Module MA3412: Topics in Commutative Algebra
Hilary Term 2010

D. R. Wilkins

Contents

9 Integral Domains

9.1 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 9.1 *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 9.2 *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 9.3 *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 9.4 *Elements x and y of an integral domain R are associates if and only if $(x) = (y)$.*

Proof This follows directly from Lemma 9.3. ▮

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 9.5 *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 9.3 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 9.6 *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. ∎

9.2 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 $\varphi\colon R^* \to \mathbb{Z}$ 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 $\varphi\colon \mathbb{Z}^* \to \mathbb{Z}$ 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 9.7 *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 $\varphi\colon R^* \to \mathbb{Z}$ 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. ▮

9.3 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 9.7 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 9.8 *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 9.9 *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 9.8). 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 9.10 *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 9.5). 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 9.8). But then $z = apz + byz$, and hence p divides z. Thus p is prime, as required. ▮

9.4 Unique Factorization in Principal Ideal Domains

A direct application of Proposition 9.6 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 9.10 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 9.11 *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 9.1). 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 $p_1 p_2 \cdots p_k$. ▌

10 Modules

10.1 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 $\varphi\colon M \to N$ are themselves R-modules. Moreover if $\varphi\colon M \to N$ is a homomorphism of R-modules, and if L is a submodule of M satisfying $L \subset \ker\varphi$, then φ induces a homomorphism $\overline{\varphi}\colon M/L \to N$. 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 10.1 *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*

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

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. ▮

10.2 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 10.2 *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 10.3 *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 $\nu\colon M \to M/L$, 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 10.4 *The direct sum $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ of Noetherian modules $M_1, M_2, \ldots N_k$ 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 10.3 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.)

10.3 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 10.2.

Proposition 10.5 *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 10.5.

Corollary 10.6 *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 $\varphi\colon R^k \to M$ be the homomorphism of R-modules sending $(r_1, r_2, \ldots, r_k) \in R^k$ to

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

It follows from Corollary 10.4 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 $\varphi\colon R^k \to M$ is surjective. It follows from Proposition 10.3 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 10.7 *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 10.8 (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 10.5). 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 10.9 *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 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 with coefficients in the polynomial ring $R[x_1, x_2, \ldots, x_{n-1}]$.) The required results therefore follows from Hilbert's Basis Theorem (Theorem 10.8) by induction on n. ▮

Corollary 10.10 *Let K be a field. Then every ideal of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ is finitely-generated.*

11 Algebraic Sets and the Zariski Topology

11.1 Polynomial Rings in Several Variables

A *monomial* in the independent indeterminates $X_1, X_2, \ldots, X_n$ is by definition an expression of the form $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, where $i_1, i_2, \ldots, i_n$ are non-negative integers. Such monomials are multiplied according to the rule

$$\left(X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}\right) \left(X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n}\right) = X_1^{i_1+j_1} X_2^{i_2+j_2} \cdots X_n^{i_n+j_n}.$$

A *polynomial* p in the independent indeterminates with coefficients in some ring R is by definition a formal linear combination of the form

$$r_1 m_1 + r_2 m_2 + \cdots + r_k m_k$$

where $r_1, r_2, \ldots, r_k \in R$ and $m_1, m_2, \ldots, m_k$ are monomials in $X_1, X_2, \ldots, X_n$. The coefficients $r_1, r_2, \ldots, r_k$ of this polynomial are uniquely determined, provided that the monomials $m_1, m_2, \ldots, m_k$ are distinct. Such polynomials are added and multiplied together in the obvious fashion. In particular

$$\left(\sum_{i=1}^{k} r_i m_i\right) \left(\sum_{j=1}^{l} s_j m'_j\right) = \sum_{i=1}^{k} \sum_{j=1}^{l} (r_i s_j)(m_i m'_j),$$

where the product $m_i m'_j$ of the monomials m_i and m'_j is defined as described above. The set of all polynomials in the independent indeterminates $X_1, X_2, \ldots, X_n$ with coefficients in the ring R is itself a ring, which we denote by $R[X_1, X_2, \ldots, X_n]$.

Example The polynomial $2X_1X_2^3 - 6X_1X_2X_3^2$ is the product of the polynomials $2X_1X_2$ and $X_2^2 - 3X_3^2$ in the ring $\mathbb{Z}[X_1, X_2, X_3]$ of polynomials in X_1, X_2, X_3 with integer coefficients.

Lemma 11.1 *Let R be an integral domain. Then the ring $R[x]$ of polynomials in the indeterminate x with coefficients in R is itself an integral domain, and* $\deg(pq) = \deg p + \deg q$ *for all non-zero polynomials $p, q \in R[x]$.*

Proof The integral domain R is commutative, hence so is $R[x]$. Moreover $R[x]$ is unital, and the multiplicative identity element of $R[x]$ is the constant polynomial whose coefficient is the multiplicative identity element 1 of the unital ring R.

Let p and q be polynomials in $R[x]$, and let a_k and b_l be the leading coefficients of p and q respectively, where $k = \deg p$ and $l = \deg q$. Now

$$p(x)q(x) = a_k b_l x^{k+l} + \text{terms of lower degree.}$$

Moreover $a_k b_l \neq 0$, since $a_k \neq 0$, $b_l \neq 0$, and the ring R of coefficients is an integral domain. Thus if $p \neq 0$ and $q \neq 0$ then $pq \neq 0$, showing that $R[x]$ is an integral domain, and $\deg(pq) = k + l = \deg p + \deg q$, as required. ∎

Let p be a polynomial in the indeterminates $X_1, X_2, \ldots, X_n$ with coefficients in the ring R, where $n > 1$. By collecting together terms involving X_n^j for each non-negative integer j, we can write the polynomial p in the form

$$p(X_1, X_2, \ldots, X_n) = \sum_{j=0}^{k} p_j(X_1, X_2, \ldots, X_{n-1}) X_n^j$$

where $p_j \in R[X_1, X_2, \ldots, X_{n-1}]$ for $j = 0, 1, \ldots, k$. Now the right hand side of the above identity can be viewed as a polynomial in the indeterminate X_n with coefficients $p_1, p_2, \ldots, p_k$ in the ring $R[X_1, \ldots, X_{n-1}]$. Moreover the polynomial p uniquely determines and is uniquely determined by the polynomials $p_1, p_2, \ldots, p_k$. It follows from this that the rings $R[X_1, X_2, \ldots, X_n]$ and $R[X_1, X_2, \ldots, X_{n-1}][X_n]$ are naturally isomorphic and can be identified with one another. We can use the identification in order to prove results concerning the structure of the polynomial ring $R[X_1, X_2, \ldots, X_n]$ by induction on the number n of independent indeterminates $X_1, X_2, \ldots, X_n$. For example, the following result follows directly by induction on n, using Lemma 11.1.

Lemma 11.2 *Let R be an integral domain. Then the ring $R[X_1, X_2, \ldots, X_n]$ is also an integral domain.*

A monomial $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ is said to be of *degree* d, where d is some non-negative integer, if $i_1 + i_2 + \cdots + i_n = d$.

Definition Let R be a ring. A polynomial $p \in R[X_1, X_2, \ldots, X_n]$ is said to be *homogeneous* of degree d if it can be expressed as a linear combination of monomials of degree d with coefficients in the ring R.

Any polynomial $p \in R[X_1, X_2, \ldots, X_n]$ can be decomposed as a sum of the form

$$p^{(0)} + p^{(1)} + \cdots + p^{(k)},$$

where k is some sufficiently large non-negative integer and each polynomial $p^{(i)}$ is a homogeneous polynomial of degree i. The homogeneous polynomial $p^{(i)}$ is referred to as the *homogeneous component* of p of degree i; it is uniquely determined by p. A non-zero polynomial p is said to be of *degree* d if $p^{(d)} \neq 0$ and $p^{(i)} = 0$ for all $i > d$. The degree of a non-zero polynomial p is denoted by $\deg p$.

Lemma 11.3 *Let R be a ring, and let p and q be non-zero polynomials belonging to $R[X_1, X_2, \ldots, X_n]$. Then*

$$\deg(p+q) \leq \max(\deg p, \deg q), \textit{ provided that } p+q \neq 0,$$

$$\deg(pq) \leq \deg p + \deg q, \textit{ provided that } pq \neq 0.$$

Moreover if R is an integral domain then $pq \neq 0$ and $\deg(pq) = \deg p + \deg q$.

Proof The inequality $(p+q) \leq \max(\deg p, \deg q)$ is obvious. Also $p^{(i)}q^{(j)}$ is homogeneous of degree $i+j$ for all i and j, since the product of a monomial of degree i and a monomial of degree j is a monomial of degree $i+j$. The inequality $\deg(pq) \leq \deg p + \deg q$ follows immediately.

Now suppose that R is an integral domain. Let $k = \deg p$ and $l = \deg q$. Then the homogeneous component $(pq)^{(k+l)}$ of pq of degree $k+l$ is given by $(pq)^{(k+l)} = p^{(k)}q^{(l)}$. But $R[X_1, X_2, \ldots, X_n]$ is an integral domain (see Lemma 11.2), and $p^{(k)}$ and $q^{(l)}$ are both non-zero. It follows that $(pq)^{(k+l)} \neq 0$, and thus $\deg(pq) = \deg p + \deg q$, as required. ▮

11.2 Algebraic Sets and the Zariski Topology

Throughout this section, let K be a field.

Definition We define *affine n-space* $\mathbb{A}^n$ over the field K to be the set K^n of all n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_1, x_2, \ldots, x_n \in K$.

Where it is necessary to specify explicitly the field K involved, we shall denote affine n-space over the field K by $\mathbb{A}^n(K)$. Thus $\mathbb{A}^n(\mathbb{R}) = \mathbb{R}^n$, and $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$.

Definition A subset of n-dimensional affine space $\mathbb{A}^n$ is said to be an *algebraic set* if it is of the form

$$\{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n : f(x_1, x_2, \ldots, x_n) = 0 \text{ for all } f \in S\}$$

for some subset S of the polynomial ring $K[X_1, X_2, \ldots, X_n]$.

Example Any point of $\mathbb{A}^n$ is an algebraic set. Indeed, given any point $(a_1, a_2, \ldots, a_n)$ of $\mathbb{A}^n$, let $f_i(X_1, X_2, \ldots, X_n) = X_i - a_i$ for $i = 1, 2, \ldots, n$. Then the given point is equal to the set

$$\{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n : f_i(x_1, x_2, \ldots, x_n) = 0 \text{ for } i = 1, 2, \ldots, n\}.$$

Example The circle $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) : x^2 + y^2 = 1\}$ is an algebraic set in the plane $\mathbb{A}^2(\mathbb{R})$.

Let $\lambda\colon K^n \to K$ be a linear functional on the vector space K^n (i.e., a linear transformation from K^n to K). It follows from elementary linear algebra that there exist $b_1, b_2, \ldots, b_n \in K$ such that

$$\lambda(x_1, x_2, \ldots, x_n) = b_1 x_1 + b_2 x_2 + \cdots + b_n x_n$$

for all $(x_1, x_2, \ldots, x_n) \in K^n$. Thus if $\lambda_1, \lambda_2, \ldots, \lambda_k$ are linear functionals on K^n, and if $c_1, c_2, \ldots, c_k$ are suitable constants belonging to the field K then

$$\{(x_1, x_2 \ldots, x_n) \in \mathbb{A}^n : \lambda_i(x_1, x_2, \ldots, x_n) = c_i \text{ for } i = 1, 2, \ldots, k\}$$

is an algebraic set in $\mathbb{A}^n$. A set of this type is referred to as an *affine subspace* of $\mathbb{A}^n$. It is said to be of dimension $n - k$, provided that the linear functionals $\lambda_1, \lambda_2, \ldots, \lambda_k$ are linearly independent. It follows directly from elementary linear algebra that, if we we identify affine n-space $\mathbb{A}^n$ with the vector space K^n, then a subset of $\mathbb{A}^n$ is an m-dimensional affine subspace if and only if it is a translate of some m-dimensional vector subspace of K^n (i.e., it is of the form $\mathbf{v} + W$ where $\mathbf{v}$ is a point of $\mathbb{A}^n$ and W is some m-dimensional vector subspace of K^n).

Lemma 11.4 *Let V be an algebraic set in $\mathbb{A}^n$, and let L be a one-dimensional affine subspace of $\mathbb{A}^n$. Then either $L \subset V$ or else $L \cap V$ is a finite set.*

Proof The affine subspace L is a translate of a one-dimensional subspace of K^n, and therefore there exist vectors $\mathbf{v}$ and $\mathbf{w}$ in K^n such that $L = \{\mathbf{v} + \mathbf{w}t : t \in K\}$ (on identifying n-dimensional affine space $\mathbb{A}^n$ with the vector space K^n). Now we can write

$$V = \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n : f(x_1, x_2, \ldots, x_n) = 0 \text{ for all } f \in S\},$$

where S is some subset of the polynomial ring $K[X_1, X_2, \ldots, X_n]$. Now either each polynomial belonging to S is zero throughout L, in which case $L \subset V$, or else there is some $f \in S$ which is non-zero at some point of L. Define $g \in K[t]$ by the formula

$$g(t) = f(v_1 + w_1 t, v_2 + w_2 t, \ldots, v_n + w_n t)$$

(where v_i and w_i denote the ith components of the vectors $\mathbf{v}$ and $\mathbf{w}$ for $i = 1, 2, \ldots, n$). Then g is a non-zero polynomial in the indeterminate t, and therefore g has at most finitely many zeros. But $g(t) = 0$ whenever the point $\mathbf{v} + \mathbf{w}t$ of L lies in V. Therefore $L \cap V$ is finite, as required. ∎

Example The sets

$$\{(x,y) \in \mathbb{A}^2(\mathbb{R}) : y = \sin x\}$$

and

$$\{(x,y) \in \mathbb{A}^2(\mathbb{R}) : x \geq 0\}$$

are not algebraic sets in $\mathbb{A}^2(\mathbb{R})$, since the line $y = 0$ is not contained in either of these sets, yet the line intersects these sets at infinitely many points of the set.

Given any subset S of $K[X_1, X_2, \ldots, X_n]$, we denote by $V(S)$ the algebraic set in $\mathbb{A}^n$ defined by

$$V(S) = \{\mathbf{x} \in \mathbb{A}^n : f(\mathbf{x}) = 0 \text{ for all } f \in S\}.$$

Also, given any $f \in K[X_1, X_2, \ldots, X_n]$, we define $V(f) = V(\{f\})$.

Given any subset Z of $\mathbb{A}^n$, we define

$$I(Z) = \{f \in K[X_1, X_2, \ldots, X_n] : f(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in Z\}.$$

Clearly $S \subset I(V(S))$ for all subsets S of $K[X_1, X_2, \ldots, X_n]$, and $Z \subset V(I(Z))$ for all subsets Z of $\mathbb{A}^n$. If S_1 and S_2 are subsets of $K[X_1, X_2, \ldots, X_n]$ satisfying $S_1 \subset S_2$ then $V(S_2) \subset V(S_1)$. Similarly, if Z_1 and Z_2 are subsets of $\mathbb{A}^n$ satisfying $Z_1 \subset Z_2$ then $I(Z_2) \subset I(Z_1)$.

Lemma 11.5 *$V(I(V(S))) = V(S)$ for all subsets S of $K[X_1, X_2, \ldots, X_n]$, and similarly $I(V(I(Z))) = I(Z)$ for all subsets Z of $\mathbb{A}^n$.*

Proof It follows from the observations above that $V(S) \subset V(I(V(S)))$, since $Z \subset V(I(Z))$ for all subsets Z of $\mathbb{A}^n$. But also $S \subset I(V(S))$, and hence $V(I(V(S))) \subset V(S)$. Therefore $V(I(V(S))) = V(S)$. An analogous argument can be used to show that $I(V(I(Z))) = I(Z)$ for all subsets Z of $\mathbb{A}^n$. ▮

Let I and J be ideals of a unital commutative ring R. We denote by IJ the ideal of R consisting of those elements of R that can be expressed as finite sums of the form $i_1 j_1 + i_2 j_2 + \cdots + i_r j_r$ with $i_1, i_2, \ldots, i_r \in I$ and $j_1, j_2, \ldots, j_r \in J$. (One can readily verify that IJ is indeed an ideal of R.)

Proposition 11.6 *Let $R = K[X_1, X_2, \ldots, X_n]$ for some field K. Then*

(i) *$V(\{0\}) = \mathbb{A}^n$ and $V(R) = \emptyset$;*

(ii) *$\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$ for every collection $\{I_\lambda : \lambda \in \Lambda\}$ of ideals of R;*

(iii) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$ *for all ideals* I *and* J *of* R.

Thus there is a well-defined topology on $\mathbb{A}^n$ *(known as the* Zariski topology*) whose closed sets are the algebraic sets in* $\mathbb{A}^n$.

Proof (i) is immediate.

If $\mu \in \Lambda$ then $I_\mu \subset \sum_{\lambda\in\Lambda} I_\lambda$, and therefore $V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) \subset V(I_\mu)$. Thus $V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) \subset \bigcap_{\lambda\in\Lambda} V(I_\lambda)$. Conversely if $\mathbf{x}$ is a point of $\bigcap_{\lambda\in\Lambda} V(I_\lambda)$ then $f(\mathbf{x}) = 0$ for all $\lambda \in \Lambda$ and $f \in I_\lambda$, and therefore $f(\mathbf{x}) = 0$ for all $f \in \sum_{\lambda\in\Lambda} I_\lambda$. Thus $\bigcap_{\lambda\in\Lambda} V(I_\lambda) \subset V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$. It follows that $\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$. This proves (ii).

Let I and J be ideals of R. Then $I \cap J \subset I$, $I \cap J \subset J$ and $IJ \subset I \cap J$, and thus $V(I) \subset V(I \cap J)$, $V(J) \subset V(I \cap J)$ and $V(I \cap J) \subset V(IJ)$. Therefore

$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ).$$

If $\mathbf{x}$ is a point of $\mathbb{A}^n$ which does not belong to $V(I) \cup V(J)$ then there exist polynomials $f \in I$ and $g \in J$ such that $f(\mathbf{x}) \neq 0$ and $g(\mathbf{x}) \neq 0$. But then $fg \in IJ$ and $f(\mathbf{x})g(\mathbf{x}) \neq 0$, and therefore $\mathbf{x} \notin V(IJ)$. Therefore $V(IJ) \subset V(I) \cup V(J)$. We conclude that

$$V(I) \cup V(J) = V(I \cap J) = V(IJ).$$

This proves (iii).

Let us define a topology on $\mathbb{A}^n$ whose open sets in $\mathbb{A}^n$ are the complements of algebraic sets. We see from (i) that $\emptyset$ and $\mathbb{A}^n$ are open. Moreover it follows from (ii) that any union of open sets is open, and it follows from (iii), using induction on the number of sets, that any finite intersection of open sets is open. Thus the topology is well-defined. ▮

Definition The *Zariski topology* on an algebraic set V in $\mathbb{A}^n$ is the topology whose open sets are of the form $V \setminus V(I)$ for some ideal I of $K[X_1, X_2, \ldots, X_n]$.

It follows from Proposition 11.6 that the Zariski topology on an algebraic set V is well-defined and is the subspace topology on V induced by the topology on $\mathbb{A}^n$ whose closed sets are the algebraic sets in $\mathbb{A}^n$. Moreover a subset V_1 of V is closed if and only if V_1 is itself an algebraic set. (This follows directly from the fact that the intersection of two algebraic sets is itself an algebraic set.)

Example Any finite subset of $\mathbb{A}^n$ is an algebraic set. This follows from the fact that any point in $\mathbb{A}^n$ is an algebraic set, and any finite union of algebraic sets is an algebraic set.

In general, the Zariski topology on an algebraic set V is not Hausdorff. It can in fact be shown that an algebraic set in $\mathbb{A}^n$ is Hausdorff (with respect to the Zariski topology) if and only if it consists of a finite set of points in $\mathbb{A}^n$.

11.3 The Structure of Algebraic Sets

Let K be a field. We shall apply Hilbert's Basis Theorem in order to study the structure of algebraic sets in n-dimensional affine space $\mathbb{A}^n$ over the field K. We shall continue to use the notation for algebraic sets in $\mathbb{A}^n$ and corresponding ideals of the polynomial ring that was established earlier.

The following result is a direct consequence of the Hilbert Basis Theorem.

Proposition 11.7 *Let V be an algebraic set in $\mathbb{A}^n$. Then there exists a finite collection $f_1, f_2, f_3, \ldots$ of polynomials in n independent indeterminates such that*

$$V = \{\mathbf{x} \in \mathbb{A}^n : f_i(\mathbf{x}) = 0 \textit{ for } i = 1, 2, \ldots, k\}.$$

Proof The set V is an algebraic set, and therefore $V = V(I)$ for some ideal I of $K[X_1, X_2, \ldots, X_n]$. Moreover it follows from Corollary 10.10 that I is generated by some finite set $\{f_1, f_2, \ldots, f_k\}$ of polynomials. But then $V = V(\{f_1, f_2, \ldots, f_k\})$, and thus V is of the required form. ▮

A *algebraic hypersurface* in $\mathbb{A}^n$ is a algebraic set of $\mathbb{A}^n$ of the form $V(f)$ for some non-constant polynomial $f \in K[X_1, X_2, \ldots, X_n]$, where

$$V(f) = \{\mathbf{x} \in \mathbb{A}^n : f(\mathbf{x}) = 0\}.$$

Corollary 11.8 *Every proper algebraic set in $\mathbb{A}^n$ is the intersection of a finite number of algebraic hypersurfaces.*

Proof The empty set in $\mathbb{A}^n$ can be represented as an intersection of two hyperplanes (e.g., $x_1 = 0$ and $x_1 = 1$). Suppose therefore that the proper algebraic set V is non-empty. It follows from Proposition 11.7 that there exists a finite set $\{f_1, f_2, \ldots, f_k\}$ polynomials belonging to $K[X_1, X_2, \ldots, X_n]$ such that $V = V(\{f_1, f_2, \ldots, f_k\})$. Moreover the polynomials $f_1, f_2, \ldots, f_k$ cannot all be zero, since $V \neq \mathbb{A}^n$; we can therefore assume (by removing the zero polynomials from the list) that the polynomials $f_1, f_2, \ldots, f_k$ are non-zero. They must then all be non-constant, since V is non-empty. But then

$$V = V(f_1) \cap V(f_2) \cap \cdots \cap V(f_k),$$

as required. ▮

Proposition 11.9 *Let $\mathcal{C}$ be a collection of subsets of $\mathbb{A}^n$ that are open with respect to the Zariski topology on $\mathbb{A}^n$. Then there exists a finite collection $D_1, D_2, \ldots, D_k$ of open sets belonging to $\mathcal{C}$ such that $D_1 \cup D_2 \cup \cdots \cup D_k$ is the union $\bigcup_{D\in\mathcal{C}} D$ of all the open sets D belonging to $\mathcal{C}$.*

Proof It follows from the definition of the Zariski topology that, for each open set D belonging to $\mathcal{C}$, there exists an ideal I_D of $K[X_1, X_2, \ldots, X_n]$ such that $D = \mathbb{A}^n \setminus V(I_D)$. Let $I = \sum_{D\in\mathcal{C}} I_D$. Then

$$\begin{aligned}\bigcup\nolimits_{D\in\mathcal{C}} D &= \bigcup\nolimits_{D\in\mathcal{C}} (\mathbb{A}^n \setminus V(I_D)) = \mathbb{A}^n \setminus \bigcap\nolimits_{D\in\mathcal{C}} V(I_D) \\ &= \mathbb{A}^n \setminus V\left(\sum\nolimits_{D\in\mathcal{C}} I_D\right) = \mathbb{A}^n \setminus V(I)\end{aligned}$$

(see Proposition 11.6). Now the ideal I is finitely-generated (Corollary 10.10). Moreover there exists a finite generating set $\{f_1, f_2, \ldots, f_k\}$ for I with the property that each generator f_i belongs to one of the ideals I_D, since if we are given any finite generating set for I, then each of the generators can be expressed as a finite sum of elements taken from the ideals I_D, and the collection of all these elements constitutes a finite generating set for I which is of the required form. Choose $D_1, D_2, \ldots, D_k \in \mathcal{C}$ such that $f_i \in I_{D_i}$ for $i = 1, 2, \ldots, k$. Then

$$I = I_{D_1} + I_{D_2} + \cdots + I_{D_k},$$

and thus

$$\bigcup\nolimits_{D\in\mathcal{C}} D = \mathbb{A}^n - V(I) = \mathbb{A}^n - V\left(\sum_{i=1}^{k} I_{D_i}\right) = \bigcup_{i=1}^{k} D_i,$$

as required. ▌

We recall that a topological space is compact if and only if every open cover of that space has a finite subcover. The following result therefore follows directly from Proposition 11.9.

Corollary 11.10 *Every subset of $\mathbb{A}^n$ is compact with respect to the Zariski topology.*

11.4 Maximal Ideals and Zorn's Lemma

Definition Let R be a ring. A proper ideal I of R is said to be *maximal* if the only ideals J of R satisfying $I \subset J \subset R$ are $J = I$ and $J = R$.

Lemma 11.11 *A unital commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.*

Proof Suppose that R is a field. Let I be a non-zero ideal of R. Then there exists $x \in I$ satisfying $x \neq 0$. Moreover there exists $x^{-1} \in R$ satisfying $xx^{-1} = 1 = x^{-1}x$. Therefore $1 \in I$, and hence $I = R$. Thus the only ideals of R are $\{0\}$ and R.

Conversely, suppose that R is a unital commutative ring with the property that the only ideals of R are $\{0\}$ and R. Let x be a non-zero element of R, and let Rx denote the subset of R consisting of all elements of R that are of the form rx for some $r \in R$. It is easy to verify that Rx is an ideal of R. (In order to show that $yr \in Rx$ for all $y \in Rx$ and $r \in R$, one must use the fact that the ring R is commutative.) Moreover $Rx \neq \{0\}$, since $x \in Rx$. We deduce that $Rx = R$. Therefore $1 \in Rx$, and hence there exists some element x^{-1} of R satisfying $x^{-1}x = 1$. This shows that R is a field, as required. ▮

Lemma 11.12 *A proper ideal I of a unital commutative ring R is maximal if and only if the quotient ring R/I is a field.*

Proof Let I be a proper ideal of the unital commutative ring R. Then the quotient ring R/I is unital and commutative. Moreover there is a one-to-one correspondence between ideals L of R/I and ideals J of R satisfying $I \subset J \subset R$: if J is any ideal of R satisfying $I \subset J \subset R$, and if L is the corresponding ideal of R/I then $I + x \in L$ if and only if $x \in J$. We deduce that I is a maximal ideal of R if and only if the only ideals of R/I are the zero ideal $\{I\}$ and R/I itself. It follows from Lemma 11.11 that I is a maximal ideal of R if and only if R/I is a field. ▮

We claim that every proper ideal of a ring R is contained in at least one maximal ideal. In order to prove this result we shall make use of Zorn's Lemma concerning the existence of maximal elements of partially ordered sets.

Definition Let $\mathcal{S}$ be a set. A *partial order* $\leq$ on $\mathcal{S}$ is a relation on $\mathcal{S}$ satisfying the following conditions:—

(i) $x \leq x$ for all $x \in \mathcal{S}$ (i.e., the relation $\leq$ is *reflexive*),

(ii) if $x, y, z \in \mathcal{S}$ satisfy $x \leq y$ and $y \leq z$ then $x \leq z$ (i.e., the relation $\leq$ is *transitive*),

(iii) if $x, y \in \mathcal{S}$ satisfy $x \leq y$ and $y \leq x$ then $x = y$ (i.e., the relation $\leq$ is *antisymmetric*).

Neither of the conditions $x \leq y$ or $y \leq x$ need necessarily be satisfied by arbitrary elements x and y of a partially ordered set $\mathcal{S}$. A subset $\mathcal{C}$ of $\mathcal{S}$ is said to be *totally ordered* if one or other of the conditions $x \leq y$ and $y \leq x$ holds for each pair $\{x, y\}$ of elements of $\mathcal{C}$.

Example Let $\mathcal{S}$ be a collection of subsets of some given set. Then $\mathcal{S}$ is partially ordered with respect to the relation $\subset$ (where $A, B \in \mathcal{S}$ satisfy $A \subset B$ if and only if A is a subset of B).

Example The set $\mathbb{N}$ of natural numbers is partially ordered with respect to the relation $|$, where $n|m$ if and only if n divides m.

Let $\leq$ be the ordering relation on a partially ordered set $\mathcal{S}$. An element u of $\mathcal{S}$ is said to be an upper bound for a subset $\mathcal{B}$ of $\mathcal{S}$ if $x \leq u$ for all $x \in \mathcal{B}$. An element m of $\mathcal{S}$ is said to be *maximal* if the only element x of $\mathcal{S}$ satisfying $m \leq x$ is m itself.

The following result is an important theorem in set theory.

> **Zorn's Lemma.** Let $\mathcal{S}$ be a non-empty partially ordered set. Suppose that there exists an upper bound for each totally ordered subset of $\mathcal{S}$. Then $\mathcal{S}$ contains a maximal element.

We use Zorn's lemma in order to prove the following existence theorem for maximal ideals.

Theorem 11.13 *Let R be a unital ring, and let I be a proper ideal of R. Then there exists a maximal ideal M of R satisfying $I \subset M \subset R$.*

Proof Let $\mathcal{S}$ be the set of all proper ideals J of R satisfying $I \subset J$. The set $\mathcal{S}$ is non-empty, since $I \in \mathcal{S}$, and is partially ordered by the inclusion relation $\subset$. We claim that there exists an upper bound for any totally ordered subset $\mathcal{C}$ of $\mathcal{S}$.

Let L be the union of all the ideals belonging to some totally ordered subset $\mathcal{C}$ of $\mathcal{S}$. We claim that L is itself a proper ideal of R. Let a and b be elements of L. Then there exist proper ideals J_1 and J_2 belonging to $\mathcal{C}$ such that $a \in J_1$ and $b \in J_2$. Moreover either $J_1 \subset J_2$ or else $J_2 \subset J_1$, since the subset $\mathcal{C}$ of $\mathcal{S}$ is totally ordered. It follows that $a + b$ belongs either to J_1 or else to J_2, and thus $a + b \in L$. Similarly $-a \in L$, $ra \in L$ and $ar \in L$ for all $r \in R$. We conclude that L is an ideal of R. Moreover $1 \notin L$, since the elements of $\mathcal{C}$ are proper ideals of R, and therefore $1 \notin J$ for every $J \in \mathcal{C}$. It follows that L is a proper ideal of R satisfying $I \subset L$. Thus $L \in \mathcal{S}$, and L is an upper bound for $\mathcal{C}$.

The conditions of Zorn's Lemma are satisfied by the partially ordered set $\mathcal{S}$. Therefore $\mathcal{S}$ contains a maximal element M. This maximal element is the required maximal ideal of R containing the ideal I. ▮

Corollary 11.14 *Every unital ring has at least one maximal ideal.*

Proof Apply Theorem 11.13 with $I = \{0\}$. ▮

11.5 Prime Ideals

Definition Let R be a unital ring. A proper ideal I is said to be *prime* if, given any ideals J and K satisfying $JK \subset I$, either $J \subset I$ or $K \subset I$.

The following result provides an alternative description of prime ideals of a ring that is both unital and commutative.

Lemma 11.15 *Let R be a unital commutative ring. An proper ideal I of R is prime if and only if, given any elements x and y of R satisfying $xy \in I$, either $x \in I$ or $y \in I$.*

Proof Let I be a proper ideal of R. Suppose that I has the property that, given any elements x and y of R satisfying $xy \in I$, either $x \in I$ or $y \in I$. Let J and K be ideals of R neither of which is a subset of the ideal I. Then there exist elements $x \in J$ and $y \in K$ which do not belong to I. But then xy belongs to JK but does not belong to I. Thus the ideal JK is not a subset of I. This shows that the ideal I is prime.

Conversely, suppose that I is a prime ideal of R. Let x and y be elements of R satisfying $xy \in I$, and let J and K be the ideals generated by x and y respectively. Then

$$J = \{rx : r \in R\}, \qquad K = \{ry : r \in R\},$$

since R is unital and commutative (see Lemma 9.2). It follows easily that $JK = \{rxy : r \in R\}$. Now $xy \in I$. It follows that $JK \subset I$. But I is prime. Therefore either $J \subset I$ or $K \subset I$, and thus either $x \in I$ or $y \in I$. ▮

Example Let n be a natural number. Then the ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers is a prime ideal if and only if n is a prime number. For an integer j belongs to the ideal $n\mathbb{Z}$ if and only if n divides j. Thus the ideal $n\mathbb{Z}$ is prime if and only if, given any integers j and k such that n divides jk, either n divides j or n divides k. But it follows easily from the Fundamental Theorem of Arithmetic that a natural number n has this property if and only if n is a prime number. (The *Fundamental Theorem of Arithmetic* states that any natural number can be factorized uniquely as a product of prime numbers.)

Lemma 11.16 *An ideal I of a unital commutative ring R is prime if and only if the quotient ring R/I is an integral domain.*

Proof If I is a proper ideal of the unital commutative ring R then the quotient ring R/I is both unital and commutative. Moreover the zero element of R/I is I itself (regarded as a coset of I in R). Thus R/I is an integral domain if and only if, given elements x and y of R such that $(I+x)(I+y) = I$, either $I + x = I$ or $I + y = I$. But $(I + x)(I + y) = I + xy$ for all $x, y \in R$, and $I + x = I$ if and only if $x \in I$. We conclude that R/I is an integral domain if and only if I is prime, as required. ▮

Lemma 11.17 *Every maximal ideal of a unital commutative ring R is a prime ideal.*

Proof Let M be a maximal ideal of R. Then the quotient ring R/M is a field (see Lemma 11.12). In particular R/M is an integral domain, and hence M is a prime ideal. ▮

11.6 Affine Varieties and Irreducibility

Definition A topological space Z is said to be *reducible* if it can be decomposed as a union $F_1 \cup F_2$ of two proper closed subsets F_1 and F_2. (A subset of Z is *proper* if it is not the whole of Z.) A topological space Z is said to be *irreducible* if it cannot be decomposed as a union of two proper closed subsets.

Lemma 11.18 *Let Z be a topological space. The following are equivalent:—*

(i) *Z is irreducible,*

(ii) *the intersection of any two non-empty open sets in Z is non-empty,*

(iii) *every non-empty open subset of Z is dense.*

Moreover a subset A of a topological space Z is irreducible (with respect to the subspace topology) if and only if its closure $\overline{A}$ is irreducible.

Proof The topological space Z is irreducible if and only if the union of any two proper closed subsets of Z is a proper subset of Z. Now the complement of any proper closed set is a non-empty open set, and vica versa. Thus on taking complements we see that Z is irreducible if and only if the intersection of any two non-empty open subsets of Z is a non-empty subset of Z. This shows the equivalence of (i) and (ii).

The equivalence of (ii) and (iii) follows from the fact that a subset of Z is dense if and only if it has non-empty intersection with every non-empty open set in Z.

Let A be a subset of Z. It follows directly from the definition of the subspace topology on A that A is irreducible if and only if, given any closed sets F_1 and F_2 such that $A \subset F_1 \cup F_2$ then either $A \subset F_1$ or $A \subset F_2$. Now if F is any closed subset of Z then $A \subset F$ if and only if $\overline{A} \subset F$. It follows that A is irreducible if and only if $\overline{A}$ is irreducible. ▮

It follows immediately from Lemma 11.18 that a non-empty irreducible topological space is Hausdorff if and only if it consists of a single point.

Lemma 11.19 *Any irreducible topological space is connected.*

Proof A topological space Z is connected if and only if the only subsets of Z that are both open and closed are the empty set $\emptyset$ and the whole set Z. Thus suppose that the topological space Z were not connected. Then there would exist a non-empty proper subset U of Z that was both open and closed. Let $V = Z \setminus U$. Then U and V would be disjoint non-empty open sets. It would then follow from Lemma 11.18 that Z could not be irreducible. ▮

Lemma 11.20 *Let V be an algebraic set, and let V_1 be a proper algebraic subset of V. Then there exists $f \in K[X_1, X_2, \ldots, X_n]$ such that $f(\mathbf{x}) = 0$ for all $\mathbf{x} \in V_1$ but $f \notin I(V)$.*

Proof The inclusion $V_1 \subset V$ implies that $I(V) \subset I(V_1)$. Now $V = V(I(V))$ and $V_1 = V(I(V_1))$. Thus if V_1 is a proper subset of V then $I(V) \neq I(V_1)$, and hence there exists $f \in I(V_1)$ such that $f \notin I(V)$. Then f is the required polynomial. ▮

Proposition 11.21 *A non-empty algebraic set V in $\mathbb{A}^n$ is irreducible (with respect to the Zariski topology) if and only if the ideal $I(V)$ is a prime ideal of $K[X_1, X_2, \ldots, X_n]$.*

Proof Suppose that the algebraic set V is irreducible. Let f and g be polynomials in $K[X_1, X_2, \ldots, X_n]$ with the property that $fg \in I(V)$. Then $V \subset V(f) \cup V(g)$, since, given any point of V, one or other of the polynomials f and g must be zero at that point. Let $V_1 = V \cap V(f)$ and $V_2 = V \cap V(g)$. Then V_1 and V_2 are algebraic subsets of V, and $V = V_1 \cup V_2$. Therefore either $V = V_1$ or $V = V_2$, since the irreducible algebraic set V cannot be expressed as a union of two proper algebraic subsets. It follows that either $f \in I(V)$ or else $g \in I(V)$. Thus $I(V)$ is prime, by Lemma 11.15.

Conversely, suppose that V is reducible. Then there exist proper algebraic subsets V_1 and V_2 of V such that $V = V_1 \cup V_2$. It then follows from Lemma 11.20 that there exist polynomials f and g in $K[X_1, X_2, \ldots, X_n]$ such that $f(\mathbf{x}) = 0$ for all $\mathbf{x} \in V_1$, $g(\mathbf{x}) = 0$ for all $\mathbf{x} \in V_2$, and neither f nor g belongs to $I(V)$. But then $f(\mathbf{x})g(\mathbf{x}) = 0$ for all $\mathbf{x} \in V$, since $V = V_1 \cup V_2$, and hence $fg \in I(V)$. Thus the ideal $I(V)$ is not prime. ∎

Definition An *affine algebraic variety* is an irreducible algebraic set in $\mathbb{A}^n$.

Theorem 11.22 *Every algebraic set in $\mathbb{A}^n$ can be expressed as a finite union of affine algebraic varieties.*

Proof Let $\mathcal{C}$ be the collection of all ideals I of $K[X_1, X_2, \ldots, X_n]$ with the property that the corresponding algebraic set $V(I)$ cannot be expressed as a finite union of affine varieties. We claim that $\mathcal{C}$ cannot contain any maximal element.

Let I be an ideal of $K[X_1, X_2, \ldots, X_n]$ belonging to $\mathcal{C}$. Then the algebraic set $V(I)$ cannot itself be an affine variety, and therefore there must exist proper algebraic subsets V_1 and V_2 of V such that $V(I) = V_1 \cup V_2$. Let $I_1 = I(V_1)$ and $I_2 = I(V_2)$. Then $I(V(I)) \subset I_1$ and $I(V(I)) \subset I_2$, since $V_1 \subset V(I)$ and $V_2 \subset V(I)$. Also $I \subset I(V(I))$. It follows that $I \subset I_1$ and $I \subset I_2$. Moreover $V(I_1) = V_1$ and $V(I_2) = V_2$, since V_1 and V_2 are algebraic sets (see Lemma 11.5), and thus $V(I_1) \neq V(I)$ and $V(I_2) \neq V(I)$. It follows that $I \neq I_1$ and $I \neq I_2$. Thus I is a proper subset of both I_1 and I_2.

Now V_1 and V_2 cannot both be finite unions of affine varieties, since $V(I)$ is not a finite union of affine varieties. Thus one or other of the ideals I_1 and I_2 must belong to the collection $\mathcal{C}$. It follows that no ideal I belonging to $\mathcal{C}$ can be maximal in $\mathcal{C}$. But every non-empty collection of ideals of the Noetherian ring $K[X_1, X_2, \ldots, X_n]$ must have a maximal element (see Proposition 10.5). Therefore $\mathcal{C}$ must be empty, and thus every algebraic set in $\mathbb{A}^n$ is a finite union of affine varieties, as required. ∎

We shall show that every algebraic set in $\mathbb{A}^n$ has an essentially unique representation as a finite union of affine varieties.

Lemma 11.23 *Let $V_1, V_2, \ldots, V_k$ be algebraic sets in $\mathbb{A}^n$, and let W be an affine variety satisfying $W \subset V_1 \cup V_2 \cup \cdots \cup V_k$. Then $W \subset V_i$ for some i.*

Proof The affine variety W is the union of the algebraic sets $W \cap V_i$ for $i = 1, 2, \ldots, k$. It follows from the irreducibility of W that the algebraic sets $W \cap V_i$ cannot all be proper subsets of W. Hence $W = W \cap V_i$ for some i, and hence $W \subset V_i$, as required. ∎

Proposition 11.24 *Let V be an algebraic set in $\mathbb{A}^n$, and let $V = V_1 \cup V_2 \cup \cdots V_k$, where $V_1, V_2, \ldots, V_k$ are affine varieties, and $V_i \not\subset V_j$ for any $j \neq i$. Then $V_1, V_2, \ldots, V_k$ are uniquely determined by V.*

Proof Suppose that $V = W_1 \cup W_2 \cup \cdots W_m$, where $W_1, W_2, \ldots, W_m$ are affine varieties, and $W_i \not\subset W_j$ for any $j \neq i$. Now it follows from Lemma 11.23 that, for each integer i between 1 and k, there exists some integer $\sigma(i)$ between 1 and m such that $V_i \subset W_{\sigma(i)}$. Similarly, for each integer j between 1 and m, there exists some integer $\tau(j)$ between 1 and k such that $W_j \subset V_{\tau(j)}$. Now $V_i \subset W_{\sigma(i)} \subset V_{\tau(\sigma(i))}$, But $V_i \not\subset V_{i'}$ for any $i' \neq i$. It follows that $i = \tau(\sigma(i))$ and $V_i = W_{\sigma(i)}$. Similarly $W_j \subset V_{\tau(j)} \subset W_{\sigma(\tau(j))}$, and thus $j = \sigma(\tau(j))$ and $W_j = V_{\tau(j)}$. We deduce that

$$\sigma\colon \{1, 2, \ldots, k\} \to \{1, 2, \ldots, m\}$$

is a bijection with inverse τ, and thus $k = m$. Moreover $V_i = W_{\sigma(i)}$, and thus the varieties $V_1, V_2, \ldots, V_k$ are uniquely determined by V, as required. ▌

Let V be an algebraic set, and let $V = V_1 \cup V_2 \cup \cdots V_k$, where $V_1, V_2, \ldots, V_k$ are affine varieties, and $V_i \not\subset V_j$ for any $j \neq i$. The varieties $V_1, V_2, \ldots, V_k$ are referred to as the *irreducible components* of V.

11.7 Radical Ideals

Definition Let R be a unital commutative ring. An ideal I of R is said to be a *radical ideal* if every element x of R with the property that $x^m \in I$ for some natural number m belongs to I.

Lemma 11.25 *Every prime ideal of a unital commutative ring R is a radical ideal.*

Proof Let I be a prime ideal. Suppose that $x \in R$ satisfies $x^m \in I$. If $m = 1$ then we are done. If not, then either $x \in I$ or $x^{m-1} \in I$, since I is prime. Thus it follows by induction on m that $x \in I$. Thus I is a radical ideal.

Lemma 11.26 *Let I be an ideal of a unital commutative ring R, and let $\sqrt{I}$ denote the set of all elements x of R with the property that $x^m \in I$ for some natural number m. Then $\sqrt{I}$ is a radical ideal of R. Moreover $I = \sqrt{I}$ if and only if I is a radical ideal of R.*

Proof Let x and y be elements of $\sqrt{I}$. Then there exist natural numbers m and n such that $x^m \in I$ and $y^n \in I$. Now

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i},$$

(where $x^0 = 1 = y^0$), and moreover, given any value of i between 0 and $m+n$, either $i \geq m$ or $m+n-i \geq n$, so that either $x^i \in I$ or $y^{m+n-i} \in I$. Therefore $(x+y)^{m+n} \in I$, and thus $x+y \in \sqrt{I}$. Also $-x \in \sqrt{I}$ and $rx \in \sqrt{I}$ for all $r \in R$. Thus $\sqrt{I}$ is an ideal of R. Clearly $\sqrt{I}$ is a radical ideal, and $I = \sqrt{I}$ if and only if I is a radical ideal. ∎

The ideal $\sqrt{I}$ is referred to as the *radical* of the ideal I.

Lemma 11.27 *Let Z be a subset of $\mathbb{A}^n$. Then $I(Z)$ is a radical ideal of the polynomial ring $K[X_1, X_2, \ldots, X_n]$. Moreover $Z = V(I(Z))$ if and only if Z is an algebraic set in $\mathbb{A}^n$.*

Proof Note that if g and h are polynomials belonging to $K[X_1, X_2, \ldots, X_n]$ which are zero throughout the set Z then the same is true of the polynomials $g+h$, $-g$ and fg for all $f \in K[X_1, X_2, \ldots, X_n]$. Therefore I is an ideal of $K[X_1, X_2, \ldots, X_n]$. Moreover g^m is identically zero on Z if and only if the same is true of g. Therefore the ideal $I(Z)$ is a radical ideal. If $Z = V(I(Z))$ then Z is clearly an algebraic set. Conversely, if Z is an algebraic set then $Z = V(S)$ for some subset S of $K[X_1, X_2, \ldots, X_n]$, and therefore

$$V(I(Z)) = V(I(V(S))) = V(S) = Z,$$

by Lemma 11.5, as required. ∎

Lemma 11.28 *Let S be a subset of the polynomial ring $K[X_1, X_2, \ldots, X_n]$, and let I be the ideal generated by S. Then $V(S) = V(I) = V(\sqrt{I})$, where $\sqrt{I}$ is the radical of the ideal I. Thus every algebraic set in $\mathbb{A}^n$ is of the form $V(I)$ for some radical ideal I of $K[X_1, X_2, \ldots, X_n]$.*

Proof The ideal $I(V(S))$ of $K[X_1, X_2, \ldots, X_n]$ contains the set S. Therefore $I \subset I(V(S))$, where I is the ideal generated by S. Moreover if $f \in \sqrt{I}$ then $f^m \in I$ for some natural number m, and thus $f^m \in I(V(S))$. But $I(V(S))$ is a radical ideal (see Lemma 11.27). Therefore $f \in I(V(S))$. Thus

$$S \subset I \subset \sqrt{I} \subset I(V(S)).$$

It follows that

$$V(I(V(S))) \subset V(\sqrt{I}) \subset V(I) \subset V(S).$$

But $V(I(V(S))) = V(S)$ (see Lemma 11.5). Therefore $V(S) = V(I) = V(\sqrt{I})$, as required. ∎

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

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

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

$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k = 0_M,$$

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

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

(see Lemma 10.1). 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*

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

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

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

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

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

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

Then

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

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

Proposition 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

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

(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

$$\varphi(r_1 x_1 + r_2 x_2 + \cdots + r_k x_k) = r_1 f(x_1) + r_2 f(x_2) + \cdots + r_k f(x_k).$$

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

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

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 $\varphi\colon M \to N$ 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 $\varphi\colon M_Y \to N$ defined on the submodules M_Y of M generated by finite subsets Y of X can be pieced together to yield the required function $\varphi\colon M \to N$. 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 $\varphi\colon M \to N$ is an R-module homomorphism. The uniqueness of the R-module homomorphisms φ_Y then ensures that $\varphi\colon M \to N$ is the unique R-module homomorphism from M to N that extends $f\colon X \to N$, 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 $\pi\colon M \to N$ be a surjective R-module homomorphism, and let $\varphi F \to N$ be an R-module homomorphism. Then there exists an R-module homomorphism $\psi\colon F \to M$ 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 $\pi\colon M \to N$ is surjective, there exists a function $f\colon F \to M$ 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 $\psi\colon F \to M$ 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 $\varphi|X \to X \to N$ 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 $\pi\colon M \to F$ 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 $\psi\colon F \to M$ with the property that $\pi(\psi(f)) = f$ for all $f \in F$. Let $\theta\colon \ker \pi \oplus F \to M$ be defined so that $\theta(k, f) = k + \psi(f)$ for all $f \in F$. Then $\theta\colon \ker \pi \oplus F \to M$ is an R-module homomorphism. Now

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

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

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

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 $\nu\colon M \to R$ be defined such that

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

Then $\nu\colon M \to R$ 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 linear 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 $\theta\colon R^k \to M$ 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 $\theta\colon R^k \to M$ 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 M 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 $\nu \colon M \to R$ be defined such that

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

Then $\nu \colon M \to R$ 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 that 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 $N \cap \ker \mu$ 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 $\varphi\colon M \to F$ 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 $\varphi\colon M \to F$ 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*

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

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

Proof Let $m_1, m_2 \in T$. Then there exist non-zero elements s_1 and s_2 of R such that $s_1 m_1 = 0_M$ and $s_2 m_2 = 0_M$. Let $s = s_1 s_2$. The requirement that the coefficient ring R be an integral domain then ensures that s is a non-zero element of R. Also $sm_1 = 0_M$, $sm_2 = 0_M$, 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 $\nu\colon M \to F$ 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. ∎