.15) Theorem. *If M and N are finitely generated torsion modules over a* PID *R, then $M \cong N$ if and only if M and N have the same elementary divisors.*

Proof. Since M is uniquely determined up to isomorphism from the invariant factors, it is sufficient to show that the invariant factors of M can be recovered from a knowledge of the elementary divisors. Thus suppose that

$$\langle s_1 \rangle \supseteq \langle s_2 \rangle \supseteq \cdots \supseteq \langle s_n \rangle$$

is the chain of invariant ideals of the finitely generated torsion module M. This means that $s_i \mid s_{i+1}$ for $1 \le i < n$. Let $p_1, \ldots, p_k$ be the set of distinct nonassociate primes that occur as a prime divisor of some invariant factor of M. Then

$$\begin{aligned} s_1 &= u_1 p_1^{e_{11}} \cdots p_k^{e_{1k}} \\ &\vdots \\ s_n &= u_n p_1^{e_{n1}} \cdots p_k^{e_{nk}} \end{aligned} \tag{7.15}$$

where the divisibility conditions imply that

$$0 \le e_{1j} \le e_{2j} \le \cdots \le e_{nj} \qquad \text{for} \quad 1 \le j \le k. \tag{7.16}$$

Thus, the elementary divisors of M are

$$\{p_j^{e_{ij}} : e_{ij} > 0\}. \tag{7.17}$$

We show that the set of invariant factors (Equation (7.15)) can be reconstructed from the set of prime powers in Equation (7.17). Indeed, if

$$e_j = \max_{1 \le i \le n} e_{ij}, \qquad 1 \le j \le k,$$

then the inequalities (7.16) imply that s_n is an associate of $p_1^{e_1} \cdots p_k^{e_k}$. Delete

$$\{p_1^{e_1}, \ldots, p_k^{e_k}\}$$

from the set of prime powers in set (7.17), and repeat the process with the set of remaining elementary divisors to obtain s_{n-1}. Continue until all prime powers have been used. At this point, all invariant factors have been recovered. Notice that the number n of invariant factors is easily recovered from the set of elementary divisors of M. Since s_1 divides every s_i, it follows that every prime dividing s_1 must also be a prime divisor of every s_i. Therefore, in the set of elementary divisors, n is the maximum number of occurrences of $p^{e_{ij}}$ for a single prime p. □

(7.16) Example. Suppose that M is the $\mathbf{Z}$-module

$$M = \mathbf{Z}_{2^2} \times \mathbf{Z}_{2^2} \times \mathbf{Z}_3 \times \mathbf{Z}_{3^2} \times \mathbf{Z}_5 \times \mathbf{Z}_7 \times \mathbf{Z}_{7^2}.$$

Then the elementary divisors of M are 2^2, 2^2, 3, 3^2, 5, 7, 7^2. Using the algorithm from Theorem 7.15, we can recover the invariant factor description of M as follows. The largest invariant factor is the product of the highest power of each prime occurring in the set of elementary divisors, i.e., the least common multiple of the set of elementary divisors. That is, $s_2 = 7^2 \cdot 5 \cdot 3^2 \cdot 2^2 = 8820$. Note that the number of invariant factors of M is 2 since powers of the primes 2, 3, and 7 occur twice in the set of elementary divisors, while no prime has three powers among this set. Deleting 7^2, 5, 3^2, 2^2 from the set of elementary divisors, we obtain $s_1 = 7 \cdot 3 \cdot 2^2 = 84$. This uses all the elementary divisors, so we obtain

$$M \cong \mathbf{Z}_{84} \times \mathbf{Z}_{8820}.$$

We now present some useful observations concerning the invariants $\mathrm{me}(M)$ and $\mathrm{co}(M)$ where M is a torsion R-module (R a PID). See Definition 7.9 for the definition of these invariants. The verification of the results that we wish to prove require some preliminary results on torsion R-modules, which are of interest in their own right. We start with the following lemmas.

(7.17) Lemma. *Let M be a module over a* PID *R and suppose that $x \in M_\tau$. If $\mathrm{Ann}(x) = \langle r \rangle$ and $a \in R$ with $(a, r) = d$ (recall that $(a, r) = \gcd\{a, r\}$), then $\mathrm{Ann}(ax) = \langle r/d \rangle$.*

Proof. Since $(r/d)(ax) = (a/d)(rx) = 0$, it follows that $\langle r/d \rangle \subseteq \mathrm{Ann}(ax)$. If $b(ax) = 0$, then $r \mid (ba)$, so $ba = rc$ for some $c \in R$. But $(a, r) = d$, so there are $s, t \in R$ with $rs + at = d$. Then $rct = bat = b(d - rs)$ and we see that $bd = r(ct + bs)$. Therefore, $b \in \langle r/d \rangle$ and hence $\mathrm{Ann}(ax) = \langle r/d \rangle$. □

(7.18) Lemma. *Let M be a module over a* PID *R, and let $x_1, \ldots, x_n \in M_\tau$ with $\mathrm{Ann}(x_i) = \langle r_i \rangle$ for $1 \leq i \leq n$. If $\{r_1, \ldots, r_n\}$ is a pairwise relatively prime subset of R and $x = x_1 + \cdots + x_n$, then $\mathrm{Ann}(x) = \langle a \rangle = \left\langle \prod_{i=1}^n r_i \right\rangle$. Conversely, if $y \in M_\tau$ is an element such that $\mathrm{Ann}(y) = \langle b \rangle = \left\langle \prod_{i=1}^n s_i \right\rangle$ where $\{s_1, \ldots, s_n\}$ is a relatively prime subset of R, then we may write $y = y_1 + \cdots + y_n$ where $\mathrm{Ann}(y_i) = \langle s_i \rangle$ for all i.*

Proof. Let $x = x_1 + \cdots + x_n$. Then $a = \prod_{i=1}^n r_i \in \mathrm{Ann}(x)$ so that $\langle a \rangle \subseteq \mathrm{Ann}(x)$. It remains to check that $\mathrm{Ann}(x) \subseteq \langle a \rangle$. Thus, suppose that $bx = 0$. By the Chinese remainder theorem (Theorem 2.2.24), there are $c_1, \ldots, c_n \in R$ such that

$$c_i \equiv \begin{cases} 1 \pmod{\langle r_i \rangle}, \\ 0 \pmod{\langle r_j \rangle}, \quad \text{if } j \neq i. \end{cases}$$

Then, since $\langle r_j \rangle = \mathrm{Ann}(x_j)$, we conclude that $c_i x_j = 0$ if $i \neq j$, so for each i with $1 \leq i \leq n$

$$0 = c_i bx = c_i b(x_1 + \cdots + x_n) = bc_i x_i.$$

Therefore, $bc_i \in \mathrm{Ann}(x_i) = \langle r_i \rangle$, and since $c_i \equiv 1 \pmod{\langle r_i \rangle}$, it follows that $r_i \mid b$ for $1 \leq i \leq n$. But $\{r_1, \ldots, r_n\}$ is pairwise relatively prime and thus a is the least common multiple of the set $\{r_1, \ldots, r_n\}$. We conclude that $a \mid b$, and hence, $\mathrm{Ann}(x) = \langle a \rangle$.

Conversely, suppose that $y \in M$ satisfies $\mathrm{Ann}(y) = \langle b \rangle = \left\langle \prod_{i=1}^n s_i \right\rangle$ where the set $\{s_1, \ldots, s_n\}$ is pairwise relatively prime. As in the above paragraph, apply the Chinese remainder theorem to get $c_1, \ldots, c_n \in R$ such that

$$c_i \equiv \begin{cases} 1 \pmod{\langle s_i \rangle}, \\ 0 \pmod{\langle s_j \rangle}, \quad \text{if } j \neq i. \end{cases}$$

Since b is the least common multiple of $\{s_1, \ldots, s_n\}$, it follows that

$$1 \equiv c_1 + \cdots + c_n \pmod{\langle b \rangle},$$

and hence, if we set $y_i = c_i y$, we have

$$y_1 + \cdots + y_n = (c_1 + \cdots + c_n)y = y.$$

Since $\langle b, c_i\rangle = \left\langle \prod_{j\neq i} s_j \right\rangle$, Lemma 7.17 shows that $\mathrm{Ann}(y_i) = \mathrm{Ann}(c_i y) = \langle s_i\rangle$. □

(7.19) Proposition. *Let R be a* PID *and suppose that M is a torsion R-module such that*

$$M \cong Rw_1 \oplus \cdots Rw_n$$

with $\mathrm{Ann}(w_i) = \langle t_i\rangle$. Then the prime power factors of the t_i $(1 \leq i \leq n)$ are the elementary divisors of M.

Proof. Let $p_1, \ldots, p_k$ be the set of distinct nonassociate primes that occur as a prime divisor of some t_i. Then we may write

$$\begin{aligned} t_1 &= u_1 p_1^{e_{11}} \cdots p_k^{e_{1k}} \\ &\vdots \\ t_n &= u_n p_1^{e_{n1}} \cdots p_k^{e_{nk}} \end{aligned} \tag{7.18}$$

where $u_1, \ldots, u_n$ are units in R and some of the exponents e_{ij} may be 0. The proof of Theorem 7.12 shows that

$$Rw_i \cong Rz_{i1} \oplus \cdots Rz_{ik}$$

where $\mathrm{Ann}(z_{ij}) = \langle p_j^{e_{ij}}\rangle$. For notational convenience we are allowing $z_{ij} = 0$ for those (i, j) with $e_{ij} = 0$. Therefore,

$$M \cong \bigoplus_{i,j} Rz_{ij} \tag{7.19}$$

where $\mathrm{Ann}(z_{ij}) = \langle p_j^{e_{ij}}\rangle$. Let $S = \{p_j^{e_{ij}}\}$ where we allow multiple occurrences of a prime power p^e, and let

$$\widetilde{S} = \{z_{ij}\}.$$

Let m be the maximum number of occurrences of positive powers of a single prime in S. If

$$f_{mj} = \max_{1\leq i\leq n} e_{ij} \qquad \text{for} \quad 1 \leq j \leq k, \tag{7.20}$$

we define

$$s_m = p_1^{f_{m1}} \cdots p_k^{f_{mk}}. \tag{7.21}$$

Note that $f_{mj} > 0$ for $1 \leq j \leq k$.

Delete $\{p_1^{f_{m1}}, \ldots, p_k^{f_{mk}}\}$ from the set S and repeat the above process with the remaining prime powers until no further positive prime powers are

available. Since a prime power for a particular prime p is used only once at each step, this will produce elements $s_1, \ldots, s_m \in R$. From the inductive description of the construction of s_i, it is clear that every prime dividing s_i also divides s_{i+1} to at least as high a power (because of Equation (7.21)). Thus,

$$s_i \mid s_{i+1} \qquad \text{for} \quad 1 \le i < m.$$

Therefore, we may write

$$\begin{aligned} s_1 &= u_1 p_1^{f_{11}} \cdots p_k^{f_{1k}} \\ &\vdots \\ s_m &= u_m p_1^{f_{m1}} \cdots p_k^{f_{mk}} \end{aligned} \tag{7.22}$$

where

$$\{p_j^{f_{ij}} : f_{ij} > 0\} = \{p_\beta^{e_{\alpha\beta}} : e_{\alpha\beta} > 0\} \tag{7.23}$$

where repetitions of prime powers are allowed and where

$$0 \le f_{1j} \le f_{2j} \le \cdots \le f_{mj} \qquad \text{for} \quad 1 \le j \le k \tag{7.24}$$

by Equation (7.20).

For each $p_j^{f_{ij}}$ $(1 \le i \le m)$, choose $w_{ij} \in \widetilde{S}$ with $\operatorname{Ann}(w_{ij}) = \langle p_j^{f_{ij}} \rangle$ and let $x_i = w_{i1} + \cdots + w_{ik}$. Lemma 7.18 shows that $\operatorname{Ann}(x_i) = \langle s_i \rangle$ for $1 \le i \le m$, and thus,

$$Rx_i \cong R/\langle s_i \rangle \cong \bigoplus_{j=1}^{k} R/\langle p_j^{f_{ij}} \rangle \cong \bigoplus_{j=1}^{k} Rw_{ij}.$$

Equation (7.19) then shows that

$$\begin{aligned} M &\cong \bigoplus_{\alpha,\beta} Rz_{\alpha\beta} \\ &\cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k} Rw_{ij} \right) \\ &\cong Rx_1 \oplus \cdots \oplus Rx_m \end{aligned}$$

where $\operatorname{Ann}(x_i) = \langle s_i \rangle$. Since $s_i \mid s_{i+1}$ for $1 \le i < m$, it follows that $\{s_1, \ldots, s_m\}$ are the invariant factors of M, and since the set of prime power factors of $\{s_1, \ldots, s_m\}$ (counting multiplicities) is the same as the set of prime power factors of $\{t_1, \ldots, t_n\}$ (see Equation (7.23)), the proof is complete. □

(7.20) Corollary. *Let R be a* PID*, let $M_1, \ldots, M_k$ be finitely generated torsion R-modules, and let $M = \oplus_{i=1}^{k} M_i$. If $\{d_{i1}, \ldots, d_{i\ell_i}\}$ is the set of elementary divisors of M_i, then*

$$S = \{d_{ij} : 1 \le i \le k; 1 \le j \le \ell_i\}$$

is the set of elementary divisors of M.

Proof. By Theorem 7.1,

$$M_i \cong Rw_{i1} \oplus \cdots \oplus Rw_{ir_i}$$

where $\mathrm{Ann}(w_{ij}) = \langle s_{ij} \rangle$ and $s_{ij} \mid s_{i,j+1}$ for $1 \le j \le r_i$. The elementary divisors of M_i are the prime power factors of $\{s_{i1}, \ldots, s_{ir_i}\}$. Then

$$M = \bigoplus_{i=1}^{k} M_i \cong \bigoplus_{i,j} Rw_{ij}$$

where $\mathrm{Ann}(w_{ij}) = \langle s_{ij} \rangle$. The result now follows from Proposition 7.19. □

(7.21) Proposition. *Let R be a* PID*, let $M_1, \ldots, M_k$ be finitely generated torsion R-modules, and let $M = \oplus_{i=1}^{k} M_i$. Then*

$$\mathrm{me}(M) = \mathrm{lcm}\{\mathrm{me}(M_1), \ldots, \mathrm{me}(M_k)\} \tag{7.25}$$

$$\mathrm{co}(M) = \prod_{i=1}^{k} \mathrm{co}(M_i). \tag{7.26}$$

Proof. Since $\mathrm{Ann}(M) = \bigcap_{i=1}^{k} \mathrm{Ann}(M_i)$, Equation (7.25) follows since $\langle \mathrm{me}(M_i) \rangle = \mathrm{Ann}(M_i)$. Since $\mathrm{co}(M)$ is the product of all invariant factors of M, which is also the product of all the elementary divisors of M, Equation (7.26) follows from Corollary 7.20. □

The special case $R = \mathbf{Z}$ is important enough to emphasize what the results mean in this case. Suppose that M is an abelian group, i.e., a $\mathbf{Z}$-module. Then an element $x \in M$ is torsion if and only if $nx = 0$ for some $n > 0$. That is to say, $x \in M_\tau$ if and only if $o(x) < \infty$. Moreover, $\mathrm{Ann}(x) = \langle n \rangle$ means that $o(x) = n$. Thus the torsion submodule of M consists of the set of elements of finite order. Furthermore, M is finitely generated and torsion if and only if M is a finite abelian group. Indeed, if $M = \langle x_1, \ldots, x_k \rangle$ then any $x \in M$ can be written $x = n_1 x_1 + \cdots + n_k x_k$ where $0 \le n_i \le o(x_i) < \infty$ for $1 \le i \le k$. Therefore, $|M| \le \prod_{i=1}^{k} o(x_i)$. Hence, the fundamental structure theorem for finitely generated abelian groups takes the following form.

(7.22) Theorem. *Any finitely generated abelian group M is isomorphic to $\mathbf{Z}^r \oplus M_1$ where $|M_1| < \infty$. The integer r is an invariant of M. Any finite abelian group is a direct sum of cyclic groups of prime power order and these prime power orders, counted with multiplicity, completely characterize*

the finite abelian group up to isomorpism. Also any finite abelian group is uniquely isomorphic to a group

$$\mathbf{Z}_{s_1} \times \cdots \times \mathbf{Z}_{s_k}$$

where $s_i \mid s_{i+1}$ *for all* i.

Proof. □

Given a natural number n it is possible to give a complete list of all abelian groups of order n, up to isomorphism, by writing $n = p_1^{r_1} \cdots p_k^{r_k}$ where $p_1, \ldots, p_k$ are the distinct prime divisors of n. Let M be an abelian group of order n. Then we may write M as a direct sum of its primary components

$$M \cong M_{p_1} \oplus \cdots \oplus M_{p_k}$$

where $|M_{p_i}| = p_i^{r_i}$. Then each primary component M_{p_i} can be written as a direct sum

$$M_{p_i} \cong \mathbf{Z}_{p_i^{e_{i1}}} \oplus \cdots \oplus \mathbf{Z}_{p_i^{e_{i\ell}}}$$

where

$$1 \leq e_{i1} \leq \cdots \leq e_{i\ell} \leq r_i$$

and

$$e_{i1} + \cdots + e_{i\ell} = r_i.$$

Furthermore, the main structure theorems state that M is determined up to isomorphism by the primes $p_1, \ldots, p_k$ and the partitions $e_{i1}, \ldots, e_{i\ell}$ of the exponents r_i. This is simply the statement that M is determined up to isomorphism by its elementary divisors. Therefore, to identify all abelian groups of order n, it is sufficient to identify all partitions of r_i, i.e., all ways to write $r_i = e_{i1} + \cdots + e_{i\ell}$ as a sum of natural numbers.

(7.23) Example. We will carry out the above procedure for $n = 600 = 2^3 \cdot 3 \cdot 5^2$. There are three primes, namely, 2, 3, and 5. The exponent of 2 is 3 and we can write $3 = 1 + 1 + 1$, $3 = 1 + 2$, and $3 = 3$. Thus there are three partitions of 3. The exponent of 3 is 1, so there is only one partition, while the exponent of 5 is 2, which has two partitions, namely, $2 = 1 + 1$ and $2 = 2$. Thus there are $3 \cdot 1 \cdot 2 = 6$ distinct, abelian groups of order 600. They are

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \cong \mathbf{Z}_2 \times \mathbf{Z}_{10} \times \mathbf{Z}_{30}$$

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_{25} \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{150}$$

$$\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \cong \mathbf{Z}_{10} \times \mathbf{Z}_{60}$$

$$\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_3 \times \mathbf{Z}_{25} \cong \mathbf{Z}_2 \times \mathbf{Z}_{300}$$

$$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \cong \mathbf{Z}_5 \times \mathbf{Z}_{120}$$

$$\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_{25} \cong \mathbf{Z}_{600}$$

where the groups on the right are expressed in invariant factor form and those on the left are decomposed following the elementary divisors.

We will conclude this section with the following result concerning the structure of finite subgroups of the multiplicative group of a field. This is an important result, which combines the structure theorem for finite abelian groups with a bound on the number of roots of a polynomial with coefficients in a field.

(7.24) Theorem. *Let F be a field and let $G \subseteq F^* = F \setminus \{0\}$ be a finite subgroup of the multiplicative group F^*. Then G is a cyclic group.*

Proof. According to Theorem 7.1, G is isomorphic to a direct sum

$$G \cong \langle z_1 \rangle \oplus \cdots \oplus \langle z_n \rangle$$

where, if we let $k_i = o(z_i) =$ order of z_i, then $k_i \mid k_{i+1}$ for $1 \leq i \leq n-1$ and

$$\mathrm{Ann}(G) = \mathrm{Ann}(z_n) = (k_n)\mathbf{Z}.$$

In the language of Definition 7.8, $\mathrm{me}(G) = k_n$. This means that $z^{k_n} = 1$ for all $z \in G$. Now consider the polynomial

$$P(X) = X^{k_n} - 1. \tag{7.27}$$

Since F is a field, the polynomial $P(X)$ has at most k_n roots, because degree $P(X) = k_n$ (Corollary 2.4.7). But, as we have observed, every element of G is a root of $P(X)$, and

$$|G| = k_1 k_2 \cdots k_n.$$

Thus, we must have $n = 1$ and $G \cong \langle z_1 \rangle$ is cyclic. □

(7.25) Corollary. *Suppose that F is a finite field with q elements. Then F^* is a cyclic group with $q-1$ elements, and every element of F is a root of the polynomial $X^q - X$.*

Proof. Exercise. □

(7.26) Corollary. *Let*

$$G_n = \{e^{2\pi i(k/n)} : 0 \leq k \leq n-1\} \subseteq \mathbf{C}^*.$$

Then G_n is the only subgroup of $\mathbf{C}^*$ of order n.

Proof. Let H be a finite subgroup of $\mathbf{C}^*$ with $|H| = n$. Then every element z of H has the property that $z^n = 1$. In other words, z is a root of the equation $X^n = 1$. Since this equation has at most n roots in $\mathbf{C}$ and since every element of G_n is a root of this equation, we have $z \in G_n$. Thus, we conclude that $H \subseteq G_n$ and hence $H = G_n$ because $n = |H| = |G_n|$. □

3.8 Complemented Submodules

We will now consider the problem of extending a linearly independent subset of a free R-module to a basis. The example $\{2\} \subseteq \mathbf{Z}$ shows that some restrictions on the basis are needed, while Theorem 6.16 shows that any primitive element of a finitely generated free R-module (R a PID) can be extended to a basis.

(8.1) Definition. *Let M be an R-module and $S \subseteq M$ a submodule. Then S is said to be* **complemented** *if there exists a submodule $T \subseteq M$ with $M \cong S \oplus T$.*

Let M be a finitely generated free R-module with basis $\{v_1, \ldots, v_n\}$ and let $S = \langle v_1, \ldots, v_s \rangle$. Then S is complemented by $T = \langle v_{s+1}, \ldots, v_n \rangle$. This example shows that if $W = \{w_1, \ldots, w_k\}$ is a linearly independent subset of M, then a necessary condition for W to extend to a basis of M is that the submodule $\langle W \rangle$ be complemented. If R is a PID, then the converse is also true. Indeed, let T be a complement of $\langle W \rangle$ in M. Since R is a PID, T is free, so let $\{x_1, \ldots, x_r\}$ be a basis of T. Then it is easy to check that $\{w_1, \ldots, w_k, x_1, \ldots, x_r\}$ is a basis of M.

(8.2) Proposition. *Let R be a* PID*, let M be a free R-module, and let S be a submodule. Consider the following conditions on S.*

(1) *S is complemented.*
(2) *M/S is free.*
(3) *If $x \in S$ and $x = ay$ for some $y \in M$, $a \neq 0 \in R$, then $y \in S$.*

Then (1) ⇒ (2) *and* (2) ⇒ (3)*, while if M is finitely generated, then* (3) ⇒ (1).

Proof. (1) ⇒ (2). If S is complemented, then there exists $T \subseteq M$ such that $S \oplus T \cong M$. Thus, $M/S \cong T$. But T is a submodule of a free module over a PID R, so T is free (Theorem 6.2).

(2) ⇒ (3). Suppose M/S is free. If $x \in S$ satisfies $x = ay$ for some $y \in M$, $a \neq 0 \in R$, then $a(y + S) = S$ in M/S. Since free modules are torsion-free, it follows that $y + S = S$, i.e., $y \in S$.

(3) $\Rightarrow$ (1). Let M be a finite rank free R-module and let $S \subseteq M$ be a submodule satisfying condition (3). Then there is a short exact sequence

$$0 \longrightarrow S \longrightarrow M \xrightarrow{\pi} M/S \longrightarrow 0 \tag{8.1}$$

where π is the projection map. Condition (3) is equivalent to the statement that M/S is torsion-free, so M/S is free by Theorem 6.6. But free modules are projective, so sequence (8.1) has a splitting $\alpha : M/S \to M$ and Theorem 3.9 shows that $M \cong S \oplus \mathrm{Im}(\alpha)$, i.e., S is complemented. □

(8.3) *Remarks.*

(1) A submodule S of M that satisfies condition (3) of Proposition 8.2 is called a **pure submodule** of M. Thus, a submodule of a finitely generated module over a PID is pure if and only if it is complemented.

(2) If R is a field, then *every* subspace $S \subseteq M$ satisfies condition (3) so that every subspace of a finite-dimensional vector space is complemented. Actually, this is true without the finite dimensionality assumption, but our argument has only been presented in the more restricted case. The fact that arbitrary subspaces of vector spaces are complemented follows from Corollary 4.21.

(3) The implication (3) $\Rightarrow$ (1) is false without the hypothesis that M be finitely generated. As an example, consider a free presentation of the $\mathbf{Z}$-module $\mathbf{Q}$:

$$0 \longrightarrow S \longrightarrow M \longrightarrow \mathbf{Q} \longrightarrow 0.$$

Since $M/S \cong \mathbf{Q}$ and $\mathbf{Q}$ is torsion-free, it follows that S satisfies condition (3) of Proposition 8.1. However, if S is complemented, then a complement $T \cong \mathbf{Q}$; so $\mathbf{Q}$ is a submodule of a free $\mathbf{Z}$-module M, and hence $\mathbf{Q}$ would be free, but $\mathbf{Q}$ is not a free $\mathbf{Z}$-module.

(8.4) Corollary. *If S is a complemented submodule of a finitely generated R-module (R a* PID*), then any basis for S extends to a basis for M.*

Proof. This was observed prior to Proposition 8.2. □

(8.5) Corollary. *If S is a complemented submodule of M, then* $\operatorname{rank} S = \operatorname{rank} M$ *if and only if $S = M$.*

Proof. A basis $\{v_1, \ldots, v_m\}$ of S extends to a basis $\{v_1, \ldots, v_n\}$ of M. But $n = m$, so $S = \langle v_1, \ldots, v_n \rangle = M$. □

If $M = \mathbf{Z}$ and $S = \langle 2 \rangle$, then $\operatorname{rank} S = \operatorname{rank} M$ but $M \neq S$. Of course, S is not complemented.

(8.6) Corollary. *If S is a complemented submodule of M, then*

$$\operatorname{rank} M = \operatorname{rank} S + \operatorname{rank}(M/S).$$

Proof. Let $S = \langle v_1, \ldots, v_m \rangle$ where $m = \operatorname{rank} S$. Extend this to a basis $\{v_1, \ldots, v_n\}$ of M. Then $T = \langle v_{m+1}, \ldots, v_n \rangle$ is a complement of S in M and $T \cong M/S$. Thus,

$$\operatorname{rank} M = n = m + (n - m) = \operatorname{rank} S + \operatorname{rank}(M/S).$$

□

(8.7) Proposition. *Let R be a* PID *and let $f : M \to N$ be an R-module homomorphism of finite rank free R-modules. Then*

(1) $\operatorname{Ker}(f)$ *is a pure submodule, but*
(2) $\operatorname{Im}(f)$ *need not be pure.*

Proof. (1) Suppose $x \in \operatorname{Ker}(f)$, $a \neq 0 \in R$, and $y \in M$ with $x = ay$. Then $0 = f(x) = f(ay) = af(y)$. But N is free and, hence, torsion-free so that $f(y) = 0$. Hence, condition (3) of Proposition 8.2 is satisfied, so $\operatorname{Ker}(f)$ is complemented.

(2) If $f : \mathbf{Z} \to \mathbf{Z}$ is defined by $f(x) = 2x$, then $\operatorname{Im}(f) = 2\mathbf{Z}$ is not a complemented submodule of $\mathbf{Z}$. □

(8.8) Proposition. *Let R be a* PID *and let $f : M \to N$ be an R-module homomorphism of finite rank free R-modules. Then*

$$\operatorname{rank} M = \operatorname{rank}(\operatorname{Ker}(f)) + \operatorname{rank}(\operatorname{Im}(f)).$$

Proof. By the first isomorphism theorem, $\operatorname{Im}(f) \cong M/\operatorname{Ker}(f)$. But $\operatorname{Ker}(f)$ is a complemented submodule of M, so the result follows from Corollary 8.6. □

(8.9) Corollary. *Let R be a* PID *and let M and N be finite rank free R-modules with* $\operatorname{rank}(M) = \operatorname{rank}(N)$. *Let $f \in \operatorname{Hom}_R(M, N)$.*

(1) *If f is a surjection, then f is an isomorphism.*
(2) *If f is an injection and* $\operatorname{Im}(f)$ *is complemented, then f is an isomorphism.*

Proof. (1) By Proposition 8.8, $\operatorname{rank}(\operatorname{Ker}(f)) = 0$, i.e., $\operatorname{Ker}(f) = \langle 0 \rangle$, so f is an injection.

(2) By Proposition 8.8, $\operatorname{rank} N = \operatorname{rank} M = \operatorname{rank}(\operatorname{Im}(f))$. Since $\operatorname{Im}(f)$ is complemented by hypothesis, f is a surjection by Corollary 8.5. □

(8.10) Proposition. *Let R be a field and let M and N be R-modules with* $\operatorname{rank}(M) = \operatorname{rank}(N)$ *finite. Let $f \in \operatorname{Hom}_R(M, N)$. Then the following are equivalent.*

(1) *f is an isomorphism.*

(2) *f is an injection.*
(3) *f is a surjection.*

Proof. Since R is a field, $\mathrm{Im}(f)$ is complemented (by Remark 8.3 (2)), so this is an immediate consequence of Corollary 8.9. □

(8.11) Proposition. *Let M be a finite rank free R-module (R a* PID*). If S and T are pure submodules, then*

$$\operatorname{rank}(S+T) + \operatorname{rank}(S \cap T) = \operatorname{rank} S + \operatorname{rank} T.$$

Proof. Note that if S and T are pure submodules of M, then $S \cap T$ is also pure. Indeed, if $ay \in S \cap T$ with $a \neq 0 \in R$, then $y \in S$ and $y \in T$ since these submodules are pure. Thus, $y \in S \cap T$, so $S \cap T$ is complemented by Proposition 8.2. Then

$$(S+T)/T \cong S/(S \cap T).$$

By Corollary 8.6, we conclude

$$\operatorname{rank}(S+T) - \operatorname{rank}(T) = \operatorname{rank}(S) - \operatorname{rank}(S \cap T).$$

□

(8.12) *Remark.* It need not be true that $S+T$ is pure, even if S and T are both pure. For example, let $S = \langle (1,\,1) \rangle \subseteq \mathbf{Z}^2$ and let $T = \langle (1,\,-1) \rangle \subseteq \mathbf{Z}^2$. Then S and T are both pure, but $S+T \neq \mathbf{Z}^2$, so it cannot be pure. In fact, $2 \cdot (1,\,0) = (2,\,0) = (1,\,1) + (1,\,-1) \in S+T$, but $(1,\,0) \notin S+T$.

3.9 Exercises

1. If M is an abelian group, then $\mathrm{End}_{\mathbf{Z}}(M)$, the set of abelian group endomorphisms of M, is a ring under addition and composition of functions.
   (a) If M is a left R-module, show that the function $\phi : R \to \mathrm{End}_{\mathbf{Z}}(M)$ defined by $\phi(r)(m) = rm$ is a ring homomorphism. Conversely, show that any ring homomorphism $\phi : R \to \mathrm{End}_{\mathbf{Z}}(M)$ determines a left R-module structure on M.
   (b) Show that giving a right R-module structure on M is the same as giving a ring homomorphism $\phi : R^{\mathrm{op}} \to \mathrm{End}_{\mathbf{Z}}(M)$.
2. Show that an abelian group G admits the structure of a $\mathbf{Z}_n$-module if and only if $nG = \langle 0 \rangle$.
3. Show that the subring $\mathbf{Z}[\frac{p}{q}]$ of $\mathbf{Q}$ is not finitely generated as a $\mathbf{Z}$-module if $\frac{p}{q} \notin \mathbf{Z}$.
4. Let M be an S-module and suppose that $R \subseteq S$ is a subring. Then M is also an R-module by Example 1.5 (10). Suppose that $N \subseteq M$ is an R-submodule. Show that the S-submodule of M generated by N is the set

$$SN = \{sn : s \in S,\ n \in N\}.$$

5. Let M be an R-module and let A, B, and C be submodules. If $C \subseteq A$, prove that
$$A \cap (B + C) = (A \cap B) + C.$$
This equality is known as the *modular law*. Show, by example, that this formula need not hold if C is not contained in A.
6. Let R be a commutative ring and let $S \subseteq R$ be a multiplicatively closed subset of R containing no zero divisors. Let M be an R-module. Mimicking the construction of R_S (Theorem 2.3.5), we define M_S as follows. Define a relation $\sim$ on $M \times S$ by setting $(x, s) \sim (y, t)$ if and only if $tx = sy$. This is easily seen to be an equivalence relation (as in the proof of Theorem 2.3.5), and we will denote the equivalence class of (x, s) by the suggestive symbol x/s.
(a) Prove that M_S is an R_S-module via the operation $(a/s)(x/t) = (ax)/(st)$.
(b) If $f : M \to N$ is an R-module homomorhism, show that
$$f_S : M_S \to N_S$$
defined by $f_S(x/s) = f(x)/s$ is an R_S-module homomorphism.
7. Let $R \subseteq F[X]$ be the subring
$$R = \{f(X) \in F[X] : f(X) = a_0 + a_2X^2 + \cdots + a_nX^n\}.$$
Thus, $f(X) \in R$ if and only if the coefficient of X is 0. Show that $F[X]$ is a finitely generated R-module that is torsion-free but not free.
8. Show that $\mathbf{Q}$ is a torsion-free $\mathbf{Z}$-module that is not free.
9. (a) Let R be an integral domain, let M be a torsion R-module, and let N be a torsion-free R-module. Show that $\mathrm{Hom}_R(M, N) = \langle 0 \rangle$.
(b) According to part (a), $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_m, \mathbf{Z}) = \langle 0 \rangle$. If $n = km$, then $\mathbf{Z}_m$ is a $\mathbf{Z}_n$-module. Show that
$$\mathrm{Hom}_{\mathbf{Z}_n}(\mathbf{Z}_m, \mathbf{Z}_n) \cong \mathbf{Z}_m.$$
10. Let R be a commutative ring with 1 and let I and J be ideals of R. Prove that $R/I \cong R/J$ as R-modules if and only if $I = J$. Suppose we only ask that R/I and R/J be isomorphic rings. Is the same conclusion valid? (Hint: Consider $F[X]/(X - a)$ where $a \in F$ and show that $F[X]/(X - a) \cong F$ as rings.)
11. Prove Theorem 2.7.
12. Prove Lemma 2.9.
13. Let M be an R-module and let $f \in \mathrm{End}_R(M)$ be an idempotent endomorphism of M, i.e., $f \circ f = f$. (That is, f is an idempotent element of the ring $\mathrm{End}_R(M)$.) Show that
$$M \cong (\mathrm{Ker}(f)) \oplus (\mathrm{Im}(f)).$$
14. Prove the remaining cases in Theorem 3.10.
15. Let R be a PID and let a and $b \in R$ be nonzero elements. Then show that $\mathrm{Hom}_R(R/Ra, R/Rb) \cong R/Rd$ where $d = (a, b)$ is the greatest common divisor of a and b.
16. Compute $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Q}, \mathbf{Z})$.
17. Give examples of short exact sequences of R-modules
$$0 \longrightarrow M_1 \xrightarrow{\phi} M \xrightarrow{\phi'} M_2 \longrightarrow 0$$

and

$$0 \longrightarrow N_1 \xrightarrow{\psi} N \xrightarrow{\psi'} N_2 \longrightarrow 0$$

such that
(a) $M_1 \cong N_1$, $M \cong N$, $M_2 \ncong N_2$;
(b) $M_1 \cong N_1$, $M \ncong N$, $M_2 \cong N_2$;
(c) $M_1 \ncong N_1$, $M \cong N$, $M_2 \cong N_2$.

18. Show that there is a split exact sequence

$$0 \longrightarrow m\mathbf{Z}_{mn} \longrightarrow \mathbf{Z}_{mn} \longrightarrow n\mathbf{Z}_{mn} \longrightarrow 0$$

of $\mathbf{Z}_{mn}$-modules if and only if $(m, n) = 1$.

19. Let N_1 and N_2 be submodules of an R-module M. Show that there is an exact sequence

$$0 \longrightarrow N_1 \cap N_2 \xrightarrow{\psi} N_1 \oplus N_2 \xrightarrow{\phi} N_1 + N_2 \longrightarrow 0$$

where $\psi(x) = (x, x)$ and $\phi(x, y) = x - y$.

20. Let R be an integral domain and let a and b be nonzero elements of R. Let $M = R/R(ab)$ and let $N = Ra/R(ab)$. Then M is an R-module and N is a submodule. Show that N is a complemented submodule in M if and only if there are $u, v \in R$ such that $ua + vb = 1$.

21. Let R be a ring, M a finitely generated R-module, and $\phi : M \to R^n$ a surjective R-module homomorphism. Show that $\mathrm{Ker}(\phi)$ is finitely generated. (Note that this is valid even when M has submodules that are not finitely generated.) (Hint: Consider the short exact sequence:

$$0 \longrightarrow K \longrightarrow M \xrightarrow{\phi} R^n \longrightarrow 0.\ )$$

22. Suppose that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\phi} & M & \xrightarrow{\phi'} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{\psi} & N & \xrightarrow{\psi'} & N_2 & \longrightarrow & 0 \end{array}$$

is a commutative diagram of R-modules and R-module homomorphisms. Assume that the rows are exact and that f and h are isomorphisms. Then prove that g is an isomorphism.

23. Let R be a commutative ring and S a multiplicatively closed subset of R containing no zero divisors. If M is an R-module, then M_S was defined in Exercise 6. Prove that the operation of forming quotients with elements of S is exact. Precisely:

    (a) Suppose that $M' \xrightarrow{f} M \xrightarrow{g} M''$ is a sequence of R-modules and homomorphisms which is exact at M. Show that the sequence

    $$M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$$

    is an exact sequence of R_S-modules and homomorphisms.
    (b) As a consequence of part (a), show that if M' is a submodule of M, then M'_S can be identified with an R_S-submodule of M_S.
    (c) If N and P are R-submodules of M, show (under the identification of part (b)) that $(N + P)_S = N_S + P_S$ and $(N \cap P)_S = N_S \cap P_S$. (That is, formation of fractions commutes with finite sums and finite intersections.)
    (d) If N is a submodule of M show that

$$(M/N)_S \cong (M_S)/(N_S).$$

(That is, formation of fractions commutes with quotients.)

24. Let F be a field and let $\{f_i(X)\}_{i=0}^{\infty}$ be any subset of $F[X]$ such that $\deg f_i(X) = i$ for each i. Show that $\{f_i(X)\}_{i=0}^{\infty}$ is a basis of $F[X]$ as an F-module.

25. Let R be a commutative ring and consider $M = R[X]$ as an R-module. Then $N = R[X^2]$ is an R-submodule. Show that M/N is isomorphic to $R[X]$ as an R-module.

26. Let G be a group and H a subgroup. If $\mathbf{F}$ is a field, then we may form the group ring $\mathbf{F}(G)$ (Example 2.1.9 (15)). Since $\mathbf{F}(G)$ is a ring and $\mathbf{F}(H)$ is a subring, we may consider $\mathbf{F}(G)$ as either a left $\mathbf{F}(H)$-module or a right $\mathbf{F}(H)$-module. As either a left or right $\mathbf{F}(H)$-module, show that $\mathbf{F}(G)$ is free of rank $[G : H]$. (Use a complete set $\{g_i\}$ of coset representatives of H as a basis.)

27. Let R and S be integral domains and let $\phi_1, \ldots, \phi_n$ be n distinct ring homomorphisms from R to S. Show that $\phi_1, \ldots, \phi_n$ are S-linearly independent in the S-module $F(R, S)$ of all functions from R to S. (Hint: Argue by induction on n, using the property $\phi_i(ax) = \phi_i(a)\phi_i(x)$, to reduce from a dependence relation with n entries to one with $n - 1$ entries.)

28. Let G be a group, let F be a field, and let $\phi_i : G \to F^*$ for $1 \leq i \leq n$ be n distinct group homomorphisms from G into the multiplicative group F^* of F. Show that $\phi_1, \ldots, \phi_n$ are linearly independent over F (viewed as elements of the F-module of all functions from G to F). (Hint: Argue by induction on n, as in Exercise 27.)

29. Let $R = \mathbf{Z}_{30}$ and let $A \in M_{2,3}(R)$ be the matrix

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{bmatrix}.$$

Show that the two rows of A are linearly independent over R, but that any two of the three columns are linearly dependent over R.

30. Let V be a finite-dimensional complex vector space. Then V is also a vector space over $\mathbf{R}$. Show that $\dim_{\mathbf{R}} V = 2 \dim_{\mathbf{C}} V$. (Hint: If

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

is a basis of V over $\mathbf{C}$, show that

$$\mathcal{B}' = \{v_1, \ldots, v_n, iv_1, \ldots, iv_n\}$$

is a basis of V over $\mathbf{R}$.)

31. Extend Exercise 30 as follows. Let L be a field and let K be a subfield of L. If V is a vector space over L, then it is also a vector space over K. Prove that

$$\dim_K V = [L : K] \dim_L V$$

where $[L : K] = \dim_K L$ is the dimension of L as a vector space over K. (Note that we are *not* assuming that $\dim_K L < \infty$.)

32. Let $K \subseteq L$ be fields and let V be a vector space over L. Suppose that $\mathcal{B} = \{u_\alpha\}_{\alpha \in \Gamma}$ is a basis of V as an L-module, and let W be the K-submodule of V generated by $\mathcal{B}$. Let $U \subseteq W$ be any K-submodule. Then, by Exercise 2,

$$LU = \{tu : t \in L, u \in U\}$$

is the L-submodule of V generated by U. Prove that

$$LU \cap W = U.$$

That is, taking L-linear combinations of elements of U does not produce any new elements of W.

33. Let $K \subseteq L$ be fields and let $A \in M_n(K)$, $b \in M_{n,1}(K)$. Show that the matrix equation $AX = b$ has a solution $X \in M_{n,1}(K)$ if and only if it has a solution $X \in M_{n,1}(L)$.

34. Prove that the Lagrange interpolation polynomials (Proposition 2.4.10) and the Newton interpolation polynomials (Remark 2.4.11) each form a basis of the vector space $\mathcal{P}_n(F)$ of polynomials of degree $\leq n$ with coefficients from F.

35. Let $\mathcal{F}$ denote the set of all functions from $\mathbf{Z}^+$ to $\mathbf{Z}^+$, and let M be the free $\mathbf{Q}$-module with basis $\mathcal{F}$. Define a multiplication on M by the formula $(fg)(n) = f(n) + g(n)$ for all $f, g \in \mathcal{F}$ and extend this multiplication by linearity to all of M. Let f_m be the function $f_m(n) = \delta_{m,n}$ for all $m, n \geq 0$. Show that each f_m is irreducible (in fact, prime) as an element of the ring R. Now consider the function $f(n) = 1$ for all $n \geq 0$. Show that f does not have a factorization into irreducible elements in M. (Hint: It may help to think of f as the "infinite monomial"

$$X_0^{f(0)} X_1^{f(1)} \cdots X_m^{f(m)} \cdots.)$$

(Compare this exercise with Example 5.13 (4).)

36. Let F be a field, and let

$$\mathcal{I} = \{p_\alpha(X) : p_\alpha(X) \text{ is an irreducible monic polynomial in } F[X]\}.$$

We will say that a rational function $h(X) = f(X)/g(X) \in F(X)$ is *proper* if $\deg(f(X)) < \deg(g(X))$. Let $F(X)_{\mathrm{pr}}$ denote the set of all proper rational functions in $F[X]$.

(a) Prove that $F(X) \cong F[X] \oplus F(X)_{\mathrm{pr}}$ as F-modules.

(b) Prove that

$$\mathcal{B} = \left\{ \frac{X^j}{(p_\alpha(X))^k} : p_\alpha(X) \in \mathcal{I}; 1 \leq j < k \deg(p_\alpha(X)) \right\}$$

is a basis of $F(X)$ as an F-module. The expansion of a rational function with respect to the basis $\mathcal{B}$ is known as the *partial fraction expansion*; it should be familiar from elementary calculus.

37. Prove that $\mathbf{Q}$ is not a projective $\mathbf{Z}$-module.

38. Let

$$R = \{f : [0, 1] \to \mathbf{R} : \quad f \text{ is continuous and } f(0) = f(1)\}$$

and let

$$M = \{f : [0, 1] \to \mathbf{R} : \quad f \text{ is continuous and } f(0) = -f(1)\}.$$

Then R is a ring under addition and multiplication of functions, and M is an R-module. Show that M is a projective R-module that is not free. (Hint: Show that $M \oplus M \cong R \oplus R$.)

39. Show that submodules of projective modules need not be projective. (Hint: Consider $p\mathbf{Z}_{p^2} \subseteq \mathbf{Z}_{p^2}$ as $\mathbf{Z}_{p^2}$-modules.) Over a PID, show that submodules of projective modules are projective.

40. (a) If R is a Dedekind domain, prove that R is Noetherian.
(b) If R is an integral domain that is a local ring (i.e., R has a unique maximal ideal), show that any invertible ideal I of R is principal.
(c) Let R be an integral domain and $S \subseteq R \setminus \{0\}$ a multiplicatively closed subset. If I is an invertible ideal of R, show that I_S is an invertible ideal of R_S.

(d) Show that in a Dedekind domain R, every nonzero prime ideal is maximal. (Hint: Let M be a maximal ideal of R containing a prime ideal P, and let $S = R \setminus M$. Apply parts (b) and (c).)

41. Show that $\mathbf{Z}[\sqrt{-3}]$ is not a Dedekind domain.

42. Show that $\mathbf{Z}[X]$ is not a Dedekind domain. More generally, let R be any integral domain that is not a field. Show that $R[X]$ is not a Dedekind domain.

43. Suppose R is a PID and $M = R\langle x\rangle$ is a cyclic R-module with $\operatorname{Ann} M = \langle a\rangle \neq \langle 0\rangle$. Show that if N is a submodule of M, then N is cyclic with $\operatorname{Ann} N = \langle b\rangle$ where b is a divisor of a. Conversely, show that M has a unique submodule N with annihilator $\langle b\rangle$ for each divisor b of a.

44. Let R be a PID, M an R-module, $x \in M$ with $\operatorname{Ann}(x) = \langle a\rangle \neq \langle 0\rangle$. Factor $a = up_1^{n_1} \cdots p_k^{n_k}$ with u a unit and $p_1, \ldots, p_k$ distinct primes. Let $y \in M$ with $\operatorname{Ann}(y) = \langle b\rangle \neq \langle 0\rangle$, where $b = u'p_1^{m_1} \cdots p_k^{m_k}$ with $0 \leq m_i < n_i$ for $1 \leq i \leq k$. Show that $\operatorname{Ann}(x + y) = \langle a\rangle$.

45. Let R be a PID, let M be a free R-module of finite rank, and let $N \subseteq M$ be a submodule. If M/N is a torsion R-module, prove that $\operatorname{rank}(M) = \operatorname{rank}(N)$.

46. Let R be a PID and let M and N be free R-modules of the same finite rank. Then an R-module homomorphism $f : M \to N$ is an injection if and only if $N/\operatorname{Im}(f)$ is a torsion R-module.

47. Let $u = (a, b) \in \mathbf{Z}^2$.
    (a) Show that there is a basis of $\mathbf{Z}^2$ containing u if and only if a and b are relatively prime.
    (b) Suppose that $u = (5, 12)$. Find a $v \in \mathbf{Z}^2$ such that $\{u, v\}$ is a basis of $\mathbf{Z}^2$.

48. Let M be a torsion module over a PID R and assume $\operatorname{Ann}(M) = (a) \neq (0)$. If $a = p_1^{r_1} \cdots p_k^{r_k}$ where $p_1, \ldots, p_k$ are the distinct prime factors of a, then show that $M_{p_i} = q_i M$ where $q_i = a/p_i^{r_i}$. Recall that if $p \in R$ is a prime, then M_p denotes the p-primary component of M.

49. Let M be a torsion-free R-module over a PID R, and assume that $x \in M$ is a primitive element. If $px = qx'$ show that $q \mid p$.

50. Find a basis and the invariant factors for the submodule of $\mathbf{Z}^3$ generated by $x_1 = (1, 0, -1)$, $x_2 = (4, 3, -1)$, $x_3 = (0, 9, 3)$, and $x_4 = (3, 12, 3)$.

51. Find a basis for the submodule of $\mathbf{Q}[X]^3$ generated by

$$f_1 = (2X-1, X, X^2+3), \qquad f_2 = (X, X, X^2), \qquad f_3 = (X+1, 2X, 2X^2-3).$$

52. Determine the structure of $\mathbf{Z}^3/K$ where K is generated by $x_1 = (2, 1, -3)$ and $x_2 = (1, -1, 2)$.

53. Let $R = \mathbf{R}[X]$ and suppose that M is a direct sum of cyclic R-modules with annihilators $(X-1)^3$, $(X^2+1)^2$, $(X-1)(X^2+1)^4$, and $(X+2)(X^2+1)^2$. Determine the elementary divisors and invariant factors of M.

54. Let R be a PID and let $p \in R$ be a prime. Show that submodules, quotient modules, and direct sums of p-primary modules are p-primary.

55. An R-module M is said to be *irreducible* if $\langle 0\rangle$ and M are the only submodules of M. Show that a torsion module M over a PID R is irreducible if and only if $M = R\langle x\rangle$ where $\operatorname{Ann}(x) = \langle p\rangle$ where p is prime. Show that if M is finitely generated, then M is *indecomposable* in the sense that M is not a direct sum of two nonzero submodules if and only if $M = R\langle x\rangle$ where $\operatorname{Ann}(x) = \langle 0\rangle$ or $\operatorname{Ann}(z) = \langle p^e\rangle$ where p is a prime.

56. Let M be an R-module where R is a PID. We say that M is *divisible* if for each nonzero $a \in R$, $aM = M$.
    (a) Show that $\mathbf{Q}$ is a divisible $\mathbf{Z}$-module.

(b) Show that any quotient of a divisible R-module is divisible. It follows for example that $\mathbf{Q}/\mathbf{Z}$ is a divisible $\mathbf{Z}$-module.
(c) If R is not a field, show that no finitely generated R-module is divisible.

57. Determine all nonisomorphic abelian groups of order 360.

58. Use elementary divisors to describe all abelian groups of order 144 and 168.

59. Use invariant factors to describe all abelian groups of orders 144 and 168.

60. If p and q are distinct primes, use invariant factors to describe all abelian groups of order
(a) p^2q^2,
(b) p^4q,
(c) p^5.

61. If p and q are distinct primes, use elementary divisors to describe all abelian groups of order p^3q^2.

62. Let G, H, and K be finitely generated abelian groups. If $G \times K \cong H \times K$, show that $G \cong H$. Show by example that this need not be true if we do not assume that the groups are finitely generated.

63. Determine all integers for which there exists a unique abelian group of order n.

64. Show that two finite abelian groups are isomorphic if and only if they have the same number of elements of each order.

65. An abelian group G has exactly 3 elements of order 2. Determine the isomorphism class of G.

66. Find a generator for the cyclic group F^* where F is each of the following fields (see Example 2.5.15 (3)):
(a) $\mathbf{F}_2[X]/\langle X^2 + X + 1\rangle$.
(b) $\mathbf{F}_3[X]/\langle X^2 + 1\rangle$.

67. Let
$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_{n+1} \longrightarrow 0$$
be an exact sequence of finite rank free modules and homomorphisms over a PID R. That is, f_1 is injective, f_n is surjective, and $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ for $1 \leq i \leq n-1$. Show that
$$\sum_{i=1}^{n+1} (-1)^{i+1} \operatorname{rank}(M_i) = 0.$$

68. If $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$, the degree of f is the highest degree of a monomial in f with nonzero coefficient, where
$$\deg(X_1^{i_1} \cdots X_n^{i_n}) = i_1 + \cdots + i_n.$$
Let F be a field. Given any five points $\{v_1, \ldots, v_5\} \subseteq F^2$, show that there is a quadratic polynomial $f(X_1, X_2) \in F[X_1, X_2]$ such that $f(v_i) = 0$ for $1 \leq i \leq 5$.

69. Let M and N be finite rank R-modules over a PID R and let $f \in \mathrm{Hom}_R(M, N)$. If $S \subseteq N$ is a complemented submodule of N, show that $f^{-1}(S)$ is a complemented submodule of M.

70. Let R be a PID, and let $f : M \to N$ be an R-module homomorphism of finite rank free R-modules. If $S \subseteq N$ is a submodule, prove that
$$\operatorname{rank}(f^{-1}(S)) = \operatorname{rank}(S \cap \mathrm{Im}(f)) + \operatorname{rank}(\mathrm{Ker}(f)).$$

71. Let $M_1 \xrightarrow{f} M \xrightarrow{g} M_2$ be a sequence of finite rank R-modules and R-module homomorphisms, where R is a PID.
(a) Show that

$$\operatorname{rank}(\operatorname{Im}(g \circ f)) = \operatorname{rank}(\operatorname{Im}(f)) - \operatorname{rank}(\operatorname{Im}(f) \cap \operatorname{Ker}(g)).$$

(b) If $\operatorname{Im}(f)$ is a complemented submodule of M, show that

$$\operatorname{rank}(\operatorname{Im}(g \circ f)) = \operatorname{rank}(\operatorname{Im}(f) + \operatorname{Ker}(g)) - \operatorname{rank}(\operatorname{Ker}(g)).$$

If R is a field, then all submodules of R-modules are complemented, so this formlula is always valid in the case of vector spaces and linear transformations. Show, by example, that this formula need not be valid if $\operatorname{Im}(f)$ is not complemented.

72. Let R be a PID, and let M, N, and P be finite rank free R-modules. Let $f : M \to N$ and $g : M \to P$ be homomorphisms. Suppose that $\operatorname{Ker}(f) \subseteq \operatorname{Ker}(g)$ and $\operatorname{Im}(f)$ is a complemented submodule of N. Then show that there is a homomorphism $h : N \to P$ such that $g = h \circ f$.

73. Let F be a field and let V be a vector space over F. Suppose that f, $g \in V^* = \operatorname{Hom}_F(V, F)$ such that $\operatorname{Ker}(f) \subseteq \operatorname{Ker}(g)$. Show that there is $a \in F$ such that $g = af$. Is this same result true if F is replaced by a PID?

74. Let R be a PID and let M be a finite rank free R-module. Let $\mathcal{C}_k(M)$ denote the set of complemented submodules of M of rank k. Let G be the group of units of the ring $\operatorname{End}_R(M)$.
(a) Show that $(\phi, N) \mapsto \phi(N)$ determines an action of the group G on the set $\mathcal{C}_k(M)$.
(b) Show that the action defined in part (a) is transitive, i.e., given N_1, $N_2 \in \mathcal{C}_k(M)$ there is $\phi \in G$ that sends N_1 to N_2.