Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 6
Hilary Term 2014

D. R. Wilkins

Contents

6 Finitely-Generated Modules over Principal Ideal Domains **113**

6.1 Linear Independence and Free Modules 113
6.2 Free Modules over Integral Domains 117
6.3 Torsion Modules 119
6.4 Free Modules of Finite Rank over Principal Ideal Domains . . 120
6.5 Torsion-Free Modules 121
6.6 Finitely-Generated Torsion Modules over Principal Ideal Domains 123
6.7 Cyclic Modules and Order Ideals 127
6.8 The Structure of Finitely-Generated Modules over Principal Ideal Domains 128
6.9 The Jordan Normal Form 132

6 Finitely-Generated Modules over Principal Ideal Domains

6.1 Linear Independence and Free Modules

Let M be a module over a unital commutative ring R, and let $x_1, x_2, \ldots, x_k$ be elements of M. A *linear combination* of the elements $x_1, x_2, \ldots, x_k$ with *coefficients* $r_1, r_2, \ldots, r_k$ is an element of M that is represented by means of an expression of the form

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k,$$

where $r_1, r_2, \ldots, r_k$ are elements of the ring R.

Definition Let M be a module over a unital commutative ring R. The elements of a subset X of M are said to be *linearly dependent* if there exist distinct elements $x_1, x_2, \ldots, x_k$ of X (where $x_i \neq x_j$ for $i \neq j$) and elements $r_1, r_2, \ldots, r_k$ of the ring R, not all zero, such that

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0_M,$$

where 0_M denotes the zero element of the module M.

The elements of a subset X of M are said to be *linearly independent* over the ring R if they are not linearly dependent over R.

Let M be a module over a unital commutative ring R, and let X be a (finite or infinite) subset of M. The set X generates M as an R-module if and only if, given any non-zero element m of M, there exist $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$ such that

$$m = r_1x_1 + r_2x_2 + \cdots + r_kx_k$$

(see Lemma 3.1). In particular, a module M over a unital commutative ring R is generated by a finite set $\{x_1, x_2, \ldots, x_k\}$ if and only if any element of M can be represented as a linear combination of $x_1, x_2, \ldots, x_k$ with coefficients in the ring R.

A module over a unital commutative ring is freely generated by the empty set if and only if it is the zero module.

Definition Let M be a module over a unital commutative ring R, and let X be a subset of M. The module M is said to be *freely generated* by the set X if the following conditions are satisfied:

(i) the elements of X are linearly independent over the ring R;

(ii) the module M is generated by the subset X.

Definition A module over a unital commutative ring is said to be *free* if there exists some subset of the module which freely generates the module.

Definition Let M be a module over a unital commutative ring R. Elements $x_1, x_2, \ldots, x_k$ of M are said to constitute a *free basis* of M if these elements are distinct, and if the R-module M is freely generated by the set $\{x_1, x_2, \ldots, x_k\}$.

Lemma 6.1 *Let M be a module over an unital commutative ring R. Elements $x_1, x_2, \ldots, x_k$ of M constitute a free basis of that module if and only if, given any element m of M, there exist uniquely determined elements $r_1, r_2, \ldots, r_k$ of the ring R such that*

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

Proof First suppose that $x_1, x_2, \ldots, x_k$ is a list of elements of M with the property that, given any element m of M, there exist uniquely determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

Then the elements $x_1, x_2, \ldots, x_k$ generate M. Also the uniqueness of the coefficients $r_1, r_2, \ldots, r_k$ ensures that the zero element 0_M of M cannot be expressed as a linear combination of $x_1, x_2, \ldots, x_k$ unless the coeffients involved are all zero. Therefore these elements are linearly independent and thus constitute a free basis of the module M.

Conversely suppose that $x_1, x_2, \ldots, x_k$ is a free basis of M. Then any element of M can be expressed as a linear combination of the free basis vectors. We must prove that the coefficients involved are uniquely determined. Let $r_1, r_2, \ldots, r_k$ and $s_1, s_2, \ldots, s_k$ be elements of the coefficient ring R satisfying

$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k = s_1 x_1 + s_2 x_2 + \cdots + s_k x_k.$$

Then

$$(r_1 - s_1)x_1 + (r_2 - s_2)x_2 + \cdots + (r_k - s_k)x_k = 0_M.$$

But then $r_j - s_j = 0$ and thus $r_j = s_j$ for $j = 1, 2, \ldots, n$, since the elements of any free basis are required to be linearly independent. This proves that any element of M can be represented in a unique fashion as a linear combination of the elements of a free basis of M, as required. ∎

Proposition 6.2 *Let M be a free module over a unital commutative ring R, and let X be a subset of M that freely generates M. Then, given any R-module N, and given any function $f: X \to N$ from X to N, there exists a unique R-module homomorphism $\varphi: M \to N$ such that $\varphi|X = f$.*

Proof We first prove the result in the special case where M is freely generated by a finite set X. Thus suppose that $X = \{x_1, x_2, \ldots, x_k\}$, where the elements $x_1, x_2, \ldots, x_k$ are distinct. Then these elements are linearly independent over R and therefore, given any element m of M, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1x_1 + r_2x_2 + \cdots + r_kx_k.$$

(see Lemma 6.1). It follows that, given any R-module N, and given any function $f: X \to N$ from X to N, there exists a function $\varphi: M \to N$ from M to N which is characterized by the property that

$$\varphi(r_1x_1 + r_2x_2 + \cdots + r_kx_k) = r_1f(x_1) + r_2f(x_2) + \cdots + r_kf(x_k).$$

for all $r_1, r_2, \ldots, r_k$. It is an easy exercise to verify that this function is an R-module homomorphism, and that it is the unique R-module homomorphism from M to N that extends $f: X \to N$.

Now consider the case when M is freely generated by an infinite set X. Let N be an R-module, and let $f: X \to N$ be a function from X to N. For each finite subset Y of X, let M_Y denote the submodule of M that is generated by Y. Then the result we have just proved for modules freely generated by finite sets ensures that there exists a unique R-module homomorphism $\varphi_Y: M_Y \to N$ from M_Y to N such that $\varphi_Y(y) = f(y)$ for all $y \in Y$.

Let Y and Z be finite subsets of X, where $Y \cap Z \neq \emptyset$. Then the restrictions of the R-module homomorphisms $\varphi_Y: M_Y \to N$ and $\varphi_Z: M_Z \to N$ to $M_{Y\cap Z}$ are R-module homomorphisms from $M_{Y\cap Z}$ to N that extend $f|Y\cap Z: Y\cap Z \to N$. But we have shown that any extension of this function to an R-module homomorphism from $M_{Y\cap Z} \to N$ is uniquely-determined. Therefore

$$\varphi_Y|M_{Y\cap Z} = \varphi_Z|M_{Y\cap Z} = \varphi_{Y\cap Z}.$$

Next we show that $M_Y \cap M_Z = M_{Y\cap Z}$. Clearly $M_{Y\cap Z} \subset M_Y$ and $M_{Y\cap Z} \subset M_Z$. Let $Y \cup Z = \{x_1, x_2, \ldots, x_k\}$, where $x_1, x_2, \ldots, x_k$ are distinct. Then, given any element m of $M_Y \cap M_Z$, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1x_1 + r_2x_2 + \cdots + r_kx_k.$$

But this element m is expressible as a linear combination of elements of Y alone, and as a linear combination of elements of Z alone. Therefore, for each index i between 1 and k, the corresponding coefficient r_i is zero unless both $x_i \in Y$ and $x_i \in Z$. But this ensures that x is expressible as a linear combination of elements that belong to $Y \cap Z$. This verifies that $M_Y \cap M_Z = M_{Y \cap Z}$.

Let $m \in M$. Then m can be represented as a linear combination of the elements of some finite subset Y of X with coefficients in the ring R. But then $m \in M_Y$. It follows that M is the union of the submodules M_Y as Y ranges over all finite subsets of the generating set X.

Now there is a well-defined function $\varphi: M \to N$ characterized by the property that $\varphi(m) = \varphi_Y(m)$ whenever m belongs to M_Y for some finite subset Y of X. Indeed suppose that some element m of M belongs to both M_Y and M_Z, where Y and Z are finite subsets of M. Then $m \in M_{Y \cap Z}$, since we have shown that $M_Y \cap M_Z = M_{Y \cap Z}$. But then $\varphi_Y(m) = \varphi_{Y \cap Z}(m) = \varphi_Z(m)$. This result ensures that the homomorphisms $\varphi: M_Y \to N$ defined on the submodules M_Y of M generated by finite subsets Y of X can be pieced together to yield the required function $\varphi: M \to N$. Moreover, given elements x and y of M, there exists some finite subset Y of M such that $x \in M_Y$ and $y \in M_Y$. Then

$$\varphi(x + y) = \varphi_Y(x + y) = \varphi_Y(x) + \varphi_Y(y) = \varphi(x) + \varphi(y),$$

and

$$\varphi(rx) = \varphi_Y(rx) = r\varphi_Y(x) = r\varphi(x)$$

for all $r \in R$. Thus the function $\varphi: M \to N$ is an R-module homomorphism. The uniqueness of the R-module homomorphisms φ_Y then ensures that $\varphi: M \to N$ is the unique R-module homomorphism from M to N that extends $f: X \to N$, as required. ∎

Proposition 6.3 *Let R be a unital commutative ring, let M and N be R-modules, let F be a free R-module, let $\pi: M \to N$ be a surjective R-module homomorphism, and let $\varphi: F \to N$ be an R-module homomorphism. Then there exists an R-module homomorphism $\psi: F \to M$ such that $\varphi = \pi \circ \psi$.*

Proof Let X be a subset of the free module F that freely generates F. Now, because the R-module homomorphism $\pi: M \to N$ is surjective, there exists a function $f: X \to M$ such that $\pi(f(x)) = \varphi(x)$ for all $x \in X$. It then follows from Proposition 6.2 that there exists an R-module homomorphism $\psi: F \to M$ such that $\psi(x) = f(x)$ for all $x \in X$. Then $\pi(\psi(x)) = \pi(f(x)) = \varphi(x)$ for all $x \in X$. But it also follows from Proposition 6.2 that any R-module homomorphism from F to N that extends $\varphi|X: X \to N$ is uniquely determined. Therefore $\pi \circ \psi = \varphi$, as required. ∎

Proposition 6.4 *Let R be a unital commutative ring, let M be an R-module, let F be a free R-module and let $\pi\colon M \to F$ be a surjective R-module homomorphism. Then $M \cong \ker \pi \oplus F$.*

Proof It follows from Proposition 6.3 (applied to the identity automorphism of F) that there exists an R-module homomorphism $\psi\colon F \to M$ with the property that $\pi(\psi(f)) = f$ for all $f \in F$. Let $\theta\colon \ker \pi \oplus F \to M$ be defined so that $\theta(k, f) = k + \psi(f)$ for all $f \in F$. Then $\theta\colon \ker \pi \oplus F \to M$ is an R-module homomorphism. Now

$$\pi(m - \psi(\pi(m))) = \pi(m) - (\pi \circ \psi)(\pi(m)) = \pi(m) - \pi(m) = 0_F,$$

where 0_F denotes the zero element of F. Therefore $m - \psi(\pi(m)) \in \ker \pi$ for all $m \in M$. But then $m = \theta(m - \psi(\pi(m)), \pi(m))$ for all $m \in M$. Thus $\theta\colon \ker \pi \oplus F \to M$ is surjective.

Now let $(k, f) \in \ker \theta$, where $k \in \ker \pi$ and $f \in F$. Then $\psi(f) = -k$. But then $f = \pi(\psi(f)) = -\pi(k) = 0_F$. Also $k = \psi(0_F) = 0_M$, where 0_M denotes the zero element of the module M. Therefore the homomorphism $\theta\colon \ker \pi \oplus F \to M$ has trivial kernel and is therefore injective. This homomorphism is also surjective. It is therefore an isomorphism between $\ker \pi \oplus F$ and M. The result follows. ∎

6.2 Free Modules over Integral Domains

Definition A module M over an integral domain R is said to be a free module of finite rank if there exist elements $b_1, b_2, \ldots, b_k \in M$ that constitute a free basis for M. These elements constitute a free basis if and only if, given any element m of M, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1 b_1 + r_2 b_2 + \cdots + r_k b_k.$$

Proposition 6.5 *Let M be a free module of finite rank over an integral domain R, let $b_1, b_2, \ldots, b_k$ be a free basis for M, and let $m_1, m_2, \ldots, m_p$ be elements of M. Suppose that $p > k$, where k is the number elements constituting the free basis of m. Then the elements $m_1, m_2, \ldots, m_p$ are linearly dependent over R.*

Proof We prove the result by induction on the number k of elements in the free basis. Suppose that $k = 1$, and that $p > 1$. If either of the elements m_1 or m_2 is the zero element 0_M then $m_1, m_2, \ldots, m_p$ are certainly linearly dependent. Suppose therefore that $m_1 \neq 0_M$ and $m_2 \neq 0_M$. Then there exist non-zero elements s_1 and s_2 of the ring R such that $m_1 = s_1 b_1$, and $m_2 = s_2 b_1$, because $\{b_1\}$ generates the module M. But then $s_2 m_1 - s_1 m_2 = 0_M$. It follows that the elements m_1 and m_2 are linearly dependent over R. This completes the proof in the case when $k = 1$.

Suppose now that M has a free basis with k elements, where $k > 1$, and that the result is true in all free modules that have a free basis with fewer than k elements. Let $b_1, b_2, \ldots, b_k$ be a free basis for M. Let $\nu: M \to R$ be defined such that

$$\nu(r_1 b_1 + r_2 b_2 + \cdots + r_k b_k) = r_1.$$

Then $\nu: M \to R$ is a well-defined homomorphism of R-modules, and $\ker \nu$ is a free R-module with free basis $b_2, b_3, \ldots, b_k$. The induction hypothesis therefore guarantees that any subset of $\ker \nu$ with more than $k - 1$ elements is linearly dependent over R.

Let $m_1, m_2, \ldots, m_p$ be a subset of M with p elements, where $p > k$. If $\nu(m_j) = 0_R$ for $j = 1, 2, \ldots, p$, where 0_R denotes the zero element of the integral domain R, then this set is a subset of $\ker \nu$, and is therefore linearly dependent. Otherwise $\nu(m_j) \neq 0_R$ for at least one value of j between 1 and p. We may assume without loss of generality that $\nu(m_1) \neq 0_R$. Let

$$m'_j = \nu(m_1) m_j - \nu(m_j) m_1 \quad \text{for} \quad j = 2, 3, \ldots, p.$$

Then $\nu(m'_j) = 0$, and thus $m'_j \in \ker \nu$ for $j = 2, 3, \ldots, p$. It follows from the induction hypothesis that the elements $m'_2, m'_3, \ldots, m'_p$ of $\ker \nu$ are linearly dependent. Thus there exist elements $r_2, r_3, \ldots, r_p$ of R, not all zero, such that

$$\sum_{j=2}^{p} r_j m'_j = 0_M.$$

But then

$$-\left(\sum_{j=2}^{p} r_j \nu(m_j) \right) m_1 + \sum_{j=2}^{p} r_j \nu(m_1) m_j = 0_M.$$

Now $\nu(m_1) \neq 0_R$. Also $r_j \neq 0_R$ for at least one value of j between 2 and p, and any product of non-zero elements of the integral domain R is a non-zero element of R. It follows that $r_j \nu(m_1) \neq 0_R$ for at least one value of j between 2 and p. We conclude therefore that the elements $m_1, m_2, \ldots, m_p$ are linearly dependent (since we have expressed the zero element of M above as a linear combination of $m_1, m_2, \ldots, m_p$ whose coefficients are not all zero). The required result therefore follows by induction on the number k of elements in the free basis of M. ∎

Corollary 6.6 *Let M be a free module of finite rank over an integral domain R. Then any two free bases of M have the same number of elements.*

Proof Suppose that $b_1, b_2, \dots, b_k$ is a free basis of M. The elements of any other free basis are linearly independent. It therefore follows from Proposition 6.5 that no free basis of M can have more than k elements. Thus the number of elements constituting one free basis of M cannot exceed the number of elements constituting any other free basis of M. The result follows. ∎

Definition The *rank* of a free module is the number of elements in any free basis for the free module.

Corollary 6.7 *Let M be a module over an integral domain R. Suppose that M is generated by some finite subset of M that has k elements. If some other subset of M has more than k elements, then those elements are linearly dependent.*

Proof Suppose that M is generated by the set $g_1, g_2, \dots, g_k$. Let $\theta: R^k \to M$ be the R-module homomorphism defined such that

$$\theta(r_1, r_2, \dots, r_k) = \sum_{j=1}^{k} r_j g_j$$

for all $(r_1, r_2, \dots, r_k) \in R^k$. Then the R-module homomorphism $\theta: R^k \to M$ is surjective.

Let $m_1, m_2, \dots, m_p$ be elements of M, where $p > k$. Then there exist elements $t_1, t_2, \dots, t_p$ of R^k such that $\theta(t_j) = m_j$ for $j = 1, 2, \dots, p$. Now R^k is a free module of rank k. It follows from Proposition 6.5 that the elements $t_1, t_2, \dots, t_p$ are linearly dependent. Therefore there exist elements $r_1, r_2, \dots, r_p$ of R, not all zero, such that

$$r_1 t_1 + r_2 t_2 + \cdots + r_p t_p$$

is the zero element of R^k. But then

$$r_1 m_1 + r_2 m_2 + \cdots + r_p m_p = \theta(r_1 t_1 + r_2 t_2 + \cdots + r_p t_p) = 0_M,$$

where 0_M denotes the zero element of the module M. Thus the elements $m_1, m_2, \dots, m_p$ are linearly dependent. The result follows. ∎

6.3 Torsion Modules

Definition A module M over an integral domain R is said to be a *torsion module* if, given any element m of M, there exists some non-zero element r of R such that $rm = 0_M$, where 0_M is the zero element of M.

Lemma 6.8 *Let M be a finitely-generated torsion module over an integral domain R. Then there exists some non-zero element t of R with the property that $tm = 0_M$ for all $m \in M$, where 0_M denotes the zero element of M.*

Proof Let M be generated as an R-module by $m_1, m_2, \ldots, m_k$. Then there exist non-zero elements $r_1, r_2, \ldots, r_k$ of R such that $r_i m_i = 0_M$ for $i = 1, 2, \ldots, k$. Let $t = r_1 r_2 \cdots r_k$. Now the product of any finite number of non-zero elements of an integral domain is non-zero. Therefore $t \neq 0$. Also $tm_i = 0_M$ for $i = 1, 2, \ldots, k$, because r_i divides t. Let $m \in M$. Then

$$m = s_1 m_1 + s_2 m_2 + \cdots + s_k m_k$$

for some $s_1, s_2, \ldots, s_k \in R$. Then

$$\begin{aligned} tm &= t(s_1 m_1 + s_2 m_2 + \cdots + s_k m_k) \\ &= s_1(tm_1) + s_2(tm_2) + \cdots + s_k(tm_k) = 0_M, \end{aligned}$$

as required. ∎

6.4 Free Modules of Finite Rank over Principal Ideal Domains

Proposition 6.9 *Let M be a free module of rank n over a principal ideal domain R. Then every submodule of M is a free module of rank at most n over R.*

Proof We prove the result by induction on the rank of the free module.

Let M be a free module of rank 1. Then there exists some element b of M that by itself constitutes a free basis of M. Then, given any element m of M, there exists a uniquely-determined element r of R such that $m = rb$. Given any non-zero submodule N of M, let

$$I = \{r \in R : rb \in N\}.$$

Then I is an ideal of R, and therefore there exists some element s of R such that $I = (s)$. Then, given $n \in N$, there is a uniquely determined element r of R such that $n = rsb$. Thus N is freely generated by sb. The result is therefore true when the module M is free of rank 1.

Suppose that the result is true for all modules over R that are free of rank less than k. We prove that the result holds for free modules of rank k. Let M be a free module of rank k over R. Then there exists a free basis $b_1, b_2, \ldots, b_k$ for M. Let $\nu\colon M \to R$ be defined such that

$$\nu(r_1 b_1 + r_2 b_2 + \cdots + r_k b_k) = r_1.$$

Then $\nu: M \to R$ is a well-defined homomorphism of R-modules, and $\ker \nu$ is a free R-module of rank $k-1$.

Let N be a submodule of M. If $N \subset \ker \nu$ the result follows immediately from the induction hypothesis. Otherwise $\nu(N)$ is a non-zero submodule of a free R-module of rank 1, and therefore there exists some element $n_1 \in N$ such that $\nu(N) = \{r\nu(n_1) : r \in R\}$. Now $N \cap \ker \nu$ is a submodule of a free module of rank $k-1$, and therefore it follows from the induction hypothesis that there exist elements $n_2, \ldots, n_p$ of $N \cap \ker \nu$ that constitute a free basis for $N \cap \ker \nu$. Moreover $p \leq k$, because the induction hypothesis ensures that the rank of $N \cap \ker \nu$ is at most $k-1$

Let $n \in N$. Then there is a uniquely-determined element r_1 of R such that $\nu(n) = r_1\nu(n_1)$. Then $n - r_1 n_1 \in N \cap \ker \nu$, and therefore there exist uniquely-determined elements $r_2, \ldots, r_p$ of R such that

$$n - r_1 n_1 = r_2 n_2 + \cdots r_p n_p.$$

It follows directly from this that $n_1, n_2, \ldots, n_p$ freely generate N. Thus N is a free R-module of finite rank, and

$$\operatorname{rank} N = p \leq k = \operatorname{rank} M.$$

The result therefore follows by induction on the rank of M. ∎

6.5 Torsion-Free Modules

Definition A module M over an integral domain R is said to be *torsion-free* if rm is non-zero for all non-zero elements r of R and for all non-zero elements m of M.

Proposition 6.10 *Let M be a finitely-generated torsion-free module over a principal ideal domain R. Then M is a free module of finite rank over R.*

Proof It follows from Corollary 6.7 that if M is generated by a finite set with k elements, then no linearly independent subset of M can have more than k elements. Therefore there exists a linearly independent subset of M which has at least as many elements as any other linearly independent subset of M. Let the elements of this subset be $b_1, b_2, \ldots, b_p$, where $b_i \neq b_j$ whenever $i \neq j$, and let F be the submodule of M generated by $b_1, b_2, \ldots, b_p$. The linear independence of $b_1, b_2, \ldots, b_p$ ensures that every element of F may be represented uniquely as a linear combination of $b_1, b_2, \ldots, b_p$. It follows that F is a free module over R with basis $b_1, b_2, \ldots, b_p$.

Let $m \in M$. The choice of $b_1, b_2, \ldots, b_p$ so as to maximize the number of members in a list of linearly-independent elements of M ensures that the elements $b_1, b_2, \ldots, b_p, m$ are linearly dependent. Therefore there exist elements $s_1, s_2, \ldots, s_p$ and r of R, not all zero, such that

$$s_1 b_1 + s_2 b_2 + \cdots + s_p b_p - rm = 0_M$$

(where 0_M denotes the zero element of M). If it were the case that $r = 0_R$, where 0_R denotes the zero element of R, then the elements $b_1, b_2, \ldots, b_p$ would be linearly dependent. The fact that these elements are chosen to be linearly independent therefore ensures that $r \neq 0_R$. It follows from this that, given any element m of M, there exists a non-zero element r of R such that $rm \in F$. Then $r(m+F) = F$ in the quotient module M/F. We have thus shown that the quotient module M/F is a torsion module. It is also finitely generated, since M is finitely generated. It follows from Lemma 6.8 that there exists some non-zero element t of the integral domain R such that $t(m+F) = F$ for all $m \in M$. Then $tm \in F$ for all $m \in M$.

Let $\varphi: M \to F$ be the function defined such that $\varphi(m) = tm$ for all $m \in M$. Then φ is a homomorphism of R-modules, and its image is a submodule of F. Now the requirement that the module M be torsion-free ensures that $tm \neq 0_M$ whenever $m \neq 0_M$. Therefore $\varphi: M \to F$ is injective. It follows that $\varphi(M) \cong M$. Now R is a principal ideal domain, and any submodule of a free module of finite rank over a principal ideal domain is itself a free module of finite rank (Proposition 6.9). Therefore $\varphi(M)$ is a free module. But this free module is isomorphic to M. Therefore the finitely-generated torsion-free module M must itself be a free module of finite rank, as required. ∎

Lemma 6.11 *Let M be a module over an integral domain R, and let*

$$T = \{m \in M : rm = 0_M \textit{ for some non-zero element } r \textit{ of } R\},$$

where 0_M denotes the zero element of M. Then T is a submodule of M.

Proof Let $m_1, m_2 \in T$. Then there exist non-zero elements s_1 and s_2 of R such that $s_1 m_1 = 0_M$ and $s_2 m_2 = 0_M$. Let $s = s_1 s_2$. The requirement that the coefficient ring R be an integral domain then ensures that s is a non-zero element of R. Also $s m_1 = 0_M$, $s m_2 = 0_M$, and $s(r m_1) = r(s m_1) = 0_M$ for all $r \in R$. Thus $m_1 + m_2 \in T$ and $r m_1 \in T$ for all $r \in R$. It follows that T is a submodule of R, as required. ∎

Definition Let M be a module over an integral domain R. The *torsion submodule* of M is the submodule T of M defined such that

$$T = \{m \in M : rm = 0_M \text{ for some non-zero element } r \text{ of } R\},$$

where 0_M denotes the zero element of M. Thus an element m of M belongs to the torsion submodule T of M if and only if there exists some non-zero element r of R for which $rm = 0_M$.

Proposition 6.12 *Let M be a finitely-generated module over a principal ideal domain R. Then there exists a torsion module T over R and a free module F of finite rank over R such that $M \cong T \oplus F$.*

Proof Let T be the torsion submodule of M. We first prove that the quotient module M/T is torsion-free.

Let $m \in M$, and let r be a non-zero element of the ring R. Suppose that $rm \in T$. Then there exists some non-zero element s of R such that $s(rm) = 0_M$. But then $(sr)m = 0_M$ and $sr \neq 0_R$ (because R is an integral domain), and therefore $m \in T$. It follows that if $m \in M$, $r \neq 0_R$ and $m \notin T$ then $rm \notin T$. Thus if $m + T$ is a non-zero element of the quotient module M/T then so is $rm + T$ for all non-zero elements r of the ring R. We have thus shown that the quotient module M/T is a torsion-free module over R.

It now follows from Proposition 6.10 that M/T is a free module of finite rank over the principal ideal domain R. Let $F = M/T$, and let $\nu: M \to F$ be the quotient homomorphism defined such that $\nu(m) = m + T$ for all $m \in M$. Then $\ker \nu = T$. It follows immediately from Proposition 6.4 that $M \cong T \oplus F$. The result follows. ∎

6.6 Finitely-Generated Torsion Modules over Principal Ideal Domains

Let M be a finitely-generated torsion module over an integral domain R. Then there exists some non-zero element t of R with the property that $tm = 0_M$ for all $m \in M$, where 0_M denotes the zero element of M (Lemma 6.8).

Proposition 6.13 *Let M be a finitely-generated torsion module over a principal ideal domain R, and let t be a non-zero element of R with the property that $tm = 0_M$ for all $m \in M$. Let $t = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where $k_1, k_2, \ldots, k_s$ are positive integers and $p_1, p_2, \ldots, p_s$ are prime elements of R that are pairwise coprime (so that p_i and p_j are coprime whenever $i \neq j$). Then there exist unique submodules $M_1, M_2, \ldots, M_s$ of M such that the following conditions are satisfied:—*

(i) *the submodule M_i is finitely generated for $i = 1, 2, \ldots, s$;*

(ii) *$M = M_1 \oplus M_2 \oplus \cdots \oplus M_s$;*

(iii) $M_i = \{m \in M : p_i^{k_i} m = 0_M\}$ *for* $i = 1, 2, \ldots, s$.

Proof The result is immediate if $s = 1$. Suppose that $s > 1$. Let $v_i = \prod_{j \neq i} p_j^{k_j}$ for $i = 1, 2, \ldots, s$ (so that v_i is the product of the factors $p_j^{k_j}$ of t for $j \neq i$). Then, for each integer i between 1 and s, the elements p_i and v_i of R are coprime, and $t = v_i p_i^{k_i}$. Moreover any prime element of R that is a common divisor of $v_1, v_2, \ldots, v_s$ must be an associate of one the prime elements $p_1, p_2, \ldots, \ldots, p_s$ of R. But p_i does not divide v_i for $i = 1, 2, \ldots, s$. It follows that no prime element of R is a common divisor of $v_1, v_2, \ldots, v_s$, and therefore any common divisor of these elements of R must be a unit of R (i.e., the elements $v_1, v_2, \ldots, v_s$ of R are coprime). It follows from Lemma 2.7 that there exist elements $w_1, w_2, \ldots, w_s$ of R such that

$$v_1 w_1 + v_2 w_2 + \cdots + v_s w_s = 1_R,$$

where 1_R denotes the multiplicative identity element of R.

Let $q_i = v_i w_i$ for $i = 1, 2, \ldots, s$. Then $q_1 + q_2 + \cdots + q_s = 1_R$, and therefore

$$m = \sum_{i=1}^{s} q_i m$$

for all $m \in M$. Now t is the product of the elements $p_i^{k_i}$ for $i = 1, 2, \ldots, s$. Also $p_j^{k_j}$ divides v_i and therefore divides q_i whenever $j \neq i$. It follows that t divides $p_i^{k_i} q_i$ for $i = 1, 2, \ldots, s$, and therefore $p_i^{k_i} q_i m = 0_M$ for all $m \in M$. Thus $q_i m \in M_i$ for $i = 1, 2, \ldots, s$, where

$$M_i = \{m \in M : p_i^{k_i} m = 0_M.\}$$

It follows that the homomorphism

$$\varphi \colon M_1 \oplus M_2 \oplus \cdots \oplus M_s \to M$$

from $M_1 \oplus M_2 \oplus \cdots \oplus M_s$ to M that sends $(m_1, m_2, \ldots, m_s)$ to $m_1 + m_2 + \cdots + m_s$ is surjective. Let $(m_1, m_2, \ldots, m_s) \in \ker \varphi$. Then $p_i^{k_i} m_i = 0$ for $i = 1, 2, \ldots, s$, and

$$m_1 + m_2 + \cdots + m_s = 0_M$$

Now $v_i m_j = 0$ when $i \neq j$ because $p_j^{k_j}$ divides v_i. It follows that $q_i m_j = 0$ whenever $i \neq j$, and therefore

$$m_j = q_1 m_j + q_2 m_j + \cdots + q_s m_j = q_j m_j$$

for $j = 1, 2, \ldots, s$. But then

$$0_M = q_i(m_1 + m_2 + \cdots + m_s) = q_i m_i = m_i.$$

Thus $\ker \varphi = \{(0_M, 0_M, \ldots, 0_M)\}$. We conclude that the homomorphism

$$\varphi\colon M_1 \oplus M_2 \oplus \cdots \oplus M_s \to M$$

is thus both injective and surjective, and is thus an isomorphism.

Moreover M_i is finitely generated for $i = 1, 2, \ldots, s$. Indeed $M_i = \{q_i m : m \in M\}$. Thus if the elements $f_1, f_2, \ldots, f_n$ generate M then the elements $q_i f_1, q_i f_2, \ldots, q_i f_n$ generate M_i. The result follows. ∎

Proposition 6.14 *Let M be a finitely-generated torsion module over a principal ideal domain R, let p be a prime element of R, and let k be a positive integer. Suppose that $p^k m = 0_M$ for all $m \in M$. Then there exist elements $b_1, b_2, \ldots, b_s$ of M and positive integers $k_1, k_2, \ldots, k_s$, where $1 \leq k_i \leq k$ for $i = 1, 2, \ldots, s$, such that the following conditions are satisfied:*

(i) *every element of M can be expressed in the form*

$$r_1 b_1 + r_2 b_2 + \cdots + r_s b_s$$

for some elements $r_1, r_2, \ldots, r_s \in R$;

(ii) *elements $r_1, r_2, \ldots, r_s$ of R satisfy*

$$r_1 b_1 + r_2 b_2 + \cdots + r_s b_s = 0_M$$

if and only if p^{k_i} divides r_i for $i = 1, 2, \ldots, s$.

Proof We prove the result by induction on the number of generators of the finitely-generated torsion module M. Suppose that M is generated by a single element g_1. Then every element of M can be represented in the form $r_1 g_1$ for some $r_1 \in R$. Let $\varphi\colon R \to M$ be defined such that $\varphi(r) = r g_1$ for all $r \in R$. Then φ is a surjective R-module homomorphism, and therefore $M \cong R/\ker \varphi$. Now $p^k \in \ker \varphi$, because $p^k m = 0_M$. Moreover R is a principal ideal domain, and therefore $\ker \varphi$ is the ideal tR generated by some element t of R. Now t divides p^k. It follows from the unique factorization property possessed by principal ideal domains (Proposition 2.21) that t is an associate of p^{k_1} for some integer k_1 satisfying $1 \leq k_1 \leq k$. But then $r_1 g_1 = 0_M$ if and only if p^{k_1} divides r_1. The proposition therefore holds when the torsion module M is generated by a single generator.

Now suppose that the stated result is true for all torsion modules over the principal ideal domain R that are generated by fewer than n generators. Let $g_1, g_2, \ldots, g_n$ be generators of the module M, and let p be a prime element of R, and suppose that there exists some positive integer k with the property that $p^k m = 0_M$ for all $m \in M$. Let k be the smallest positive integer with this property. Now if h is a positive integer with the property that $p^h g_i = 0_M$ for $i = 1, 2, \ldots, n$ then $p^h m = 0_M$ for all $m \in M$, and therefore $h \geq k$. It follows that there exists some integer i between 1 and n such that $p^{k-1} g_i \neq 0_M$. Without loss of generality, we may assume that the generators have been ordered so that $p^{k-1} g_1 \neq 0_M$. Let $b_1 = g_1$ and $k_1 = k$. Then an element r of R satisfies $r b_1 = 0_M$ if and only if p^k divides r.

Let L be the submodule of M generated by b_1. Then the quotient module M/L is generated by $L + g_2, L + g_3, \ldots, L + g_n$. It follows from the induction hypothesis that the proposition is true for the quotient module M/L, and therefore there exist elements $\hat{b}_2, \hat{b}_3, \ldots, \hat{b}_s$ of M/L such that generate M/L and positive integers $k_2, k_3, \ldots, k_s$ such that

$$r_2 \hat{b}_2 + r_3 \hat{b}_3 + \cdots + r_s \hat{b}_s = 0_{M/L}$$

if and only if p^{k_i} divides r_i for $i = 2, 3, \ldots, s$. Let $m_2, m_3, \ldots, m_s$ be elements of M chosen such that $m_i + L = \hat{b}_i$ for $i = 2, 3, \ldots, s$. Then $p^{k_i} m_i \in L$ for $i = 1, 2, \ldots, s$, and therefore $p^{k_i} m_i = t_i b_1$ for some element t_i of R, where $k_i \leq k$. Moreover

$$0_M = p^k m_i = p^{k-k_i} p^{k_i} m_i = p^{k-k_i} t_i b_1,$$

and therefore p^k divides $p^{k-k_i} t_i$ in R. It follows that p^{k_i} divides t_i in R for $i = 2, 3, \ldots, s$. Let $v_2, v_3, \ldots, v_s \in R$ be chosen such that $t_i = p^{k_i} v_i$ for $i = 2, 3, \ldots, s$, and let $b_i = m_i - v_i b_1$. Then $p^{k_i} b_i = p^{k_i} m_i - t_i b_1 = 0_M$ and $b_i + L = \hat{b}_i$ for $i = 2, 3, \ldots, s$.

Now, given $m \in M$, there exist elements $r_2, r_3, \ldots, r_s \in R$ such that

$$m + L = r_2 \hat{b}_2 + r_3 \hat{b}_3 + \cdots + r_s \hat{b}_s = r_2 b_2 + r_3 b_3 + \cdots + r_s b_s + L.$$

Then

$$r_2 b_2 + r_3 b_3 + \cdots + r_s b_s - m \in L$$

and therefore there exists $r_1 \in R$ such that

$$r_2 b_2 + r_3 b_3 + \cdots + r_s b_s - m = -r_1 b_1,$$

and thus

$$m = r_1 b_1 + r_2 b_2 + r_3 b_3 + \cdots + r_s b_s.$$

This shows that the elements $b_1, b_2, \ldots, b_s$ of M generate the R-module M.

Now suppose that $r_1, r_2, \ldots, r_s$ are elements of R with the property that

$$r_1 b_1 + r_2 b_2 + r_3 b_3 + \cdots + r_s b_s = 0_M.$$

Then

$$r_2 \hat{b}_2 + r_3 \hat{b}_3 + \cdots + r_s \hat{b}_s = 0_{M/L},$$

because $b_1 \in L$ and $b_i + L = \hat{b}_i$ when $i > 1$, and therefore p^{k_i} divides r_i for $i = 2, 3, \ldots, s$. But then $r_i b_i = 0_M$ for $i = 2, 3, \ldots, s$, and thus $r_1 b_1 = 0_M$. But then p^{k_1} divides r_1. The result follows. ∎

Corollary 6.15 *Let M be a finitely-generated torsion module over a principal ideal domain R, let p be a prime element of R, and let k be a positive integer. Suppose that $p^k m = 0_M$ for all $m \in M$. Then there exist submodules $L_1, L_2, \ldots, L_s$ of M and positive integers $k_1, k_2, \ldots, k_s$, where $1 \leq k_i \leq k_s$ for $i = 1, 2, \ldots, s$, such that*

$$M = L_1 \oplus L_2 \oplus \cdots \oplus L_s$$

and

$$L_i \cong R/p^{k_i} R$$

for $i = 1, 2, \ldots, s$, where $p^{k_i} R$ denotes the ideal of R generated by p^{k_i}.

Proof Let $b_1, b_2, \ldots, b_s$ and $k_1, k_2, \ldots, k_s$ have the properties listed in the statement of Proposition 6.14. Then each b_i generates a submodule L_i of M that is isomorphic to $R/p^{k_i} R$. Moreover M is the direct sum of these submodules, as required. ∎

6.7 Cyclic Modules and Order Ideals

Definition A module M over a unital commutative ring R is said to be *cyclic* if there exists some element b of M that generates M.

Let M be a cyclic module over a unital commutative ring R, and let b be a generator of M. Let $\varphi: R \to M$ be the R-module homomorphism defined such that $\varphi(r) = rb$ for all $r \in R$. Then $\ker \varphi$ is an ideal of R. Moreover if $s \in \ker \varphi$ then $srb = rsb = 0_M$ for all $r \in R$, and therefore $sm = 0_M$ for all $m \in M$. Thus

$$\ker \varphi = \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Definition Let M be a cyclic module over a unital commutative ring R. The *order ideal* $\mathbf{o}(M)$ is the ideal

$$\mathbf{o}(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Lemma 6.16 *Let M be a cyclic module over a unital commutative ring R, and let $\mathbf{o}(M)$ the the order ideal of M. Then $M \cong R/\mathbf{o}(M)$.*

Proof Choose a generator b of M. The R-module homomorphism that sends $r \in R$ to rb is surjective, and its kernel is $\mathbf{o}(M)$. The result follows. ∎

6.8 The Structure of Finitely-Generated Modules over Principal Ideal Domains

Proposition 6.17 *Let M be a finitely generated module over a principal ideal domain R. Then M can be decomposed as a direct sum of cyclic modules.*

Proof Let T be the torsion submodule of M. Then there exists a submodule F of M such that $M = T \oplus F$ and F is a free module of finite rank (Proposition 6.12). Now $F \cong R^d$, where d is the rank of F. Indeed if $b_1, b_2, \ldots, b_d$ is a free basis for F then the function sending $(r_1, r_2, \ldots, r_d)$ to

$$r_1 b_1 + r_2 b_2 + \cdots + r_d b_d$$

is an R-module isomorphism from the direct sum R^d of d copies of the ring R to F. Moreover R is itself a cyclic R-module, since it is generated by its multiplicative identity element 1_R.

On applying Proposition 6.13 to the torsion module T, we conclude that there exist positive integers $k_1, k_2, \ldots, k_s$, prime elements $p_1, p_2, \ldots, p_s$ of R that are pairwise coprime, and uniquely-determined finitely-generated submodules such that $T_i = \{m \in M : p_i^{k_i} m = 0_M\}$ for $i = 1, 2, \ldots, s$ and

$$T = T_1 \oplus T_2 \oplus \cdots \oplus T_s.$$

It then follows from Corollary 6.15 that each T_i can in turn be decomposed as a direct sum of cyclic submodules. The result follows. ∎

Let R, M, T and F, d, $T_1, T_2, \ldots, T_s$, $p_1, p_2, \ldots, p_s$ and $k_1, k_2, \ldots, k_s$ be defined as in the proof of Proposition 6.17. Then $F \cong M/T$. Now any two free bases of F have the same number of elements, and thus the rank of F is well-defined (Corollary 6.6). Therefore d is uniquely-determined.

Also the prime elements $p_1, p_2, \ldots, p_s$ of R are uniquely-determined up to multiplication by units, and the corresponding submodules $T_1, T_2, \ldots, T_s$ are determined by $p_1, p_2, \ldots, p_s$.

However the splitting of the submodule T_i of M determined by p_i into cyclic submodules is in general not determined.

Lemma 6.18 *Let R be a principal ideal domain and p is a prime element of R. Then R/pR is a field.*

Proof Let I be an ideal satisfying $pR \subset I \subset R$ then there exists some element s of R such that $I = sR$. But then s divides p, and p is prime, and therefore either s is a unit, in which case $I = R$, or else s is an associate of p, in which case $I = pR$. In other words the ideal pR is a maximal ideal of the principal ideal domain R whenever $p \in R$ is prime. But then the only ideals of R/pR are the zero ideal and the quotient ring R/pR itself, and therefore R/pR is a field, as required. ∎

Lemma 6.19 *Let R be a principal ideal domain, and let p be a prime element of R. Then $p^j R/p^{j+1}R \cong R/pR$ for all positive integers j.*

Proof Let $\theta_j \colon R \to p^j R/p^{j+1}R$ be the R-module homomorphism that sends $r \in R$ to $p^j r + p^{j+1}R$ for all $r \in R$. Then

$$\ker \theta_j = \{r \in R : p^j r \in p^{j+1}R\} = pR.$$

Indeed if $r \in R$ satisfies $p^j r \in p^{j+1}R$ then $p^j r = p^{j+1}s$ for some $s \in R$. But then $p^j(r - ps) = 0_R$ and therefore $r = ps$, because R is an integral domain. It follows that $\theta_h \colon R \to p^j R/p^{j+1}R$ induces an isomorphism from R/pR to $p^j R/p^{j+1}R$, and thus

$$R/pR \cong p^j R/p^{j+1}R$$

for all positive integers j, as required. ∎

Proposition 6.20 *Let R be a principal ideal domain, let p be a prime element of R, and let L be a cyclic R-module, where $L \cong R/p^k R$ for some positive integer k. Then $p^j L/p^{j+1}L \cong R/pR$ when $j < k$, and $p^j L/p^{j+1}L$ is the zero module when $j \geq k$.*

Proof Suppose that $j < k$. Then

$$p^j L/p^{j+1}L \cong \frac{p^j R/p^k R}{p^{j+1}R/p^k R} \cong p^j R/p^{j+1}R \cong R/pR.$$

Indeed the R-module homomorphism from R/p^kR to $p^jR/p^{j+1}R$ that sends p^jr+p^kR to $p^jr+p^{j+1}R$ is surjective, and its kernel is the subgroup $p^{j+1}R/p^kR$ of p^jR/p^kR. But $p^jR/p^{j+1}R \cong R/pR$ (Lemma 6.19). This completes the proof when $j < k$. When $j \geq k$ then p^jL and $p^{j+1}L$ are both equal to the zero submodule of L and therefore their quotient is the zero module. The result follows. ∎

Let R be a principal ideal domain, let p be a prime element of R, and let $K = R/pR$. Then K is a field (Lemma 6.18). Let M be an R-module. Then $p^jM/p^{j+1}M$ is a vector space over the field K for all non-negative integers j. Indeed there is a well-defined multiplication operation $K \times (p^jM/p^{j+1}M) \to M/p^{j+1}M$ defined such that $(r + pR)(p^jx + p^{j+1}M) = p^jrx + p^{j+1}M$ for all $r \in R$ and $x \in M$, and this multiplication operation satisfies all the vector space axioms.

Proposition 6.21 *Let M be a finitely-generated module over a principal ideal domain R. Suppose that $p^kM = \{0_M\}$ for some prime element p of R. Let $k_1, k_2, \ldots, k_s$ be non-negative integers chosen such that*

$$M = L_1 \oplus L_2 \oplus \cdots \oplus L_s$$

and

$$L_i \cong R/p^{k_i}R$$

for $i = 1, 2, \ldots, s$. Let K be the vector space R/pR. Then, for each non-negative integer j, the dimension $\dim_K p^jM/p^{j+1}M$ of $p^jM/p^{j+1}M$ is equal to the number of values of i satisfying $1 \leq i \leq s$ for which $k_i > j$.

Proof Let L be a cyclic R-module, where $L \cong R/p^kR$ for some positive integer k. Then For each value of i between 1 and s, the quotient module $p^jL_i/p^{j+1}L_i$ is a field over the vector space K. Now

$$p^jM/p^{j+1}M \cong p^jL_1/p^{j+1}L_1 \oplus p^jL_2/p^{j+1}L_2 \oplus \cdots \oplus p^jL_s/p^{j+1}L_s,$$

and therefore

$$\dim_K p^jM/p^{j+1}M = \sum_{i=1}^{s} \dim_K p^jL_i/p^{j+1}L_i.$$

It then follows from Proposition 6.20 that

$$\dim_K p^jL_i/p^{j+1}L_i = \begin{cases} 1 & \text{if } j < k_i; \\ 0 & \text{if } j \geq k_i. \end{cases}$$

Therefore $\dim_K p^jM/p^{j+1}M$ is equal to the number of values of i between 1 and s for which $k_i > j$, as required. ∎

Proposition 6.22 *Let M be a finitely-generated module over a principal ideal domain R. Suppose that $p^k M = \{0_M\}$ for some prime element p of R. Then the isomorphism class of M is determined by the sequence of values of* $\dim_K p^j M/p^{j+1}M$*, where $0 \leq j < k$.*

Proof It follows from Corollary 6.15 that there exist non-negative integers $k_1, k_2, \ldots, k_s$ such that

$$M = L_1 \oplus L_2 \oplus \cdots \oplus L_s$$

and

$$L_i \cong R/p^{k_i}R$$

for $i = 1, 2, \ldots, s$. Let K be the vector space R/pR. Suppose that the exponents $k_1, k_2, \ldots, k_s$ are ordered such that $k_1 \leq k_2 \leq \cdots \leq k_s$. Then, for each non-negative integer j, the dimension $\dim_K p^j M/p^{j+1}M$ is equal to the number of values of i satisfying $1 \leq i \leq s$ for which $k_i > j$. Therefore $s - \dim_K M/pM$ is equal to the number of values of i satisfying $1 \leq i \leq s$ for which $k_i = 0$, and, for $j > 1$, $\dim_K p^j M/p^{j+1}M - p^{j-1}M/p^j M$ is equal to the number of values of i satisfying $1 \leq i \leq s$ for which $k_i = j$. These quantities determine $k_1, k_2, \ldots, k_s$, and therefore determine the isomorphism class of M, as required. ∎

Theorem 6.23 (Structure Theorem for Finitely-Generated Modules over a Principal Ideal Domain) *Let M be a finitely-generated module over a principal ideal domain R. Then there exist prime elements $p_1, p_2, \ldots, p_s$ of R and uniquely-determined non-negative integers d and $k_{i,1}, k_{i,2}, \ldots, k_{i,m_i}$, where*

$$k_{i,1} \leq k_{i,2} \leq \cdots \leq k_{i,m_i},$$

such that M is isomorphic to the direct sum of the free R-module R^d and the cyclic modules $R/p_i^{k_{i,j}}R$ for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, m_i$. The non-negative integer d is uniquely determined, the prime elements $p_1, p_2, \ldots, p_s$ are deteremined subject to reordering and replacement by associates, and the non-negative integers $k_{i,1}, k_{i,2}, \ldots, k_{i,m_i}$ are uniquely determined, once p_i has been determined for $i = 1, 2, \ldots, s$, subject to the requirement that

$$k_{i,1} \leq k_{i,2} \leq \ldots \leq k_{i,m_i}.$$

Proof The existence of the integer d and the prime elements $p_1, p_2, \ldots, p_s$ and the non-negative integers $k_{i,j}$ follow from Proposition 6.17, Proposition 6.12, and Proposition 6.13. The uniqueness of d follows from the fact that d is equal to the rank of M/T, where T is the torson submodule of M. The uniqueness of $k_{i,1}, k_{i,2}, \ldots, k_{i,m_i}$ for $i = 1, 2, \ldots, s$, given $p_1, p_2, \ldots, p_s$ then follows on applying Proposition 6.22. ∎

6.9 The Jordan Normal Form

Let K be a field, and let V be a $K[x]$-module, where $K[x]$ is the ring of polynomials in the indeterminate x with coefficients in the field K. Let $T: V \to V$ be the function defined such that $Tv = xv$ for all $v \in V$. Then the function T is a linear operator on V. Thus any $K[x]$ module is a vector space that is provided with some linear operator T that determines the effect of multiplying elements of V by the polynomial x.

Now let $T: V \to V$ be a linear operator on a vector space V over some field K. Given any polynomial f with coefficients in K, let $f(x)v = f(T)v$ for all $v \in V$, so that

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)v = a_n T^n v + a_{n-1}T^{n-1}v + \cdots + a_0 v$$

for all $v \in V$. Then this operation of multiplication of elements of V by polynomials with coefficients in the field K gives V the structure of a module over the ring $K[x]$ of polynomials with coefficients in the field K.

Lemma 6.24 *Let V be a finite-dimensional vector space over a field K. let $T: V \to V$ be a linear operator on V, and let $f(x)v = f(T)v$ for all polynomials $f(x)$ with coefficients in the field K. Then V is a finitely-generated torsion module over the polynomial ring $K[x]$.*

Proof Let $\dim_K V = n$, and let $e_1, e_2, \ldots, e_n$ be a basis of V as a vector space over K. Then $e_1, e_2, \ldots, e_n$ generate V as a vector space over K, and therefore also generate V is a $K[x]$-module. Now, for each integer i between 1 and n, the elements

$$e_i, Te_i, T^2e_i, \ldots, T^n e_i$$

are linearly dependent, because the number of elements in this list exceeds the dimension of the vector space V, and therefore there exist elements $a_{i,0}, a_{i,1}, \ldots, a_{i,n}$ of K such that

$$a_{i,n}T^n e_i + a_{i,n-1}T^{n-1}e_i + \cdots + a_{i,0}e_i = 0_V,$$

where 0_V denotes the zero element of the vector space V. Let

$$f_i(x) = a_{i,n}x^n + a_{i,n-1}x^{n-1} + \cdots + a_{i,0},$$

and let $f(x) = f_1(x)\, f_2(x) \cdots f_n(x)$. Then $f_i(T)e_i = 0$ and thus $f(T)e_i = 0_V$ for $i = 1, 2, \ldots, n$ and for all $v \in V$. It follows that $f(T)v = 0_V$ for all $v \in V$. Thus V is a torsion module over the polynomial ring $K[x]$. ∎

A field K is said to be *algebraically closed* if every non-zero polynomial has at least one root in the field K. A polynomial $f(x)$ with coefficients in an algebraically closed field K is irreducible if and only if $f(x) = x - \lambda$ for some $\lambda \in K$.

Proposition 6.25 *Let V be a finite-dimensional vector space over an algebraically closed field K, and let $T: V \to V$ be a linear operator on V. Then there exist elements $\lambda_1, \lambda_2, \ldots, \lambda_s$ of K, and non-negative integers*

$$k_{i,1}, k_{i,2}, \ldots, k_{i,m_i} \quad (1 \leq i \leq s)$$

elements

$$v_{i,1}, v_{i,2}, \ldots, v_{i,m_i} \quad (1 \leq i \leq s)$$

of V, and vector subspaces

$$V_{i,1}, V_{i,2}, \ldots, V_{i,m_i} \quad (1 \leq i \leq s)$$

of V such that the following conditions are satisfied:—

(i) *V is the direct some of the vector subspaces $V_{i,j}$ for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, m_i$;*

(ii) *$V_{i,j} = \{f(T)v_{i,j} : f(x) \in K[x]\}$ for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, m_i$;*

(iii) *the ideal $\{f(x) \in K[x] : f(T)v_{i,j} = 0_V\}$ of the polynomial ring $K[x]$ is generated by the polynomial $(x - \lambda_i)^{k_{i,j}}$ for $i = 1, 2, \ldots, s$ and $j = 1, 2, \ldots, m_i$.*

Proof This result follows directly from Theorem 6.23 and Lemma 6.24. ∎

Let V be a finite-dimensional vector space over a field K, let $T: V \to V$ be a linear transformation, let v be an element of V with the property that

$$V = \{f(T)v : f \in K[x]\},$$

let k be a positive integer, and let λ be an element of the field K with the property that the ideal

$$\{f(x) \in K[x] : f(T)v = 0_V\}$$

of the polynomial ring $K[x]$ is generated by the polynomial $(x - \lambda)^k$. Let $v_j = (T - \lambda)^j v$ for $j = 0, 1, \ldots, k - 1$. Then V is a finite-dimensional vector space with basis $v_0, v_1, \ldots, v_{k-1}$ and $Tv_j = \lambda v_j + v_{j+1}$ for $j = 0, 1, \ldots, k$. The matrix of the linear operator V with respect to this basis then takes the form

$$\begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 & 0 \\ 1 & \lambda & 0 & \ldots & 0 & 0 \\ 0 & 1 & \lambda & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 0 \\ 0 & 0 & 0 & \ldots & 1 & \lambda \end{pmatrix}.$$

It follows from Proposition 6.25 that, given any vector space V over an algebraically closed field K, and given any linear operator $T: V \to V$ on V, there exists a basis of V with respect to which the matrix of T is a block diagonal matrix where the blocks are of the above form, and where the values occurring on the leading diagonal are the eigenvalues of the linear operator T. This result ensures in particular that any square matrix with complex coefficients is similar to a matrix in Jordan normal form.