Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 2
Hilary Term 2014

D. R. Wilkins

Contents

2 Integral Domains **12**

2.1 Factorization in Integral Domains 12
2.2 Euclidean Domains 14
2.3 Principal Ideal Domains 16
2.4 Fermat's Two Squares Theorem 17
2.5 Maximal Ideals and Prime Ideals 20
2.6 Unique Factorization Domains 23
2.7 Prime Ideals of Principal Ideal Domains 25
2.8 An Integral Domain lacking Unique Factorization 26
2.9 Rings of Polynomials with Coefficients in a Unique Factorization Domain 30
2.10 Polynomial Rings in Several Indeterminates 36
2.11 Rings of Fractions 39
2.12 Integrally Closed Domains 46
2.13 Irreducibility of Polynomials over Fields of Fractions 47
2.14 Requirements for Unique Factorization Of Ideals 47

2 Integral Domains

2.1 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 2.1 *Let x, y and z be elements of an integral domain R. Suppose that $x \neq 0_R$ and $xy = xz$. Then $y = z$.*

Proof Suppose that these elements x, y and z satisfy $xy = xz$. Then $x(y - z) = 0_R$. 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 $x \neq 0_R$ and $x(y - z) = 0_R$ then $y - z = 0_R$. 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.

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 2.2 *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 $x = 0_R$ or $y = 0_R$ 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 $x(uv-1) = 0_R$. But then $uv = 1$, since $x \neq 0_R$ 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 2.3 *Elements x and y of an integral domain R are associates if and only if $(x) = (y)$.*

Proof This follows directly from Lemma 2.2. ∎

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.

Note that if x is an irreducible element of an integral domain R and if u is a unit of R then ux is also an irreducible element of R. Indeed suppose that $ux = yz$ where y and z are elements of R. There exists some element v of R such that $uv = 1_R$. Then Then $x = (vy)z$. Because x is irreducible, one or other of the elements vy and z must be a unit of R. It follows that one of the elements y and z must be a unit of R, and the other must therefore be an associate of ux. Thus ux is an irreducible element of R. We conclude that any associate of an irreducible element of an integral domain must itself be an irreducible element of that integral domain.

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 2.4 *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 2.2 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. ∎

Proposition 2.5 *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. ∎

2.2 Euclidean Domains

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

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

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

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

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

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

Example Let K be a field, and let $K[x]$ be the ring of polynomials in a single indeterminate x with coefficients in the field K. The degree $\deg p$ of each non-zero polynomial p is a non-negative integer. If p and q are non-zero polynomials in $K[x]$, and if p divides q, then $\deg p \leq \deg q$. Also, given any non-zero polynomials m and p in $K[x]$ there exist polynomials $q, r \in K[x]$ such that $p = qm + r$ and either $r = 0_K$ 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 2.6 *Every ideal of a Euclidean domain is a principal ideal.*

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

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

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

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 $r = 0_R$ 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 $r = 0_R$. 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. ∎

2.3 Principal Ideal Domains

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

It follows directly from Proposition 2.6 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.

Let $x_1, x_2, \ldots, x_k$ be elements of a unital commutative ring R. Then the ideal $(x_1, x_2, \ldots, x_k)$ generated by $x_1, x_2, \ldots, x_k$ is the smallest ideal of R

that contains the set $\{x_1, x_2, \ldots, x_k\}$, and consists of all elements of R that can be represented in the form $a_1x_1 + a_2x_2 + \cdots + a_kx_k$ for some elements $a_1, a_2, \ldots, a_k$ of R.

Lemma 2.7 *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 2.8 *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 2.7). 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 2.9 *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 2.4). 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 2.7). But then $z = apz + byz$, and hence p divides z. Thus p is prime, as required. ∎

2.4 Fermat's Two Squares Theorem

We shall use the fact that the ring of Gaussian integers is a principal ideal domain to prove a theorem, originally claimed by Fermat, that states that

an odd prime number p can be represented in the form $p = x^2 + y^2$ for some integers x and y if and only if $p \equiv 1 \pmod 4$. We make use of the following theorem, claimed and used by Ibn al-Haytham some time around the year 1000, and subsequently stated by Leibniz and by John Wilson, and proved by Lagrange in 1771.

Theorem 2.10 (Wilson's Theorem) $(p-1)!+1$ *is divisible by* p *for all prime numbers* p.

Proof Let p be a prime number. If x is an integer satisfying $x^2 \equiv 1 \pmod p$ then p divides $(x-1)(x+1)$ and hence either p divides either $x-1$ or $x+1$. Thus if $1 \leq x \leq p-1$ and $x^2 \equiv 1 \pmod p$ then either $x = 1$ or $x = p-1$.

For each integer x satisfying $2 \leq x \leq p-2$, there exists exactly one integer y satisfying $2 \leq y \leq p-2$ such that $xy \equiv 1 \pmod p$, and moreover $y \neq x$. It follows that $(p-2)!$ is a product of numbers of the form xy, where x and y are distinct integers between 2 and $p-2$ that satisfy $xy \equiv 1 \pmod p$. It follows that $(p-2)! \equiv 1 \pmod p$. But then $(p-1)! \equiv p-1 \pmod p$, and hence $(p-1)!+1$ is divisible by p, as required. ∎

Corollary 2.11 *Let* p *be an odd prime number, and let* $m = \frac{1}{2}(p-1)$. *Then* $(m!)^2 + (-1)^m$ *is divisible by* p.

Proof The factorial $(p-1)!$ is the product of the integers $k(p-k)$ for $k = 1, 2, \ldots, m$. Moreover $k(p-k) \equiv -k^2 \pmod p$ for $k = 1, 2, \ldots, m$. Therefore

$$(p-1)! = \prod_{k=1}^{m} k(p-k) \equiv \prod_{k=1}^{m} (-k^2) = (-1)^m (m!)^2 \pmod p.$$

Thus

$$(m!)^2 + (-1)^m \equiv (-1)^m ((p-1)! + 1) \pmod p.$$

It follows from Wilson's Theorem (Theorem 2.10) that $(m!)^2 + (-1)^m$ is divisible by p, as required. ∎

We now prove Fermat's Two Squares Theorem using a method based on properties of the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers published by Richard Dedekind in 1894.

Theorem 2.12 (Fermat's Two Squares Theorem) *Let* p *be an odd prime number. Then there exist integers* x *and* y *such that* $p = x^2 + y^2$ *if and only if* $p \equiv 1 \pmod 4$.

Proof If x is an even integer then $x^2 \equiv 0 \pmod 4$. If x is an odd integer then $x^2 \equiv 1 \pmod 4$. It follows that if x and y are integers, and if $x^2 + y^2$ is an odd integer then $x^2 + y^2 \equiv 1 \pmod 4$. (It is not possible to represent an integer congruent to 3 modulo 4 as a sum of two squares.) Thus only odd primes p satisfying $p \equiv 1 \pmod 4$ can be represented as the sum of two squares.

Now let p be an odd prime satisfying $p \equiv 1 \pmod 4$, and let $m = \frac{1}{2}(p-1)$. Then m is an even integer. It follows from Corollary 2.11 that p divides $(m!)^2 + 1$.

We now consider the nature of the prime number p, considered as an element of the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers, where

$$\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} : x, y \in \mathbb{Z}\}.$$

Now $(m!)^2 + 1$ factorizes as the product

$$(m!)^2 + 1 = (m! + \sqrt{-1})(m! - \sqrt{-1})$$

of Gaussian integers $m! + \sqrt{-1}$ and $m! - \sqrt{-1}$. But neither $m! + \sqrt{-1}$ nor $m! - \sqrt{-1}$ is divisible by the prime number p in the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers, despite the fact that p divides the product of these two Gaussian integers. It follows that if the prime number p satisfies $p \equiv 1 \pmod 4$ then p is not a prime element of the ring $\mathbb{Z}[\sqrt{-1}]$. But $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain, and is thus a principal ideal domain (Proposition 2.6), and therefore every irreducible element of $\mathbb{Z}[\sqrt{-1}]$ is prime (Theorem 2.9). Because p is not a prime element of $\mathbb{Z}[\sqrt{-1}]$, it cannot be an irreducible element of $\mathbb{Z}[\sqrt{-1}]$, and therefore there must exist Gaussian integers $\omega, \theta \in \mathbb{Z}[\sqrt{-1}]$ such that $p = \omega\theta$, where neither ω nor θ is a unit of $\mathbb{Z}[\sqrt{-1}]$. Now the norm $x^2 + y^2$ of any non-zero Gaussian integer $x + y\sqrt{-1}$ is a positive integer, and has the value one if and only if $x + y\sqrt{-1}$ is a unit of $\mathbb{Z}[\sqrt{-1}]$. It follows that $|\omega|^2$ and $|\theta|^2$ are positive integers satisfying $|\omega|^2 > 1$ and $|\theta|^2 > 1$. But $|\omega|^2|\theta|^2 = p^2$, and the only factors of p^2 are 1, p and p^2. It follows that $|\omega|^2 = |\theta|^2 = p$. Let $\omega = x + y\sqrt{-1}$. Then $p = |\omega|^2 = x^2 + y^2$. Thus a prime number p satisfying $p \equiv 1 \pmod 4$ can be represented in the form $p = x^2 + y^2$ for some integers x and y, as required. ∎

Remark The above proof of Fermat's Two Squares theorem uses the fact that if p is a prime number satisfying $p \equiv 1 \pmod 4$ then there exists an integer w satisfying the congruence $w^2 \equiv -1 \pmod p$. The existence of such an integer shows that the number -1 is a *quadratic residue* of p when $p \equiv 1 \pmod 4$, and can be proved in various ways. One of these ways involves the use of Wilson's Theorem, as explained above, to show that if $p \equiv 1 \pmod 4$ then $-1 \equiv (m!)^2 \pmod p$, where $m = (p-1)/2$.

An integer z is said to be a *quadratic residue* of a prime number p if there exists some integer w such that $z \equiv w^2 \pmod{p}$. Now the non-zero elements of any field constitute a group under multiplication, and every finite subgroup of the group of non-zero elements of a field is cyclic.

This result can be applied to the field of congruence classes of integers modulo p to deduce that, given any prime number p, there exists some integer g whose congruence class generates the group of non-zero elements of this field. Then, given any integer z coprime to p, there exists some integer k such that $z \equiv g^k \pmod{p}$. Such an integer g is said to be a *primitive root* of p.

In the case where $p \neq 2$ the group of congruence classes modulo p of integers coprime to p is of even order and it follows from this that an integer z is a quadratic residue of p if and only if $z \equiv g^k \pmod{p}$ for some even integer k, where g is some primitive root of p, and this is the case if and only if $z^{(p-1)/2} \equiv 1 \pmod{p}$. In particular, -1 is a quadratic residue of p if and only if $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. It follows that -1 is a quadratic residue of an odd prime p if and only if $p \equiv 1 \pmod{4}$.

2.5 Maximal Ideals and Prime Ideals

Definition Let R be a unital commutative ring. An ideal M of R is said to be *maximal* if it is a proper ideal of R and if the only ideals I satisfying $M \subset I \subset R$ are the maximal ideal M and the ring R itself.

Lemma 2.13 *An ideal M of a unital commutative ring R is a maximal ideal of R if and only if the quotient ring R/M is a field.*

Proof The preimage $\nu^{-1}(J)$ of any ideal of R/M under the quotient homomorphism $\nu: R \to R/M$ is an ideal of R satisfying $M \subset \nu^{-1}(J) \subset R$. Also each ideal I of R satisfying $M \subset I \subset R$ determines an ideal I/M of R/M satisfying $\nu^{-1}(I/M) = I$, and moreover an ideal J of R/M satisfies $J = I/M$ if and only if $\nu{-}1(J) = I$. Thus the ideals I of R that satisfy $M \subset I \subset R$ are in one-to-one correspondence with the ideals of the quotient ring R/M. It follows that an ideal M of R is maximal if and only if the only ideals of the quotient ring R/M are the zero ideal and the whole of the quotient ring. The quotient R/M of a unital commutative ring R by a proper ideal M is a commutative ring with a non-zero multiplicative identity element $M + 1_R$. But a unital commutative ring is a field if and only if the only ideals of that ring are the zero ideal and the ring itself. (Lemma 1.4). It follows that an ideal M of a unital commutative ring R is a maximal ideal of R if and only if the corresponding quotient ring R/M is a field. ∎

Definition Let R be a unital commutative ring. An ideal P of R is said to be *prime* if P is a proper ideal of R and, for all elements x and y of R satisfying $xy \in P$, either $x \in P$ or $y \in P$.

Lemma 2.14 *An ideal P of a unital commutative ring R is a prime ideal of R if and only if the quotient ring R/P is an integral domain.*

Proof Let P be an ideal of R. Then P is prime if and only if P is a proper ideal of R and, given elements x and y that do not belong to the ideal P, the product xy of those elements does not belong to P. Now an element x of R belongs to an ideal P if and only if the image $x + P$ of x under the quotient homomorphism is the zero element of R/P. It follows that the ideal P of R is prime if and only if R/P is a commutative ring with a non-zero multiplicative identity element $P + 1_R$ in which the product of any two non-zero elements of the quotient ring R/P is always a non-zero element of that quotient ring. It then follows from the definition of integral domains that an ideal P of a unital commutative ring R is prime if and only if R/P is an integral domain. ∎

Lemma 2.15 *Every maximal ideal of a unital commutative ring R is a prime ideal of R.*

Proof Every field is an integral domain. The result therefore follows immediately from Lemma 2.13 and Lemma 2.14. ∎

Lemma 2.16 *The zero ideal $\{0_R\}$ of a unital commutative ring R is a prime ideal of R if and only if R is an integral domain.*

Proof The zero ideal of a unital commutative ring R is a proper ideal of R. It is therefore prime if and only if the product of non-zero elements of R is always non-zero, and thus is prime if and only if R is an integral domain. ∎

Lemma 2.17 *An integral domain with only finitely many elements is a field.*

Proof Let R be an integral domain with only finitely many elements, and let x be a non-zero element of R. Then x determines an injective function $\lambda_x : R \to R$ from R to itself, where $\lambda_x(y) = xy$ for all $y \in R$. This injective function must be surjective, because R is a finite set. Therefore there exists some element y of R such that $\lambda_x(y) = 1_R$, where 1_R is the multiplicative identity element of R. Then $xy = 1_R$. This proves that every non-zero element of the integral domain R is a unit of R, and therefore R is a field. ∎

Lemma 2.18 *Let R be a unital commutative ring, and let P be a prime ideal of R. Suppose that the number of cosets of P in R is finite. Then P is a maximal ideal of R.*

Proof The quotient ring R/P is an integral domain, because the ideal P is prime (Lemma 2.14). This integral domain has only finitely many elements because those elements are the cosets of P in R. Therefore R/P is a field (Lemma 2.17), and thus the prime ideal P is a maximal ideal (Lemma 2.13).

Lemma 2.19 *Let x be an element of an integral domain R. Then x is a prime element of R if and only if the principal ideal (x) generated by x is a non-zero prime ideal of R.*

Proof Let x be a prime element of R. Then x is non-zero and is not a unit of R. It follows that (x) is a non-zero proper ideal of R. Let y and z be elements of R satisfying $yz \in (x)$. Then $x|yz$. Therefore either $x|y$ or $x|z$, because x is a prime element of R, and thus either $y \in (x)$ or $z \in (x)$. Thus the principal ideal (x) is a non-zero prime ideal of R.

Conversely let x be an element of R for which the corresponding principal ideal (x) is a non-zero prime ideal of R. Then $x \neq 0_R$. Also (x) is a proper ideal of R, because the definition of prime ideals requires such ideals to be proper ideals of R, and therefore x is not a unit of R. Let y and z be elements of R. Then $yz \in (x)$ if and only if either $y \in (x)$ or $z \in (x)$. It follows that $x|yz$ if and only if either $x|y$ or $x|z$. Therefore x is a prime element of R. ∎

Definition Let $I_1, I_2, \ldots, I_k$ be ideals of a unital commutative ring R. The *product* $I_1 I_2 \cdots I_k$ of the ideals $I_1, I_2, \ldots, I_k$ is the ideal of R generated by all products of the form $x_1 x_2 \cdots x_k$ where $x_i \in I_i$ for $i = 1, 2, \ldots, k$.

It follows from the definition of the product of ideals that any element of the product IJ of ideals I and J of a unital commutative ring R can be represented as a sum of the form

$$y_1 z_1 + y_2 z_2 + \cdots + y_m z_m,$$

where $y_j \in I$ and $z_j \in J$ for $j = 1, 2, \ldots, m$. Indeed all elements of R representable in this form must belong to the ideal generated by the set

$$\{yz : y \in J \text{ and } z \in K\}.$$

But the set of elements of R representable as a sum of the above form is itself an ideal of R and is thus the ideal generated by the set of all products yz with $y \in I$ and $z \in J$.

More generally, given ideals $I_1, I_2, \ldots, I_k$ of a unital commutative ring R, the product $I_1 I_2 \cdots I_k$ of those ideals consists of those elements of R that can be represented as sums of products belonging to the set

$$\{x_1 x_2 \cdots x_k : x_i \in I_i \text{ for } i = 1, 2, \ldots, k\}.$$

Lemma 2.20 *A proper ideal P of a unital commutative ring R is prime if and only if, given any ideals I and J of R satisfying $IJ \subset P$, either $I \subset P$ or $J \subset P$.*

Proof Let P be a prime ideal of R. If $I \not\subset P$ and $J \not\subset P$ then there exist elements $y \in I$ and $z \in J$ such that $y \notin P$ and $z \notin P$. Then $yz \notin P$, because the ideal P is prime. But $yz \in IJ$. It follows that $IJ \not\subset P$.

Thus if P is a prime ideal of a unital commutative ring R, and if I and J are ideals of R satisfying $IJ \subset P$, then either $I \subset P$ or $J \subset P$.

Conversely, suppose that P is a proper ideal of R, and that, for all ideals I and J of R satisfying $IJ \subset P$, either $I \subset P$ or $J \subset P$. Let x and y be elements of R satisfying $xy \in P$. Then $(x)(y) = (xy)$, and therefore $(x)(y) \subset P$. It follows that either $(x) \subset P$, in which case $x \in P$, or else $(y) \subset P$, in which case $y \in P$. This proves that the ideal P is prime. The result follows. ∎

2.6 Unique Factorization Domains

The Fundamental Theorem of Arithmetic states that every integer greater than one can be factored uniquely as a product of one or more prime numbers. We now introduce a class of integral domains that possess a unique factorization property that generalizes in an appropriate fashion the Fundamental Theorem of Arithmetic.

The following proposition guarantees that any factorization of an element of a principal ideal domain as the product of one or more *prime* elements of that domain is unique up to the order of the factors and the replacement of any factor by an associate of that factor.

Proposition 2.21 *Let R be an integral domain, and let x be a 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 $p_1, p_2, \ldots, p_k$ are prime elements of R and $q_1, q_2, \ldots, q_l$ are irreducible elements of R. Then $l = k$, and there exists some permutation σ of the set $\{1, 2, \ldots, k\}$ such that q_i and $p_{\sigma(i)}$ are associates for $i = 1, 2, \ldots, k$.

Proof The result holds when $k = 1$, because every prime element of R is irreducible, and therefore cannot be factored as a product of two or more irreducible elements.

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 $p_1, p_2, \ldots, p_k$ are prime elements of R and $q_1, q_2, \ldots, q_l$ are irreducible 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 irreducible 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 $p_1 \neq 0_R$, and therefore $p_2 p_3 \cdots p_k = (u q_2) q_3 \cdots q_l$. (see Lemma 2.1). Moreover $u q_2$ is an irreducible 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 $p_1 p_2 \cdots p_k$. ∎

Definition An integral domain R is said to be a *unique factorization domain* if every non-zero element of R that is not a unit of R can be factored as the product of one or more prime elements of R.

Lemma 2.22 *An integral domain R is a unique factorization domain if and only if it has the following two properties:*

(i) *any non-zero element of R that is not a unit of R can be factored as the product of one or more irreducible elements of R;*

(ii) *every irreducible element of R is a prime element of R.*

Proof It follows directly from the definition of unique factorization domains given above that every integral domain with these two properties is a unique factorization domain. Also every prime element of an integral domain is irreducible (Lemma 2.4), and therefore every unique factorization domain

satisfies the first of these two properties. Moreover an irreducible element of a unique factorization domain R must factor as a product of one or more prime elements of R. But, being irreducible, it can only have one prime factor, and therefore it must itself be prime. Thus every unique factorization domain satisfies property (ii). ∎

Lemma 2.23 *Every principal ideal domain is a unique factorization domain.*

Proof Every ideal of a principal ideal domain can be generated by a single element of the domain, and is thus finitely generated. A direct application of Proposition 2.5 therefore 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 2.9 guarantees that every irreducible element of a principal ideal domain is prime. The result therefore follows from Lemma 2.22. ∎

2.7 Prime Ideals of Principal Ideal Domains

Lemma 2.24 *Let R be a principal ideal domain. Then every non-zero prime ideal of R is a maximal ideal of R. Moreover every non-zero prime ideal of R is a principal ideal generated by some prime element of R.*

Proof Let P be a non-zero prime ideal of R. Then there exists some non-zero element x of R such that $P = (x)$. The ideal (x) is a non-zero proper ideal of R. It follows from Lemma 2.19 that x is a prime element of R. Then x is an irreducible element of R, because all prime elements of a principal ideal domain are irreducible. Let I be an ideal of R satisfying $(x) \subset I \subset R$. Then $I = (y)$ for some element y of R. But then $(x) \subset (y)$, and therefore $y|x$. It follows from the irreducibility of x that either y is a unit, in which case $I = R$, or y is an associate of x, in which case $I = (x)$. Therefore the ideal (x) is a maximal ideal of R, as required. ∎

Remark Let R be a principal ideal domain, and let x be a prime element of R. The ideal (x) generated by x is then a non-zero prime ideal of R. It follows from Lemma 2.24 that the ideal (x) generated by x is a maximal ideal of R. It then follows from Lemma 2.13 that the quotient ring $R/(x)$ is a field. These results therefore combine to provide an alternative proof of Lemma 2.8.

Lemma 2.25 *Let R be a principal ideal domain. Then every non-zero proper ideal I of R factors as a product*

$$I = P_1 P_2 \cdots P_k$$

where $P_1, P_2, \ldots, P_k$ are non-zero prime ideals of R. Moreover this factorization of I as a product of prime ideals is unique: if

$$P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_l,$$

where $P_1, P_2, \ldots, P_k$ and $Q_1, Q_2, \ldots, Q_l$ are prime ideals of R, then $k = l$, and there exists some permutation σ of the set $\{1, 2, \ldots, k\}$ such that $Q_i = P_{\sigma(i)}$ for $i = 1, 2, \ldots, k$.

Proof Let I be a non-zero proper ideal of R. Then there exists some non-zero element x of R such that $I = (x)$. Moreover x is not a unit of R. The principal ideal domain R is a unique factorization domain (Lemma 2.23). Therefore there exist prime elements $p_1, p_2, \ldots, p_k$ such that $x = p_1 p_2 \cdots p_k$. Let $P_i = (p_i)$ for $i = 1, 2, \ldots, k$. Then each ideal P_i is a non-zero prime ideal of R, and $I = P_1 P_2 \cdots P_k$.

Two prime elements of R generate the same prime ideal of R if and only if they are associates. The uniqueness of the factorization of I as a product of prime ideals therefore follows directly from Proposition 2.21. ∎

2.8 An Integral Domain lacking Unique Factorization

The integral domain $\mathbb{Z}[\sqrt{-5}]$ consists of all all complex numbers that are of the form $x + y\sqrt{-5}$ for some integers x and y. We define the *norm* $N(x + y\sqrt{-5})$ of an element $x + y\sqrt{-5}$ of $\mathbb{Z}[\sqrt{-5}]$ to be $x^2 + 5y^2$. The norm $N(\omega)$ of an element ω of $\mathbb{Z}[\sqrt{-5}]$ is thus a non-negative integer. Moreover

$$\begin{aligned} N((x + y\sqrt{-5})(u + v\sqrt{-5})) &= N(xu - 5yv + (xv + yu)\sqrt{-5}) \\ &= (xu - 5yv)^2 + 5(xv + yu)^2 \\ &= x^2u^2 + 25y^2v^2 + 5x^2v^2 + 5y^2u^2 \\ &= (x^2 + 5y^2)(u^2 + 5v^2) \\ &= N(x + y\sqrt{-5})N(u + v\sqrt{-5}) \end{aligned}$$

for all integers x, y, u and v. Thus $N(\omega\theta) = N(\omega)N(\theta)$ for all $\omega, \theta \in \mathbb{Z}[\sqrt{-5}]$.

If ω is a unit of the integral domain $\mathbb{Z}[\sqrt{-5}]$ then $\omega^{-1} \in \mathbb{Z}[\sqrt{-5}]$, and therefore $N(\omega)$ and $N(\omega^{-1})$ are both positive integers satisfying

$$N(\omega)N(\omega^{-1}) = N(1) = 1.$$

It follows that if ω is a unit of $\mathbb{Z}[\sqrt{-5}]$ then $N(\omega) = 1$. From this it follows that the only units of $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1.

Now

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

where the factors 2, 3 and $1 \pm \sqrt{-5}$ are all elements of $\mathbb{Z}[\sqrt{-5}]$. Now $N(2) = 4$. Now there is no element ω of $\mathbb{Z}[\sqrt{-5}]$ that satisfies $N(\omega) = 2$ or $N(\omega) = 3$. Thus if ω and θ are elements of $\mathbb{Z}[\sqrt{-5}]$ satisfying $\omega\theta = 2$ then $N(\omega)N(\theta) = 4$, and therefore either $N(\omega) = 1$, in which case ω is a unit of $\mathbb{Z}[\sqrt{-5}]$, or else $N(\theta) = 1$, in which case θ is a unit of $\mathbb{Z}[\sqrt{-5}]$. It follows that the integer 2 is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$. Analogous arguments show that 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$.

The irreducible elements 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ of $\mathbb{Z}[\sqrt{-5}]$ are not prime elements of $\mathbb{Z}[\sqrt{-5}]$. Indeed 2 and 3 divide the product of $1+\sqrt{-5}$ and $1 - \sqrt{-5}$, but do not divide either factor of this product. Similarly $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ divide the product of 2 and 3 but do not divide either 2 or 3. The principal ideals generated by these elements are neither prime nor maximal.

Let a, b, c and d be integers. Then

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac - 5bd + (ad + bc)\sqrt{-5}.$$

If $a \equiv b \pmod 2$ then $ac - 5bd \equiv a(c + d) \pmod 2$ and $ad + bc \equiv a(c + d) \pmod 2$. It follows that $ac - 5bd \equiv ad + bc \pmod 2$ whenever $a \equiv b \pmod 2$. Thus if

$$P_1 = \{x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] : x \equiv y \pmod 2\}$$

then P_1 is an ideal of $\mathbb{Z}[\sqrt{-5}]$. This ideal contains the elements 2, $1+\sqrt{-5}$ and $1-\sqrt{-5}$. Given any element $x+y\sqrt{-5}$ of P_1 there exists $u+v\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that $x + y\sqrt{-5} - 2(u + v\sqrt{-5}) \in \{0, 1 + \sqrt{-5}\}$. It follows that

$$P_1 = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}).$$

The ideal P_1 is not a principal ideal of $\mathbb{Z}[\sqrt{-5}]$ because there is no element of $\mathbb{Z}[\sqrt{-5}]$ that is not a unit but divides both 2 and $1 + \sqrt{-5}$. The quotient ring $\mathbb{Z}[\sqrt{-5}]/P_1$ is a finite field of order 2, and therefore the ideal P_1 is a maximal ideal of $\mathbb{Z}[\sqrt{-5}]$. The ideal P_1^2 is generated by products $\alpha\beta$ where α and β run over a set $\{2, 1 + \sqrt{-5}\}$ of generators of the ideal P_1. Moreover $(1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5}$. Therefore P_1^2 is the ideal of $\mathbb{Z}[\sqrt{-5}]$ generated by 4, $2(1+\sqrt{-5})$ and $-4+2\sqrt{-5}$. Now the generators of P_1^2 are all divisible in $\mathbb{Z}[\sqrt{-5}]$ by 2, and moreover

$$2 = 2(1 + \sqrt{-5}) - (-4 + 2\sqrt{-5}) - 4 \in P_1^2.$$

It follows from this that $P_1^2 = (2)$.

If a, b, c and d are integers, and if $a \equiv b \pmod 3$ then

$$ac - 5bd \equiv a(c+d) \equiv ad + bc \pmod 3.$$

Similarly if $a \equiv -b \pmod 3$ then

$$ac - 5bd \equiv a(c-d) \equiv -(ad+bc) \pmod 3.$$

It follows that P_2 and P_3 are ideals of $\mathbb{Z}[\sqrt{-5}]$, where

$$\begin{aligned} P_2 &= \{x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] : x \equiv y \pmod 3\}, \\ P_3 &= \{x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] : x \equiv -y \pmod 3\}. \end{aligned}$$

These ideals are maximal ideals of $\mathbb{Z}[\sqrt{-5}]$, and the quotient rings $\mathbb{Z}[\sqrt{-5}]/P_2$ and $\mathbb{Z}[\sqrt{-5}]/P_3$ are finite fields of order 3. Moreover

$$P_2 = (3, 1 + \sqrt{-5}) \quad \text{and} \quad P_3 = (3, 1 - \sqrt{-5}).$$

The ideal P_2 of $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal, because there is no element of $\mathbb{Z}[\sqrt{-5}]$ that is not a unit but that divides both 3 and $1+\sqrt{-5}$. Similarly the ideal P_3 is not a principal ideal. The product P_2P_3 of the ideals P_2 and P_3 is generated by products of the form $\alpha\beta$, where α runs over a set $\{3, 1+\sqrt{-5}\}$ of generators for P_2 and β runs over a set $\{3, 1-\sqrt{-5}\}$ of generators for P_3. Moreover $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$. It follows that P_2P_3 is generated by 9, $3(1+\sqrt{-5})$, $3(1-\sqrt{-5})$ and 6. Therefore $3 \in P_2P_3$, because $3 = 9 - 6$, and thus $P_2P_3 = (3)$.

Next we note that the ideal P_1P_2 is generated by 6, $2(1+\sqrt{-5})$, $3(1+\sqrt{-5})$ and $(1+\sqrt{-5})^2$. It follows that $1 + \sqrt{-5} \in P_1P_2$, because

$$1 + \sqrt{-5} = 3(1 + \sqrt{-5}) - 2(1 + \sqrt{-5}).$$

Moreover $1 + \sqrt{-5}$ divides all the listed generators of P_1P_2. It follows that P_1P_2 is the principal ideal $(1 + \sqrt{-5})$ generated by $1 + \sqrt{-5}$. Similarly $P_1P_3 = (1 - \sqrt{-5})$.

We have shown that $P_1^2 = (2)$ and $P_2P_3 = (3)$. It follows that the principal ideal (6) factors as a product $(6) = P_1^2P_2P_3$, where P_1, P_2 and P_3 are prime ideals.

This factorization of (6) as a product of prime ideals of $\mathbb{Z}[\sqrt{-5}]$ is in fact unique. To show this, we first note that every non-zero prime ideal of $\mathbb{Z}[\sqrt{-5}]$ is maximal.

Let $R = \mathbb{Z}[\sqrt{-5}]$, let P be a non-zero prime ideal of R, and let $u + v\sqrt{-5}$ be an element of P. Then $m \in P$, where

$$m = N(u + v\sqrt{-5}) = u^2 + 5v^2 = (u + v\sqrt{-5})(u - v\sqrt{-5}).$$

Now if $a+b\sqrt{-5}$ and $c+d\sqrt{-5}$ and if $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$ then $a+b\sqrt{-5}+(m) = c+d\sqrt{-5}+(m)$, and therefore $a+b\sqrt{-5}+P = c+d\sqrt{-5}+P$. It follows that the number of cosets of P in R cannot exceed m^2. But a prime ideal of R that has only finitely many cosets in R must be a maximal ideal of R (Lemma 2.18). (This is a consequence of the fact that an integral domain with only finitely many elements is a field.) Thus every non-zero prime ideal of R is maximal.

It follows that if P and Q are non-zero prime ideals of R, and if $Q \subset P$, then $Q = P$.

We can now prove the uniqueness of the factorization of the principal ideal (6) as a product $P_1^2P_2P_3$ of prime ideals, where P_1, P_2 and P_3 are defined as described above. Suppose that

$$(6) = P_1^2P_2P_3 = Q_1Q_2\cdots Q_l.$$

Then $Q_1Q_2\cdots Q_l \subset P_1$. It follows from repeated applications of Lemma 2.20 that at least one of the prime ideals $Q_1, Q_2, \ldots, Q_k$ is contained in the prime ideal P_1. We reorder $Q_1, Q_2, \ldots, Q_l$, if necessary, so that $Q_1 \subset P_1$. Then $Q_1 = P_1$, and thus $P_1^2P_2P_3 = P_1Q_2Q_3\cdots Q_l$. If we then multiply both sides of this identity by the ideal P_1, we find that

$$(2)P_1P_2P_3 = P_1^3P_2P_3 = P_1^2Q_2Q_3\cdots Q_l = (2)Q_2Q_3\cdots Q_l.$$

But the ideals $(2)P_1P_2P_3$ and $(2)Q_2Q_3\cdots Q_l$ are the images of the ideals $P_1P_2P_3$ and $Q_2Q_3\cdots Q_l$ under the injective function from R to itself that multiplies all elements of R by 2. It therefore follows that $P_1P_2P_3 = Q_2Q_3\cdots Q_l$. We now note that at least one of the ideals $Q_2, Q_3, \ldots, Q_l$ must be contained in the ideal P_1. We can therefore reorder these ideals, if necessary, to ensure that $Q_2 \subset P_1$. Then $Q_2 = P_1$. If we then multiply both sides of the identiy by P_1, we find that

$$(2)P_2P_3 = P_1^2P_2P_3 = P_1^2Q_3Q_4\cdots Q_l = (2)Q_3Q_4\cdots Q_l.$$

It follows that $P_2P_3 = Q_3Q_4\cdots Q_l$. Repetition of the argument shows that at least one of the ideals $Q_3Q_4\cdots Q_l$ is in P_2. We may suppose that $Q_3 \subset P_2$. Then $Q_3 = P_2$, and thus $P_2P_3 = P_2Q_4\cdots Q_l$. If we then multiply both sides of this identity by the ideal P_3, we find that

$$(3)P_3 = P_3P_2P_3 = P_3P_2Q_3\cdots Q_l = (3)Q_4\cdots Q_l.$$

It follows that $P_3 = Q_4\cdots Q_l$. Then at least one of the ideals $Q_4, \ldots, Q_l$ must be contained in P_3. We may suppose that $Q_4 \subset P_3$, and therefore $Q_4 = P_3$. It cannot be the case that $l > 4$, because multiplying both sides

of the identity $P_3 = P_3 Q_5 \cdots Q_l$ by the ideal P_2 would lead to the identity $(3) = (3)Q_5 \cdots Q_l$, from which it would follow that the product of $Q_5 \cdots Q_l$ would be the whole of the ring R, which is impossible. Therefore $l = 4$, and we have shown that Q_1, Q_2, Q_3, Q_4 can be ordered so that $Q_1 = Q_2 = P_1$, $Q_3 = P_2$ and $Q_4 = P_3$. This proves that the factorization of the principal ideal (6) as $(6) = P_1^2 P_2 P_3$ is unique, subject only to reordering of the factors.

The integral domain $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. We have shown that the element 6 of the domain cannot be factorized as a product of prime elements of the domain. Nevertheless the corresponding principal ideal (6) can be factorized uniquely as a product of prime ideals. In fact, every non-zero ideal of $\mathbb{Z}[\sqrt{-5}]$ can be factorized uniquely as a product of prime ideals. The same is true of many analogous integral domains that arise in algebraic number theory.

An *algebraic number field* is a subfield of the complex numbers that is a finite-dimensional vector space over the field of rational numbers. A complex number is said to be an *algebraic integer* if it is the root of a monic polynomial with integer coefficients. The set of algebraic integers contained within any algebraic number field constitute an integral domain embedded within that number field. A significant theorem of algebraic number theory, due to Richard Dedekind, guarantees that every non-zero proper ideal of the ring of algebraic integers in any algebraic number field can be factored uniquely as a product of prime ideals of that ring.

The integral domain $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of the algebraic number field $\mathbb{Q}(\sqrt{-5})$ that consists of all complex numbers that are of the form $a + b\sqrt{-5}$ for some rational numbers a and b. Therefore every non-zero ideal of this domain must factorize uniquely as a product of prime ideals.

2.9 Rings of Polynomials with Coefficients in a Unique Factorization Domain

Let R be a unique factorization domain. We shall prove that the ring $R[x]$ of polynomials with coefficients in R is also a unique factorization domain.

We say that a polynomial $f(x)$ with coefficients in the unique factorization domain R is *primitive* if the only elements of R that divide all the coefficients of $f(x)$ are the units of R. Any non-zero element of R that is not a unit of R can be factored as a product of one or more prime elements of R, and is thus divisible by some prime element of R. It follows that a polynomial $f(x)$ with coefficients in R is primitive if and only if there is no prime element of R that divides all the coefficients of $f(x)$.

Lemma 2.26 *Let R be a unique factorization domain, and let $f(x)$ be a non-zero polynomial with coefficients in R. Then there exists a non-zero element c of R and a primitive polynomial $\hat{f}(x)$ with coefficients in R such that $f(x) = c\hat{f}(x)$.*

Proof If the polynomial $f(x)$ is itself primitive, there is nothing to prove. Suppose that $f(x)$ is not primitive. Let m be the largest positive integer with the property that all coefficients of the polynomial $f(x)$ are divisible by some product of m prime elements of R. Such a positive integer must exist, because the number of factors in a product of prime elements of R dividing a non-zero coefficient of $f(x)$ cannot exceed the number of factors in a representation of that coefficient as a product of prime elements of the ring R. Let c be a non-zero element of R dividing all the coefficients of $f(x)$ that is a product of m prime elements of R. Then $f(x) = c\hat{f}(x)$ for some polynomial $\hat{f}(x)$ with coefficients in R. Moreover the polynomial $\hat{f}(x)$ is primitive, for if it were not primitive, then there would exist some prime element p of R dividing all the coefficients of $\hat{f}(x)$, and then cp would divide all the coefficients of $f(x)$ and would be a product of more than m prime elements of R, contradicting the definition of m. The result follows. ∎

The following result is a generalization of Gauss's Lemma concerning products of primitive polynomials with integer coefficients.

Lemma 2.27 *Let R be a unique factorization domain, and let $f(x)$ and $g(x)$ be polynomials with coefficients in R. If $f(x)$ and $g(x)$ are both primitive then so is their product $f(x)g(x)$.*

Proof Let p be a prime element of R, and let $R_p = R/(p)$. Then (p) is a prime ideal of R, and therefore the quotient ring R_p is an integral domain (Lemma 2.14). Let $\nu_p \colon R \to R_p$ be the quotient homomorphism defined such that $\nu_p(a) = a + (p)$ for all $a \in R$. Then ν_p induces a ring homomorphism $\nu_{p*} \colon R[x] \to R_p[x]$, where

$$\nu_{p*}\left(\sum_{k=0}^{m} a_k x^k\right) = \sum_{k=0}^{m} \nu_p(a_k) x^k$$

for all $a_0, a_1, \ldots, a_m \in R$. Let $\overline{f} = \nu_p(f)$ and $\overline{g} = \nu_p(g)$. Then $\overline{f}(x)$ and $\overline{g}(x)$ are polynomials with coefficients in the quotient ring R_p whose coefficients are the images of the corresponding coefficients of $f(x)$ and $g(x)$ under the quotient homomorphism $\nu_p \colon R \to R_p$. Moreover $\overline{f}(x)\overline{g}(x)$ is a polynomial in $R_p[x]$ whose coefficients are the images of the corresponding coefficients of $f(x)g(x)$ under the quotient homomorphism.

Now $f(x)$ is a primitive polynomial, and therefore the prime element p of R does not divide all the coefficients of $f(x)$. It follows that the polynomial $\overline{f}(x)$ is a non-zero polynomial in $R_p[x]$. Similarly $\overline{g}(x)$ is a non-zero polynomial in $R_p[x]$. Now the coefficient ring R_p is an integral domain. It follows that $\overline{f}(x)\overline{g}(x)$ is a non-zero polynomial whose leading coefficient is the product of the leading coefficients of $\overline{f}(x)$ and $\overline{g}(x)$. Therefore $f(x)g(x)$ has at least one coefficient that is not divisible by the prime element p of R. We have thus shown that there cannot exist any prime element of R that divides all the coefficients of $f(x)g(x)$. It follows that $f(x)g(x)$ is a primitive polynomial, as required. ∎

Lemma 2.28 *Let $f(x)$ and $g(x)$ be polynomials with coefficients in a unique factorization domain R. Suppose that the polynomial $f(x)$ is primitive and that there exists some non-zero element c of R such that $f(x)$ divides $cg(x)$ in the polynomial ring $R[x]$. Then $f(x)$ divides $g(x)$ in the polynomial ring $R[x]$.*

Proof The result follows immediately in the case where c is a unit of the coefficient ring R.

Suppose that the primitive polynomial $f(x)$ divides $pg(x)$, where p is a prime element of R. Then $pg(x) = f(x)h(x)$ for some non-zero polynomial $h(x)$ with coefficients in R. Moreover there exists a primitive polynomial $k(x)$ and a non-zero element b of R such that $h(x) = bk(x)$ (Lemma 2.26). Then $pg(x) = bf(x)k(x)$. But $f(x)k(x)$, being a product of primitive polynomials, is itself a primitive polynomial (Lemma 2.27). It follows that at least one coefficient of $f(x)k(x)$ is not divisible by the prime element p of R, and therefore p must divide b. Let $b = pa$. Then $g(x) = af(x)k(x)$, and thus $f(x)$ divides $g(x)$ in the polynomial ring $R[x]$.

If the multiplier c is neither a unit nor a prime element of R then it is the product of a finite number of prime elements of R, because R is a unique factorization domain. We have proved the result in the special case where the multiplier is a prime element of R. It follows that if the primitive polynomial $f(x)$ divides $p_1p_2\cdots p_kg(x)$ then $f(x)$ divides $p_2p_3\cdots p_kg(x)$. The result in the general case therefore follows by induction on the number of prime factors of the multiplier. ∎

Let R be a unique factorization domain. The units of the polynomial ring $R[x]$ are the polynomials of degree zero whose coeffficients are units of the ring R. (Thus a polynomial with coefficients in R is a unit of $R[x]$ if and only if it is a 'constant polynomial' whose 'value' is a unit of R.)

It is not possible for a polynomial of degree zero to divide a primitive polynomial unless it is a unit of $R[x]$. It follows that a primitive polynomial

with coefficients in R is an irreducible element of $R[x]$ if and only if it cannot be factored as a product of polynomials of lower degree with coefficients in R. We define an *irreducible primitive polynomial* with coefficients in R to be a primitive polynomial of degree greater than zero that cannot be factored as a product of polynomials of lower degree.

Lemma 2.29 *Let R be a unique factorization domain. Then the irreducible elements of the polynomial ring R are the polynomials of degree zero whose coefficients are prime elements of R and the irreducible primitive polynomials of positive degree. Moreover every non-zero polynomial in $R[x]$ that is not itself a unit of $R[x]$ may be factored as a product of one or more irreducible elements of $R[x]$.*

Proof The subring of $R[x]$ consisting of the polynomials of degree zero is isomorphic to the coefficient ring R, and the factors of a polynomial of degree zero must themselves be polynomials of degree zero. It follows that the irreducible elements of $R[x]$ that are of degree zero are those polynomials of degree zero whose coefficients are prime elements of $R[x]$.

Any polynomial of positive degree that is not primitive is divisible by some non-zero element of the coefficient ring R that is not a unit of R, and thus cannot be an irreducible element of R. It follows that the irreducible elements of $R[x]$ that are of positive degree are the irreducible primitive polynomials with coefficients in R.

Any primitive polynomial of positive degree with coefficients in R that is not itself an irreducible primitive polynomial can be factored as a product of polynomials of lower degree. The factors must themselves be primitive polynomials. It follows by induction on the degree of the primitive polynomial that any primitive polynomial of positive degree with coefficients in R can be factored as a product of a finite number of irreducible primitive polynomials. Therefore any non-zero polynomial with coefficients in R that is not a unit of $R[x]$ can be factored as the product of a polynomial of degree zero and a primitive polynomial, and can therefore be factored as a product of irreducible elements of the polynomial ring $R[x]$. ∎

Lemma 2.30 *Let R be a unique factorization domain. Then any polynomial of degree zero whose coefficient is a prime element of R is a prime element of the polynomial ring $R[x]$.*

Proof Let p be a prime element of R, and let $g(x)$ and $h(x)$ be polynomials with coefficients in R. Then there exist primitive polynomials $\hat{g}(x)$ and $\hat{h}(x)$ and elements a and b of R such that $g(x) = a\hat{g}(x)$ and $h(x) = b\hat{h}(x)$. Suppose

that p divides all the coefficients of the polynomial $g(x)h(x)$. Now $g(x)h(x) = ab\hat{g}(x)\hat{h}(x)$. Moroever $\hat{g}(x)\hat{h}(x)$ is a primitive polynomial, because the product of two primitive polynomials is always primitive (Lemma 2.27). It follows that there must exist at least one coefficient of $\hat{g}(x)\hat{h}(x)$ that is not divisible by the prime element p of R, and therefore ab is divisible by p. But then either a is divisible by p, in which case all the coefficients of $g(x)$ are divisible by p, or else b is divisible by p, in which case all the coefficients of $h(x)$ are divisible by p. Thus the polynomial of degree zero with coefficient p is a prime element of the polynomial ring $R[x]$. ∎

Lemma 2.31 *Let R be an integral domain, let I be a non-zero ideal of the polynomial ring $R[x]$, and let $w(x)$ be a non-zero polynomial belonging to I whose degree is less than or equal to the degree of every other non-zero polynomial belonging to the ideal I. Then, given any polynomial $g(x)$ belonging to I, there exists some non-zero element c of R with the property that $cg(x)$ is divisible in $R[x]$ by $w[x]$.*

Proof Let m be the degree of the polynomial $w(x)$, and let let k be an integer satisfying $k \geq m$. Suppose that, given any non-zero polynomial $h(x)$ in I of degree less than k, there exists some non-zero element b of R with the property that $bh(x)$ is divisible by $w(x)$ in $R[x]$. Let $g(x)$ be a polynomial in I of degree k. Then there exist non-zero elements d and a of R such that $dg(x)$ and $ax^{k-m}w(x)$ have the same leading coefficient. Then either $dg(x) - ax^{k-m}w(x) = 0_R$ or else $dg(x) - ax^{k-m}w(x)$ is a non-zero polynomial belonging to the ideal I whose degree is less than k. There must then exist some non-zero element b for which $b(dg(x) - ax^{k-1}w(x))$ is divisible by $w(x)$. Let $c = bd$. Then c is non-zero and $cg(x)$ is divisible in $R[x]$ by $w[x]$. The result therefore follows by induction on the degree of the polynomial $g(x)$. ∎

Lemma 2.32 *Let R be a unique factorization domain, let $f(x)$ be an irreducible primitive polynomial with coefficients in R, and let $g(x)$ and $h(x)$ be polynomials with coefficients in R. Suppose that $f(x)$ divides $g(x)h(x)$ in $R[x]$. Then either $f(x)$ divides $g(x)$ in $R[x]$ or $f(x)$ divides $h(x)$ in $R[x]$. Thus every irreducible primitive polynomial with coefficients in R is a prime element of $R[x]$.*

Proof Suppose that the irreducible primitive polynomial $f(x)$ does not divide $g(x)$ in $R[x]$. We must prove that $f(x)$ then divides $h(x)$ in $R[x]$. Let I the ideal of $R[x]$ generated by the polynomials $f(x)$ and $g(x)$, and let m be the smallest non-negative integer with the property that the ideal I contains a non-zero polynomial of degree m. Then there exists a primitive polynomial

$k(x)$ of degree m and a non-zero element a of R such that $ak(x) \in I$. It then follows from Lemma 2.31 that there exist non-zero elements c and d of R such that $cf(x)$ and $dg(x)$ are divisible by $k(x)$. It then follows from Lemma 2.28 that $f(x)$ and $g(x)$ are both divisible by the primitive polynomial $k(x)$ in $R[x]$. But $f(x)$ is an irreducible element of $R[x]$ (Lemma 2.29) and no associate of $f(x)$ in $R[x]$ can divide $g(x)$. It follows that $k(x)$ must be a unit of the ring $R[x]$, and therefore $k(x)$ is a polynomial of degree zero whose coefficient u is a unit of the ring R. The polynomial of degree zero with coefficient au then belongs to the ideal I generated by $f(x)$ and $g(x)$. It follows that there exist polynomials $q(x)$ and $r(x)$ such that $q(x)f(x) + r(x)g(x) = au$. Then

$$q(x)f(x)h(x) + r(x)g(x)h(x) = auh(x).$$

It follows that $f(x)$ divides $auh(x)$ in $R[x]$, because $f(x)$ divides $g(x)h(x)$ in $R[x]$. It then follows from Lemma 2.28 that $f(x)$ divides $h(x)$ in $R[x]$, as required. ∎

Proposition 2.33 *Let R be a unique factorization domain. Then the ring $R[x]$ of polynomials with coefficients in R is also a unique factorization domain.*

Proof An integral domain is a unique factorization domain if and only if every non-zero element of the domain that is not a unit can be factored as the product of one or more prime elements of the domain. We have shown that any non-zero polynomial in $R[x]$ that is not a unit can be factored as a product of irreducible elements of $R[x]$, and that the irreducible elements of $R[x]$ are the polynomials of degree zero whose coefficients are prime elements of R and the primitive irreducible polynomials of positive degree in $R[x]$ (Lemma 2.29). Moreover the polynomials of degree zero whose coefficients are prime are prime elements of $R[x]$ (Lemma 2.30), and the irreducible primitive polynomials are also prime elements of $R[x]$. (Lemma 2.32). Therefore every element of $R[x]$ that is not a unit can be factored as a product of one or more prime elements of $R[x]$, and thus $R[x]$ is a unique factorization domain. ∎

Example It follows from Proposition 2.33 that the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is a unique factorization domain. This integral domain is not a principal ideal domain. Indeed let p be a prime number, and let

$$I_p = \{f(x) \in \mathbb{Z}[x] : p \text{ divides } f(0)\}.$$

Then I_p is a prime ideal of $\mathbb{Z}[x]$, for if $f(x)$ and $g(x)$ are polynomials with integer coefficients, and if $fg \in I_p$ then $p|f(0)g(0)$. But then either $p|f(0)$ or

else $p|g(0)$, and thus either $f \in I_p$ or $g \in I_p$. The prime ideal I_p is generated by the constant polynomial p and the polynomial x. However this prime ideal is not a principal ideal, because the only common divisors of p and x in $\mathbb{Z}[x]$ are the constant polynomials with values ± 1.

2.10 Polynomial Rings in Several Indeterminates

Let R be a unital commutative ring. We define the ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in independent interminates $x_1, x_2, \ldots, x_n$ with coefficients in the ring R.

We define a *multi-index* of dimension n to be an n-tuple $(j_1, j_2, \ldots, j_n)$ of non-negative integers. A polynomial in the independent indeterminates $x_1, x_2, \ldots, x_n$ is represented as a finite sum

$$\sum_{(j_1,j_2,\ldots,j_n)\in M} r_{j_1,j_2,\ldots,j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

where the sum is taken over a finite set M of multi-indices of dimension n, and where $r_{j_1,j_2,\ldots,j_n} \in R$ for all $(j_1, j_2, \ldots, j_n) \in M$. We may then represent this polynomial formally as a sum

$$\sum_{j_1,j_2,\ldots,j_n=0}^{\infty} r_{j_1,j_2,\ldots,j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

taken over all multi-indices $(j_1, j_2, \ldots, j_n)$, where the coefficients $r_{j_1,j_2,\ldots,j_n}$ belong to the coefficient ring R, and where only finitely many of these coefficients are non-zero. The coefficients of a polynomial in $x_1, x_2, \ldots, x_n$ determine and are determined by that polynomial. Thus a polynomial is specified uniquely and completely by specifying the coefficient $r_{j_1,j_2,\ldots,j_n}$ of that polynomial associated with each multi-index $(j_1, j_2, \ldots, j_n)$.

Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be polynomials in the independent indeterminates $x_1, x_2, \ldots, x_n$ and let

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= \sum_{j_1,j_2,\ldots,j_n=0}^{\infty} r_{j_1,j_2,\ldots,j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}, \\ g(x_1, x_2, \ldots, x_n) &= \sum_{j_1,j_2,\ldots,j_n=0}^{\infty} s_{j_1,j_2,\ldots,j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}. \end{aligned}$$

Then the sum and product of these polynomials are defined such that

$$\begin{aligned} &f(x_1, x_2, \ldots, x_n) + g(x_1, x_2, \ldots, x_n) \\ &\qquad = \sum_{j_1,j_2,\ldots,j_n=0}^{\infty} (r_{j_1,j_2,\ldots,j_n} + s_{j_1,j_2,\ldots,j_n}) x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \end{aligned}$$

and

$$f(x_1, x_2, \ldots, x_n)g(x_1, x_2, \ldots, x_n) = \sum_{j_1,j_2,\ldots,j_n=0}^{\infty} t_{j_1,j_2,\ldots,j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n},$$

where

$$t_{j_1,j_2,\ldots,j_n} = \sum_{k_1=0}^{j_1} \sum_{k_2=0}^{j_2} \cdots \sum_{k_n=0}^{j_n} r_{k_1,k_2,\ldots,k_n} s_{j_1-k_1,j_2-k_2,\ldots,j_n-k_n}$$

for each multi-index $(j_1, j_2, \ldots, j_n)$ of dimension n. The set $R[x_1, x_2, \ldots, x_n]$ of all polynomials in the independent inteterminates $x_1, x_2, \ldots, x_n$ with coefficients in the ring R is then a unital commutative ring with respect to these operations of addition and multiplication. Moreover $R[x_1, x_2, \ldots, x_n]$ is naturally isomorphic to $R[x_1, \ldots, x_{n-1}][x_n]$ for all $n > 1$. Indeed any polynomial in the independent indeterminates $x_1, x_2, \ldots, x_n$ may be viewed as a polynomial in the indeterminate x_n with coefficients in the polynomial ring $R[x_1, \ldots, x_{n-1}]$, and the definitions of addition and multiplication in the polynomial ring $R[x_1, x_2, \ldots, x_n]$ are consistent with this way of regarding polynomials in $x_1, x_2, \ldots, x_n$ as polynomials in x_n with coefficients in $R[x_1, \ldots, x_{n-1}]$. This observation allows one to obtain results concerning polynomial rings in several independent indeterminates by induction on the number of indeterminates. Results that can be proved by induction on the number of indeterminates include the following.

Proposition 2.34 *The ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in n independent indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in an integral domain R is itself an integral domain.*

Proof The result in the case $n = 1$ follows from the fact that the product of the leading coefficients of two non-zero polynomials $f(x_1)$ and $g(x_1)$ is a non-zero element of the integral domain R, and is thus the leading coefficient of the product polynomial $f(x_1)g(x_1)$. The result when $n > 1$ then follows by induction on the number n of indeterminates in view of the fact that $R[x_1, x_2, \ldots, x_n] \cong R[x_1, \ldots, x_{n-1}][x_n]$ for all $n > 1$. ∎

Proposition 2.35 *The ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in n independent indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in a unique factorization domain R is itself a unique factorization domain.*

Proof The result for $n = 1$ was proved as Proposition 2.33. The result for $n > 1$ then follows by induction on the number n of indeterminates in view of the fact that $R[x_1, x_2, \ldots, x_n] \cong R[x_1, \ldots, x_{n-1}][x_n]$ for all $n > 1$. ∎

Corollary 2.36 *The ring $K[x_1, x_2, \ldots, x_n]$ of polynomials in n independent indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in a field K is a unique factorization domain.*

Corollary 2.37 *The ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ of polynomials in n independent indeterminates $x_1, x_2, \ldots, x_n$ with integer coefficients is a unique factorization domain.*

Example Let K be a field, and let $K[x, y]$ be the ring of polynomials in two independent interminates x and y. Any polynomial $f(x, y)$ in x and y with coefficients in K can be represented in the form $g_0(x) + \sum_{j=1}^{d} g_j(x)y^j$, where $g_0(x), g_1(x), \ldots, g_d(x)$ are polynomials in the indeterminate x with coefficients in K. These polynomials $g_0, g_1, \ldots, g_d$ are uniquely determined by the polynomial $f(x)$. There is thus a well-defined function $\varphi\colon K[x, y] \to K[x]$, where

$$\varphi\left(g_0(x) + \sum_{j=1}^{d} g_j(x)y^j\right) = g_0(x).$$

for all $g_0, g_1, \ldots, g_d \in K[x]$. Moreover $\varphi(f)(x) = f(x, 0_K)$ for all $f \in K[x, y]$, where $f(x, 0_K)$ denotes the polynomial in the indeterminate x obtained by substituting the zero element 0_K of the field K for the indeterminate y. The function $\varphi\colon K[x, y] \to K[x]$ is a surjective ring homomorphism, and its kernel is the ideal P of $K[x, y]$ generated by the polynomial y. Now $K[x, y]/P \cong K[x]$, and $K[x]$ is an integral domain. It follows that the principal ideal P of $K[x, y]$ generated by the polynomial y is a prime ideal of $K[x, y]$ (see Lemma 2.14). The function $\varepsilon\colon K[x, y] \to K$ that maps a polynomial $f(x, y)$ to its value $f(0_K, 0_K)$ at $(0_K, 0_K)$ is also a surjective ring homomorphism. It satisfies

$$\varepsilon\left(\sum_{j=0}^{d_x}\sum_{k=0}^{d_y} a_{j,k}x^j y^k\right) = a_{0,0}$$

for all coefficients $a_{j,k}$, where $a_{j,k} \in K$ for $j = 0, 1, \ldots, d_x$ and $k = 0, 1, \ldots, d_y$. The kernel of this homomorphism is the ideal M generated by the polynomials x and y. It follows that $K[x, y]/M$ is a field isomorphic to the field K of coefficients, and thus M is a maximal ideal of $K[x, y]$ (see Lemma 2.13). This maximal ideal M is not a principal ideal, because there is no polynomial dividing both generators x and y of M that is not a unit of $K[x, y]$. We see therefore that polynomial ring $K[x, y]$ in two independent indeterminates x and y with coefficients in a field K is a unique factorization domain, but it is not a principal ideal domain, and it contains non-zero prime ideals that are not maximal ideals of $K[x, y]$.

Each pair (a, b) of elements of K determines a corresponding maximal ideal $(x-a, y-b)$ of the polynomial ring $K[x, y]$ generated by the polynomials $x - a$ and $y - b$. This maximal ideal is the kernel of the homomorphism that sends each polynomial $f(x, y)$ with coefficients in K to its value $f(a, b)$ when $x = a$ and $y = b$. Also each irreducible polynomial $f(x, y)$ is a prime element of the polynomial ring $K[x, y]$, because all irreducible elements of a unique factorization domain are prime. It follows that each irreducible polynomial $f(x, y)$ generates a prime ideal of $K[x, y]$, and therefore the corresponding quotient ring $K[x, y]/(f)$ is an integral domain for all irreducible polynomials $f(x, y)$ in the indeterminates x and y.

Consider now the zero sets of polynomials in n indeterminates. Each subset S of the ring $K[X_1, X_2, \ldots, X_n]$ of polynomials in the indeterminates $X_1, X_2, \ldots, X_n$ with coefficients in the field K determines a corresponding subset $V(S)$ of *affine n-dimensional space* K^n, where

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

The subset $V(S)$ of K^n is the set of common zeros of all the polynomials belonging to the subset S of the polynomial ring. Such subsets of K^n are referred to as *algebraic sets*. An *affine algebraic variety* is an algebraic set $V(P)$ determined by a prime ideal P of the polynomial ring $K[X_1, X_2, \ldots, X_n]$. It can be shown that every algebraic set in K^n is a finite union of affine algebraic varieties.

A field K is said to be *algebraically closed* if each polynomial in $K[x]$ of degree greater than zero has a root in the field K. If the field K is algebraically closed then each polynomial in $K[x]$ splits over K. David Hilbert proved a fundamental theorem, known as *Hilbert's Nullstellensatz*, which guarantees that there is a one-to-one correspondence between prime ideals of the polynomial ring $K[X_1, X_2, \ldots, X_n]$ and affine algebraic varieties in K^n, provided that the ground field K is algebraically closed. This result is applicable in the classical case where K is the field $\mathbb{C}$ of complex numbers.

2.11 Rings of Fractions

Definition Let R be a unital commutative ring. A subset S of R is said to be a *multiplicatively closed subset* of R if $1_R \in S$ and $uv \in S$ for all $u \in S$ and $v \in S$.

Lemma 2.38 *Let S be a multiplicatively closed subset of a unital commutative ring R, and let $\sim_S$ be the relation on $R \times S$ defined so that elements (r, s) and (r', s') of $R \times S$ satisfy $(r, s) \sim_S (r', s')$ if and only if there exists some*

element u of S for which $us'r = usr'$. Then the relation $\sim_S$ is an equivalence relation on $R \times S$.

Proof It is clear from the definition of the relation $\sim_S$ that $(r, s) \sim_S (r, s)$ for all $(r, s) \in R \times S$. Moreover elements (r, s) and (r', s') of $R \times S$ satisfy $(r, s) \sim_S (r', s')$ if and only if $(r', s') \sim_S (r, s)$. Thus the relation $\sim_S$ on $R \times S$ is both reflexive and symmetric.

Let (r, s), (r', s') and (r'', s'') be elements of $R \times S$. Suppose that $(r, s) \sim_S (r', s')$ and $(r', s') \sim_S (r'', s'')$. Then there exist elements u and v of S such that $us'r = usr'$ and $vs''r' = vs'r''$. Then

$$\begin{aligned}(uvs')(s''r) &= (vs'')(us'r) = (vs'')(usr') \\ &= (us)(vs''r') = (us)(vs'r'') \\ &= (uvs')(sr''),\end{aligned}$$

and $uvs' \in S$, and therefore $(r, s) \sim_S (r'', s'')$. Thus the relation $\sim_S$ on $R \times S$ is transitive. It follows that this relation is an equivalence relation on $R \times S$. ∎

Lemma 2.39 *Let S be a multiplicatively closed subset of a unital commutative ring R, and let $\sim_S$ be the equivalence relation on $R \times S$ defined so that elements (r, s) and (r', s') of $R \times S$ satisfy $(r, s) \sim_S (r', s')$ if and only if there exists some element u of S for which $us'r = usr'$. Let (r_1, s_1), (r'_1, s'_1), (r_2, s_2) and (r'_2, s'_2) be elements of $R \times S$ satisfying $(r_1, s_1) \sim_S (r'_1, s'_1)$ and $(r_2, s_2) \sim_S (r'_2, s'_2)$. Then*

$$(s_2r_1 + s_1r_2, s_1s_2) \sim_S (s'_2r'_1 + s'_1r'_2, s'_1s'_2)$$

and

$$(r_1r_2, s_1s_2) \sim_S (r'_1r'_2, s'_1s'_2).$$

Proof There exist elements u_1 and u_2 of S such that $u_1s'_1r_1 = u_1s_1r'_1$ and $u_2s'_2r_2 = u_2s_2r'_2$. Then

$$\begin{aligned}(u_1u_2)(s'_1s'_2)(s_2r_1 + s_1r_2) &= (u_2s_2s'_2)(u_1s'_1r_1) + (u_1s_1s'_1)(u_2s'_2r_2) \\ &= (u_2s_2s'_2)(u_1s_1r'_1) + (u_1s_1s'_1)(u_2s_2r'_2) \\ &= (u_1u_2)(s_1s_2)(s'_2r'_1 + s'_1r'_2),\end{aligned}$$

and $u_1u_2 \in S$, and therefore

$$(s_2r_1 + s_1r_2, s_1s_2) \sim_S (s'_2r'_1 + s'_1r'_2, s'_1s'_2).$$

Also

$$\begin{aligned}(u_1u_2)(s_1's_2')(r_1r_2) &= (u_1s_1'r_1)(u_2s_2'r_2) = (u_1s_1r_1')(u_2s_2r_2') \\ &= (u_1u_2)(s_1s_2)(r_1'r_2'),\end{aligned}$$

and therefore

$$(r_1r_2, s_1s_2) \sim_S (r_1'r_2', s_1's_2'),$$

as required. ∎

Let S be a multiplicatively closed subset of a unital commutative ring R, and let $\sim_S$ be the equivalence relation on $R \times S$ defined so that elements (r, s) and (r', s') of $R \times S$ satisfy $(r, s) \sim_S (r', s')$ if and only if there exists some element u of S for which $us'r = usr'$. Then the equivalence relation $\sim_S$ partitions the set $R \times S$ into equivalence classes. We denote by r/s the equivalence class of an element (r, s) of $R \times S$. Then $r, r' \in R$ and $s, s' \in S$ satisfy $r/s = r'/s'$ if and only if there exists some element u of S for which $us'r = urs'$. It follows from Lemma 2.39 that there are well-defined operations of addition and multiplication defined on $S^{-1}R$, where

$$(r_1/s_1) + (r_2s_2) = (s_2r_1 + s_1r_2)/(s_1s_2) \quad \text{and} \quad (r_1/s_1)(r_2/s_2) = (r_1r_2)/(s_1s_2).$$

If $0_R \in S$ then $S^{-1}R$ is the zero ring, consisting of a single element. We now show that if $0_R \notin S$ then $S^{-1}R$ is a unital commutative ring.

Proposition 2.40 *Let S be a multiplicatively closed subset of a unital commutative ring R, where $0_R \notin S$, and let $\sim_S$ be the equivalence relation on $R \times S$ defined so that elements (r, s) and (r', s') of $R \times S$ satisfy $(r, s) \sim_S (r', s')$ if and only if there exists some element u of S for which $us'r = usr'$. Let $S^{-1}R$ be the set of equivalence classes r/s of elements (r, s) of $R \times S$ with respect to this equivalence relation, with operations of addition and multiplication of equivalence classes defined such that*

$$(r_1/s_1) + (r_2s_2) = (s_2r_1 + s_1r_2)/(s_1s_2) \quad \text{and} \quad (r_1/s_1)(r_2/s_2) = (r_1r_2)/(s_1s_2)$$

for all $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Then $S^{-1}R$ is a unital commutative ring with zero element $0_R/1_R$ and identity element $1_R/1_R$. Moreover s_1/s_2 is a unit of $S^{-1}R$ for all elements $s_1, s_2 \in S$, and $(s_1/s_2)^{-1} = s_2/s_1$.

Proof The definition of addition on $S^{-1}R$ ensures that the operations of addition and multiplication are commutative, and that multiplication is distributive over addition. Let $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$. Then

$$\begin{aligned}((r_1/s_1) + (r_2/s_2)) + (r_3/s_3) &= ((s_2r_1 + s_1r_2)/(s_1s_2)) + (r_3/s_3) \\ &= (s_3s_2r_1 + s_3s_1r_2 + s_1s_2r_3)/(s_1s_2s_3) \\ &= (r_1/s_1) + ((s_3r_2 + s_2r_3)/(s_2s_3)) \\ &= (r_1/s_1) + ((r_2/s_2) + (r_3/s_3))\end{aligned}$$

and

$$\begin{aligned}((r_1/s_1)(r_2/s_2))(r_3/s_3) &= ((r_1r_2)/(s_1s_2))(r_3/s_3)\\ &= (r_1r_2r_3)/(s_1s_2s_3)\\ &= (r_1/s_1)((r_2r_3)/(s_2s_3))\\ &= (r_1/s_1)((r_2/s_2)(r_3/s_3)).\end{aligned}$$

Thus the operations of addition and multiplication on $S^{-1}R$ are associative.

The definition of addition on $S^{-1}R$ ensures that $(r/s) + (0_R/1_R) = r/s$ and

$$(r/s) + (-r/s) = 0_R/s^2 = 0_R/1_R$$

for all $r \in R$ and $s \in S$. Therefore $S^{-1}R$ is an Abelian group with respect to addition, and the zero element of $S^{-1}R$ is $0_R/1_R$. Moreover multiplication is commutative, associative and distributive over addition, and therefore $S^{-1}R$ is a commutative ring.

The proposition is applicable only in the case where $0_R \notin S$. This ensures that $u1_R1_R \neq u1_R0_R$ for all $u \in S$, and therefore $1_R/1_R \neq 0_R/1_R$. Thus $S^{-1}R$ has a multiplicative identity element $1_R/1_R$ that is distinct from the zero element $0_R/1_R$ of the ring, and is thus $S^{-1}R$ is a unital commutative ring.

Finally we note that $(s_1/s_2)(s_2/s_1) = (s_1s_2)/(s_1s_2) = 1_R/1_R$ for all $s_1, s_2 \in S$. It follows that s_1/s_2 is a unit of $S^{-1}R$ for all $s_1, s_2 \in S$, and that $(s_1/s_2)^{-1} = s_2/s_1$. ∎

Lemma 2.41 *Let R be a unital commutative ring, and let S be a multiplicatively closed subset of S, where $0_R \notin S$. Then there is a natural unital homomorphism $\lambda\colon R \to S^{-1}R$, where $\lambda(r) = r/1_R$ for all $r \in R$. Moreover, given any unital ring T, and given any unital homomorphism $\varphi\colon R \to T$ that maps the multiplicatively closed subset S into the group of units of T, there exists a unique unital homomorphism $\hat{\varphi}\colon S^{-1}R \to T$ such that $\varphi = \hat{\varphi} \circ \lambda$. This homomorphism $\hat{\varphi}$ satisfies $\hat{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$ for all $r \in R$ and $s \in S$.*

Proof It follows directly from the definition of addition and multiplication on $S^{-1}R$ that $(r_1/1_R) + (r_2/1_R) = (r_1 + r_2)/1_R$ and $(r_1/1_R)(r_2/1_R) = (r_1r_2)/1_R$ for all $r_1, r_2 \in R$. Therefore $\lambda\colon R \to S^{-1}R$ is a homomorphism. Moreover this homomorphism maps the identity element 1_R of R to the identity element $1_R/1_R$ of $S^{-1}R$.

Let $\varphi\colon R \to T$ be a unital homomorphism from R to a unital ring T that maps the multiplicatively closed subset S of R to the group of units of T, and let $r, r' \in R$ and $s, s' \in S$ satisfy $r/s = r'/s'$. Then there exists some element u of S such that $us'r = usr'$. Then $\varphi(u)\varphi(s')\varphi(r) = \varphi(u)\varphi(s)\varphi(r')$.

But $\varphi(u)$, $\varphi(s)$ and $\varphi(s')$ are units of T. It follows that $\varphi(r)\varphi(s)^{-1} = \varphi(r')\varphi(s')^{-1}$. There is thus a well-defined function $\hat{\varphi}\colon S^{-1}R \to T$ satisfying $\hat{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$ for all $r \in R$ and $s \in S$. Moreover

$$\begin{aligned}
\hat{\varphi}((r_1/s_1) + (r_2/s_2)) &= \hat{\varphi}((s_2r_1 + s_1r_2)/(s_1s_2)) \\
&= \varphi(s_2r_1 + s_1r_2)\varphi(s_1s_2)^{-1} \\
&= (\varphi(s_2)\varphi(r_1) + \varphi(s_1)\varphi(r_2))\varphi(s_1)^{-1}\varphi(s_2)^{-1} \\
&= \varphi(r_1)\varphi(s_1)^{-1} + \varphi(r_2)\varphi(s_2)^{-1} \\
&= \hat{\varphi}(r_1/s_1) + \hat{\varphi}(r_2/s_2)
\end{aligned}$$

and

$$\begin{aligned}
\hat{\varphi}((r_1/s_1)(r_2/s_2)) &= \hat{\varphi}((r_1r_2)/(s_1s_2)) \\
&= \varphi(r_1r_2)\varphi(s_1s_2)^{-1} \\
&= \varphi(r_1)\varphi(r_2)\varphi(s_1)^{-1}\varphi(s_2)^{-1} \\
&= \hat{\varphi}(r_1/s_1)\hat{\varphi}(r_2/s_2)
\end{aligned}$$

for all $r_1, r_2 \in R$ and $s_1, s_2 \in S$, and $\hat{\varphi}(1_R/1_R) = 1_T$, where 1_T is the multiplicative identity element of T. Also $\hat{\varphi}(\lambda(r)) = \hat{\varphi}(r/1_R) = \varphi(r)$ for all $r \in R$. It follows that $\hat{\varphi}\colon S^{-1}R \to T$ is a unital homomorphism that satisfies $\hat{\varphi} \circ \lambda = \varphi$.

Now let $\psi\colon S^{-1}R \to T$ be a unital homomorphism that satisfies $\psi \circ \lambda = \varphi$, and let r and s be elements of R and S respectively. Then $(r/s)(s/1_R) = r/1_R$. Moreover $\psi(r/1_R) = \psi(\lambda(r)) = \varphi(r)$ and $\psi(s/1_R) = \psi(\lambda(s)) = \varphi(s)$. Therefore $\psi(r/s)\varphi(s) = \varphi(r)$, and thus $\psi(r/s) = \varphi(r)\varphi(s)^{-1} = \hat{\varphi}(r/s)$. This shows that $\hat{\varphi}\colon S^{-1}R \to T$ is the unique unital homomorphism from $S^{-1}R \to T$ that satisfies $\hat{\varphi} \circ \lambda = \varphi$. ∎

Let R be a unital commutative ring. An element x of R is said to be a *zero divisor* if there exists some non-zero element y of R for which $xy = 0_R$. The multiplicative identity element 1_R of R is not a zero divisor.

Definition An element x of a unital commutative ring R is said to be *regular* if it is not a zero divisor.

The multiplicative identity element 1_R is regular. Let x and y be regular elements of R. Then x and y are non-zero elements of R, because the zero element of R is a zero divisor. Moreover $xyz \neq 0_R$ for all non-zero elements z if R. It follows that xy is a regular element of R. Thus the set R_{reg} of regular elements of the unital commutative ring R is a multiplicatively closed set. We can therefore form the corresponding ring of fractions $Q(R)$, where $Q(R) = R_{\text{reg}}^{-1}R$.

Definition Let R be a unital commutative ring. The *total ring of fractions* $Q(R)$ of R is the ring $R_{\text{reg}}^{-1}R$, where R_{reg} is the set consisting of all regular elements of R.

Lemma 2.42 *Let R be a unital commutative ring, and let S be a multiplicatively closed subset of S, where $0_R \notin S$. Let $\lambda\colon R \to S^{-1}R$ be the natural homomorphism that maps each element r of R to $r/1_R$. Then the homomorphism λ is injective if and only if every element of the set S is a regular element of R.*

Proof Suppose that $u \in S$ is a zero divisor. Then there exists some non-zero element r of R for which $ur = 0_R$. But then $\lambda(r) = 0_R/1_R$, and thus $r \in \ker\lambda$. Thus if S contains a zero divisor then the homomorphism λ is not injective. Conversely if the homomorphism λ is not injective then there exists some non-zero element r of R satisfying $r/1_R = 0_R/1_R$. There must then exist some element $u \in S$ satisfying $ur = 0_R$, and this element u is a zero divisor of R. It follows that the multiplicative subset S of R contains a zero divisor if and only if the natural homomorphism $\lambda\colon R \to S^{-1}R$ is not injective. The result follows. ∎

Let R be a unital commutative ring. It follows from Lemma 2.42 that the homomorphism $\lambda_0\colon R \to Q(R)$ from R to its total ring of fractions $Q(R)$ that sends each element r of R to $r/1_R$ is injective. Moreover if S is a multiplicatively closed subset of R, and if the homomorphism $\lambda\colon R \to S^{-1}R$ sending each element r of R to $r/1_R$ is injective, then S is a subset of the set R_{reg} of regular elements of R, and the ring $S^{-1}R$ can therefore be embedded as a subring of $Q(R)$. Thus the total ring of fractions $Q(R)$ of R is the largest ring of fractions into which the ring R can be embedded.

Other important rings of fractions arise through a process known as *localization*. Let R be a unital commutative ring, let P be a prime ideal of R, and let S be the complement of P in R. It follows from the definition of prime ideals that S is a multiplicatively closed subset of R. Indeed an ideal of R is prime if and only if its complement is multiplicatively closed. We define $R_P = S^{-1}R$, where $S = R \setminus P$. The ring R_P is the *localization* of R at the prime ideal P. Each ideal I of R determines a corresponding ideal I_P of R_P, where

$$I_P = \{x/s \in R_P : x \in I \text{ and } s \in R \setminus P\}.$$

Lemma 2.43 *Let R be a unital commutative ring, let P be a prime ideal of R, and let R_P be the localization $(R \setminus P)^{-1}R$ of R at the prime ideal P. Then the ideal P_P of R_P consisting of all elements of R_P that are of the form x/s for some $x \in P$ and $s \in R \setminus P$ is a maximal ideal of R_P. Moreover it is the only maximal ideal of R_P.*

Proof We show that P_P is a proper ideal of R_P. Suppose that there were to exist $x \in P$ and $s \in R \setminus P$ such that $x/s = 1_R/1_R$. Then there would exist some element u of $R \setminus P$ such that $ux = us$. But this is impossible, because ux would be an element of the ideal P and us would be an element of the complement $R \setminus P$ of P. Therefore the identity element of R_P does not belong to the ideal P_P, and hence this ideal is a proper ideal of R_P.

If $r \in R$, $s \in R \setminus P$ and $r/s \in R_P \setminus P_P$ then $r \in R \setminus P$, and therefore r/s is a unit of R_P with inverse s/r. It follows that no proper ideal of R_P can intersect the complement of P_P and therefore all proper ideals of R_P are contained in P_P. It follows that P_P is a maximal ideal of R_P, and is the only maximal ideal of R_P. ∎

Let f be an element of a unital commutative ring R, and let S be the set $\{1_R, f, f^2, f^3, \ldots\}$ of powers of f. Then S is a multiplicatively closed subset of R which therefore gives rise to a corresponding ring of fractions R_f, where $R_f = S^{-1}R$. Elements of R_f are represented as fractions of the form r/f^k, where $r \in R$ and k is some non-negative integer. If $f^n = 0_R$ for some positive integer n then R_f is the zero ring.

If R is an integral domain then the set R^* of non-zero elements of R is a multiplicatively closed subset of R. There is thus a corresponding ring $R^{*-1}R$ of fractions. The non-zero elements of $R^{*-1}R$ are the elements that are of the form s_1/s_2, where $s_1, s_2 \in R^*$. Each of these elements is a unit of $R^{*-1}R$. It follows that $R^{*-1}R$ is a field. In this case the set of non-zero elements of the integral domain R coincides with the set of regular elements of R. It follows that the field $R^{*-1}R$ is the total ring of fractions of R. It is also the localization of R at the zero ideal of R.

Definition Let R be an integral domain. The *field of fractions* $\mathrm{Frac}(R)$ of R is the field $R^{*-1}R$, where R^* is the set $R \setminus \{0_R\}$ of non-zero elements of R.

The basic properties of the field of fractions of an integral domain are summarized in the following results which follow from the discussion above.

Proposition 2.44 *Let R be an integral domain, and let $\mathrm{Frac}(R)$ be its field of fractions. Then every element of $\mathrm{Frac}(R)$ is represented by a quotient of the form r/s, where $r, s \in R$ and $s \neq 0_R$. Moreover if r, r', s and s' are elements of R, and if $s \neq 0_R$ and $s' \neq 0_R$, then $r/s = r'/s'$ if and only if $s'r = sr'$. The operations of addition and multiplication are defined on the field of fractions $\mathrm{Frac}(R)$ so that*

$$(r_1/s_1) + (r_2 s_2) = (s_2 r_1 + s_1 r_2)/(s_1 s_2) \quad \textit{and} \quad (r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2)$$

for all $r_1, r_2 \in R$ *and* $s_1, s_2 \in R \setminus \{0_R\}$. *The zero element of* $\mathrm{Frac}(R)$ *is* $0_R/1_R$, *and the multiplicative identity element is* $1_R/1_R$. *The function that sends each element* r *of the integral domain* R *to* $r/1_R$ *is an injective unital homomorphism that embeds the integral domain* R *in its field of fractions.*

Lemma 2.45 *Let* R *be an integral domain, and let* $\mathrm{Frac}(R)$ *be the field of fractions of* R. *Then every unital ring homomorphism from* R *to a field* L *extends uniquely to a homomorphism from* $\mathrm{Frac}(R)$ *to* L.

Lemma 2.46 *Let* R *be an integral domain, let* $\mathrm{Frac}(R)$ *be the field of fractions of* R, *and let* S *be a multiplicatively closed subset of* R *that does not contain the zero element of* R. *Then the embedding of* R *in* $\mathrm{Frac}(R)$ *induces an embedding of the ring of fractions* $S^{-1}R$ *in the field* $\mathrm{Frac}(R)$.

2.12 Integrally Closed Domains

Definition Let R and T be unital commutative rings, where $R \subset T$. The ring R is said to be *integrally closed* in T if every element of T that is a root of some monic polynomial with coefficients in R belongs to R.

Definition An integral domain R is said to be *integrally closed* if it is integrally closed in its field of fractions. An *integrally closed domain* is an integral domain that is integrally closed.

Proposition 2.47 *All unique factorization domains are integrally closed.*

Proof Let R be a unique factorization domain, and let r and s be elements of R, where $s \neq 0_R$. Suppose that the quotient r/s of r and s in the field of fractions of R is a root of some monic polynomial $f(x)$ of degree n with coefficients in R. Then $n > 0$. Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^n.$$

Then

$$0 = s^n f(r/s) = a_0 s^n + a_1 s^{n-1} r + \cdots + a_{n-1} s r^{n-1} + r^n,$$

and thus

$$r^n = -s(a_0 s^{n-1} + a_1 s^{n-2} r + \cdots + a_{n-1} r^{n-1}).$$

It follows that s divides r^n. If s is a unit of R then there is nothing to prove. If s is not a unit of R, then s factors as a product of prime elements of R, because R is a unique factorization domain. Let p be a prime factor of s. Then p divides r^n, and therefore p divides r. Let $r = pr'$ and $s = ps'$. Then $r/s = r'/s'$. Moreover if s is a product of k prime elements of R, where $k > 1$, then s' is a product of $k - 1$ prime elements of R, and if s is itself prime then s' is a unit of R. The result therefore follows by induction on the number of prime factors of s. ∎

2.13 Irreducibility of Polynomials over Fields of Fractions

A polynomial with integer coefficients is irreducible over the field of rational numbers if and only if it cannot be factored as a product of polynomials of lower degree with integer coefficients. This result can be generalized so as to apply to polynomials with coefficients in any unique factorization domain.

Proposition 2.48 *Let $f(x)$ be a polynomial with coefficients in a unique factorization domain R. Suppose that $f(x)$ cannot be factored as a product of polynomials of lower degree with coefficients in R. Then $f(x)$ is irreducible over the field of fractions of R.*

Proof Let $\mathrm{Frac}(R)$ be the field of fractions of R. The natural homomorphism from R to $\mathrm{Frac}(R)$ that sends each element r of R to $r/1_R$ is injective, and therefore embeds R into $\mathrm{Frac}(R)$. We can identify the unique factorization domain R with its image under this embedding. We therefore regard R as a subring of the field $\mathrm{Frac}(R)$.

Let $g(x)$ be a polynomial with coefficients in $\mathrm{Frac}(R)$ that divides $f(x)$ in $\mathrm{Frac}(R)[x]$. The 'denominators' of the coefficients of $g(x)$ can be 'cleared' by multiplying the polynomial $g(x)$ by some non-zero element a of R so that the coefficients of the resulting polynomial $ag(x)$ belong to R. There then exists an element c of R and a primitive polynomial $h(x)$ with coefficients in R such that $ag(x) = ch(x)$ (Lemma 2.26). The primitive polynomial $h(x)$ divides $af(x)$ in the polynomial ring $R[x]$. It follows from Lemma 2.28 that $h(x)$ divides $f(x)$ in $R[x]$. (Note that this result follows from a straightforward application of Lemma 2.27, which generalizes Gauss's Lemma to polynomials with coefficients in any unique factorization domain.) But $f(x)$ cannot be factored as a product of polynomials of lower degree with coefficients in R. Therefore either $\deg h = \deg f$ or $\deg h = 0$. But $g(x) = (c/a)h(x)$. It follows that either $g(x)$ is a 'constant' polynomial of degree zero or else $g(x) = \rho f(x)$ for some $\rho \in \mathrm{Frac}(R)$. Thus $f(x)$ is irreducible over the field $\mathrm{Frac}(R)$, as required. ∎

2.14 Requirements for Unique Factorization Of Ideals

Every non-zero proper ideal of a principal ideal domain factors uniquely as a product of maximal ideals. There are integral domains with this property that are not principal ideal domains. Such integral domains are known as *Dedekind domains*.

Definition A *Dedekind domain* (or *Dedekind ring*) is a unital commutative ring R satisfying the following four properties:—

(i) R is an integral domain;

(ii) every ideal of R is finitely generated;

(iii) R is integrally closed;

(iv) every non-zero prime ideal of R is maximal.

It can be shown that an integral domain is a Dedekind domain if and only if every non-zero proper ideal of the domain factors as a product of maximal ideals. Such a factorization of a non-zero proper ideal as a product of maximal ideals is necessarily unique up to the order of the factors.

An *algebraic number field* is a subfield of the field of complex numbers that is a finite-dimensional vector space over the field of rational numbers. An *algebraic integer* is a complex number that is the root of some monic polynomial with integer coefficients. The set of algebraic integers within any algebraic number field is an integral domain, and this integral domain is a Dedekind domain. Therefore any non-zero proper ideal of the ring of algebraic integers in any algebraic number field can be factorized uniquely as a product of maximal ideals. This fact was established by the work of Kummer and Dedekind in the nineteenth century.

An integral domain is said to be a *Noetherian domain* if every ideal of the domain is finitely generated. Principal ideal domains and Dedekind domains are Noetherian domains. It follows from these definitions that an integral domain is a Dedekind domain if and only if it is an integrally closed Noetherian domain with the property that every non-zero prime ideal is maximal.