Course 311: Abstract Algebra
Academic year 2007-08

D. R. Wilkins

Contents

4 Commutative Algebra and Algebraic Geometry

4.1 Modules

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

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

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

(iii) the identities

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

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

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

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

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

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

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

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

Let M and N be modules over some unital commutative ring R. A function $\varphi\colon M \to N$ is said to be a *homomorphism of R-modules* if $\varphi(x+y) =$

$\varphi(x)+\varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $x, y \in M$ and $r \in R$. A homomorphism of R-modules is said to be an isomorphism if it is invertible. The kernel $\ker\varphi$ and image $\varphi(M)$ of any homomorphism $\varphi: M \to N$ are themselves R-modules. Moreover if $\varphi: M \to N$ is a homomorphism of R-modules, and if L is a submodule of M satisfying $L \subset \ker\varphi$, then φ induces a homomorphism $\overline{\varphi}: M/L \to N$. This induced homomorphism is an isomorphism if and only if $L = \ker\varphi$ and $N = \varphi(M)$.

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

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

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

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

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

Lemma 4.1 *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. ∎

4.2 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 4.2 *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 4.3 *Let R be a unital commutative ring, let M be an R-module, and let L be a submodule of M. Then M is Noetherian if and only if L and M/L are Noetherian.*

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

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

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

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

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

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

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

is a generating set for J.

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

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

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

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

and thus

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

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

Corollary 4.4 *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 4.3 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.)

4.3 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 4.2.

Proposition 4.5 *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 4.5.

Corollary 4.6 *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 4.4 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 4.3 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 4.7 *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

$$x = r_1a_1 + r_2a_2 + \cdots + r_ka_k$$

, 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 4.8 (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 4.5). 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 4.9 *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 4.8) by induction on n. ∎

Corollary 4.10 *Let K be a field. Then every ideal of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ is finitely-generated.*

4.4 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 4.11 *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 4.11.

Lemma 4.12 *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 4.13 *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*

$\deg(p + q) \leq \max(\deg p, \deg q)$, *provided that* $p + q \neq 0$,

$\deg(pq) \leq \deg p + \deg q$, *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 4.12), 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. ∎

4.5 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 4.14 *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 4.15 *$V(I(V(S))) = V(S)$ 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 4.16 *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 4.16 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 $\mathbb{A}^n$.

4.6 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 4.17 *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 4.10 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 4.18 *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 4.17 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 4.19 *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

$$\begin{aligned} \bigcup_{D \in \mathcal{C}} D &= \bigcup_{D \in \mathcal{C}} (\mathbb{A}^n \setminus V(I_D)) = \mathbb{A}^n \setminus \bigcap_{D \in \mathcal{C}} V(I_D) \\ &= \mathbb{A}^n \setminus V\left(\sum_{D \in \mathcal{C}} I_D\right) = \mathbb{A}^n \setminus V(I) \end{aligned}$$

(see Proposition 4.16). Now the ideal I is finitely-generated (Corollary 4.10). 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

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

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 4.19.

Corollary 4.20 *Every subset of $\mathbb{A}^n$ is compact with respect to the Zariski topology.*

4.7 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 4.21 *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 2.4 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 4.22 *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 4.23 *Every unital ring has at least one maximal ideal.*

Proof Apply Theorem 4.22 with $I = \{0\}$. ∎

4.8 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 4.24 *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 2.5). 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 4.25 *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 4.26 *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 4.21). In particular R/M is an integral domain, and hence M is a prime ideal. ∎

4.9 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 4.27 *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 4.27 that a non-empty irreducible topological space is Hausdorff if and only if it consists of a single point.

Lemma 4.28 *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 4.27 that Z could not be irreducible. ∎

Lemma 4.29 *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 4.30 *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 4.24.

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 4.29 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 4.31 *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 4.15), 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 4.5). 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 4.32 *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 4.33 *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 4.32 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.

4.10 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 4.34 *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 4.35 *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 4.36 *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 4.15, as required. ∎

Lemma 4.37 *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 4.36). 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 4.15). Therefore $V(S) = V(I) = V(\sqrt{I})$, as required. ∎

4.11 Commutative Algebras of Finite Type

Definition Let K be a field. A unital ring R is said to be a K-*algebra* if $K \subset R$, the multiplicative identity elements of K and R coincide, and $ab = ba$ for all $a \in K$ and $b \in R$.

It follows from this definition that a unital commutative ring R is a K-algebra if $K \subset R$ and K and R have the same multiplicative identity element. Note that if $L: K$ is a field extension, then the field L is a unital K-algebra.

Definition Let K be a field, and let R_1 and R_2 be K-algebras. A ring homomorphism $\varphi: R_1 \to R_2$ is said to be a K-homomorphism if $\varphi(k) = k$ for all $k \in K$.

Given any subset A of a unital commutative K-algebra R, we denote by $K[A]$ the subring of R generated by $K \cup A$ (i.e., the smallest subring of R containing $K \cup A$). In particular, if $a_1, a_2, \ldots, a_k$ are elements of R then we denote by $K[a_1, a_2, \ldots, a_k]$ the subring of R generated by $K \cup \{a_1, a_2, \ldots, a_k\}$. If $R = K[A]$ then we say that the set A *generates* the K-algebra R.

Note that any element of $K[a_1, a_2, \ldots, a_k]$ is of the form $f(a_1, a_2, \ldots, a_k)$ for some polynomial f in k independent indeterminates with coefficients in K. Indeed the set of elements of R that are of this form is a subring of R, and is clearly the smallest subring of R containing $K \cup \{a_1, a_2, \ldots, a_k\}$.

Definition Let K be a field. A unital commutative ring R is said to be a K-*algebra of finite type* if $K \subset R$, the identity elements of K and R coincide, and there exists a finite subset $a_1, a_2, \ldots, a_k$ of R such that $R = K[a_1, a_2, \ldots, a_k]$.

Lemma 4.38 *Let K be a field. Then every K-algebra of finite type is a Noetherian ring.*

Proof Let R be a K-algebra of finite type. Then there exist $a_1, a_2, \ldots, a_k \in R$ such that $R = K[a_1, a_2, \ldots, a_k]$. Now it follows from the Hilbert Basis Theorem that the ring $K[X_1, X_2, \ldots, X_k]$ of polynomials in the independent indeterminates $X_1, X_2, \ldots, X_k$ with coefficients in K is a Noetherian ring (see Corollary 4.10). Moreover $R \cong K[X_1, X_2, \ldots, X_k]/\mathfrak{a}$, where $\mathfrak{a}$ is the kernel of the homomorphism

$$\varepsilon\colon K[X_1, X_2, \ldots, X_k] \to R$$

that sends $f \in K[X_1, X_2, \ldots, X_k]$ to $f(a_1, a_2, \ldots, a_k)$. (Note that the homomorphism ε is surjective; indeed the image of this homomorphism is a subring of R containing K and a_i for $i = 1, 2, \ldots, k$, and is therefore the whole of R.) Thus R is isomorphic to the quotient of a Noetherian ring, and is therefore itself Noetherian (see Lemma 4.7). ∎

If $K(\alpha)\colon K$ is a simple algebraic extension then $K(\alpha)$ is a K-algebra of finite type. Indeed $K(\alpha)$ is a finite-dimensional vector space over K (see Theorem 3.4). If $a_1, a_2, \ldots, a_k$ span $K(\alpha)$ as a vector space over K then clearly $K(\alpha) = K[a_1, a_2, \ldots, a_k]$.

4.12 Zariski's Theorem

Proposition 4.39 *Let K and L be fields, with $K \subset L$. Suppose that $L\colon K$ is a simple field extension and that L is a K-algebra of finite type. Then the extension $L\colon K$ is finite.*

Proof The field L is a K-algebra of finite type, and therefore there exist elements $\beta_1, \beta_2, \ldots, \beta_m$ of L such that $L = K[\beta_1, \beta_2, \ldots, \beta_m]$. Also the field extension $L\colon K$ is simple, and therefore $L = K(\alpha)$ for some element α of K. Now, given any element β of L there exist polynomials f and g in $K(x)$ such that $g(\alpha) \neq 0$ and $\beta = f(\alpha)g(\alpha)^{-1}$. Indeed one may readily verify that the set of elements of L that may be expressed in the form $f(\alpha)g(\alpha)^{-1}$ for some polynomials $f, g \in K[X]$ with $g(\alpha) \neq 0$ is a subfield of L which contains $K \cup \{\alpha\}$. It is therefore the whole of L, since $L = K(\alpha)$. It follows that there exist polynomials f_i and g_i in $K[X]$ such that $g_i(\alpha) \neq 0$ and $\beta_i = f_i(\alpha)g_i(\alpha)^{-1}$ for $i = 1, 2, \ldots, m$. Let $e(x) = g_1(x)g_2(x)\ldots, g_m(x)$. We shall show that if the element α of L were not algebraic over K then every irreducible polynomial with coefficients in K would divide $e(x)$, Let $p \in K[X]$ be an irreducible polynomial with coefficients in K, where $p(\alpha) \neq 0$. Now $L = K[\beta_1, \beta_2, \ldots, \beta_m]$, and therefore every element of L is expressible as a polynomial in $\beta_1, \beta_2, \ldots, \beta_m$ with coefficients in K. Thus there exists some polynomial H_p in m indeterminates, with coefficents in K, such that

$$p(\alpha)^{-1} = H_p(\beta_1, \beta_2, \ldots, \beta_m).$$

Let d be the total degree of H. One can readily verify that

$$e(\alpha)^d H_p(\beta_1, \beta_2, \ldots, \beta_m) = q(\alpha),$$

for some polynomial $q(x)$ with coefficients in K. But then $p(\alpha)q(\alpha) = e(\alpha)^d$, and therefore α is a zero of the polynomial $pq - e^d$. If it were the case that α were not algebraic over K then this polynomial $pq - e^d$ would be the zero polynomial, and thus $p(x)q(x) = e(x)^d$. But it follows from Proposition 2.14 that an irreducible polynomial divides a product of polynomials if and only if it divides at least one of the factors. Therefore the irreducible polynomial p would be an irreducible factor of the polynomial e, and so would be an irreducible factor of one of the polynomials $g_1, g_2, \ldots, g_m$. We see therefore that if α were not algebraic over K then the polynomial e would be divisible by every irreducible polynomial in $K[X]$. But this is impossible, because a given polynomial in $K[X]$ can have only finitely many irreducible factors, whereas $K[X]$ contains infinitely many irreducible polynomials (Lemma 2.13). We conclude therefore that α must be algebraic over K. But any simple algebraic field extension is finite (Theorem 3.4). Therefore $L: K$ is finite, as required. ∎

Lemma 4.40 *Suppose that $K \subset A \subset B$, where A and B are unital commutative rings, and B is both a K-algebra of finite type and a finitely generated A-module. Then A is also a K-algebra of finite type.*

Proof There exist $\alpha_1, \alpha_2, \ldots, \alpha_m \in B$ such that $B = K[\alpha_1, \alpha_2, \ldots, \alpha_m]$, since B is a K-algebra of finite type. Also there exist $\beta_1, \beta_2, \ldots, \beta_n \in B$ such that

$$B = A\beta_1 + A\beta_2 + \cdots + A\beta_n,$$

since B is a finitely generated A-module. Moreover we can choose $\beta_1 = 1$. But then there exist elements λ_{qi} of A such that $\alpha_q = \sum_{i=1}^n \lambda_{qi}\beta_i$ for $q = 1, 2, \ldots, n$. Also there exist elements μ_{ijk} of A such that $\beta_i\beta_j = \sum_{k=1}^n \mu_{ijk}\beta_k$ for $i, j = 1, 2 \ldots, n$. Let

$$S = \{\lambda_{qi} : 1 \leq q \leq m,\ 1 \leq i \leq n\} \cup \{\mu_{ijk} : 1 \leq i, j, k \leq n\},$$

let $A_0 = K[S]$, and let

$$B_0 = A_0\beta_1 + A_0\beta_2 + \cdots + A_0\beta_n.$$

Now each product $\beta_i\beta_j$ is a linear combination of $\beta_1, \beta_2, \ldots, \beta_n$ with coefficients μ_{ijk} in A_0, and therefore $\beta_i\beta_j \in B_0$ for all i and j. It follows from this that the product of any two elements of B_0 must itself belong to B_0. Therefore B_0 is a subring of B. Now $K \subset B_0$, since $K \subset A_0$ and $\beta_1 = 1$. Also $\alpha_q \in B_0$ for $q = 1, 2, \ldots, m$. But $B = K(\alpha_1, \alpha_2, \cdots \alpha_m)$. It follows that $B_0 = B$, and therefore B is a finitely-generated A_0-module.

Now any K-algebra of finite type is a Noetherian ring (Lemma 4.38). It follows that A_0 is a Noetherian ring, and therefore any finitely-generated module over A_0 is Noetherian (see Corollary 4.6). In particular B is a Noetherian A_0-module, and therefore every submodule of B is a finitely-generated A_0-module. In particular, A is a finitely-generated A_0-module. Let $\gamma_1, \gamma_2, \ldots, \gamma_p$ be a finite collection of elements of A that generate A as an A_0-module. Then any element a of A can be written in the form

$$a = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_p\gamma_p,$$

where $a_l \in A_0$ for $l = 1, 2, \ldots, p$. But each element of A_0 can be expressed as a polynomial in the elements λ_{qi} and μ_{ijk} with coefficients in K. It follows that each element of A can be expressed as a polynomial in the elements λ_{qi}, μ_{ijk} and γ_l (with coefficients in K), and thus $A = K[T]$, where

$$T = S \cup \{\gamma_l : 1 \leq l \leq p\}.$$

Thus A is a K-algebra of finite type, as required. ∎

Theorem 4.41 (Zariski) *Let $L{:}\,K$ be a field extension. Suppose that the field L is a K-algebra of finite type. Then $L{:}\,K$ is a finite extension of K.*

Proof We prove the result by induction on the number of elements required to generate L as a K-algebra. Thus suppose that $L = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$, and that the result is true for all field extensions $L_1{:}\,K_1$ with the property that L_1 is generated as a K_1-algebra by fewer than n elements (i.e., there exist elements $\beta_1, \beta_2, \ldots, \beta_m$ of L_1, where $m < n$, such that $L_1 = K_1[\beta_1, \beta_2, \ldots, \beta_m]$). Let $K_1 = K(\alpha_1)$. Then $L = K_1[\alpha_2, \alpha_3, \cdots, \alpha_n]$. It follows from the induction hypothesis that $L{:}\,K_1$ is a finite field extension (and thus L is a finitely-generated K_1-module). It then follows from Lemma 4.40 that K_1 is a K-algebra of finite type.

But the extension $K_1{:}\,K$ is a simple extension. It therefore follows from Proposition 4.39 that the extension $K_1{:}\,K$ is finite. Thus both $L{:}\,K_1$ and $K_1{:}\,K$ are finite extensions. It follows from the Tower Law (Proposition 3.1) that $L{:}\,K$ is a finite extension, as required. ∎

4.13 Hilbert's Nullstellensatz

Proposition 4.42 *Let K be an algebraically closed field, let R be a commutative K-algebra of finite type, and let $\mathfrak{m}$ be a maximal ideal of R. Then there exists a surjective K-homomorphism $\xi\colon R \to K$ from R to K such that $\mathfrak{m} = \ker \xi$.*

Proof Let $L = R/\mathfrak{m}$, and let $\varphi\colon R \to L$ denote the quotient homomorphism. Then L is a field (Lemma 4.21). Now $\mathfrak{m} = \ker \varphi$ and $1 \notin \mathfrak{m}$, and therefore $\varphi|K \neq 0$. It follows that $\mathfrak{m} \cap K$ is a proper ideal of the field K. But the only proper ideal of a field is the zero ideal (Lemma 2.4). Therefore $\mathfrak{m} \cap K = \{0\}$. It follows that the restriction of φ to K is injective and maps K isomorphically onto a subfield of L. Let $K_1 = \varphi(K)$, and let $\iota\colon K \to K_1$ be the isomorphism obtained on restricting $\varphi\colon R \to L$ to K. Then $L\colon K_1$ is a field extension, and L is a K_1-algebra of finite type. It follows from Zariski's Theorem (Theorem 4.41) that $L\colon K_1$ is a finite field extension. But then $L = K_1$, since the field K_1 is algebraically closed (Lemma 3.7). Let $\xi = \iota^{-1} \circ \varphi$. Then $\xi\colon R \to K$ is the required K-homomorphism from R to K.

Theorem 4.43 *Let K be an algebraically closed field, and let R be a commutative K-algebra of finite type. Let $\mathfrak{a}$ be a proper ideal of R. Then there exists a K-homomorphism $\xi\colon R \to K$ from R to K such that $\mathfrak{a} \subset \ker \xi$.*

Proof Every proper ideal of R is contained in some maximal ideal (Theorem 4.22). Let $\mathfrak{m}$ be a maximal ideal of R with $\mathfrak{a} \subset \mathfrak{m}$. It follows from Proposition 4.42 that $\mathfrak{m} = \ker \xi$ for some K-homomorphism $\xi\colon R \to K$. Then $\mathfrak{a} \subset \ker \xi$, as required. ∎

Theorem 4.44 (Weak Nullstellensatz) *Let K be an algebraically closed field, and let $\mathfrak{a}$ be a proper ideal of the polynomial ring $K[X_1, X_2, \ldots, X_n]$, where $X_1, X_2, \ldots, X_n$ are independent indeterminates. Then there exists some point $(a_1, a_2, \ldots, a_n)$ of $\mathbb{A}^n(K)$ such that $f(a_1, a_2, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$.*

Proof Let $R = K[X_1, X_2, \ldots, X_n]$. Then R is a K-algebra of finite type. It follows from Theorem 4.43 that there exists a K-homomorphism $\xi\colon R \to K$ such that $\mathfrak{a} \subset \ker \xi$. Let $a_i = \xi(X_i)$ for $i = 1, 2, \ldots, n$. Then $\xi(f) = f(a_1, a_2, \ldots, a_n)$ for all $f \in R$. It follows that $f(a_1, a_2, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$, as required. ∎

Theorem 4.45 (Strong Nullstellensatz) *Let K be an algebraically closed field, let $\mathfrak{a}$ be an ideal of the polynomial ring $K[X_1, X_2, \ldots, X_n]$, and let $f \in$*

$K[X_1, X_2, \ldots, X_n]$ be a polynomial with the property that $f(x_1, x_2, \ldots, x_n) = 0$ for all $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$, where

$$V(\mathfrak{a}) = \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(K) : g(x_1, x_2, \ldots, x_n) = 0 \textit{ for all } g \in \mathfrak{a}\}.$$

Then $f^r \in \mathfrak{a}$ for some natural number r.

Proof Let $R = K[X_1, X_2, \ldots, X_n]$, and let S denote the ring $R[Y]$ of polynomials in a single indeterminate Y with coefficients in the ring R. Then S can be viewed as the ring $K[X_1, X_2, \ldots, X_n, Y]$ of polynomials in the $n+1$ indeterminate indeterminates $X_1, X_2, \ldots, X_n, Y$ with coefficients in the field K. The ideal $\mathfrak{a}$ of R determines a corresponding ideal $\mathfrak{b}$ of S consisting of those elements of S that are of the form

$$g_0 + g_1 Y + g_2 Y^2 + \cdots + g_r Y^r$$

with $g_0, g_1, \ldots, g_r \in \mathfrak{a}$. (Thus the ideal $\mathfrak{b}$ consists of those elements of the ring S that can be considered as polynomials in the indeterminate Y with coefficients in the ideal $\mathfrak{a}$ of R.)

Let $f \in R$ be a polynomial in the indeterminates $X_1, X_2, \ldots, X_n$ with the property that $f(x_1, x_2, \ldots, x_n) = 0$ for all $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$, and let $\mathfrak{c}$ be the ideal of S defined by

$$\mathfrak{c} = \mathfrak{b} + (1 - fY).$$

(Here $(1 - fY)$ denotes the ideal of the polynomial ring S generated by the polynomial $1 - f(X_1, X_2, \ldots, X_n)Y$.) Let $V(\mathfrak{c})$ be the subset of $(n+1)$-dimensional affine space $\mathbb{A}^{n+1}(K)$ consisting of all points $(x_1, x_2, \ldots, x_n, y) \in \mathbb{A}^{n+1}(K)$ with the property that $h(x_1, x_2, \ldots, x_n, y) = 0$ for all $h \in \mathfrak{c}$. We claim that $V(\mathfrak{c}) = \emptyset$.

Let $(x_1, x_2, \ldots, x_n, y)$ be a point of $V(\mathfrak{b})$. Then $g(x_1, x_2, \ldots, x_n) = 0$ for all $g \in \mathfrak{a}$, and therefore $(x_1, x_2, \ldots, x_n) \in V(\mathfrak{a})$. But the polynomial f has the value zero at each point of $V(\mathfrak{a})$. It follows that the polynomial $1 - fY$ has the value 1 at each point of $V(\mathfrak{b})$, and therefore

$$V(\mathfrak{c}) = V(\mathfrak{b}) \cap V(1 - fY) = \emptyset.$$

It now follows immediately from the Weak Nullstellensatz (Theorem 4.44) that $\mathfrak{c}$ cannot be a proper ideal of S, and therefore $1 \in \mathfrak{c}$. Thus there exists a polynomial h belonging to the ideal $\mathfrak{b}$ of S such that $h - 1 \in (1 - fY)$. Moreover this polynomial h is of the form

$$h(X_1, X_2, \ldots, X_n, Y) = \sum_{j=0}^{r} g_j(X_1, X_2, \ldots, X_n) Y^j,$$

where $g_1, g_2, \ldots, g_n \in \mathfrak{a}$.

Let $g \in \mathfrak{a}$ be defined by $g = \sum_{j=0}^{r} g_j f^{r-j}$. Now $g - f^r = g - f^r h + f^r(h-1)$. Also

$$g - f^r h = \sum_{j=0}^{r} g_j f^{r-j}(1 - f^j Y^j) \in (1 - fY),$$

since the polynomial $1 - f^j Y^j$ is divisible by the polynomial $1 - fY$ for all positive integers j. It follows that $g - f^r \in (1 - fY)$. But the polynomial $g - f^r$ is a polynomial in the indeterminates $X_1, X_2, \ldots, X_n$, and, if non-zero, would be of degree zero when considered as a polynomial in the indeterminate Y with coefficients in the ring R. Also any non-zero element of the ideal $(1 - fY)$ of S is divisible by the polynomial $1 - fY$, and is therefore of strictly positive degree when considered as a polynomial in the indeterminate Y with coefficients in R. We conclude, therefore that $g - f^r = 0$. But $g \in \mathfrak{a}$. Therefore $f^r \in \mathfrak{a}$, as required. ∎