Module MA3412: Integral Domains, Modules and Algebraic Integers
Hilary Term 2012

D. R. Wilkins

Contents

10 Integral Domains

10.1 Factorization in Integral Domains

An *integral domain* is a unital commutative ring in which the product of any two non-zero elements is itself a non-zero element.

Lemma 10.1 *Let x, y and z be elements of an integral domain. Suppose that $x \neq 0$ and $xy = xz$. Then $y = z$.*

Proof Suppose that these elements x, y and z satisfy $xy = xz$. Then $x(y - z) = 0$. Now the definition of an integral domain ensures that if a product of elements of an integral domain is zero, then at least one of the factors must be zero. Thus if $x \neq 0$ and $x(y - z) = 0$ then $y - z = 0$. But then $x = y$, as required. ∎

Definition An element u of an integral domain R is said to be a *unit* if there exists some element u^{-1} of R such that $uu^{-1} = 1$.

If u and v are units in an integral domain R then so are u^{-1} and uv. Indeed $(uv)(v^{-1}u^{-1}) = 1$, and thus $(uv)^{-1} = v^{-1}u^{-1}$. The set of units of R is thus a group with respect to the operation of multiplication.

Example The units of the ring $\mathbb{Z}$ of integers are 1 and -1.

Example Let K be a field. Then the units of the polynomial ring $K[x]$ are the non-zero constant polynomials.

Definition Elements x and y of an integral domain R are said to be *associates* if $y = xu$ (and $x = yu^{-1}$) for some unit u.

An *ideal* of a ring R is a subset I of R with the property that $0 \in I$, $x + y \in I$, $-x \in I$, $rx \in I$ and $xr \in I$ for all $x, y \in I$ and $r \in R$. A set X of elements of the ring R is said to *generate* the ideal I if there is no ideal J of R for which $X \subset J \subset I$ and $J \neq I$. The ideal generated by a subset X of R is the intersection of all ideals of R that contain this subset X. The following lemma characterizes the elements of ideals generated by subsets of unital commutative rings.

Lemma 10.2 *Let R be a unital commutative ring, and let X be a subset of R. Then the ideal generated by X coincides with the set of all elements of R that can be expressed as a finite sum of the form $r_1x_1 + r_2x_2 + \cdots + r_kx_k$, where $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$.*

Proof Let I be the subset of R consisting of all these finite sums. If J is any ideal of R which contains the set X then J must contain each of these finite sums, and thus $I \subset J$. Let a and b be elements of I. It follows immediately from the definition of I that $0 \in I$, $a + b \in I$, $-a \in I$, and $ra \in I$ for all $r \in R$. Also $ar = ra$, since R is commutative, and thus $ar \in I$. Thus I is an ideal of R. Moreover $X \subset I$, since the ring R is unital and $x = 1x$ for all $x \in X$. Thus I is the smallest ideal of R containing the set X, as required. ∎

Definition A *principal ideal* of an integral domain R is an ideal (x) generated by a single element x of R.

Let x and y be elements of an integral domain R. We write $x \mid y$ if and only if x divides y (i.e., $y = rx$ for some $r \in R$). Now $x \mid y$ if and only if $y \in (x)$, where (x) is the principal ideal of R generated by x. Thus $x \mid y$ if and only if $(y) \subset (x)$. Moreover an element u of R is a unit of R if and only if $(u) = R$.

Example Non zero integers x and y are associates in the ring $\mathbb{Z}$ of integers if and only if $|x| = |y|$.

Example Let K be a field. Then non-zero polynomials $p(x)$ and $q(x)$ with coefficients in the field K are associates in the polynomial ring $K[x]$ if and only if one polynomial is a constant multiple of the other.

Lemma 10.3 *Elements x and y of an integral domain R are associates if and only if $x|y$ and $y|x$.*

Proof If x and y are associates then clearly each divides the other. Conversely suppose that $x|y$ and $y|x$. If $x = 0$ or $y = 0$ there is nothing to prove. If x and y are non-zero then $y = xu$ and $x = yv$ for some $u, v \in R$. It follows that $x = xuv$ and thus $x(uv - 1) = 0$. But then $uv = 1$, since $x \neq 0$ and the product of any two non-zero elements of an integral domain is itself non-zero. Thus u and v are units of R, and hence x and y are associates, as required. ∎

Lemma 10.4 *Elements x and y of an integral domain R are associates if and only if $(x) = (y)$.*

Proof This follows directly from Lemma 10.3. ∎

Definition An element x of an integral domain R is *irreducible* if x is not a unit of R and, given any factorization of x of the form $x = yz$, one of the factors y and z is a unit of R and the other is an associate of x.

Example An integer n is an irreducible element of the ring $\mathbb{Z}$ of integers if and only if $|n|$ is a prime number.

Definition An element p of an integral domain R is said to be *prime* if p is neither zero nor a unit and, given any two elements r and s of R such that $p \mid rs$, either $p \mid r$ or $p \mid s$.

Lemma 10.5 *Any prime element of an integral domain is irreducible.*

Proof Let x be a prime element of an integral domain R. Then x is neither zero nor a unit of R. Suppose that $x = yz$ for some $y, z \in R$. Then either $x|y$ or $x|z$. If $x|y$, then it follows from Lemma 10.3 that x and y are associates, in which case z is a unit of R. If $x|z$ then x and z are associates and y is a unit of R. Thus x is irreducible. ∎

Let R be an integral domain, and let I be an ideal of R. A finite list $g_1, g_2, \ldots, g_k$ of elements of I is said to *generate* the ideal I if

$$I = \{r_1 g_1 + r_2 g_2 + \cdots + r_k g_k : r_1, r_2, \ldots, r_k \in R\}.$$

The ideal I is said to be *finitely-generated* if there exists a finite list of elements of I that generate I. Note that if elements $g_1, g_2, \ldots, g_k$ of an ideal I generate that ideal, then any element of R that divides each of $g_1, g_2, \ldots, g_k$ will divide every element of the ideal I.

Proposition 10.6 *Let R be an integral domain. Suppose that every ideal of R is finitely generated. Then any non-zero element of R that is not a unit of R can be factored as a finite product of irreducible elements of R.*

Proof Let R be an integral domain, and let S be the subset of R consisting of zero, all units of R, and all finite products of irreducible elements of R. Then $xy \in S$ for all $x \in S$ and $y \in S$. We shall prove that if $R \setminus S$ is non-empty, then R contains an ideal that is not finitely generated.

Let x be an element of $R \setminus S$. Then x is non-zero and is neither a unit nor an irreducible element of R, and therefore there exist elements y and z of R, such that $x = yz$ and neither y nor z is a unit of R. Then neither y not z is an associate of x. Moreover either $y \in R \setminus S$ or $z \in R \setminus S$, since the product of any two elements of S belongs to S. Thus we may construct, by induction on n, an infinite sequence $x_1, x_2, x_3, \ldots$ of elements of $R \setminus S$ such that $x_1 = x$, x_{n+1} divides x_n but is not an associate of x_n for all $n \in N$. Thus if m and n are natural numbers satisfying $m < n$, then x_n divides x_m but x_m does not divide x_n.

Let $I = \{r \in R : x_n | r \text{ for some } n \in \mathbb{N}\}$. Then I is an ideal of R. We claim that this ideal is not finitely generated.

Let $g_1, g_2, \ldots, g_k$ be a finite list of elements of I. Now there exists some natural number m large enough to ensure that that $x_m | g_j$ for $j = 1, 2, \ldots, k$. If I were generated by these elements $g_1, g_2, \ldots, g_k$, then $x_m | r$ for all $r \in I$. In particular x_m would divide all x_n for all $n \in \mathbb{N}$, which is impossible. Thus the ideal I cannot be finitely generated.

We have shown that if the set S defined above is a proper subset of some integral domain R, then R contains some ideal that is not finitely generated. The result follows. ∎

10.2 Euclidean Domains

Definition Let R be an integral domain, and let R^* denote the set $R \setminus \{0\}$ of non-zero elements of R. An integer-valued function $\varphi: R^* \to \mathbb{Z}$ defined on R^* is said to be a *Euclidean function* if it satisfies the following properties:—

(i) $\varphi(r) \geq 0$ for all $r \in R^*$;

(ii) if $x, y \in R^*$ satisfy $x | y$ then $\varphi(x) \leq \varphi(y)$;

(iii) given $x, y \in R^*$, there exist $q, r \in R$ such that $x = qy + r$, where either $r = 0$ or $\varphi(r) < \varphi(y)$.

Definition A *Euclidean domain* is an integral domain on which is defined a Euclidean function.

Example Let $\mathbb{Z}^*$ denote the set of non-zero integers, and let $\varphi: \mathbb{Z}^* \to \mathbb{Z}$ be the function defined such that $\varphi(x) = |x|$ for all non-zero integers x. Then φ is a Euclidean function. It follows that $\mathbb{Z}$ is a Euclidean domain.

Example Let K be a field, and let $K[x]$ be the ring of polynomials in a single indeterminate x with coefficients in the field K. The degree $\deg p$ of each non-zero polynomial p is a non-negative integer. If p and q are non-zero polynomials in $K[x]$, and if p divides q, then $\deg p \leq \deg q$. Also, given any non-zero polynomials m and p in $K[x]$ there exist polynomials $q, r \in K[x]$ such that $p = qm + r$ and either $r = 0$ or else $\deg r < \deg m$. We conclude from this that the function that maps each non-zero polynomial in $K[x]$ to its degree is a Euclidean function for $K[x]$. Thus $K[x]$ is a Euclidean domain.

Example A *Gaussian integer* is a complex number of the form $x + y\sqrt{-1}$, where x and y are integers. The set of all Gaussian integers is a subring of the

field of complex numbers, and is an integral domain. We denote the ring of Gaussian integers by $\mathbb{Z}[\sqrt{-1}]$. We define $\varphi(z) = |z|^2$ for all non-zero Gaussian integers z. Then $\varphi(z)$ is an non-negative integer for all non-zero Gaussian integers z, for if $z = x + y\sqrt{-1}$, where $x, y \in \mathbb{Z}$, then $\varphi(z) = x^2 + y^2$. If z and w are non-zero Gaussian integers, and if z divides w in the ring $\mathbb{Z}[\sqrt{-1}]$, then there exists a non-zero Gaussian integer t such that $w = tz$. But then $\varphi(w) = \varphi(t)\varphi(z)$, where $\varphi(t) \geq 1$, and therefore $\varphi(z) \leq \varphi(w)$.

Let z and w be non-zero Gaussian integers. Then the ratio z/w lies in some square in the complex plane, where the sides of the square are of unit length, and the corners of the square are given by Gaussian integers. There is at least one corner of the square whose distance from z/w does not exceed $1/\sqrt{2}$. Thus there exists some Gaussian integer q such that

$$\left|\frac{z}{w} - q\right| \leq \frac{1}{\sqrt{2}}.$$

Let $r = z - qw$. Then either $r = 0$, or else

$$\varphi(r) = |r|^2 = \left|\frac{z}{w} - q\right|^2 |w|^2 = \left|\frac{z}{w} - q\right|^2 \varphi(w) \leq \frac{1}{2}\varphi(w) < \varphi(w).$$

Thus the function that maps each non-zero Gaussian integer z to the positive integer $|z|^2$ is a Euclidean function for the ring of Gaussian integers. The ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers is thus a Euclidean domain.

Each unit of the ring of Gaussian integers divides every other non-zero Gaussian integer. Thus if u is a unit of this ring then $\varphi(u) \leq \varphi(z)$ for all non-zero Gaussian integers z. It follows that $\varphi(u) = 1$. Now the only Gaussian integers satisfying this condition are 1, -1, i and $-i$ (where $i = \sqrt{-1}$). Moreover each of these Gaussian integers is a unit. We conclude from this that the units of the ring of Gaussian integers are 1, -1, i and $-i$.

Proposition 10.7 *Every ideal of a Euclidean domain is a principal ideal.*

Proof Let R be a Euclidean domain, let R^* be the set of non-zero elements of R, and let $\varphi: R^* \to \mathbb{Z}$ be a Euclidean function. Now the zero ideal of R is generated by the zero element of R. It remains therefore to show that every non-zero ideal of R is a principal ideal.

Let I be a non-zero ideal of R. Now

$$\{\varphi(x) : x \in I \text{ and } x \neq 0\}$$

is a set of non-negative integers, and therefore has a least element. It follows that there exists some non-zero element m of I with the property that $\varphi(m) \leq$

$\varphi(x)$ for all non-zero elements x of I. It then follows from the definition of Euclidean functions that, given any non-zero element x of the ideal I, there exist elements q and r of R such that $x = qm + r$ and either $r = 0$ or $\varphi(r) < \varphi(m)$. But then $r \in I$, since $r = x - qm$ and $x, m \in I$. But there are no non-zero elements r of I satisfying $\varphi(r) < \varphi(m)$. It follows therefore that $r = 0$. But then $x = qm$, and thus $x \in (m)$. We have thus shown that $I = (m)$. Thus every non-zero ideal of R is a principal ideal, as required. ∎

10.3 Principal Ideal Domains

Definition An integral domain R is said to be a *principal ideal domain* (or *PID*) if every ideal of R is a principal ideal.

It follows directly from Proposition 10.7 that every Euclidean domain is a principal ideal domain.

In particular the ring $\mathbb{Z}$ of integers is a principal ideal domain, the ring $K[x]$ of polynomials with coefficients in some field K is a principal ideal domain, and the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers is a principal ideal domain.

Lemma 10.8 *Let $x_1, x_2, \ldots, x_k$ be elements of a principal ideal domain R, where these elements are not all zero. Suppose that the units of R are the only non-zero elements of R that divide each of $x_1, x_2, \ldots, x_k$. Then there exist elements $a_1, a_2, \ldots, a_k$ of R such that $a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1$.*

Proof Let I be the ideal of R generated by $x_1, x_2, \ldots, x_k$. Then $I = (d)$ for some $d \in R$, since R is a principal ideal domain. Then d divides x_i for $i = 1, 2, \ldots, k$, and therefore d is a unit of R. It follows that $I = R$. But then $1 \in I$, and therefore $1 = a_1x_1 + a_2x_2 + \cdots + a_kx_k$ for some $a_1, a_2, \ldots, a_k \in R$, as required. ∎

Lemma 10.9 *Let p be an irreducible element of a principal ideal domain R. Then the quotient ring $R/(p)$ is a field.*

Proof Let x be an element of R that does not belong to (p). Then p does not divide x, and therefore any common divisor of x and p must be a unit of R. Therefore there exist elements y and z of R such that $xy + pz = 1$ (Lemma 10.8). But then $y + (p)$ is a multiplicative inverse of $x + (p)$ in the quotient ring $R/(p)$, and therefore the set of non-zero elements of $R/(p)$ is an Abelian group with respect to multiplication. Thus $R/(p)$ is a field, as required. ∎

Theorem 10.10 *An element of a principal ideal domain is prime if and only if it is irreducible.*

Proof We have already shown that any prime element of an integral domain is irreducible (Lemma 10.5). Let p be an irreducible element of a principal ideal domain R. Then p is neither zero nor a unit of R. Suppose that $p \mid yz$ for some $y, z \in R$. Now any divisor of p is either an associate of p or a unit of R. Thus if p does not divide y then any element of R that divides both p and y must be a unit of R. Therefore there exist elements a and b of R such that $ap + by = 1$ (Lemma 10.8). But then $z = apz + byz$, and hence p divides z. Thus p is prime, as required. ∎

10.4 Unique Factorization in Principal Ideal Domains

A direct application of Proposition 10.6 shows that any non-zero element of a principal ideal domain that is not a unit can be factored as a finite product of irreducible elements of the domain. Moreover Theorem 10.10 ensures that these irreducible factors are prime elements of the domain. The following proposition ensures that these prime factors are essentially unique. Indeed this proposition guarantees that if some element x of the domain satisfies

$$x = p_1 p_2 \cdots p_k = q_1 q_2, \cdots, q_l,$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are prime elements of R, then $l = k$, and moreover $q_1, q_1, \ldots, q_k$ may be reordered and relabelled to ensure that, given any value i between 1 and k, the corresponding prime factors p_i and q_i are associates. There will then exist units $u_1, u_2, \ldots, u_k$ of R such that $q_i = u_i p_i$ for $i = 1, 2, \ldots, k$.

Proposition 10.11 *Let R be a principal ideal domain, and let x be an non-zero element of R that is not a unit of R. Suppose that*

$$x = p_1 p_2 \cdots p_k = q_1 q_2, \cdots, q_l,$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are prime elements of R. Then $l = k$, and there exists some permutation σ of $\{1, 2, \ldots, k\}$ such that q_i and $p_{\sigma(i)}$ are associates for $i = 1, 2, \ldots, k$.

Proof Let k be an integer greater than 1, and suppose that the stated result holds for all non-zero elements of R that are not units of R and that can be factored as a product of fewer than k prime elements of R. We shall prove that the result then holds for any non-zero element x of R that is not a unit of R and that can be factored as a product $p_1 p_2 \cdots p_k$ of k prime elements $p_1, p_2, \ldots, p_k$ of R. The required result will then follow by induction on k.

So, suppose that x is an non-zero element of R that is not a unit of R, and that

$$x = p_1 p_2 \cdots p_k = q_1 q_2, \cdots, q_l,$$

where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_l$ are prime elements of R. Now p_1 divides the product $q_1 q_2, \cdots, q_l$, and therefore p_1 divides at least one of the factors q_i of this product. We may reorder and relabel the prime elements $q_1, q_2, \ldots q_l$ to ensure that p_1 divides q_1. The irreducibility of q_1 then ensures that p_1 is an associate of q_1, and therefore there exists some unit u in R such that $q_1 = p_1 u$. But then $p_1(p_2 p_3 \cdots p_k) = p_1(u q_2 q_3 \cdots q_l)$ and $p_1 \neq 0$, and therefore $p_2 p_3 \cdots p_k = (u q_2) q_3 \cdots q_l$. (see Lemma 10.1). Moreover $u q_2$ is a prime element of R that is an associate of q_2. Now it follows from the induction hypothesis that the desired result holds for the product $p_2 p_3 \cdots p_k$. Therefore $l = k$ and moreover $q_2, q_3, \ldots, q_k$ can be reordered and relabeled so that p_i and q_i are associates for $i = 2, 3, \ldots, k$. The stated result therefore follows by induction on the number of prime factors occuring in the product $p_1 p_2 \cdots p_k$. ∎

11 Noetherian Modules

11.1 Modules over a Unital Commutative Ring

Definition Let R be a unital commutative ring. A set M is said to be a *module over* R (or *R-module*) if

(i) given any $x, y \in M$ and $r \in R$, there are well-defined elements $x + y$ and rx of M,

(ii) M is an Abelian group with respect to the operation $+$ of addition,

(iii) the identities

$$r(x + y) = rx + ry, \qquad (r + s)x = rx + sx,$$

$$(rs)x = r(sx), \qquad 1x = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$.

Example If K is a field, then a K-module is by definition a vector space over K.

Example Let $(M, +)$ be an Abelian group, and let $x \in M$. If n is a positive integer then we define nx to be the sum $x + x + \cdots + x$ of n copies of x. If n is a negative integer then we define $nx = -(|n|x)$, and we define $0x = 0$. This enables us to regard any Abelian group as a module over the ring $\mathbb{Z}$ of integers. Conversely, any module over $\mathbb{Z}$ is also an Abelian group.

Example Any unital commutative ring can be regarded as a module over itself in the obvious fashion.

Let R be a unital commutative ring, and let M be an R-module. A subset L of M is said to be a *submodule* of M if $x + y \in L$ and $rx \in L$ for all $x, y \in L$ and $r \in R$. If M is an R-module and L is a submodule of M then the quotient group M/L can itself be regarded as an R-module, where $r(L + x) \equiv L + rx$ for all $L + x \in M/L$ and $r \in R$. The R-module M/L is referred to as the *quotient* of the module M by the submodule L.

Note that a subset I of a unital commutative ring R is a submodule of R if and only if I is an ideal of R.

Let M and N be modules over some unital commutative ring R. A function $\varphi\colon M \to N$ is said to be a *homomorphism of R-modules* if $\varphi(x+y) = \varphi(x)+\varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $x, y \in M$ and $r \in R$. A homomorphism of R-modules is said to be an isomorphism if it is invertible. The kernel

$\ker \varphi$ and image $\varphi(M)$ of any homomorphism $\varphi: M \to N$ are themselves R-modules. Moreover if $\varphi: M \to N$ is a homomorphism of R-modules, and if L is a submodule of M satisfying $L \subset \ker \varphi$, then φ induces a homomorphism $\overline{\varphi}: M/L \to N$. This induced homomorphism is an isomorphism if and only if $L = \ker \varphi$ and $N = \varphi(M)$.

Definition Let $M_1, M_2, \ldots, M_k$ be modules over a unital commutative ring R. The *direct sum* $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ is defined to be the set of ordered k-tuples $(x_1, x_2, \ldots, x_k)$, where $x_i \in M_i$ for $i = 1, 2, \ldots, k$. This direct sum is itself an R-module:

$$\begin{aligned}(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) &= (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k), \\ r(x_1, x_2, \ldots, x_k) &= (rx_1, rx_2, \ldots, rx_k)\end{aligned}$$

for all $x_i, y_i \in M_i$ and $r \in R$.

If K is any field, then K^n is the direct sum of n copies of K.

Definition Let M be a module over some unital commutative ring R. Given any subset X of M, the submodule of M generated by the set X is defined to be the intersection of all submodules of M that contain the set X. It is therefore the smallest submodule of M that contains the set X. An R-module M is said to be *finitely-generated* if it is generated by some finite subset of itself.

Lemma 11.1 *Let M be a module over some unital commutative ring R, and let $\{x_1, x_2, \ldots, x_k\}$ be a finite subset of M. Then the submodule of M generated by this set consists of all elements of M that are of the form*

$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k$$

for some $r_1, r_2, \ldots, r_k \in R$.

Proof The subset of M consisting of all elements of M of this form is clearly a submodule of M. Moreover it is contained in every submodule of M that contains the set $\{x_1, x_2, \ldots, x_k\}$. The result follows. ∎

11.2 Noetherian Modules

Definition Let R be a unital commutative ring. An R-module M is said to be *Noetherian* if every submodule of M is finitely-generated.

Proposition 11.2 *Let R be a unital commutative ring, and let M be a module over R. Then the following are equivalent:—*

(i) (Ascending Chain Condition) *if $L_1 \subset L_2 \subset L_3 \subset \cdots$ is an ascending chain of submodules of M then there exists an integer N such that $L_n = L_N$ for all $n \geq N$;*

(ii) (Maximal Condition) *every non-empty collection of submodules of M has a maximal element (i.e., an submodule which is not contained in any other submodule belonging to the collection);*

(iii) (Finite Basis Condition) *M is a Noetherian R-module (i.e., every submodule of M is finitely-generated).*

Proof Suppose that M satisfies the Ascending Chain Condition. Let $\mathcal{C}$ be a non-empty collection of submodules of M. Choose $L_1 \in \mathcal{C}$. If $\mathcal{C}$ were to contain no maximal element then we could choose, by induction on n, an ascending chain $L_1 \subset L_2 \subset L_3 \subset \cdots$ of submodules belonging to $\mathcal{C}$ such that $L_n \neq L_{n+1}$ for all n, which would contradict the Ascending Chain Condition. Thus M must satisfy the Maximal Condition.

Next suppose that M satisfies the Maximal Condition. Let L be an submodule of M, and let $\mathcal{C}$ be the collection of all finitely-generated submodules of M that are contained in L. Now the zero submodule $\{0\}$ belongs to $\mathcal{C}$, hence $\mathcal{C}$ contains a maximal element J, and J is generated by some finite subset $\{a_1, a_2, \ldots, a_k\}$ of M. Let $x \in L$, and let K be the submodule generated by $\{x, a_1, a_2, \ldots, a_k\}$. Then $K \in \mathcal{C}$, and $J \subset K$. It follows from the maximality of J that $J = K$, and thus $x \in J$. Therefore $J = L$, and thus L is finitely-generated. Thus M must satisfy the Finite Basis Condition.

Finally suppose that M satisfies the Finite Basis Condition. Let $L_1 \subset L_2 \subset L_3 \subset \cdots$ be an ascending chain of submodules of M, and let L be the union $\bigcup_{n=1}^{+\infty} L_n$ of the submodules L_n. Then L is itself an submodule of M. Indeed if a and b are elements of L then a and b both belong to L_n for some sufficiently large n, and hence $a + b$, $-a$ and ra belong to L_n, and thus to L, for all $r \in M$. But the submodule L is finitely-generated. Let $\{a_1, a_2, \ldots, a_k\}$ be a generating set of L. Choose N large enough to ensure that $a_i \in L_N$ for $i = 1, 2, \ldots, k$. Then $L \subset L_N$, and hence $L_N = L_n = L$ for all $n \geq N$. Thus M must satisfy the Ascending Chain Condition, as required. ∎

Proposition 11.3 *Let R be a unital commutative ring, let M be an R-module, and let L be a submodule of M. Then M is Noetherian if and only if L and M/L are Noetherian.*

Proof Suppose that the R-module M is Noetherian. Then the submodule L is also Noetherian, since any submodule of L is also a submodule of M and is therefore finitely-generated. Also any submodule K of M/L is of the form $\{L + x : x \in J\}$ for some submodule J of M satisfying $L \subset J$. But J is finitely-generated (since M is Noetherian). Let $x_1, x_2, \ldots, x_k$ be a finite generating set for J. Then

$$L + x_1, L + x_2, \ldots, L + x_k$$

is a finite generating set for K. Thus M/L is Noetherian.

Conversely, suppose that L and M/L are Noetherian. We must show that M is Noetherian. Let J be any submodule of M, and let $\nu(J)$ be the image of J under the quotient homomorphism $\nu: M \to M/L$, where $\nu(x) = L + x$ for all $x \in M$. Then $\nu(J)$ is a submodule of the Noetherian module M/L and is therefore finitely-generated. It follows that there exist elements $x_1, x_2, \ldots, x_k$ of J such that $\nu(J)$ is generated by

$$L + x_1, L + x_2, \ldots, L + x_k.$$

Also $J \cap L$ is a submodule of the Noetherian module L, and therefore there exists a finite generating set $y_1, y_2, \ldots, y_m$ for $J \cap L$. We claim that

$$\{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_m\}$$

is a generating set for J.

Let $z \in J$. Then there exist $r_1, r_2, \ldots, r_k \in R$ such that

$$\nu(z) = r_1(L+x_1)+r_2(L+x_2)+\cdots+r_k(L+x_k) = L+r_1x_1+r_2x_2+\cdots+r_kx_k.$$

But then $z-(r_1x_1+r_2x_2+\cdots+r_kx_k) \in J\cap L$ (since $L = \ker\nu$), and therefore there exist $s_1, s_2, \ldots, s_m$ such that

$$z - (r_1x_1 + r_2x_2 + \cdots + r_kx_k) = s_1y_1 + s_2y_2 + \cdots + s_my_m,$$

and thus

$$z = \sum_{i=1}^{k} r_ix_i + \sum_{j=1}^{m} s_iy_i.$$

This shows that the submodule J of M is finitely-generated. We deduce that M is Noetherian, as required. ∎

Corollary 11.4 *The direct sum $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ of Noetherian modules $M_1, M_2, \ldots M_k$ over some unital commutative ring R is itself a Noetherian module over R.*

Proof The result follows easily by induction on k once it has been proved in the case $k = 2$.

Let M_1 and M_2 be Noetherian R-modules. Then $M_1 \oplus \{0\}$ is a Noetherian submodule of $M_1 \oplus M_2$ isomorphic to M_1, and the quotient of $M_1 \oplus M_2$ by this submodule is a Noetherian R-module isomorphic to M_2. It follows from Proposition 11.3 that $M_1 \oplus M_2$ is Noetherian, as required. ∎

One can define also the concept of a module over a non-commutative ring. Let R be a unital ring (not necessarily commutative), and let M be an Abelian group. We say that M is a *left R-module* if each $r \in R$ and $m \in M$ determine an element rm of M, and the identities

$$r(x+y) = rx + ry, \qquad (r+s)x = rx + sx, \qquad (rs)x = r(sx), \qquad 1x = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$. Similarly we say that M is a *right R-module* if each $r \in R$ and $m \in M$ determine an element mr of M, and the identities

$$(x+y)r = xr + yr, \qquad x(r+s) = xr + xs, \qquad x(rs) = (xr)s, \qquad x1 = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$. (If R is commutative then the distinction between left R-modules and right R-modules is simply a question of notation; this is not the case if R is non-commutative.)

11.3 Noetherian Rings and Hilbert's Basis Theorem

Let R be a unital commutative ring. We can regard the ring R as an R-module, where the ring R acts on itself by left multiplication (so that $r \,.\, r'$ is the product rr' of r and r' for all elements r and r' of R). We then find that a subset of R is an ideal of R if and only if it is a submodule of R. The following result therefore follows directly from Proposition 11.2.

Proposition 11.5 *Let R be a unital commutative ring. Then the following are equivalent:—*

(i) (Ascending Chain Condition) *if $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an ascending chain of ideals of R then there exists an integer N such that $I_n = I_N$ for all $n \geq N$;*

(ii) (Maximal Condition) *every non-empty collection of ideals of R has a maximal element (i.e., an ideal which is not contained in any other ideal belonging to the collection);*

(iii) (Finite Basis Condition) *every ideal of R is finitely-generated.*

Definition A unital commutative ring is said to be a *Noetherian ring* if every ideal of the ring is finitely-generated. A *Noetherian domain* is a Noetherian ring that is also an integral domain.

Note that a unital commutative ring R is Noetherian if it satisfies any one of the conditions of Proposition 11.5.

Corollary 11.6 *Let M be a finitely-generated module over a Noetherian ring R. Then M is a Noetherian R-module.*

Proof Let $\{x_1, x_2, \ldots, x_k\}$ be a finite generating set for M. Let R^k be the direct sum of k copies of R, and let $\varphi: R^k \to M$ be the homomorphism of R-modules sending $(r_1, r_2, \ldots, r_k) \in R^k$ to

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

It follows from Corollary 11.4 that R^k is a Noetherian R-module (since the Noetherian ring R is itself a Noetherian R-module). Moreover M is isomorphic to $R^k/\ker\varphi$, since $\varphi: R^k \to M$ is surjective. It follows from Proposition 11.3 that M is Noetherian, as required. ∎

If I is a proper ideal of a Noetherian ring R then the collection of all proper ideals of R that contain the ideal I is clearly non-empty (since I itself belongs to the collection). It follows immediately from the Maximal Condition that I is contained in some maximal ideal of R.

Lemma 11.7 *Let R be a Noetherian ring, and let I be an ideal of R. Then the quotient ring R/I is Noetherian.*

Proof Let L be an ideal of R/I, and let $J = \{x \in R : I + x \in L\}$. Then J is an ideal of R, and therefore there exists a finite subset $\{a_1, a_2, \ldots, a_k\}$ of J which generates J. But then L is generated by $I + a_i$ for $i = 1, 2, \ldots, k$. Indeed every element of L is of the form $I + x$ for some $x \in J$, and if

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$$

, where $r_1, r_2, \ldots, r_k \in R$, then

$$I + x = r_1(I + a_1) + r_2(I + a_2) + \cdots + r_k(I + a_k),$$

as required. ∎

Hilbert showed that if R is a field or is the ring $\mathbb{Z}$ of integers, then every ideal of $R[x_1, x_2, \ldots, x_n]$ is finitely-generated. The method that Hilbert used to prove this result can be generalized to yield the following theorem.

Theorem 11.8 (Hilbert's Basis Theorem) *If R is a Noetherian ring, then so is the polynomial ring $R[x]$.*

Proof Let I be an ideal of $R[x]$, and, for each non-negative integer n, let I_n denote the subset of R consisting of those elements of R that occur as leading coefficients of polynomials of degree n belonging to I, together with the zero element of R. Then I_n is an ideal of R. Moreover $I_n \subset I_{n+1}$, for if $p(x)$ is a polynomial of degree n belonging to I then $xp(x)$ is a polynomial of degree $n+1$ belonging to I which has the same leading coefficient. Thus $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals of R. But the Noetherian ring R satisfies the Ascending Chain Condition (see Proposition 11.5). Therefore there exists some natural number m such that $I_n = I_m$ for all $n \geq m$.

Now each ideal I_n is finitely-generated, hence, for each $n \leq m$, we can choose a finite set $\{a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}\}$ which generates I_n. Moreover each generator $a_{n,i}$ is the leading coefficient of some polynomial $q_{n,i}$ of degree n belonging to I. Let J be the ideal of $R[x]$ generated by the polynomials $q_{n,i}$ for all $0 \leq n \leq m$ and $1 \leq i \leq k_n$. Then J is finitely-generated. We shall show by induction on $\deg p$ that every polynomial p belonging to I must belong to J, and thus $I = J$. Now if $p \in I$ and $\deg p = 0$ then p is a constant polynomial whose value belongs to I_0 (by definition of I_0), and thus p is a linear combination of the constant polynomials $q_{0,i}$ (since the values $a_{0,i}$ of the constant polynomials $q_{0,i}$ generate I_0), showing that $p \in J$. Thus the result holds for all $p \in I$ of degree 0.

Now suppose that $p \in I$ is a polynomial of degree n and that the result is true for all polynomials p in I of degree less than n. Consider first the case when $n \leq m$. Let b be the leading coefficient of p. Then there exist $c_1, c_2, \ldots, c_{k_n} \in R$ such that

$$b = c_1 a_{n,1} + c_2 a_{n,2} + \cdots + c_{k_n} a_{n,k_n},$$

since $a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}$ generate the ideal I_n of R. Then

$$p(x) = c_1 q_{n,1}(x) + c_2 q_{n,2}(x) + \cdots + c_k q_{n,k}(x) + r(x),$$

where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p \leq m$.

Finally suppose that $p \in I$ is a polynomial of degree n where $n > m$, and that the result has been verified for all polynomials of degree less than n.

Then the leading coefficient b of p belongs to I_n. But $I_n = I_m$, since $n \geq m$. As before, we see that there exist $c_1, c_2, \ldots, c_{k_m} \in R$ such that

$$b = c_1 a_{m,1} + c_2 a_{m,2} + \cdots + c_{k_n} a_{m,k_m},$$

since $a_{m,1}, a_{m,2}, \ldots, a_{m,k_m}$ generate the ideal I_n of R. Then

$$p(x) = c_1 x^{n-m} q_{m,1}(x) + c_2 x^{n-m} q_{m,2}(x) + \cdots + c_k x^{n-m} q_{m,k}(x) + r(x),$$

where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p > m$. Therefore $I = J$, and thus I is finitely-generated, as required. ∎

Theorem 11.9 *Let R be a Noetherian ring. Then the ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in the indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in R is a Noetherian ring.*

Proof It is easy to see that $R[x_1, x_2, \ldots, x_n]$ is naturally isomorphic to $R[x_1, x_2, \ldots, x_{n-1}][x_n]$ when $n > 1$. (Any polynomial in the indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in the ring R may be viewed as a polynomial in the indeterminate x_n whose coefficients are in the polynomial ring $R[x_1, x_2, \ldots, x_{n-1}]$.) The required results therefore follows from Hilbert's Basis Theorem (Theorem 11.8) by induction on n. ∎

Corollary 11.10 *Let K be a field. Then every ideal of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ is finitely-generated.*

12 Finitely-Generated Modules over Principal Ideal Domains

12.1 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 11.1). 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 12.1 *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*

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

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

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

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

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k = s_1x_1 + s_2x_2 + \cdots + s_kx_k.$$

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 12.2 *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 $f\colon X \to N$ from X to N, there exists a unique R-module homomorphism $\varphi\colon M \to N$ 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 12.1). It follows that, given any R-module N, and given any function $f\colon X \to N$ from X to N, there exists a function $\varphi\colon M \to N$ 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 $f\colon X \to N$.

Now consider the case when M is freely generated by an infinite set X. Let N be an R-module, and let $f\colon X \to N$ 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 $\varphi_Y\colon M_Y \to N$ 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 $\varphi_Y\colon M_Y \to N$ and $\varphi_Z\colon M_Z \to N$ to $M_{Y\cap Z}$ are R-module homomorphisms from $M_{Y\cap Z}$ to N that extend $f|Y \cap Z\colon Y \cap Z \to N$. 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 12.3 *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 12.2 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 12.2 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 12.4 *Let R be a unital commutative ring, let M be an R-module, let F be a free R-module and let $\pi: M \to F$ be a surjective R-module homomorphism. Then $M \cong \ker \pi \oplus F$.*

Proof It follows from Proposition 12.3 (applied to the identity automorphism of F) that there exists an R-module homomorphism $\psi: F \to M$ with the property that $\pi(\psi(f)) = f$ for all $f \in F$. Let $\theta: \ker \pi \oplus F \to M$ be defined so that $\theta(k, f) = k + \psi(f)$ for all $f \in F$. Then $\theta: \ker \pi \oplus F \to M$ 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 $\theta: \ker \pi \oplus F \to M$ 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 $\theta: \ker \pi \oplus F \to M$ 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. ∎

12.2 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 12.5 *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 12.6 *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 $b_1, b_2, \ldots, b_k$ is a free basis of M. The elements of any other free basis are linearly independent. It therefore follows from Proposition 12.5 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 12.7 *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 $g_1, g_2, \ldots, g_k$. Let $\theta: R^k \to M$ be the R-module homomorphism defined such that

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

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

Let $m_1, m_2, \ldots, m_p$ be elements of M, where $p > k$. Then there exist elements $t_1, t_2, \ldots, t_p$ of R^k such that $\theta(t_j) = m_j$ for $j = 1, 2, \ldots, p$. Now R^k is a free module of rank k. It follows from Proposition 12.5 that the elements $t_1, t_2, \ldots, t_p$ are linearly dependent. Therefore there exist elements $r_1, r_2, \ldots, r_p$ 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 $m_1, m_2, \ldots, m_p$ are linearly dependent. The result follows. ∎

12.3 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 12.8 *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. ∎

12.4 Free Modules of Finite Rank over Principal Ideal Domains

Proposition 12.9 *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 $\nu : M \to R$ 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. ∎

12.5 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 12.10 *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 12.7 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 12.8 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 12.9). 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 12.11 *Let M be a module over an integral domain R, and let*

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

where 0_M denotes the zero element of M. 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 $sm_1 = 0_M$, $sm_2 = 0_M$, and $s(rm_1) = r(sm_1) = 0_M$ for all $r \in R$. Thus $m_1 + m_2 \in T$ and $rm_1 \in T$ 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 12.12 *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 12.10 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 12.4 that $M \cong T \oplus F$. The result follows. ∎

12.6 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 12.8).

Proposition 12.13 *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 10.8 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 12.14 *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 10.11) 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 12.15 *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 12.14. 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. ∎

12.7 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 12.16 *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. ∎

12.8 The Structure Theorem for Finitely-Generated Modules over Principal Ideal Domains

Proposition 12.17 *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 12.12). 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 12.13 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 12.15 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 12.17. 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 12.6). 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 12.18 *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 12.19 *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 12.20 *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 12.19). 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 12.18). 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 12.21 *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 12.20 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 12.22 *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 12.15 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 $\dim_K p^j M/p^{j+1}M$ 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 12.23 (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 12.17, Proposition 12.12, and Proposition 12.13. 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 12.22. ∎

12.9 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 12.24 *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 12.25 *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 12.23 and Lemma 12.24. ∎

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 12.25 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.

13 Algebraic Numbers and Algebraic Integers

13.1 Basic Properties of Field Extensions

Let K be a field. A field extension $L\colon K$ is determined by an embedding of the *ground field* K in some *extension field* L. If K and L are both subfields of some larger field N then L is an extension field of K if and only if $K \subset L$. (This applies in particular when the field N is the field of complex numbers. Thus if K and L are subfields of the field of complex numbers, then $L\colon K$ is a field extension if and only if $K \subset L$.)

If $L\colon K$ is a field extension, then the extension field L may be regarded as a vector space over the ground field K. A field extension $L\colon K$ is *finite* if L is a finite-dimensional vector space over K. The *degree* $[L\colon K]$ of a finite field extension $L\colon K$ is defined to be the dimension of L, when L is regarded as a vector space over the ground field K. A basic result known as the *Tower Law* ensures that if K, L and M are fields, and if $K \subset L$ and $L \subset M$, then the field extension $M\colon K$ is finite if and only if both the field extensions $M\colon L$ and $L\colon K$ are finite, in which case

$$[M\colon K] = [M\colon L][L\colon K].$$

Let K be a field, and let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be elements of some extension field of K. We denote by $K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ the smallest subfield of this extension field that contains the set $K \cup \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$. A field extension $L\colon K$ is said to be *simple* if there exists some element α of L such that $L = K(\alpha)$.

Let K be a field, and let α be an element of some extension field of K. The element α is said to be *algebraic* over K if there exists some non-zero polynomial with coefficients in K such that $f(\alpha) = 0$.

A polynomial $f(x)$ with coefficients in some field K is said to be *monic* if the leading coefficient of $f(x)$ is equal to the identity element 1_K of the field K.

Let K be a field, and let α be an element of some extension field of K. Suppose that α is algebraic over K. Then there exists a unique monic polynomial $m_\alpha(x)$ with coefficients in K that satisfies $m_\alpha(\alpha) = 0$ and divides every other polynomial that has α as a root. This polynomial $m_\alpha(x)$ is the *minimum polynomial* of α over K. If $f(x)$ is a polynomial with coefficients in the field K, and if $f(\alpha) = 0$, then $f(x) = m_\alpha(x)g(x)$ for some polynomial $g(x)$ with coefficients in K. Moreover if the polynomial $f(x)$ is non-zero then $\deg f \geq m_\alpha$.

It is a basic result in the theory of field extensions that a simple field extension $K(\alpha)\colon K$ is finite if and only if the element α of the extension field

$K(\alpha)$ is algebraic over K, in which case the degree $[K(\alpha):K]$ of the simple field extension $K(\alpha):K$ is equal to the degree of the minimum polynomial of α over the ground field K.

13.2 Algebraic Numbers and Algebraic Integers

Definition A complex number α is an *algebraic number* if it is a root of some non-zero polynomial with integer coefficients.

Definition A complex number θ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients.

The number $\sqrt{2}$ is an algebraic integer, since it is a root of the monic polynomial $x^2 - 2$. More generally, $\sqrt[n]{m}$ is an algebraic integer for all positive integers n and m, since this number is a root of the polynomial $x^n - m$. The complex numbers i and $-\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$ are also algebraic integers, where $i = \sqrt{-1}$, since they are roots of the polynomials $x^2 + 1$ and $x^3 - 1$ respectively.

Lemma 13.1 *Let α be an algebraic number. Then there exists some non-zero integer m such that $m\alpha$ is an algebraic integer.*

Proof Let α be an algebraic number. Then there exist rational numbers $q_0, q_1, q_2, \ldots, q_{n-1}$ such that

$$\alpha^n + q_{n-1}\alpha^{n-1} + q_{n-2}\alpha^{n-2} + \cdots + q_0\alpha^0 = 0.$$

Let m be a non-zero integer with the property that mq_j is an integer for $j = 0, 1, \ldots, n-1$, and let $a_j = mq_j$ for $j = 0, 1, \ldots, n-1$. Then

$$\begin{aligned} &= m^n\alpha^n + m^n q_{n-1}\alpha^{n-1} + m^n q_{n-2}\alpha^{n-2} + \cdots + m^n q_0 \\ &= (m\alpha)^n + a_{n-1}(m\alpha)^{n-1} + ma_{n-2}(m\alpha)^{n-2} + \cdots + m^{n-1}a_0. \end{aligned}$$

Therefore $m\alpha$ the root of a monic polynomial with integer coefficients, and is therefore an algebraic integer. The result follows. ∎

A polynomial with integer coefficients is said to be *primitive* if there is no prime number that divides all the coefficients of the polynomial. A basic result known as *Gauss's Lemma* ensures that the product of two primitive polynomials with integer coefficients is itself primitive. This in turn ensures that a polynomial with integer coefficients is irreducible over the field $\mathbb{Q}$ of rational numbers if and only if it cannot be factored as a product of polynomials of lower degree with integer coefficients. Indeed let $f(x)$ be a

polynomial with integer coefficients. Suppose that $f(x)$ can be factored as a product of polynomials of lower degree with rational coefficients. Now, given a factorization of the polynomial $f(x)$ that is of the form $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials with rational coefficients, there exist integers u and v such that $ug(x)$ and $vh(x)$ are polynomials with integer coefficients. Then there exist integers m and w, where $m \geq 1$ and primitive polynomials $g_*(x)$ and $h_*(x)$ with integer coefficients such that $mf(x) = wg_*(x)h_*(x)$. Now the product polynomial $g_*(x)h_*(x)$ is a primitive polynomial, by Gauss's Lemma. It follows from this that the prime factors of m must all cancel off with prime factors of w, and therefore there exists some integer w_0 such that $f(x) = w_0 f_*(x)g_*(x)$. Thus if the polynomial $f(x)$ can be factored as a product of polynomials of lower degree with rational coefficients, then it can be factored as a product of polynomials of lower degree with integer coefficients.

Proposition 13.2 *A complex number is an algebraic integer if and only if its minimum polynomial over the field $\mathbb{Q}$ of rational numbers has integer coefficients.*

Proof Let θ be a complex number. If the minimum polynomial of θ has integer coefficients then it follows directly from the definition of an algebraic integer that θ is an algebraic integer.

Conversely suppose that θ is an algebraic integer. Then θ is the root of some monic polynomial with integer coefficients. Now if a polynomial with integer coefficients is not itself irreducible over the field $\mathbb{Q}$ of rational numbers, then it can be factored as a product of polynomials of lower degree with integer coefficients. Now the leading coefficient of a product of polynomials is the product of the leading coefficients of the factors. Therefore, if the product polynomial is a monic polynomial, then its leading coefficient has the value 1, and therefore the leading coefficients of the factors must be ± 1. The individual factors can therefore be each be multiplied by -1, if necessary, in order to ensure that they also are monic polynomials. We conclude that if a monic polynomial with integer coefficients is not itself irreducible over the field $\mathbb{Q}$ of rational numbers, then it can be factored as a product of monic polynomials of lower degree with integer coefficients.

A straightforward proof by induction on the degree of the polynomial therefore shows that any polynomial with integer coefficients can be factored as a finite product of irreducible polynomials with integer coefficients. It follows that any monic polynomial with integer coefficients can be factored as a product of monic irreducible polynomials with integer coefficients. One of those irreducible polynomials has the algebraic number θ as a root, and is

therefore the minimum polynomial of θ over the field $\mathbb{Q}$ of rational numbers (by definition of the minimum polynomial of an algebraic number). The result follows. ∎

13.3 Number Fields and the Primitive Element Theorem

Definition A subfield K of the complex numbers is said to be an *algebraic number field* (or *number field*) if the field extension $K:\mathbb{Q}$ is finite.

It follows from this definition that a subfield K of the complex numbers is an algebraic number field if and only if K is a finite-dimensional vector space over the field $\mathbb{Q}$ of rational numbers.

Definition The *degree* of an algebraic number field K is the dimension $[K:\mathbb{Q}]$ of K, when K is considered as a vector space over the field $\mathbb{Q}$ of rational numbers.

The *Primitive Element Theorem* guarantees that every finite separable field extension is simple. It is an immediate consequence of the Primitive Element Theorem that every algebraic number field is a simple extension of the field $\mathbb{Q}$ of rational numbers. Thus, given any algebraic number field K, there exists some element α of K such that $K = \mathbb{Q}(\alpha)$.

Lemma 13.3 *Let K be an algebraic number field. Then there exists an algebraic integer θ such that $K = \mathbb{Q}(\theta)$.*

Proof The Primitive Element Theorem ensures the existence of some element α of K such that $K = \mathbb{Q}(\alpha)$. Each element of K is algebraic over $\mathbb{Q}$. It follows that α is an algebraic number. It then follows from Lemma 13.1 that there exists some integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer. Let $\theta = m\alpha$. Then $K = \mathbb{Q}(\theta)$. The result follows. ∎

13.4 Rings of Algebraic Numbers

A subset R of the field $\mathbb{C}$ of complex numbers is a unital subring of $\mathbb{C}$ if $1 \in R$ and also $\alpha + \beta \in R$, $\alpha - \beta \in R$ and $\alpha\beta \in R$ for all $\alpha, \beta \in R$.

Let R be a unital subring of the field $\mathbb{C}$ of complex numbers, and let $\theta_1, \theta_2, \ldots, \theta_m$ be complex numbers. We denote by $R[\theta_1, \theta_2, \ldots, \theta_m]$ the smallest unital subring of $\mathbb{C}$ that contains the set $R \cup \{\theta_1, \theta_2, \ldots, \theta_m\}$. In particular $\mathbb{Z}[\theta_1, \theta_2, \ldots, \theta_m]$ denotes the smallest unital subring of $\mathbb{C}$ that contains $\theta_1, \theta_2, \ldots, \theta_m$.

Note that if R is a unital subring of $\mathbb{C}$, and if θ is a complex number then

$$R[\theta] = \{g(\theta) : g \in R[x]\},$$

where $R[x]$ denotes the ring of polynomials in the indeterminate x with coefficients in the unital ring R.

Definition Let R be a unital subring of the field $\mathbb{C}$ of complex numbers, and let θ be a complex number. The number θ is said to be *integral* over R if θ is a root of some monic polynomial with coefficients in R.

It follows from this definition that a complex number θ is integral over some unital subring R of $\mathbb{C}$ if and only if there exist elements $a_0, a_1, \ldots, a_{n-1}$ of R such that

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0 = 0.$$

A complex number is thus an algebraic integer if and only if it is integral over the ring $\mathbb{Z}$ of (rational) integers.

Remark Algebraic number theorists often refer to the whole numbers

$$0, \pm 1, \pm 2, \pm 3, \ldots$$

as *rational integers*, so as to distinguish them from *algebraic integers*. With this terminology, $\mathbb{Z}$ denotes the ring of rational integers.

Proposition 13.4 *Let R be a unital subring of the field $\mathbb{C}$, and let θ be a complex number. Suppose that there exists some monic polynomial $f(x)$ with coefficients in the ring R such that $f(\theta) = 0$. Then $R[\theta]$ is a finitely-generated R-module.*

Proof Let $f(x)$ be a monic polynomial of degree n, with coefficients in the ring R with the property that $f(\theta) = 0$. Then

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

where $a_0, a_1, \ldots, a_{n-1} \in R$. Then

$$\theta^{n+k} = -a_{n-1}\theta^{n+k-1} - a_{n-2}\theta^{n+k-2} - \cdots - a_0\theta^k$$

for all non-negative integers k. A straightforward argument by induction on s then shows that, for any integer s satisfying $s \geq n$, there exist elements $r_{s,0}, r_{s,1}, , r_{s,2}, \ldots, r_{s,n-1}$ of the ring R such that

$$\theta^s = r_{s,0} + r_{s,1}\theta + r_{s,2}\theta^2 + \cdots + r_{s,n-1}\theta^{n-1}.$$

It follows that, for each polynomial $g(x)$ with coefficients in the unital ring R, there exists a polynomial $h(x)$ with coefficients in R such that $g(\theta) = h(\theta)$ and either $h = 0$ or else $\deg h < n$. Therefore the ring $R[\theta]$ is generated as an R-module by $1, \theta, \theta^2, \ldots, \theta^{n-1}$, and is thus a finitely-generated R-module. ∎

Corollary 13.5 *Let R be a unital subring of the field $\mathbb{C}$ of complex numbers, and let α and β complex numbers that are integral over R. Then $R[\alpha, \beta]$ is a finitely-generated R-module.*

Proof The complex number β is integral over $R[\alpha]$, because it is a root of some monic polynomial with coefficients in R. Moreover it follows directly from the relevant definitions that $R[\alpha, \beta] = R[\alpha][\beta]$. Now it follows from Proposition 13.4 that there exist elements $\lambda_1, \lambda_2, \ldots, \lambda_s$ of $R[\alpha]$ such that any element of $R[\alpha]$ may be expressed as a linear combination

$$r_1\lambda_1 + r_2\lambda_2 + \cdots + r_s\lambda_s$$

of $\lambda_1, \lambda_2, \ldots, \lambda_s$ with coefficients in R. It also follows from Proposition 13.4 that there exist elements $\mu_1, \mu_2, \ldots, \mu_t$ of $R[\alpha, \beta]$ such that every element of $R[\alpha, \beta]$ may be expressed as a linear combination of $\mu_1, \mu_2, \ldots, \mu_t$ with coefficients in $R[\alpha]$. These coefficients can each be expressed as a linear combination of $\lambda_1, \lambda_2, \ldots, \lambda_s$ with coefficients in R. It follows that each element of $R[\alpha, \beta]$ may be expressed as a linear combination of the elements of the finite set

$$\{\lambda_j\mu_k : 1 \leq j \leq s, \ \ 1 \leq k \leq t\}$$

with coefficients in the ring R. Thus $R[\alpha, \beta]$ is a finitely-generated R-module, as required. ∎

Proposition 13.6 *Let R be a subring of the field $\mathbb{C}$ of complex numbers. Suppose that R is a finitely-generated Abelian group with respect to the operation of addition. Then every element of R is an algebraic integer.*

Proof The ring R is a torsion-free Abelian group, because it is a contained in the field of complex numbers. Therefore R is both finitely-generated and torsion-free, and is therefore a free Abelian group of finite rank. (This result is a special case of Proposition 12.10) It follows that there exist elements $b_1, b_2, \ldots, b_n$ of R such that every element z of R can be represented in the form

$$z = m_1b_1 + m_2b_2 + \cdots + m_nb_n$$

for some uniquely-determined (rational) integers $m_1, m_2, \ldots, m_n$. Let $\theta \in R$. Then there exist (rational) integers $M_{jk}(\theta)$ for $1 \leq j, k \leq n$ such that

$$\theta b_k = \sum_{j=1}^{n} M_{jk}(\theta)b_j$$

for $k = 1, 2, \ldots, n$. It follows that

$$\sum_{j=1}^{n} (\theta I_{jk} - M_{jk}(\theta)) b_j = 0,$$

where

$$I_{jk} = \begin{cases} 1 & \text{if } j = k; \\ 0 & \text{if } j \neq k. \end{cases}$$

Let $\theta I - M(\theta)$ be the $n \times n$ matrix with integer coefficients whose entry in the jth row and kth column is $\theta I_{jk} - M_{jk}(\theta)$, and let b be the row-vector of complex numbers defined such that $b = (b_1, b_2, \ldots, b_n)$. Then $b(\theta I - M(\theta)) = 0$. It follows that the transpose of b is annihilated by the transpose of the matrix $\theta I - M(\theta)$, and therefore θ is an eigenvalue of the matrix $M(\theta)$. But then $\det(\theta I - M(\theta)) = 0$, since every eigenvalue of a square matrix is a root of its characteristic equation. Moreover

$$\det(\theta I - M(\theta)) = \theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0,$$

and thus $f_\theta(\theta) = 0$, where

$$f_\theta(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Moreover each of the coefficients $a_0, a_1, \ldots, a_{n-1}$ can be expressed as the sum of the determinants of matrices obtained from M by omitting appropriate rows and columns, multiplied by ± 1. It follows that each of the coefficients $a_0, a_1, \ldots, a_{n-1}$ is a (rational) integer. Thus each element θ of R is the root of a monic polynomial f_θ with (rational) integer coefficients, and is thus an algebraic integer, as required. ∎

Proposition 13.7 *The set $\mathbb{B}$ of algebraic integers is a unital subring of the field $\mathbb{C}$ of complex numbers. Moreover $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$.* ∎

Proof Let α and β be algebraic integers. Then α and β are integral over the ring $\mathbb{Z}$ of (rational) integers. It follows from Corollary 13.5 that $\mathbb{Z}[\alpha, \beta]$ is a finitely-generated $\mathbb{Z}$-module, and is thus a finitely-generated Abelian group. It then follows from Proposition 13.6 that every element of $\mathbb{Z}[\alpha, \beta]$ is an algebraic integer. In particular $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are algebraic integers. This proves that $\mathbb{B}$ is a unital subring of $\mathbb{C}$.

Clearly $\mathbb{Z} \subset \mathbb{B} \cap \mathbb{Q}$. Let $\alpha \in \mathbb{B} \cap \mathbb{Q}$. It follows from Proposition 13.2 that the minimum polynomial of α over $\mathbb{Q}$ has integer coefficients. But that minimum polynomial is $x - \alpha$. Therefore $\alpha \in \mathbb{Z}$. Thus Clearly $\mathbb{B} \cap \mathbb{Q} = \mathbb{Z}$, as required. ∎