The main purpose of this chapter is to prove a structure theorem for finitely generated modules over particularly nice rings, namely Principal Ideal Domains. This theorem is an example of the ideal structure of the ring (which is particularly simple for P.I.D.s) being reflected in the structure of its modules. If we apply this result in the case where the P.I.D. is the ring of integers $\mathbb{Z}$ then we obtain a proof of the Fundamental Theorem of Finitely Generated Abelian Groups (which we examined in Chapter 5 without proof). If instead we apply this structure theorem in the case where the P.I.D. is the ring $F[x]$ of polynomials in $x$ with coefficients in a field $F$ we shall obtain the basic results on the so-called rational and Jordan canonical forms for a matrix. Before proceeding to the proof we briefly discuss these two important applications.

We have already discussed in Chapter 5 the result that any finitely generated abelian group is isomorphic to the direct sum of cyclic abelian groups, either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some positive integer $n \neq 0$. Recall also that an abelian group is the same thing as a $\mathbb{Z}$-module. Since the ideals of $\mathbb{Z}$ are precisely the trivial ideal $(0)$ and the principal ideals $(n) = n\mathbb{Z}$ generated by positive integers $n$, we see that the Fundamental Theorem of Finitely Generated Abelian Groups in the language of modules says that any finitely generated $\mathbb{Z}$-module is the direct sum of modules of the form $\mathbb{Z}/I$ where $I$ is an ideal of $\mathbb{Z}$ (these are the cyclic $\mathbb{Z}$-modules), together with a uniqueness statement when the direct sum is written in a particular form. Note the correspondence between the ideal structure of $\mathbb{Z}$ and the structure of its (finitely generated) modules, the finitely generated abelian groups.

The Fundamental Theorem of Finitely Generated Modules over a P.I.D. states that the same result holds when the Principal Ideal Domain $\mathbb{Z}$ is replaced by any P.I.D. In particular, we have seen in Chapter 10 that a module over the ring $F[x]$ of polynomials in $x$ with coefficients in the field $F$ is the same thing as a vector space $V$ together with a fixed linear transformation $T$ of $V$ (where the element $x$ acts on $V$ by the linear transformation $T$). The Fundamental Theorem in this case will say that such a vector space is the direct sum of modules of the form $F[x]/I$ where $I$ is an ideal of $F[x]$, hence is either the trivial ideal $(0)$ or a principal ideal $(f(x))$ generated by some nonzero polynomial $f(x)$ (these are the cyclic $F[x]$-modules), again with a uniqueness statement when the direct sum is written in a particular form. If this is translated back into the language of vector spaces and linear transformations we can obtain information on the
linear transformation $T$.

For example, suppose $V$ is a vector space of dimension $n$ over $F$ and we choose a basis for $V$. Then giving a linear transformation $T$ of $V$ to itself is the same thing as giving an $n \times n$ matrix $A$ with coefficients in $F$ (and choosing a different basis for $V$ gives a different matrix $B$ for $T$ which is similar to $A$ i.e., is of the form $P^{-1}AP$ for some invertible matrix $P$ which defines the change of basis). We shall see that the Fundamental Theorem in this situation implies (under the assumption that the field $F$ contains all the "eigenvalues" for the given linear transformation $T$) that there is a basis for $V$ so that the associated matrix for $T$ is as close to being a diagonal matrix as possible and so has a particularly simple form. This is the Jordan canonical form. The rational canonical form is another simple form for the matrix for $T$ (that does not require the eigenvalues for $T$ to be elements of $F$). In this way we shall be able to give canonical forms for arbitrary $n \times n$ matrices over fields $F$, that is, find matrices which are similar to a given $n \times n$ matrix and which are particularly simple (almost diagonal, for example).

Example

Let $V = \mathbb{Q}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{Q}\}$ be the usual 3-dimensional vector space of ordered 3-tuples with entries from the field $F = \mathbb{Q}$ of rational numbers and suppose $T$ is the linear transformation

$$T(x, y, z) = (9x + 4y + 5z, -4x - 3z, -6x - 4y - 2z), \quad x, y, z \in \mathbb{Q}.$$ 

If we take the standard basis $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$ for $V$ then the matrix $A$ representing this linear transformation is

$$A = \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix}.$$ 

We shall see that the Jordan canonical form for this matrix $A$ is the much simpler matrix

$$B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

obtained by taking instead the basis $f_1 = (2, -1, -2), f_2 = (1, 0, -1), f_3 = (3, -2, -2)$ for $V$, since in this case

$$T(f_1) = T(2, -1, -2) = (4, -2, -4) = 2 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3,$$

$$T(f_2) = T(1, 0, -1) = (4, -1, -4) = 1 \cdot f_1 + 2 \cdot f_2 + 0 \cdot f_3,$$

$$T(f_3) = T(3, -2, -2) = (9, -6, -6) = 0 \cdot f_1 + 0 \cdot f_2 + 3 \cdot f_3,$$

so the columns of the matrix representing $T$ with respect to this basis are $(2, 0, 0), (1, 2, 0)$ and $(0, 0, 3)$, i.e., $T$ has matrix $B$ with respect to this basis. In particular $A$ is similar to the simpler matrix $B$.

In fact this linear transformation $T$ cannot be diagonalized (i.e., there is no choice of basis for $V$ for which the corresponding matrix is a diagonal matrix) so that the matrix $B$ is as close to a diagonal matrix for $T$ as is possible.
The first section below gives some general definitions and states and proves the Fundamental Theorem over an arbitrary P.I.D., after which we return to the application to canonical forms (the application to abelian groups appears in Chapter 5). These applications can be read independently of the general proof. An alternate and computationally useful proof valid for Euclidean Domains (so in particular for the rings \( \mathbb{Z} \) and \( F[x] \)) along the lines of row and column operations is outlined in the exercises.

### 12.1 THE BASIC THEORY

We first describe some general finiteness conditions. Let \( R \) be a ring and let \( M \) be a left \( R \)-module.

**Definition.**

1. The left \( R \)-module \( M \) is said to be a **Noetherian \( R \)-module** or to satisfy the *ascending chain condition on submodules* (or *A.C.C. on submodules*) if there are no infinite increasing chains of submodules, i.e., whenever

\[
M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots
\]

is an increasing chain of submodules of \( M \), then there is a positive integer \( m \) such that for all \( k \geq m \), \( M_k = M_m \) (so the chain becomes stationary at stage \( m \): \( M_m = M_{m+1} = M_{m+2} = \ldots \)).

2. The ring \( R \) is said to be **Noetherian** if it is Noetherian as a left module over itself, i.e., if there are no infinite increasing chains of left ideals in \( R \).

One can formulate analogous notions of A.C.C. on right and on two-sided ideals in a (possibly noncommutative) ring \( R \). For noncommutative rings these properties need not be related.

**Theorem 1.** Let \( R \) be a ring and let \( M \) be a left \( R \)-module. Then the following are equivalent:

1. \( M \) is a Noetherian \( R \)-module.
2. Every nonempty set of submodules of \( M \) contains a maximal element under inclusion.
3. Every submodule of \( M \) is finitely generated.

**Proof:** [(1) implies (2)] Assume \( M \) is Noetherian and let \( \Sigma \) be any nonempty collection of submodules of \( M \). Choose any \( M_1 \in \Sigma \). If \( M_1 \) is a maximal element of \( \Sigma \), (2) holds, so assume \( M_1 \) is not maximal. Then there is some \( M_2 \in \Sigma \) such that \( M_1 \subset M_2 \). If \( M_2 \) is maximal in \( \Sigma \), (2) holds, so we may assume there is an \( M_3 \in \Sigma \) properly containing \( M_2 \). Proceeding in this way one sees that if (2) fails we can produce by the Axiom of Choice an infinite strictly increasing chain of elements of \( \Sigma \), contrary to (1).

[(2) implies (3)] Assume (2) holds and let \( N \) be any submodule of \( M \). Let \( \Sigma \) be the collection of all finitely generated submodules of \( N \). Since \( \{0\} \in \Sigma \), this collection is nonempty. By (2) \( \Sigma \) contains a maximal element \( N' \). If \( N' \neq N \), let \( x \in N - N' \). Since \( N' \in \Sigma \), the submodule \( N' \) is finitely generated by assumption, hence also the

458

Chap. 12 Modules over Principal Ideal Domains
submodule generated by \(N'\) and \(x\) is finitely generated. This contradicts the maximality of \(N'\), so \(N = N'\) is finitely generated.

\((3)\) implies \((1)\) Assume \((3)\) holds and let \(M_1 \subseteq M_2 \subseteq M_3 \ldots\) be a chain of submodules of \(M\). Let
\[
N = \bigcup_{i=1}^{\infty} M_i
\]
and note that \(N\) is a submodule. By \((3)\) \(N\) is finitely generated by, say, \(a_1, a_2, \ldots, a_n\). Since \(a_i \in N\) for all \(i\), each \(a_i\) lies in one of the submodules in the chain, say \(M_{j_i}\). Let \(m = \max\{j_1, j_2, \ldots, j_n\}\). Then \(a_i \in M_m\) for all \(i\) so the module they generate is contained in \(M_m\), i.e., \(N \subseteq M_m\). This implies \(M_m = N = M_k\) for all \(k \geq m\), which proves \((1)\).

**Corollary 2.** If \(R\) is a P.I.D. then every nonempty set of ideals of \(R\) has a maximal element and \(R\) is a Noetherian ring.

**Proof:** The P.I.D. \(R\) satisfies condition \((3)\) in the theorem with \(M = R\).

Recall that even if \(M\) itself is a finitely generated \(R\)-module, submodules of \(M\) need not be finitely generated, so the condition that \(M\) be a Noetherian \(R\)-module is in general stronger than the condition that \(M\) be a finitely generated \(R\)-module.

We require a result on "linear dependence" before turning to the main results of this chapter.

**Proposition 3.** Let \(R\) be an integral domain and let \(M\) be a free \(R\)-module of rank \(n < \infty\). Then any \(n + 1\) elements of \(M\) are \(R\)-linearly dependent, i.e., for any \(y_1, y_2, \ldots, y_{n+1} \in M\) there are elements \(r_1, r_2, \ldots, r_{n+1} \in R\), not all zero, such that
\[
r_1y_1 + r_2y_2 + \ldots + r_{n+1}y_{n+1} = 0.
\]

**Proof:** The quickest way of proving this is to embed \(R\) in its quotient field \(F\) (since \(R\) is an integral domain) and observe that since \(M \cong R \oplus R \oplus \cdots \oplus R\) \((n\) times) we obtain \(M \subseteq F \oplus F \oplus \cdots \oplus F\). The latter is an \(n\)-dimensional vector space over \(F\) so any \(n + 1\) elements of \(M\) are \(F\)-linearly dependent. By clearing the denominators of the scalars (by multiplying through by the product of all the denominators, for example), we obtain an \(R\)-linear dependence relation among the \(n + 1\) elements of \(M\).

Alternatively, let \(e_1, \ldots, e_n\) be a basis of the free \(R\)-module \(M\) and let \(y_1, \ldots, y_{n+1}\) be any \(n + 1\) elements of \(M\). For \(1 \leq i \leq n + 1\) write \(y_i = a_{1i}e_1 + a_{2i}e_2 + \ldots + a_{ni}e_i\) in terms of the basis \(e_1, e_2, \ldots, e_n\). Let \(A\) be the \((n + 1) \times (n + 1)\) matrix whose \(i, j\) entry is \(a_{ij}\), \(1 \leq i \leq n\), \(1 \leq j \leq n + 1\) and whose last row is zero, so certainly \(\det A = 0\).

Since \(R\) is an integral domain, Corollary 27 of Section 11.4 shows that the columns of \(A\) are \(R\)-linearly dependent. Any dependence relation on the columns of \(A\) gives a dependence relation on the \(y_i\)'s, completing the proof.

If \(R\) is any integral domain and \(M\) is any \(R\)-module recall that
\[
\text{Tor}(M) = \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}
\]
is a submodule of \( M \) (called the torsion submodule of \( M \)) and if \( N \) is any submodule of \( \text{Tor}(M) \), \( N \) is called a torsion submodule of \( M \) (so the torsion submodule of \( M \) is the union of all torsion submodules of \( M \), i.e., is the maximal torsion submodule of \( M \)). If \( \text{Tor}(M) = 0 \), the module \( M \) is said to be torsion free.

For any submodule \( N \) of \( M \), the annihilator of \( N \) is the ideal of \( R \) defined by

\[
\text{Ann}(N) = \{ r \in R \mid rn = 0 \text{ for all } n \in N \}.
\]

Note that if \( N \) is not a torsion submodule of \( M \) then \( \text{Ann}(N) = (0) \). It is easy to see that if \( N, L \) are submodules of \( M \) with \( N \subseteq L \), then \( \text{Ann}(L) \subseteq \text{Ann}(N) \). If \( R \) is a P.I.D. and \( N \subseteq L \subseteq M \) with \( \text{Ann}(N) = (a) \) and \( \text{Ann}(L) = (b) \), then \( a \mid b \). In particular, the annihilator of any element \( x \) of \( M \) divides the annihilator of \( M \) (this is implied by Lagrange's Theorem when \( R = \mathbb{Z} \)).

**Definition.** For any integral domain \( R \) the rank of an \( R \)-module \( M \) is the maximum number of \( R \)-linearly independent elements of \( M \).

The preceding proposition states that for a free \( R \)-module \( M \) over an integral domain the rank of a submodule is bounded by the rank of \( M \). This notion of rank agrees with previous uses of the same term. If the ring \( R = F \) is a field, then the rank of an \( R \)-module \( M \) is the dimension of \( M \) as a vector space over \( F \) and any maximal set of \( F \)-linearly independent elements is a basis for \( M \). For a general integral domain, however, an \( R \)-module \( M \) of rank \( n \) need not have a "basis," i.e., need not be a free \( R \)-module even if \( M \) is torsion free, so some care is necessary with the notion of rank, particularly with respect to the torsion elements of \( M \). Exercises 1 to 6 and 20 give an alternate characterization of the rank and provide some examples of (torsion free) \( R \)-modules (of rank 1) that are not free.

The next important result shows that if \( N \) is a submodule of a free module of finite rank over a P.I.D. then \( N \) is again a free module of finite rank and furthermore it is possible to choose generators for the two modules which are related in a simple way.

**Theorem 4.** Let \( R \) be a Principal Ideal Domain, let \( M \) be a free \( R \)-module of finite rank \( n \) and let \( N \) be a submodule of \( M \). Then

1. \( N \) is free of rank \( m \), \( m \leq n \) and
2. there exists a basis \( y_1, y_2, \ldots, y_n \) of \( M \) so that \( a_1y_1, a_2y_2, \ldots, a_my_m \) is a basis of \( N \) where \( a_1, a_2, \ldots, a_m \) are nonzero elements of \( R \) with the divisibility relations

\[
a_1 \mid a_2 \mid \cdots \mid a_m.
\]

**Proof:** The theorem is trivial for \( N = \{0\} \), so assume \( N \neq \{0\} \). For each \( R \)-module homomorphism \( \varphi \) of \( M \) into \( R \), the image \( \varphi(N) \) of \( N \) is a submodule of \( R \), i.e., an ideal in \( R \). Since \( R \) is a P.I.D. this ideal must be principal, say \( \varphi(N) = (a_\varphi) \), for some \( a_\varphi \in R \). Let

\[
\Sigma = \{(a_\varphi) \mid \varphi \in \text{Hom}_R(M, R)\}
\]

be the collection of the principal ideals in \( R \) obtained in this way from the \( R \)-module homomorphisms of \( M \) into \( R \). The collection \( \Sigma \) is certainly nonempty since taking \( \varphi \)
to be the trivial homomorphism shows that \((0) \in \Sigma\). By Corollary 2, \(\Sigma\) has at least one maximal element i.e., there is at least one homomorphism \(v\) of \(M\) to \(R\) so that the principal ideal \(v(N) = (a_i)\) is not properly contained in any other element of \(\Sigma\). Let \(a_1 = a_i\) for this maximal element and let \(y \in N\) be an element mapping to the generator \(a_1\) under the homomorphism \(v\): \(v(y) = a_1\).

We now show the element \(a_1\) is nonzero. Let \(x_1, x_2, \ldots, x_n\) be any basis of the free module \(M\) and let \(\pi_i \in \text{Hom}_R(M, R)\) be the natural projection homomorphism onto the \(i\)th coordinate with respect to this basis. Since \(N \neq \{0\}\), there exists an \(i\) such that \(\pi_i(N) \neq 0\), which in particular shows that \(\Sigma\) contains more than just the trivial ideal \((0)\). Since \((a_1)\) is a maximal element of \(\Sigma\) it follows that \(a_1 \neq 0\).

We next show that this element \(a_1\) divides \(\varphi(y)\) for every \(\varphi \in \text{Hom}_R(M, R)\). To see this let \(d\) be a generator for the principal ideal generated by \(a_1\) and \(\varphi(y)\). Then \(d\) is a divisor of both \(a_1\) and \(\varphi(y)\) in \(R\) and \(d = r_1a_1 + r_2\varphi(y)\) for some \(r_1, r_2 \in R\). Consider the homomorphism \(\psi = r_1v + r_2\varphi\) from \(M\) to \(R\). Then \(\psi(y) = (r_1v + r_2\varphi)(y) = r_1a_1 + r_2\varphi(y) = d\) so that \(d \in \psi(N)\), hence also \((d) \subseteq \psi(N)\). But \(d\) is a divisor of \(a_1\) so we also have \((a_1) \subseteq (d)\). Then \((a_1) \subseteq (d) \subseteq \psi(N)\) and by the maximality of \((a_1)\) we must have equality: \((a_1) = (d) = \psi(N)\). In particular \((a_1) = (d)\) shows that \(a_1 \mid \varphi(y)\) since \(d\) divides \(\varphi(y)\).

If we apply this to the projection homomorphisms \(\pi_i\) we see that \(a_1\) divides \(\pi_i(y)\) for all \(i\). Write \(\pi_i(y) = a_1b_i\) for some \(b_i \in R\), \(1 \leq i \leq n\) and define

\[
y_1 = \sum_{i=1}^{n} b_i x_i.
\]

Note that \(a_1y_1 = y\). Since \(a_1 = v(y) = v(a_1y_1) = a_1v(y_1)\) and \(a_1\) is a nonzero element of the integral domain \(R\) this shows

\[
v(y_1) = 1.
\]

We now verify that this element \(y_1\) can be taken as one element in a basis for \(M\) and that \(a_1y_1\) can be taken as one element in a basis for \(N\), namely that we have

(a) \(M = Ry_1 \oplus \ker v\), and
(b) \(N = Ra_1y_1 \oplus (N \cap \ker v)\).

To see (a) let \(x\) be an arbitrary element in \(M\) and write \(x = v(x)y_1 + (x - v(x)y_1)\). Since

\[
v(x - v(x)y_1) = v(x) - v(x)v(y_1)
\]

\[
= v(x) - v(x) \cdot 1
\]

\[
= 0
\]

we see that \(x - v(x)y_1\) is an element in the kernel of \(v\). This shows that \(x\) can be written as the sum of an element in \(Ry_1\) and an element in the kernel of \(v\), so \(M = Ry_1 + \ker v\). To see that the sum is direct, suppose \(ry_1\) is also an element in the kernel of \(v\). Then \(0 = v(ry_1) = rv(y_1) = r\) shows that this element is indeed \(0\).

For (b) observe that \(v(x')\) is divisible by \(a_1\) for every \(x' \in N\) by the definition of \(a_1\) as a generator for \(v(N)\). If we write \(v(x') = ba_1\) where \(b \in R\) then the decomposition we used in (a) above is \(x' = v(x')y_1 + (x' - v(x')y_1) = ba_1y_1 + (x' - ba_1y_1)\) where the second summand is in the kernel of \(v\) and is an element of \(N\). This shows that
\( N = R \alpha_1 y_1 + (N \cap \ker \nu) \). The fact that the sum in (b) is direct is a special case of the directness of the sum in (a).

We now prove part (1) of the theorem by induction on the rank, \( m \), of \( N \). If \( m = 0 \), then \( N \) is a torsion module, hence \( N = 0 \) since a free module is torsion free, so (1) holds trivially. Assume then that \( m > 0 \). Since the sum in (b) above is direct we see easily that \( N \cap \ker \nu \) has rank \( m - 1 \) (cf. Exercise 3). By induction \( N \cap \ker \nu \) is then a free \( R \)-module of rank \( m - 1 \). Again by the directness of the sum in (b) we see that adjoining \( a_1 y_1 \) to any basis of \( N \cap \ker \nu \) gives a basis of \( N \), so \( N \) is also free (of rank \( m \)), which proves (1).

Finally, we prove (2) by induction on \( n \), the rank of \( M \). Applying (1) to the submodule \( \ker \nu \) shows that this submodule is free and because the sum in (a) is direct it is free of rank \( n - 1 \). By the induction assumption applied to the module \( \ker \nu \) (which plays the role of \( M \)) and its submodule \( \ker \nu \cap N \) (which plays the role of \( N \)), we see that there is a basis \( y_2, y_3, \ldots, y_n \) of \( \ker \nu \) such that \( a_2 y_2, a_3 y_3, \ldots, a_m y_m \) is a basis of \( N \cap \ker \nu \) for some elements \( a_2, a_3, \ldots, a_m \) of \( R \) with \( a_2 \mid a_3 \mid \cdots \mid a_m \). Since the sums (a) and (b) are direct, \( y_1, y_2, \ldots, y_n \) is a basis of \( M \) and \( a_1 y_1, a_2 y_2, \ldots, a_m y_m \) is a basis of \( N \). To complete the induction it remains to show that \( a_1 \) divides \( a_2 \). Define a homomorphism \( \varphi \) from \( M \) to \( R \) by defining \( \varphi(y_1) = \varphi(y_2) = 1 \) and \( \varphi(y_i) = 0 \), for all \( i > 2 \), on the basis for \( M \). Then for this homomorphism \( \varphi \) we have \( a_1 = \varphi(a_1 y_1) \) so \( a_1 \in \varphi(N) \) hence also \( (a_1) \subseteq \varphi(N) \). By the maximality of \( (a_1) \) in \( \Sigma \) it follows that \( (a_1) = \varphi(N) \). Since \( a_2 = \varphi(a_2 y_2) \in \varphi(N) \) we then have \( a_2 \in (a_1) \) i.e., \( a_1 \mid a_2 \). This completes the proof of the theorem.

Recall that the left \( R \)-module \( C \) is a cyclic \( R \)-module (for any ring \( R \), not necessarily commutative nor with 1) if there is an element \( x \in C \) such that \( C = Rx \). We can then define an \( R \)-module homomorphism

\[ \pi : R \to C \]

by \( \pi(r) = rx \), which will be surjective by the assumption \( C = Rx \). The First Isomorphism Theorem gives an isomorphism of (left) \( R \)-modules

\[ R / \ker \pi \cong C. \]

If \( R \) is a P.I.D., \( \ker \pi \) is a principal ideal, \( (a) \), so we see that the cyclic \( R \)-modules \( C \) are of the form \( R / (a) \) where \( (a) = \text{Ann}(C) \).

The cyclic modules are the simplest modules (since they require only one generator). The existence portion of the Fundamental Theorem states that any finitely generated module over a P.I.D. is isomorphic to the direct sum of finitely many cyclic modules.

**Theorem 5.** (Fundamental Theorem, Existence: Invariant Factor Form) Let \( R \) be a P.I.D. and let \( M \) be a finitely generated \( R \)-module.

1. Then \( M \) is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

\[ M \cong R' \oplus R / (a_1) \oplus R / (a_2) \oplus \cdots \oplus R / (a_m) \]

for some integer \( r \geq 0 \) and nonzero elements \( a_1, a_2, \ldots, a_m \) of \( R \) which are not units in \( R \) and which satisfy the divisibility relations

\[ a_1 \mid a_2 \mid \cdots \mid a_m. \]
(2) $M$ is torsion free if and only if $M$ is free.

(3) In the decomposition in (1),

$$\text{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

In particular $M$ is a torsion module if and only if $r = 0$ and in this case the annihilator of $M$ is the ideal $(a_m)$.

**Proof:** The module $M$ can be generated by a finite set of elements by assumption so let $x_1, x_2, \ldots, x_n$ be a set of generators of $M$ of minimal cardinality. Let $R^n$ be the free $R$-module of rank $n$ with basis $b_1, b_2, \ldots, b_n$ and define the homomorphism $\pi : R^n \to M$ by defining $\pi(b_i) = x_i$ for all $i$, which is automatically surjective since $x_1, \ldots, x_n$ generate $M$. By the First Isomorphism Theorem for modules we have $R^n / \ker \pi \cong M$. Now, by Theorem 4 applied to $R^n$ and the submodule $\ker \pi$ we can choose another basis $y_1, y_2, \ldots, y_n$ of $R^n$ so that $a_1y_1, a_2y_2, \ldots, a_my_m$ is a basis of $\ker \pi$ for some elements $a_1, a_2, \ldots, a_m$ of $R$ with $a_1 | a_2 | \cdots | a_m$. This implies

$$M \cong R^n / \ker \pi = (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n) / (Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m).$$

To identify the quotient on the right hand side we use the natural surjective $R$-module homomorphism

$$Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$

that maps $(\alpha_1y_1, \ldots, \alpha_ny_n)$ to $(\alpha_1 \text{ mod } (a_1), \ldots, \alpha_m \text{ mod } (a_m), \alpha_{m+1}, \ldots, \alpha_n)$. The kernel of this map is clearly the set of elements where $a_i$ divides $\alpha_i$, $i = 1, 2, \ldots, m$, i.e., $Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m$ (cf. Exercise 7). Hence we obtain

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

If $a$ is a unit in $R$ then $R/(a) = 0$, so in this direct sum we may remove any of the initial $a_i$ which are units. This gives the decomposition in (1) (with $r = n - m$).

Since $R/(a)$ is a torsion $R$-module for any nonzero element $a$ of $R$, (1) immediately implies $M$ is a torsion free module if and only if $M \cong R^r$, which is (2). Part (3) is immediate from the definitions since the annihilator of $R/(a)$ is evidently the ideal $(a)$.

We shall shortly prove the uniqueness of the decomposition in Theorem 5, namely that if we have

$$M \cong R^{r'} \oplus R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_{m'})$$

for some integer $r' \geq 0$ and nonzero elements $b_1, b_2, \ldots, b_{m'}$ of $R$ which are not units with

$$b_1 \mid b_2 \mid \cdots \mid b_{m'},$$

then $r = r'$, $m = m'$ and $(a_i) = (b_i)$ (so $a_i = b_i$ up to units) for all $i$. It is precisely the divisibility condition $a_1 | a_2 | \cdots | a_m$ which gives this uniqueness.
Definition. The integer $r$ in Theorem 5 is called the **free rank** or the **Betti number** of $M$ and the elements $a_1, a_2, \ldots, a_m \in R$ (defined up to multiplication by units in $R$) are called the **invariant factors** of $M$.

Note that until we have proved that the invariant factors of $M$ are unique we should properly refer to a set of invariant factors for $M$ (and similarly for the free rank), by which we mean any elements giving a decomposition for $M$ as in (1) of the theorem above.

Using the Chinese Remainder Theorem it is possible to decompose the cyclic modules in Theorem 5 further so that $M$ is the direct sum of cyclic modules whose annihilators are as simple as possible (namely $(0)$ or generated by powers of primes in $R$). This gives an alternate decomposition which we shall also see is unique and which we now describe.

Suppose $a$ is a nonzero element of the Principal Ideal Domain $R$. Then since $R$ is also a Unique Factorization Domain we can write

$$a = u p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$$

where the $p_i$ are distinct primes in $R$ and $u$ is a unit. This factorization is unique up to units, so the ideals $(p_i^{a_i}), \ i = 1, \ldots, s$ are uniquely defined. For $i \neq j$ we have $(p_i^{a_i}) + (p_j^{a_j}) = R$ since the sum of these two ideals is generated by a greatest common divisor, which is 1 for distinct primes $p_i, p_j$. Put another way, the ideals $(p_i^{a_i}), \ i = 1, \ldots, s$, are comaximal in pairs. The intersection of all these ideals is the ideal $(a)$ since $a$ is the least common multiple of $p_1^{a_1}, p_2^{a_2}, \ldots, p_s^{a_s}$. Then the Chinese Remainder Theorem (Theorem 7.17) shows that

$$R/(a) \cong R/(p_1^{a_1}) \oplus R/(p_2^{a_2}) \oplus \cdots \oplus R/(p_s^{a_s})$$

as rings and also as $R$-modules.

Applying this to the modules in Theorem 5 allows us to write each of the direct summands $R/(a_i)$ for the invariant factor $a_i$ of $M$ as a direct sum of cyclic modules whose annihilators are the prime power divisors of $a_i$. This proves:

**Theorem 6. (Fundamental Theorem, Existence: Elementary Divisor Form)** Let $R$ be a P.I.D. and let $M$ be a finitely generated $R$-module. Then $M$ is the direct sum of a finite number of cyclic modules whose annihilators are either $(0)$ or generated by powers of primes in $R$, i.e.,

$$M \cong R' \oplus R/(p_1^{a_1}) \oplus R/(p_2^{a_2}) \oplus \cdots \oplus R/(p_t^{a_t})$$

where $r \geq 0$ is an integer and $p_1^{a_1}, \ldots, p_t^{a_t}$ are positive powers of (not necessarily distinct) primes in $R$.

We proved Theorem 6 by using the prime power factors of the invariant factors for $M$. In fact we shall see that the decomposition of $M$ into a direct sum of cyclic modules whose annihilators are $(0)$ or prime powers as in Theorem 6 is unique, i.e., the integer $r$ and the ideals $(p_1^{a_1}), \ldots, (p_t^{a_t})$ are uniquely defined for $M$. These prime powers are given a name:
**Definition.** Let \( R \) be a P.I.D. and let \( M \) be a finitely generated \( R \)-module as in Theorem 6. The prime powers \( p_1^{\alpha_1}, \ldots, p_n^{\alpha_n} \) (defined up to multiplication by units in \( R \)) are called the elementary divisors of \( M \).

Suppose \( M \) is a finitely generated torsion module over the Principal Ideal Domain \( R \). If for the distinct primes \( p_1, p_2, \ldots, p_n \) occurring in the decomposition in Theorem 6 we group together all the cyclic factors corresponding to the same prime \( p_i \) we see in particular that \( M \) can be written as a direct sum

\[
M = N_1 \oplus N_2 \oplus \cdots \oplus N_n
\]

where \( N_i \) consists of all the elements of \( M \) which are annihilated by some power of the prime \( p_i \). This result holds also for modules over \( R \) which may not be finitely generated:

**Theorem 7.** *(The Primary Decomposition Theorem)* Let \( R \) be a P.I.D. and let \( M \) be a nonzero torsion \( R \)-module (not necessarily finitely generated) with nonzero annihilator \( a \). Suppose the factorization of \( a \) into distinct prime powers in \( R \) is

\[
a = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}
\]

and let \( N_i = \{ x \in M \mid p_i^{\alpha_i} x = 0 \}, 1 \leq i \leq n \). Then \( N_i \) is a submodule of \( M \) with annihilator \( p_i^{\alpha_i} \) and is the submodule of \( M \) of all elements annihilated by some power of \( p_i \). We have

\[
M = N_1 \oplus N_2 \oplus \cdots \oplus N_n.
\]

If \( M \) is finitely generated then each \( N_i \) is the direct sum of finitely many cyclic modules whose annihilators are divisors of \( p_i^{\alpha_i} \).

**Proof:** We have already proved these results in the case where \( M \) is finitely generated over \( R \). In the general case it is clear that \( N_i \) is a submodule of \( M \) with annihilator dividing \( p_i^{\alpha_i} \). Since \( R \) is a P.I.D. the ideals \((p_i^{\alpha_i})\) and \((p_j^{\alpha_j})\) are comaximal for \( i \neq j \), so the direct sum decomposition of \( M \) can be proved easily by modifying the argument in the proof of the Chinese Remainder Theorem to apply it to modules. Using this direct sum decomposition it is easy to see that the annihilator of \( N_i \) is precisely \( p_i^{\alpha_i} \).

**Definition.** The submodule \( N_i \) in the previous theorem is called the \( p_i \)-primary component of \( M \).

Notice that with this terminology the elementary divisors of a finitely generated module \( M \) are just the invariant factors of the primary components of \( \text{Tor}(M) \).

We now prove the uniqueness statements regarding the decompositions in the Fundamental Theorem.

Note that if \( M \) is any module over a commutative ring \( R \) and \( a \) is an element of \( R \) then \( aM = \{ am \mid m \in M \} \) is a submodule of \( M \). Recall also that in a Principal Ideal Domain \( R \) the nonzero prime ideals are maximal, hence the quotient of \( R \) by a nonzero prime ideal is a field.

Sec. 12.1 \ The Basic Theory 465
Lemma 8. Let $R$ be a P.I.D. and let $p$ be a prime in $R$. Let $F$ denote the field $R/(p)$.

(1) Let $M = R'$. Then $M/pM \cong F'$.

(2) Let $M = R/(a)$ where $a$ is a nonzero element of $R$. Then

$$M/pM \cong \begin{cases} F & \text{if } p \text{ divides } a \text{ in } R \\ 0 & \text{if } p \text{ does not divide } a \text{ in } R. \end{cases}$$

(3) Let $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ where each $a_i$ is divisible by $p$.

Then $M/pM \cong F^k$.

Proof: (1) There is a natural map from $R'$ to $(R/(p))^r$ defined by mapping $(\alpha_1, \ldots, \alpha_r)$ to $(\alpha_1 \mod (p), \ldots, \alpha_r \mod (p))$. This is clearly a surjective $R$-module homomorphism with kernel consisting of the $r$-tuples all of whose coordinates are divisible by $p$, i.e., $pR'$, so $R'/pR' \cong (R/(p))^r$, which is (1).

(2) This follows from the Isomorphism Theorems: note first that $p(R/(a))$ is the image of the ideal $(p)$ in the quotient $R/(a)$, hence is $(p) + (a)/(a)$. The ideal $(p) + (a)$ is generated by a greatest common divisor of $p$ and $a$, hence is $(p)$ if $p$ divides $a$ and is $R = (1)$ otherwise. Hence $pM = (p)/(a)$ if $p$ divides $a$ and is $R/(a) = M$ otherwise.

If $p$ divides $a$ then $M/pM = (R/(a))/(p)/(a) \cong R/(p)$, and if $p$ does not divide $a$ then $M/pM = M/M = 0$, which proves (2).

(3) This follows from (2) as in the proof of part (1) of Theorem 5.

Theorem 9. (Fundamental Theorem, Uniqueness) Let $R$ be a P.I.D.

(1) Two finitely generated $R$-modules $M_1$ and $M_2$ are isomorphic if and only if they have the same free rank and the same list of invariant factors.

(2) Two finitely generated $R$-modules $M_1$ and $M_2$ are isomorphic if and only if they have the same free rank and the same list of elementary divisors.

Proof: If $M_1$ and $M_2$ have the same free rank and list of invariant factors or the same free rank and list of elementary divisors then they are clearly isomorphic.

Suppose that $M_1$ and $M_2$ are isomorphic. Any isomorphism between $M_1$ and $M_2$ maps the torsion in $M_1$ to the torsion in $M_2$ so we must have Tor($M_1$) $\cong$ Tor($M_2$). Then $R^{r_1} \cong M_1/\text{Tor}(M_1) \cong M_2/\text{Tor}(M_2) \cong R^{r_2}$ where $r_1$ is the free rank of $M_1$ and $r_2$ is the free rank of $M_2$. Let $p$ be any nonzero prime in $R$. Then from $R^{r_1} \cong R^{r_2}$ we obtain $R^{r_1}/pR^{r_1} \cong R^{r_2}/pR^{r_2}$. By (1) of the previous lemma, this implies $F^{r_1} \cong F^{r_2}$ where $F$ is the field $R/pR$. Hence we have an isomorphism of an $r_1$-dimensional vector space over $F$ with an $r_2$-dimensional vector space over $F$, so that $r_1 = r_2$ and $M_1$ and $M_2$ have the same free rank.

We are reduced to showing that $M_1$ and $M_2$ have the same lists of invariant factors and elementary divisors. To do this we need only work with the isomorphic torsion modules Tor($M_1$) and Tor($M_2$), i.e., we may as well assume that both $M_1$ and $M_2$ are torsion $R$-modules.

We first show they have the same elementary divisors. It suffices to show that for any fixed prime $p$ the elementary divisors which are a power of $p$ are the same for both $M_1$ and $M_2$. If $M_1 \cong M_2$ then the $p$-primary submodule of $M_1$ ( = the direct
sum of the cyclic factors whose elementary divisors are powers of $p$) is isomorphic to the $p$-primary submodule of $M_2$, since these are the submodules of elements which are annihilated by some power of $p$. We are therefore reduced to the case of proving that if two modules $M_1$ and $M_2$ which have annihilator a power of $p$ are isomorphic then they have the same elementary divisors.

We proceed by induction on the power of $p$ in the annihilator of $M_1$ (which is the same as the annihilator of $M_2$ since $M_1$ and $M_2$ are isomorphic). If this power is 0, then both $M_1$ and $M_2$ are 0 and we are done. Otherwise $M_1$ (and $M_2$) have nontrivial elementary divisors. Suppose the elementary divisors of $M_1$ are given by

$$\text{elementary divisors of } M_1: \underbrace{p, p, \ldots, p}_{m \text{ times}}, \ p^{\alpha_1}, \ p^{\alpha_2}, \ldots, \ p^{\alpha_s},$$

where $2 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_s$, i.e., $M_1$ is the direct sum of cyclic modules with generators $x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_{m+s}$, say, whose annihilators are $(p), (p), \ldots, (p), (p^{\alpha_1}), (p^{\alpha_2}), \ldots, (p^{\alpha_s})$, respectively. Then the submodule $pM_1$ has elementary divisors

$$\text{elementary divisors of } pM_1: \ p^{\alpha_1 - 1}, \ p^{\alpha_2 - 1}, \ldots, \ p^{\alpha_s - 1}$$

since $pM_1$ is the direct sum of the cyclic modules with generators $px_1, px_2, \ldots, px_m, px_{m+1}, \ldots, px_{m+s}$ whose annihilators are $(1), (1), \ldots, (1), (p^{\alpha_1 - 1}), \ldots, (p^{\alpha_s - 1})$, respectively. Similarly, if the elementary divisors of $M_2$ are given by

$$\text{elementary divisors of } M_2: \underbrace{p, p, \ldots, p}_{n \text{ times}}, \ p^{\beta_1}, \ p^{\beta_2}, \ldots, \ p^{\beta_t},$$

where $2 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_t$, then $pM_2$ has elementary divisors

$$\text{elementary divisors of } pM_2: \ p^{\beta_1 - 1}, \ p^{\beta_2 - 1}, \ldots, \ p^{\beta_t - 1}.$$

Since $M_1 \cong M_2$, also $pM_1 \cong pM_2$ and the power of $p$ in the annihilator of $pM_1$ is one less than the power of $p$ in the annihilator of $M_1$. By induction, the elementary divisors for $pM_1$ are the same as the elementary divisors for $pM_2$, i.e., $s = t$ and $\alpha_i - 1 = \beta_i - 1$ for $i = 1, 2, \ldots, s$, hence $\alpha_i = \beta_i$ for $i = 1, 2, \ldots, s$. Finally, since also $M_1/pM_1 \cong M_2/pM_2$ we see from (3) of the lemma above that $F^{m+s} \cong F^{n+t}$, which shows that $m + s = n + t$ hence $m = n$ since we have already seen $s = t$. This proves that the set of elementary divisors for $M_1$ is the same as the set of elementary divisors for $M_2$.

We now show that $M_1$ and $M_2$ must have the same invariant factors. Suppose $\alpha_1 | \alpha_2 | \cdots | \alpha_m$ are invariant factors for $M_1$. We obtain a set of elementary divisors for $M_1$ by taking the prime power factors of these elements. Note that then the divisibility relations on the invariant factors imply that $a_m$ is the product of the largest of the prime powers among these elementary divisors, $a_{m-1}$ is the product of the largest prime powers among these elementary divisors once the factors for $a_m$ have been removed, and so on. If $b_1 | b_2 | \cdots | b_n$ are invariant factors for $M_2$ then we similarly obtain a set of elementary divisors for $M_2$ by taking the prime power factors of these elements. But we showed above that the elementary divisors for $M_1$ and $M_2$ are the same, and it follows that the same is true of the invariant factors.
Corollary 10. Let $R$ be a P.I.D. and let $M$ be a finitely generated $R$-module.

(1) The elementary divisors of $M$ are the prime power factors of the invariant factors of $M$.

(2) The largest invariant factor of $M$ is the product of the largest of the distinct prime powers among the elementary divisors of $M$, the next largest invariant factor is the product of the largest of the distinct prime powers among the remaining elementary divisors of $M$, and so on.

Proof: The procedure in (1) gives a set of elementary divisors and since the elementary divisors for $M$ are unique by the theorem, it follows that the procedure in (1) gives the set of elementary divisors. Similarly for (2).

Corollary 11. (The Fundamental Theorem of Finitely Generated Abelian Groups) See Theorem 5.3 and Theorem 5.5.

Proof: Take $R = \mathbb{Z}$ in Theorems 5, 6 and 9 (note however that the invariant factors are listed in reverse order in Chapter 5 for computational convenience).

The procedure for passing between elementary divisors and invariant factors in Corollary 10 is described in some detail in Chapter 5 in the case of finitely generated abelian groups.

Note also that if a finitely generated module $M$ is written as a direct sum of cyclic modules of the form $R/(a)$ then the ideals $(a)$ which occur are not in general unique unless some additional conditions are imposed (such as the divisibility condition for the invariant factors or the condition that $a$ be the power of a prime in the case of the elementary divisors). To decide whether two modules are isomorphic it is necessary to first write them in such a standard (or canonical) form.

EXERCISES

1. Let $M$ be a module over the integral domain $R$.
   (a) Suppose $x$ is a nonzero torsion element in $M$. Show that $x$ and 0 are "linearly dependent." Conclude that the rank of $\text{Tor}(M)$ is 0, so that in particular any torsion $R$-module has rank 0.
   (b) Show that the rank of $M$ is the same as the rank of the (torsion free) quotient $M/\text{Tor}M$.

2. Let $M$ be a module over the integral domain $R$.
   (a) Suppose that $M$ has rank $n$ and that $x_1, x_2, \ldots, x_n$ is any maximal set of linearly independent elements of $M$. Let $N = R x_1 + \cdots + R x_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that $N$ is isomorphic to $R^n$ and that the quotient $M/N$ is a torsion $R$-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that $ry$ can be written as a linear combination $r_1 x_1 + \cdots + r_n x_n$ of the $x_i$).
   (b) Prove conversely that if $M$ contains a submodule $N$ that is free of rank $n$ (i.e., $N \cong R^n$) such that the quotient $M/N$ is a torsion $R$-module then $M$ has rank $n$. [Let $y_1, y_2, \ldots, y_{n+1}$ be any $n + 1$ elements of $M$. Use the fact that $M/N$ is torsion to write $r_1 y_1$ as a linear combination of $N$ for some nonzero elements $r_1, \ldots, r_{n+1}$ of $R$. Use an argument as in the proof of Proposition 3 to see that the $r_i y_i$, and hence also the $y_i$, are linearly dependent.]