CHAPTER 12

Factoring

You probably think that one knows everything about polynomials.

—Serge Lang

12.1 FACTORING INTEGERS

We study division in rings in this chapter, modeling our investigation on properties of the ring of integers, and we begin by reviewing those properties. Some have been used without comment in earlier chapters of the book, and some have been proved before.

A property from which many others follow is division with remainder: If a and b are integers and a is positive, there exist integers q and r so that

$$b = aq + r, \quad \text{and } 0 \leq r < a. \tag{12.1.1}$$

We've seen some of its important consequences:

Theorem 12.1.2

(a) Every ideal of the ring $\mathbb{Z}$ of integers is principal.

(b) A pair a, b of integers, not both zero, has a *greatest common divisor*, a positive integer d with these properties:

- **(i)** $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$,
- **(ii)** d divides a and d divides b,
- **(iii)** if an integer e divides a and b, then e divides d.
- **(iv)** There are integers r and s such that $d = ra + sb$.

(c) If a prime integer p divides a product ab of integers, then p divides a or p divides b.

(d) *Fundamental Theorem of Arithmetic:* Every positive integer $a \neq 1$ can be written as a product $a = p_1 \cdots p_k$, where the p_i are positive prime integers, and $k > 0$. This expression is unique except for the ordering of the prime factors.

The proofs of these facts will be reviewed in a more general setting in the next section.

12.2 UNIQUE FACTORIZATION DOMAINS

It is natural to ask which rings have properties analogous to those of the ring of integers, and we investigate this question here. There are relatively few rings for which all parts of Theorem 12.1.2 can be extended, but polynomial rings over fields are important cases in which they do extend.

When discussing factoring, we assume that the ring R is an integral domain, so that the Cancellation Law 11.7.1 is available, and we exclude the element zero from consideration. Here is some terminology that we use:

(12.2.1)

u is a *unit*	if	u has a multiplicative inverse in R.
a *divides* b	if	$b = aq$ for some q in R.
a is a *proper divisor* of b	if	$b = aq$ and neither a nor q is a unit.
a and b are *associates*	if	each divides the other, or if $b = ua$, and u is a unit.
a is *irreducible*	if	a is not a unit, and it has no proper divisor – its only divisors are units and associates.
p is a *prime element*	if	p is not a unit, and whenever p divides a product ab, then p divides a or p divides b.

These concepts can be interpreted in terms of the principal ideals generated by the elements. Recall that the principal ideal (a) generated by an element a consists of all elements of R that are are divisible by a. Then

(12.2.2)

u is a unit	$\Leftrightarrow$	$(u) = (1)$.
a divides b	$\Leftrightarrow$	$(b) \subset (a)$.
a is a proper divisor of b	$\Leftrightarrow$	$(b) < (a) < (1)$.
a and b are associates	$\Leftrightarrow$	$(a) = (b)$.
a is irreducible	$\Leftrightarrow$	$(a) < (1)$, and there is no principal ideal (c) such that $(a) < (c) < (1)$.
p is a prime element	$\Leftrightarrow$	$ab \in (p)$ implies $a \in (p)$ or $b \in (p)$.

Before continuing, we note one of the simplest examples of a ring element that has more than one factorization. The ring is $R = \mathbb{Z}[\sqrt{-5}]$. It consists of all complex numbers of the form $a + b\sqrt{-5}$, where a and b are integers. We will use this ring as an example several times in this chapter and the next. In R, the integer 6 can be factored in two ways:

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{12.2.3}$$

It isn't hard to show that none of the four terms 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ can be factored further; they are irreducible elements of the ring.

We abstract the procedure of division with remainder first. To make sense of division with remainder, we need a measure of size of an element. A *size function* on an integral domain R can be any function σ whose domain is the set of nonzero elements of R, and

whose range is the set of nonnegative integers. An integral domain R is a *Euclidean domain* if there is a size function σ on R such that division with remainder is possible, in the following sense:

(12.2.4) Let a and b be elements of R, and suppose that a is not zero. There are elements q and r in R such that $b = aq + r$, and either $r = 0$ or else $\sigma(r) < \sigma(a)$.

The most important fact about division with remainder is that r is zero, if and only if a divides b.

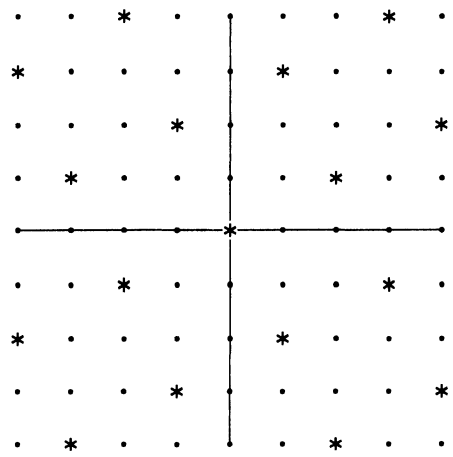
Proposition 12.2.5

(a) The ring $\mathbb{Z}$ of integers is a Euclidean domain, with size function $\sigma(\alpha) = |\alpha|$.

(b) A polynomial ring $F[x]$ in one variable over a field F is a Euclidean domain, with $\sigma(f) =$ degree of f.

(c) The ring $\mathbb{Z}[i]$ of Gauss integers is a Euclidean domain, with $\sigma(a) = |a|^2$.

The ring of integers and the polynomial rings were discussed in Chapter 11. We show here that the ring of Gauss integers is a Euclidean domain. The elements of $\mathbb{Z}[i]$ form a square lattice in the complex plane, and the multiples of a given nonzero element α form the principal ideal (α), which is a similar geometric figure. If we write $\alpha = re^{i\theta}$, then (α) is obtained from the lattice $\mathbb{Z}[i]$ by rotating through the angle θ and stretching by the factor r, as is illustrated below with $\alpha = 2 + i$:



(12.2.6) A Principal Ideal in the Ring of Gauss Integers.

For any complex number β, there is a point of the lattice (α) whose square distance from β is less than $|\alpha|^2$. We choose such a point, say $\gamma = \alpha q$, and let $r = \beta - \gamma$. Then $\beta = \alpha q + r$, and $|r|^2 < |\alpha|^2$, as required. Here q is in $\mathbb{Z}[i]$, and if β is in $\mathbb{Z}[i]$, so is r.

Division with remainder is not unique: There may be as many as four choices for the element γ. □

- An integral domain in which every ideal is principal is called a *principal ideal domain.*

Proposition 12.2.7 A Euclidean domain is a principal ideal domain.

Proof. We mimic the proof that the ring of integers is a principal ideal domain once more. Let R be a Euclidean domain with size function σ, and let A be an ideal of R. We must show that A is principal. The zero ideal is principal, so we may assume that A is not the zero ideal. Then A contains a nonzero element. We choose a nonzero element a of A such that $\sigma(a)$ is as small as possible, and we show that A is the principal ideal (a) of multiples of a.

Because A is an ideal and a is in A, any multiple aq with q in R is in A. So $(a) \subset A$. To show that $A \subset (a)$, we take an arbitrary element b of A. We use division with remainder to write $b = aq + r$, where either $r = 0$, or $\sigma(r) < \sigma(a)$. Then b and aq are in A, so $r = b - aq$ is in A too. Since $\sigma(a)$ is minimal, we can't have $\sigma(r) < \sigma(a)$, and it follows that $r = 0$. This shows that a divides b, and hence that b is in the principal ideal (a). Since b is arbitrary, $A \subset (a)$, and therefore $A = (a)$. □

Let a and b be elements of an integral domain R, not both zero. A *greatest common divisor* d of a and b is an element with the following properties:

(a) d divides a and b.

(b) If an element e divides a and b, then e divides d.

Any two greatest common divisors d and d' are associate elements. The first condition tells us that both d and d' divide a and b, and then the second one tells us that d' divides d and also that d divides d'.

However, a greatest common divisor may not exist. There will often be a common divisor m that is maximal, meaning that a/m and b/m have no proper divisor in common. But this element may fail to satisfy condition **(b)**. For instance, in the ring $\mathbb{Z}[\sqrt{-5}]$ considered above (12.2.3), the elements $a = 6$ and $b = 2 + 2\sqrt{-5}$ are divisible both by 2 and by $1 + \sqrt{-5}$. These are maximal elements among common divisors, but neither one divides the other.

One case in which a greatest common divisor does exist is that a and b have no common factors except units. Then 1 is a greatest common divisor. When this is so, a and b are said to be *relatively prime*.

Greatest common divisors always exist in a principal ideal domain:

Proposition 12.2.8 Let R be a principal ideal domain, and let a and b be elements of R, which are not both zero. An element d that generates the ideal $(a, b) = Ra + Rb$ is a greatest common divisor of a and b. It has these properties:

(a) $Rd = Ra + Rb$,

(b) d divides a and b.

(c) If an element e of R divides both a and b, it also divides d.

(d) There are elements r and s in R such that $d = ra + sb$.

Proof. This is essentially the same proof as for the ring of integers. **(a)** restates that d generates the ideal (a, b). **(b)** states that a and b are in Rd, and **(d)** states that d is in the ideal $Ra + Rb$. For **(c)**, we note that if e divides a and b then a and b are elements of Re. In that case, Re contains $Ra + Rb = Rd$, so e divides d. □

Corollary 12.2.9 Let R be a principal ideal domain.

(a) If elements a and b of R are relatively prime, then 1 is a linear combination $ra + sb$.

(b) An element of R is irreducible if and only if it is a prime element.

(c) The maximal ideals of R are the principal ideals generated by the irreducible elements.

Proof. **(a)** This follows from Proposition 12.2.8**(d)**.

(b) In any integral domain, a prime element is irreducible. We prove this below, in Lemma 12.2.10. Suppose that R is a principal ideal domain and that an irreducible element q of R divides a product ab. We have to show that if q does not divide a, then q divides b. Let d be a greatest common divisor of a and q. Since q is irreducible, the divisors of q are the units and the associates of q. Since q does not divide a, d is not an associate of q. So d is a unit, q and a are relatively prime, and $1 = ra+sq$ with r and s in R. We multiply by b: $b = rab+sqb$. Both terms on the right side of this equation are divisible by q, so q divides the left side, b.

(c) Let q be an irreducible element. Its divisors are units and associates. Therefore the only principal ideals that contain (q) are (q) itself and the unit ideal (1) (see (12.2.2)). Since every ideal of R is principal, these are the only ideals that contain (q). Therefore (q) is a maximal ideal. Conversely, if an element b has a proper divisor a, then $(b) < (a) < (1)$, so (b) is not a maximal ideal. □

Lemma 12.2.10 In an integral domain R, a prime element is irreducible.

Proof. Suppose that a prime element p is a product, say $p = ab$. Then p divides one of the factors, say a. But the equation $p = ab$ shows that a divides p too. So a and p are associates and b is a unit. The factorization is not proper. □

What analogy to the Fundamental Theorem of Arithmetic 12.1.2**(d)** could one hope for in an integral domain? We may divide the desired statement of uniqueness of factorization into two parts. First, a given element should be a product of irreducible elements, and second, that product should be essentially unique.

Units in a ring complicate the statement of uniqueness. Unit factors must be disregarded and associate factors must be considered equivalent. The units in the ring of integers are ± 1, and in this ring it is natural to work with positive integers. Similarly, in the polynomial ring $F[x]$ over a field, it is natural to work with monic polynomials. But we don't have a reasonable way to normalize elements in an arbitrary integral domain; it is best not to try.

We say that factoring in an integral domain R is unique if, whenever an element a of R is written in two ways as a product of irreducible elements, say

$$p_1 \cdots p_m = a = q_1 \cdots q_n, \tag{12.2.11}$$

then $m = n$, and if the right side is rearranged suitably, q_i is an associate of p_i for each i. So in the statement of uniqueness, associate factorizations are considered equivalent.

For example, in the ring of Gauss integers,

$$(2 + i)(2 - i) = 5 = (1 + 2i)(1 - 2i).$$

These two factorizations of the element 5 are equivalent because the terms that appear on the left and right sides are associates: $-i(2 + i) = 1 - 2i$ and $i(2 - i) = 1 + 2i$.

It is neater to work with principal ideals than with elements, because associates generate the same principal ideal. However, it isn't too cumbersome to use elements and we will stay with them here. The importance of ideals will become clear in the next chapter.

When we attempt to write an element a as a product of irreducible elements, we always assume that it is not zero and not a unit. Then we attempt to factor a, proceeding this way: If a is irreducible, we stop. If not, then a has a proper factor, so it decomposes in some way as a product, say $a = a_1b_1$, where neither a_1 nor b_1 is a unit. We continue factoring a_1 and b_1, if possible, and we hope that this procedure terminates; in other words, we hope that after a finite number of steps all the factors are irreducible. We say that *factoring terminates* in R if this is always true, and we refer to a factorization into irreducible elements as an *irreducible factorization*.

An integral domain R is a *unique factorization domain* if it has these properties:

(12.2.12)

- Factoring terminates.
- The irreducible factorization of an element a is unique in the sense described above.

The condition that factoring terminates has a useful description in terms of principal ideals:

Proposition 12.2.13 Let R be an integral domain. The following conditions are equivalent:

- Factoring terminates.
- R does not contain an infinite strictly increasing chain $(a_1) < (a_2) < (a_3) < \cdots$ of principal ideals.

Proof. If the process of factoring doesn't terminate, there will be an element a_1 with a proper factorization such that the process fails to terminate for at least one of the factors. Let's say that the proper factorization is $a_1 = a_2b_2$, and that the process fails to terminate for the factor we call a_2. Since a_2 is a proper divisor of a_1, $(a_1) < (a_2)$ (see (12.2.2)). We replace a_1 by a_2 and repeat. In this way we obtain an infinite chain.

Conversely, if there is a strictly increasing chain $(a_1) < (a_2) < \cdots$, then none of the ideals (a_n) is the unit ideal, and therefore a_2 is a proper divisor of a_1, a_3 is a proper divisor of a_2, and so on (12.2.2). This gives us a nonterminating process. □

We will rarely encounter rings in which factoring fails to terminate, and we will prove a theorem that explains the reason later (see (14.6.9)), so we won't worry much about it here. In practice it is the uniqueness that gives trouble. Factoring into irreducible elements will usually be possible, but it will not be unique, even when one takes into account the ambiguity of associate factors.

Going back to the ring $R = \mathbb{Z}[\sqrt{-5}]$, it isn't hard to show that all of the elements 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible, and that the units of R are 1 and -1. So 2 is not an associate of $1 + \sqrt{-5}$ or of $1 - \sqrt{-5}$. Therefore $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are essentially different factorizations: R is not a unique factorization domain.

Proposition 12.2.14

(a) Let R be an integral domain. Suppose that factoring terminates in R. Then R is a unique factorization domain if and only if every irreducible element is a prime element.

(b) A principal ideal domain is a unique factorization domain.

(c) The rings $\mathbb{Z}$, $\mathbb{Z}[i]$ and the polynomial ring $F[x]$ in one variable over a field F are unique factorization domains.

Thus the phrases *irreducible factorization* and *prime factorization* are synonymous in unique factorization domains, but most rings contain irreducible elements that are not prime. In the ring $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible. It is not prime because, though it divides the product $(1 + \sqrt{-5})(1 - \sqrt{-5})$, it does not divide either factor.

The converse of **(b)** is not true. We will see in the next section that the ring $\mathbb{Z}[x]$ of integer polynomials is a unique factorization domain, though it isn't a principal ideal domain.

Proof of Proposition (12.2.14). First of all, **(c)** follows from **(b)** because the rings mentioned in **(c)** are Euclidean domains, and therefore principal ideal domains.

(a) Let R be a ring in which every irreducible element is prime, and suppose that an element a factors in two ways into irreducible elements, say $p_1 \cdots p_m = a = q_1 \cdots q_n$, where $m \leq n$. If $n = 1$, then $m = 1$ and $p_1 = q_1$. Suppose that $n > 1$. Since p_1 is prime, it divides one of the factors $q_1, \ldots, q_n$, say q_1. Since q_1 is irreducible and since p_1 is not a unit, q_1 and p_1 are associates, say $p_1 = uq_1$, where u is a unit. We move the unit factor over to q_2, replacing q_1 by uq_1 and q_2 by $u^{-1}q_2$. The result is that now $p_1 = q_1$. Then we cancel p_1 and use induction on n.

Conversely, suppose that there is an irreducible element p that is not prime. Then there are elements a and b such that p divides the product $r = ab$, say $r = pc$, but p does not divide a or b. By factoring a, b, and c into irreducible elements, we obtain two inequivalent factorizations of r.

(b) Let R be a principal ideal domain. Since every irreducible element of R is prime (12.2.8), we need only prove that factoring terminates (12.2.14). We do this by showing that R contains no infinite strictly increasing chain of principal ideals. We suppose given an infinite weakly increasing chain

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots,$$

and we prove that it cannot be strictly increasing.

Lemma 12.2.15 Let $I_1 \subset I_2 \subset I_3 \subset \ldots$ be an increasing chain of ideals in a ring R. The union $J = \bigcup I_n$ is an ideal.

Proof. If u and v are in J, they are both in I_n for some n. Then $u + v$ and ru, for any r in R, are also in I_n, and therefore they are in J. This shows that J is an ideal. □

We apply this lemma to our chain of principal ideals, with $I_v = (a_v)$, and we use the hypothesis that R is a principal ideal domain to conclude that the union J is a principal ideal, say $J = (b)$. Then since b is in the union of the ideals (a_n), it is in one of those ideals.

But if b is in (a_n), then $(b) \subset (a_n)$. On the other hand, $(a_n) \subset (a_{n+1}) \subset (b)$. Therefore $(b) = (a_n) = (a_{n+1})$. The chain is not strictly increasing. □

One can decide whether an element a divides another element b in a unique factorization domain, in terms of their irreducible factorizations.

Proposition 12.2.16 Let R be a unique factorization domain.

(a) Let $a = p_1 \cdots p_m$ and $b = q_1 \cdots q_n$ be irreducible factorizations of two elements of R. Then a divides b in R if and only if $m \leq n$ and, when the factors q_j are arranged suitably, p_i is an associate of q_i for $i = 1, \ldots, m$.

(b) Any pair of elements a, b, not both zero, has a greatest common divisor.

Proof. **(a)** This is very similar to the proof of Proposition 12.2.14**(a)**. The irreducible factors of a are prime elements. If a divides b, then p_1 divides b, and therefore p_1 divides some q_i, say q_1. Then p_1 and q_1 are associates. The assertion follows by induction when we cancel p_1 from a and q_1 from b. We omit the proof of **(b)**. □

Note: Any two greatest common divisors of a and b are associates. But unless a unique factorization domain is a principal ideal domain, the greatest common divisor, though it exists, needn't have the form $ra + sb$. The greatest common divisor of 2 and x in the unique factorization domain $\mathbb{Z}[x]$ is 1, but we cannot write 1 as a linear combination of those elements with integer polynomials as coefficients. □

We review the results we have obtained for the important case of a polynomial ring $F[x]$ over a field. The units in the polynomial ring $F[x]$ are the nonzero constants. We can factor the leading coefficient out of a nonzero polynomial to make it monic, and the only monic associate of a monic polynomial f is f itself. By working with monic polynomials, the ambiguity of associate factorizations can be avoided. With this taken into account, the next theorem follows from Proposition 12.2.14.

Theorem 12.2.17 Let $F[x]$ be the polynomial ring in one variable over a field F.

(a) Two polynomials f and g, not both zero, have a unique monic greatest common divisor d, and there are polynomials r and s such that $rf + sg = d$.

(b) If two polynomials f and g have no nonconstant factor in common, then there are polynomials r and s such that $rf + sg = 1$.

(c) Every irreducible polynomial p in $F[x]$ is a prime element of $F[x]$: If p divides a product fg, then p divides f or p divides g.

(d) *Unique factorization:* Every monic polynomial in $F[x]$ can be written as a product $p_1 \cdots p_k$, where p_i are monic irreducible polynomials in $F[x]$ and $k \geq 0$. This factorization is unique except for the ordering of the terms. □

In the future, when we speak of the greatest common divisor of two polynomials with coefficients in a field, we will mean the unique monic polynomial with the properties **(a)** above. This greatest common divisor will sometimes be denoted by $\gcd(f, g)$.

The greatest common divisor $\gcd(f, g)$ of two polynomials f and g, not both zero, with coefficients in a field F can be found by repeated division with remainder, the process

called the *Euclidean algorithm* that we mentioned in Section 2.3 for the ring of integers: Suppose that the degree of g is at least equal to the degree of f. We write $g = fq + r$ where the remainder r, if it is not zero, has degree less than that of f. Then $\gcd(f, g) = \gcd(f, r)$. If $r = 0$, $\gcd(f, g) = f$. If not, we replace f and g by r and f, and repeat the process. Since degrees are being lowered, the process is finite. The analogous method can be used to determine greatest common divisors in any Euclidean domain.

Over the complex numbers, every polynomial of positive degree has a root α, and therefore a divisor of the form $x - \alpha$. The irreducible polynomials are linear, and the irreducible factorization of a monic polynomial has the form

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \tag{12.2.18}$$

where α_i are the roots of $f(x)$, with repetitions for multiple roots. The uniqueness of this factorization is not surprising.

When $F = \mathbb{R}$, there are two classes of irreducible polynomials: linear and quadratic. A real quadratic polynomial $x^2 + bx + c$ is irreducible if and only if its discriminant $b^2 - 4c$ is negative, in which case it has a pair of complex conjugate roots. The fact that every irreducible polynomial over the complex numbers is linear implies that no real polynomial of degree >2 is irreducible.

Proposition 12.2.19 Let α be a complex, not real, root of a real polynomial f. Then the complex conjugate $\overline{\alpha}$ is also a root of f. The quadratic polynomial $q = (x - \alpha)(x - \overline{\alpha})$ has real coefficients, and it divides f. □

Factoring polynomials in the ring $\mathbb{Q}[x]$ of polynomials with rational coefficients is more interesting, because there exist irreducible polynomials in $\mathbb{Q}[x]$ of arbitrary degree. This is explained in the next two sections. Neither the form of the irreducible factorization nor its uniqueness are intuitively clear in this case.

For future reference, we note the following elementary fact:

Proposition 12.2.20 A polynomial f of degree n with coefficients in a field F has at most n roots in F.

Proof. An element α is a root of f if and only if $x - \alpha$ divides f (11.2.11). If so, we can write $f(x) = (x - \alpha)q(x)$, where $q(x)$ is a polynomial of degree $n - 1$. Let β be a root of f different from α. Substituting $x = \beta$, we obtain $0 = (\beta - \alpha)q(\beta)$. Since β is not equal to α, it must be a root of q. By induction on the degree, q has at most $n - 1$ roots in F. Putting those roots together with α, we see that f has at most n roots. □

12.3 GAUSS'S LEMMA

Every monic polynomial $f(x)$ with rational coefficients can be expressed uniquely in the form $p_1 \cdots p_k$, where p_i are monic polynomials that are irreducible elements in the ring $\mathbb{Q}[x]$. But suppose that a polynomial $f(x)$ has integer coefficients, and that it factors in $\mathbb{Q}[x]$. Can it be factored without leaving the ring $\mathbb{Z}[x]$ of integer polynomials? We will see that it can, and also that $\mathbb{Z}[x]$ is a unique factorization domain.

Here is an example of an irreducible factorization in integer polynomials:

$$6x^3 + 9x^2 + 9x + 3 = 3(2x + 1)(x^2 + x + 1).$$

As we see, irreducible factorizations are slightly more complicated in $\mathbb{Z}[x]$ than in $\mathbb{Q}[x]$. Prime integers are irreducible elements of $\mathbb{Z}[x]$, and they may appear in the factorization of a polynomial. And, if we want to stay with integer coefficients, we can't require monic factors.

We have two main tools for studying factoring in $\mathbb{Z}[x]$. The first is the inclusion of the integer polynomial ring into the ring of polynomials with rational coefficients:

$$\mathbb{Z}[x] \subset \mathbb{Q}[x].$$

This can be useful because algebra in the ring $\mathbb{Q}[x]$ is simpler.

The second tool is reduction modulo some integer prime p, the homomorphism

$$\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x] \tag{12.3.1}$$

that sends $x \rightsquigarrow x$ (11.3.6). We'll often denote the image $\psi_p(f)$ of an integer polynomial by $\overline{f}$, though this notation is ambiguous because it doesn't mention p.

The next lemma should be clear.

Lemma 12.3.2 Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be an integer polynomial, and let p be an integer prime. The following are equivalent:

- p divides every coefficient a_i of f in $\mathbb{Z}$,
- p divides f in $\mathbb{Z}[x]$,
- f is in the kernel of ψ_p. □

The lemma shows that the kernel of ψ_p can be interpreted easily without mentioning the map. But the facts that ψ_p is a homomorphism and that its image $\mathbb{F}_p[x]$ is an integral domain make the interpretation as a kernel useful.

• A polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with rational coefficients is called *primitive* if it is an integer polynomial of positive degree, the greatest commmon divisor of its coefficients $a_0, \ldots, a_n$ in the integers is 1, and its leading coefficient a_n is positive.

Lemma 12.3.3 Let f be an integer polynomial f of positive degree, with positive leading coefficient. The following conditions are equivalent:

- f is primitive,
- f is not divisible by any integer prime p,
- for every integer prime p, $\psi_p(f) \neq 0$. □

Proposition 12.3.4

(a) An integer is a prime element of $\mathbb{Z}[x]$ if and only if it is a prime integer. So a prime integer p divides a product fg of integer polynomials if and only if p divides f or p divides g.

(b) *(Gauss's Lemma)* The product of primitive polynomials is primitive.

Proof. **(a)** It is obvious that an integer must be a prime if it is an irreducible element of $\mathbb{Z}[x]$. Let p be a prime integer. We use bar notation: $\overline{f} = \psi_p(f)$. Then p divides fg if and only if $\overline{fg} = 0$, and since $\mathbb{F}_p[x]$ is a domain, this is true if and only if $\overline{f} = 0$ or $\overline{g} = 0$, i.e., if and only if p divides f or p divides g.

(b) Suppose that f and g are primitive polynomials. Since their leading coefficients are positive, the leading coefficient of fg is also positive. Moreover, no prime p divides f or g, and by **(a)**, no prime divides fg. So fg is primitive. □

Lemma 12.3.5 Every polynomial $f(x)$ of positive degree with rational coefficients can be written *uniquely* as a product $f(x) = cf_0(x)$, where c is a rational number and $f_0(x)$ is a primitive polynomial. Moreover, c is an integer if and only if f is an integer polynomial. If f is an integer polynomial, then the greatest common divisor of the coefficients of f is $\pm c$.

Proof. To find f_0, we first multiply f by an integer d to clear the denominators in its coefficients. This will give us a polynomial $df = f_1$ with integer coefficients. Then we factor out the greatest common divisor of the coefficients of f_1 and adjust the sign of the leading coefficient. The resulting polynomial f_0 is primitive, and $f = cf_0$ for some rational number c. This proves existence.

If f is an integer polynomial, we don't need to clear the denominator. Then c will be an integer, and up to sign, it is the greatest common divisor of the coefficients, as stated.

The uniqueness of this product is important, so we check it carefully. Suppose given rational numbers c and c' and primitive polynomials f_0 and f_0' such that $cf_0 = c'f_0'$. We will show that $f_0 = f_0'$. Since $\mathbb{Q}[x]$ is a domain, it will follow that $c = c'$.

We multiply the equation $cf_0 = c'f_0'$ by an integer and adjust the sign if necessary, to reduce to the case that c and c' are positive integers. If $c \neq 1$, we choose a prime integer p that divides c. Then p divides $c'f_0'$. Proposition 12.3.4**(a)** shows that p divides one of the factors c' or f_0'. Since f_0' is primitive, it isn't divisible by p, so p divides c'. We cancel p from both sides of the equation. Induction reduces us to the case that $c = 1$, and the same reasoning shows that then $c' = 1$. So $f_0 = f_0'$. □

Theorem 12.3.6

(a) Let f_0 be a primitive polynomial, and let g be an integer polynomial. If f_0 divides g in $\mathbb{Q}[x]$, then f_0 divides g in $\mathbb{Z}[x]$.

(b) If two integer polynomials f and g have a common nonconstant factor in $\mathbb{Q}[x]$, they have a common nonconstant factor in $\mathbb{Z}[x]$.

Proof. **(a)** Say that $g = f_0q$ where q has rational coefficients. We show that q has integer coefficients. We write $g = cg_0$, and $q = c'q_0$, with g_0 and q_0 primitive. Then $cg_0 = c'f_0q_0$. Gauss's Lemma tells us that f_0q_0 is primitive. Therefore by the uniqueness assertion of Lemma 12.3.5, $c = c'$ and $g_0 = f_0q_0$. Since g is an integer polynomial, c is an integer. So $q = cq_0$ is an integer polynomial.

(b) If the integer polynomials f and g have a common factor h in $\mathbb{Q}[x]$ and if we write $h = ch_0$, where h_0 is primitive, then h_0 also divides f and g in $\mathbb{Q}[x]$, and by **(a)**, h_0 divides both f and g in $\mathbb{Z}[x]$. □

Proposition 12.3.7

(a) Let f be an integer polynomial with positive leading coefficient. Then f is an irreducible element of $\mathbb{Z}[x]$ if and only if it is either a prime integer or a primitive polynomial that is irreducible in $\mathbb{Q}[x]$.

(b) Every irreducible element of $\mathbb{Z}[x]$ is a prime element.

Proof. Proposition 12.3.4**(a)** proves **(a)** and **(b)** for a constant polynomial. If f is irreducible and not constant, it cannot have an integer factor different from ± 1, so if its leading coefficient is positive, it will be primitive. Suppose that f is a primitive polynomial and that it has a proper factorization in $\mathbb{Q}[x]$, say $f = gh$. We write $g = cg_0$ and $h = c'h_0$, with g_0 and h_0 primitive. Then g_0h_0 is primitive. Since f is also primitive, $f = g_0h_0$. Therefore f has a proper factorization in $\mathbb{Z}[x]$ too. So if f is reducible in $\mathbb{Q}[x]$, it is reducible in $\mathbb{Z}[x]$. The fact that a primitive polynomial that is reducible in $\mathbb{Z}[x]$ is also reducible in $\mathbb{Q}[x]$ is clear. This proves **(a)**.

Let f be a primitive irreducible polynomial that divides a product gh of integer polynomials. Then f is irreducible in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a principal ideal domain, f is a prime element of $\mathbb{Q}[x]$ (12.2.8). So f divides g or h in $\mathbb{Q}[x]$. By (12.3.6) f divides g or h in $\mathbb{Z}[x]$. This shows that f is a prime element, which proves **(b)**. □

Theorem 12.3.8 The polynomial ring $\mathbb{Z}[x]$ is a unique factorization domain. Every nonzero polynomial $f(x) \in \mathbb{Z}[x]$ that is not ± 1 can be written as a product

$$f(x) = \pm p_1 \cdots p_m q_1(x) \cdots q_n(x),$$

where p_i are integer primes and $q_j(x)$ are primitive irreducible polynomials. This expression is unique except for the order of the factors.

Proof. It is easy to see that factoring terminates in $\mathbb{Z}[x]$, so this theorem follows from Propositions 12.3.7 and 12.2.14. □

The results of this section have analogues for the polynomial ring $F[t, x]$ in two variables over a field F. To set up the analogy, we regard $F[t, x]$ as the ring $F[t][x]$ of polynomials in x whose coefficients are polynomials in t. The analogue of the field $\mathbb{Q}$ will be the field $F(t)$ of rational functions in t, the field of fractions of $F[t]$. We'll denote this field by $\mathcal{F}$. Then $F[t, x]$ is a subring of the ring $\mathcal{F}[x]$ of polynomials

$$f = a_n(t)x^n + \cdots + a_1(t)x + a_0(t)$$

whose coefficients $a_i(t)$ are rational functions in t. This can be useful because every ideal of $\mathcal{F}[x]$ is principal.

The polynomial f is called *primitive* if it has positive degree, its coefficients $a_i(t)$ are polynomials in $F[t]$ whose greatest common divisor is equal to 1, and the leading coefficient $a_n(t)$ is monic. A primitive polynomial will be an element of the polynomial ring $F[t, x]$.

It is true again that the product of primitive polynomials is primitive, and that every element $f(t, x)$ of $\mathcal{F}[x]$ can be written in the form $c(t)f_0(t, x)$, where f_0 is a primitive polynomial in $F[t, x]$ and c is a rational function in t, both uniquely determined up to constant factor.

The proofs of the next assertions are almost identical to the proofs of Proposition 12.3.4 and Theorems 12.3.6 and 12.3.8.

Theorem 12.3.9 Let $F[t]$ be a polynomial ring in one variable over a field F, and let $\mathcal{F} = F(t)$ be its field of fractions.

(a) The product of primitive polynomials in $F[t, x]$ is primitive.

(b) Let f_0 be a primitive polynomial, and let g be a polynomial in $F[t, x]$. If f_0 divides g in $\mathcal{F}[x]$, then f_0 divides g in $F[t, x]$.

(c) If two polynomials f and g in $F[t, x]$ have a common nonconstant factor in $\mathcal{F}[x]$, they have a common nonconstant factor in $F[t, x]$.

(d) Let f be an element of $F[t, x]$ whose leading coefficient is monic. Then f is an irreducible element of $F[t, x]$ if and only if it is either an irreducible polynomial in t alone, or a primitive polynomial that is irreducible in $\mathcal{F}[x]$.

(e) The ring $F[t, x]$ is a unique factorization domain. □

The results about factoring in $\mathbb{Z}[x]$ also have analogues for polynomials with coefficients in any unique factorization domain R.

Theorem 12.3.10 If R is a unique factorization domain, the polynomial ring $R[x_1, \ldots, x_n]$ in any number of variables is a unique factorization domain.

Note: In contrast to the case of one variable, where every complex polynomial is a product of linear polynomials, complex polynomials in two variables are often irreducible, and therefore prime elements, of $\mathbb{C}[t, x]$. □

12.4 FACTORING INTEGER POLYNOMIALS

We pose the problem of factoring an integer polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \tag{12.4.1}$$

with $a_n \neq 0$. Linear factors can be found fairly easily.

Lemma 12.4.2

(a) If an integer polynomial $b_1 x + b_0$ divides f in $\mathbb{Z}[x]$, then b_1 divides a_n and b_0 divides a_0.

(b) A primitive polynomial $b_1 x + b_0$ divides f in $\mathbb{Z}[x]$ if and only if the rational number $-b_0/b_1$ is a root of f.

(c) A rational root of a monic integer polynomial f is an integer.

Proof. **(a)** The constant coefficient of a product $(b_1 x + b_0)(q_{n-1}x^{n-1} + \cdots + q_0)$ is $b_0 q_0$, and if $q_{n-1} \neq 0$, the leading coefficient is $b_1 q_{n-1}$.

(b) According to Theorem 12.3.10**(c)**, $b_1 x + b_0$ divides f in $\mathbb{Z}[x]$ if and only if it divides f in $\mathbb{Q}[x]$, and this is true if and only if $x + b_0/b_1$ divides f, i.e., $-b_0/b_1$ is a root.

(c) If $\alpha = a/b$ is a root, written with $b > 0$, and if $\gcd(a, b) = 1$, then $bx - a$ is a primitive polynomial that divides the monic polynomial f, so $b = 1$ and α is an integer. □

The homomorphism $\psi_p : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ (12.3.1) is useful for explicit factoring, one reason being that there are only finitely many polynomials in $\mathbb{F}_p[x]$ of each degree.

Proposition 12.4.3 Let $f(x) = a_n x^n + \cdots + a_0$ be an integer polynomial, and let p be a prime integer that does not divide the leading coefficient a_n. If the residue $\overline{f}$ of f modulo p is an irreducible element of $\mathbb{F}_p[x]$, then f is an irreducible element of $\mathbb{Q}[x]$.

Proof. We prove the contrapositive, that if f is reducible, then $\overline{f}$ is reducible. Suppose that $f = gh$ is a proper factorization of f in $\mathbb{Q}[x]$. We may assume that g and h are in $\mathbb{Z}[x]$ (12.3.6). Since the factorization in $\mathbb{Q}[x]$ is proper, both g and h have positive degree, and, if $\deg f$ denotes the degree of f, then $\deg f = \deg g + \deg h$.

Since ψ_p is a homomorphism, $\overline{f} = \overline{g}\overline{h}$, so $\deg \overline{f} = \deg \overline{g} + \deg \overline{h}$. For any integer polynomial p, $\deg \overline{p} \leq \deg p$. Our assumption on the leading coefficient of f tells us that $\deg \overline{f} = \deg f$. This being so we must have $\deg \overline{g} = \deg g$ and $\deg \overline{h} = \deg h$. Therefore the factorization $\overline{f} = \overline{g}\overline{h}$ is proper. □

If p divides the leading coefficient of f, then $\overline{f}$ has lower degree, and using reduction modulo p becomes harder.

If we suspect that an integer polynomial is irreducible, we can try reduction modulo p for a small prime, $p = 2$ or 3 for instance, and hope that $\overline{f}$ turns out to be irreducible and of the same degree as f. If so, f will be irreducible too. Unfortunately, there exist irreducible integer polynomials that can be factored modulo every prime p. The polynomial $x^4 - 10x^2 + 1$ is an example. So the method of reduction modulo p may not work. But it does work quite often.

The irreducible polynomials in $\mathbb{F}_p[x]$ can be found by the "sieve" method. The *sieve of Eratosthenes* is the name given to the following method of determining the prime integers less than a given number n. We list the integers from 2 to n. The first one, 2, is prime because any proper factor of 2 must be smaller than 2, and there is no smaller integer on our list. We note that 2 is prime, and we cross out the multiples of 2 from our list. Except for 2 itself, they are not prime. The first integer that is left, 3, is a prime because it isn't divisible by any smaller prime. We note that 3 is a prime and then cross out the multiples of 3 from our list. Again, the smallest remaining integer, 5, is a prime, and so on.

$$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \ldots$$

The same method will determine the irreducible polynomials in $\mathbb{F}_p[x]$. We list the monic polynomials, degree by degree, and cross out products. For example, the linear polynomials in $\mathbb{F}_2[x]$ are x and $x + 1$. They are irreducible. The polynomials of degree 2 are x^2, $x^2 + x$, $x^2 + 1$, and $x^2 + x + 1$. The first three have roots in $\mathbb{F}_2$, so they are divisible by x or by $x + 1$. The last one, $x^2 + x + 1$, is the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$.

(12.4.4) The irreducible polynomials of degree ≤ 4 in $\mathbb{F}_2[x]$:

$$x,\ x+1;\quad x^2+x+1;\quad x^3+x^2+1,\ x^3+x+1;$$

$$x^4+x^3+1,\ x^4+x+1,\ x^4+x^3+x^2+x+1.$$

By trying the polynomials on this list, we can factor polynomials of degree at most 9 in $\mathbb{F}_2[x]$. For example, let's factor $f(x) = x^5 + x^3 + 1$ in $\mathbb{F}_2[x]$. If it factors, there must be an irreducible factor of degree at most 2. Neither 0 nor 1 is a root, so f has no linear factor. There is only one irreducible polynomial of degree 2, namely $p = x^2 + x + 1$. We carry out division with remainder: $f(x) = p(x)(x^3 + x^2 + x) + (x + 1)$. So p doesn't divide f, and therefore f is irreducible.

Consequently, the integer polynomial $x^5 - 64x^4 + 127x^3 - 200x + 99$ is irreducible in $\mathbb{Q}[x]$, because its residue in $\mathbb{F}_2[x]$ is the irreducible polynomial $x^5 + x^3 + 1$.

(12.4.5) The monic irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$:

$$x^2+1,\quad x^2+x-1,\quad x^2-x-1.$$

Reduction modulo p may help describe the factorization of a polynomial also when the residue is reducible. Consider the polynomial $f(x) = x^3 + 3x^2 + 9x + 6$. Reducing modulo 3, we obtain x^3. This doesn't look like a promising tool. However, suppose that $f(x)$ were reducible in $\mathbb{Z}[x]$, say $f(x) = (x+a)(x^2+bx+c)$. Then the residue of $x+a$ would divide x^3 in $\mathbb{F}_3[x]$, which would imply $a \equiv 0$ modulo 3. Similarly, we could conclude $c \equiv 0$ modulo 3. It is impossible to satisfy both of these conditions because the constant term ac of the product is supposed to be equal to 6. Therefore no such factorization exists, and $f(x)$ is irreducible.

The principle at work in this example is called the Eisenstein Criterion.

Proposition 12.4.6 Eisenstein Criterion. Let $f(x) = a_n x^n + \cdots + a_0$ be an integer polynomial and let p be a prime integer. Suppose that the coefficients of f satisfy the following conditions:

- p does not divide a_n;
- p divides all other coefficients $a_{n-1}, \ldots, a_0$;
- p^2 does not divide a_0.

Then f is an irreducible element of $\mathbb{Q}[x]$.

For example, the polynomial $x^4 + 25x^2 + 30x + 20$ is irreducible in $\mathbb{Q}[x]$.

Proof of the Eisenstein Criterion. Assume that f satisfies the conditions, and let $\overline{f}$ denote the residue of f modulo p. The hypotheses imply that $\overline{f} = \overline{a}_n x^n$ and that $\overline{a}_n \neq 0$. If f is reducible in $\mathbb{Q}[x]$, it will factor in $\mathbb{Z}[x]$ into factors of positive degree, say $f = gh$, where $g(x) = b_r x^r + \cdots + b_0$ and $h(x) = c_s x^s + \cdots + c_0$. Then $\overline{g}$ divides $\overline{a}_n x^n$, so $\overline{g}$ has the form $\overline{b}_r x^r$. Every coefficient of g except the leading coefficient is divisible by p. The same is true of h. The constant coefficient a_0 of f will be equal to $b_0 c_0$, and since p divides b_0 and c_0, p^2 must divide a_0. This contradicts the third condition. Therefore f is irreducible. □

One application of the Eisenstein Criterion is to prove the irreducibility of the *cyclotomic polynomial* $\Phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, where p is a prime. Its roots are the pth roots of unity, the powers of $\zeta = e^{2\pi i/p}$ different from 1:

$$(x-1)\,\Phi(x) = x^p - 1. \tag{12.4.7}$$

Lemma 12.4.8 Let p be a prime integer. The binomial coefficient $\binom{p}{r}$ is an integer divisible exactly once by p for every r in the range $1 < r < p$.

Proof. The binomial coefficient $\binom{p}{r}$ is

$$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r(r-1)\cdots 1}.$$

When $r < p$, the terms in the denominator are all less than p, so they cannot cancel the single p that is in the numerator. Therefore $\binom{p}{r}$ is divisible exactly once by p. □

Theorem 12.4.9 Let p be a prime. The cyclotomic polynomial $\Phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Proof. We substitute $x = y + 1$ into (12.4.7) and expand the result:

$$y\,\Phi(y+1) = (y+1)^p - 1 = y^p + \binom{p}{1}y^{p-1} + \cdots + \binom{p}{p-1}y + 1 - 1.$$

We cancel y. The lemma shows that the Eisenstein Criterion applies, and that $\Phi(y+1)$ is irreducible. It follows that $\Phi(x)$ is irreducible too. □

Estimating the Coefficients

Computer programs factor integer polynomials by factoring modulo powers of a prime, usually the prime $p = 2$. There are fast algorithms, the *Berlekamp algorithms*, to do this. The simplest case is that f is a monic integer polynomial whose residue modulo p is the product of relatively prime monic polynomials, say $\overline{f} = \overline{g}\overline{h}$ in $\mathbb{F}_p[x]$. Then there will be a unique way to factor f modulo any power of p. (We won't take the time to prove this.) Let's suppose that this is so, and that we (or the computer) have factored modulo the powers $p, p^2, p^3, \ldots$ If f factors in $\mathbb{Z}[x]$, the coefficients of the factors modulo p^k will stabilize when they are represented by integers between $-p^k/2$ and $p^k/2$, and this will produce the integer factorization. If f is irreducible in $\mathbb{Z}[x]$, the coefficients of the factors won't stabilize. When they get too big, one can conclude that the polynomial is irreducible.

The next theorem of Cauchy can be used to estimate how big the coefficients of the integer factors could be.

Theorem 12.4.10 Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial with complex coefficients, and let r be the maximum of the absolute values $|a_i|$ of its coefficients. The roots of f have absolute value less than $r + 1$.

Proof of Theorem 12.4.10. The trick is to rewrite the expression for f in the form

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

and to use the triangle inequality:

$$\begin{aligned} |x|^n &\le |f(x)| + |a_{n-1}||x|^{n-1} + \cdots + |a_1||x| + |a_0| \\ &\le |f(x)| + r\big(|x|^{n-1} + \cdots + |x| + 1\big) = |f(x)| + r\frac{|x|^n - 1}{|x| - 1}. \end{aligned} \tag{12.4.11}$$

Let α be a complex number with absolute value $|\alpha| \ge r+1$. Then $\dfrac{r}{|\alpha| - 1} \le 1$. We substitute $x = \alpha$ into (12.4.11):

$$|\alpha|^n \le |f(\alpha)| + r\frac{|\alpha|^n - 1}{|\alpha| - 1} \le |f(\alpha)| + |\alpha|^n - 1.$$

Therefore $|f(\alpha)| \ge 1$, and α is not a root of f. ∎

We give two examples in which $r = 1$.

Examples 12.4.12 **(a)** Let $f(x) = x^6 + x^4 + x^3 + x^2 + 1$. The irreducible factorization modulo 2 is

$$x^6 + x^4 + x^3 + x^2 + 1 = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Since the factors are distinct, there is just one way to factor f modulo 2^2, and it is

$$x^6 + x^4 + x^3 + x^2 + 1 = (x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1), \quad \text{modulo } 4.$$

The factorizations modulo 2^3 and modulo 2^4 are the same. If we had made these computations, we would guess that this is an integer factorization, which it is.

(b) Let $f(x) = x^6 - x^4 + x^3 + x^2 + 1$. This polynomial factors in the same way modulo 2. If f were reducible in $\mathbb{Z}[x]$, it would have a quadratic factor $x^2 + ax + b$, and b would be the product of two roots of f. Cauchy's theorem tells us that the roots have absolute value less than 2, so $|b| < 4$. Computing modulo 2^4,

$$x^6 - x^4 + x^3 + x^2 + 1 = (x^2 + x - 5)(x^4 - x^3 + 5x^2 + 7x + 3), \quad \text{modulo } 16.$$

The constant coefficient of the quadratic factor is -5. This is too big, so f is irreducible.

Note: It isn't necessary to use Cauchy's Theorem here. Since the constant coefficient of f is 1, the fact that $-5 \not\equiv \pm 1$ modulo 16 also proves that f is irreducible. □

The computer implementations for factoring are interesting, but they are painful to carry out by hand. It is unpleasant to determine a factorization modulo 16 such as the one above by hand, though it can be done by linear algebra. We won't discuss computer methods further. If you want to pursue this topic, see [LL&L].

12.5 GAUSS PRIMES

We have seen that the ring $\mathbb{Z}[i]$ of Gauss integers is a Euclidean domain. Every element that is not zero and not a unit is a product of prime elements. In this section we describe these prime elements, called *Gauss primes*, and their relation to integer primes.

In $\mathbb{Z}[i]$, $5 = (2+i)(2-i)$, and the factors $2+i$ and $2-i$ are Gauss primes. On the other hand, the integer 3 doesn't have a proper factor in $\mathbb{Z}[i]$. It is itself a Gauss prime. These examples exhibit the two ways that prime integers can factor in the ring of Gauss integers.

The next lemma follows directly from the definition of a Gauss integer:

Lemma 12.5.1

- A Gauss integer that is a real number is an integer.
- An integer d divides a Gauss integer $a+bi$ in the ring $\mathbb{Z}[i]$ if and only if d divides both a and b in $\mathbb{Z}$. □

Theorem 12.5.2

(a) Let π be a Gauss prime, and let $\overline{\pi}$ be its complex conjugate. Then $\overline{\pi}\pi$ is either an integer prime or the square of an integer prime.

(b) Let p be an integer prime. Then p is either a Gauss prime or the product $\overline{\pi}\pi$ of a Gauss prime and its complex conjugate.

(c) The integer primes p that are Gauss primes are those congruent to 3 modulo 4: $p = 3, 7, 11, 19, \ldots$

(d) Let p be an integer prime. The following are equivalent:

- **(i)** p is the product of complex conjugate Gauss primes.
- **(ii)** p is congruent 1 modulo 4, or $p = 2$: $p = 2, 5, 13, 17, \ldots$
- **(iii)** p is the sum of two integer squares: $p = a^2 + b^2$.
- **(iv)** The residue of -1 is a square modulo p.

Proof of Theorem 12.5.2 **(a)** Let π be a Gauss prime, say $\pi = a+bi$. We factor the positive integer $\overline{\pi}\pi = a^2 + b^2$ in the ring of integers: $\overline{\pi}\pi = p_1 \cdots p_k$. This equation is also true in the Gauss integers, though it is not necessarily a prime factorization in that ring. We continue factoring each p_i if possible, to arrive at a prime factorization in $\mathbb{Z}[i]$. Because the Gauss integers have unique factorization, the prime factors we obtain must be associates of the two factors π and $\overline{\pi}$. Therefore k is at most two. Either $\overline{\pi}\pi$ is an integer prime, or else it is the product of two integer primes. Suppose that $\overline{\pi}\pi = p_1 p_2$, and say that π is an associate of the integer prime p_1, i.e., that $\pi = \pm p_1$ or $\pm i p_1$. Then $\overline{\pi}$ is also an associate of p_1, so is $\overline{\pi}$, so $p_1 = p_2$, and $\overline{\pi}\pi = p_1^2$.

(b) If p is an integer prime, it is not a unit in $\mathbb{Z}[i]$. (The units are $\pm 1, \pm i$.) So p is divisible by a Gauss prime π. Then $\overline{\pi}$ divides $\overline{p}$, and $\overline{p} = p$. So the integer $\overline{\pi}\pi$ divides p^2 in $\mathbb{Z}[i]$ and also in $\mathbb{Z}$. Therefore $\overline{\pi}\pi$ is equal to p or p^2. If $\overline{\pi}\pi = p^2$, then π and p are associates, so p is a Gauss prime.

Part **(c)** of the theorem follows from **(b)** and **(d)**, so we need not consider it further, and we turn to the proof of **(d)**. It is easy to see that **(d)(i)** and **(d)(iii)** are equivalent: If $p = \overline{\pi}\pi$

for some Gauss prime, say $\pi = a + bi$, then $p = a^2 + b^2$ is a sum of two integer squares. Conversely, if $p = a^2 + b^2$, then p factors in the Gauss integers: $p = (a - bi)(a + bi)$, and **(a)** shows that the two factors are Gauss primes. □

Lemma 12.5.3 below shows that **(d)(i)** and **(d)(iv)** are equivalent, because (12.5.3)**(a)** is the negation of **(d)(i)** and (12.5.3)**(c)** is the negation of **(d)(iv)**.

Lemma 12.5.3 Let p be an integer prime. The following statements are equivalent:

(a) p is a Gauss prime;

(b) the quotient ring $\overline{R} = \mathbb{Z}[i]/(p)$ is a field;

(c) $x^2 + 1$ is an irreducible element of $\mathbb{F}_p[x]$ (12.2.8)**(c)**.

Proof. The equivalence of the first two statements follows from the fact that $\mathbb{Z}[i]/(p)$ is a field if and only if the principal ideal (p) of $\mathbb{Z}[i]$ is a maximal ideal, and this is true if and only if p is a Gauss prime (see (12.2.9)).

What we are really after is the equivalence of **(a)** and **(c)**, and at a first glance these statements don't seem to be related at all. It is in order to obtain this equivalence that we introduce the auxiliary ring $\overline{R} = \mathbb{Z}[i]/(p)$. This ring can be obtained from the polynomial ring $\mathbb{Z}[x]$ in two steps: first killing the polynomial $x^2 + 1$, which yields a ring isomorphic to $\mathbb{Z}[i]$, and then killing the prime p in that ring. We may just as well introduce these relations in the opposite order. Killing the prime p first gives us the polynomial ring $\mathbb{F}_p[x]$, and then killing $x^2 + 1$ yields $\overline{R}$ again, as is summed up in the diagram below.

(12.5.4)
$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow[p]{\text{kill}} & \mathbb{F}_p[x] \\ {\scriptstyle \text{kill}\atop \scriptstyle x^2+1}\downarrow & & \downarrow{\scriptstyle \text{kill}\atop \scriptstyle x^2+1} \\ \mathbb{Z}[i] & \xrightarrow[p]{\text{kill}} & \overline{R} \end{array} ,$$

We now have two ways to decide whether or not $\overline{R}$ is a field. First, $\overline{R}$ will be a field if and only if the ideal (p) in the ring $\mathbb{Z}[i]$ is a maximal ideal, which will be true if and only if p is a Gauss prime. Second, $\overline{R}$ will be a field if and only if the ideal $(x^2 + 1)$ in the ring $\mathbb{F}_p[x]$ is a maximal ideal, which will be true if and only if $x^2 + 1$ is an irreducible element of that ring (12.2.9). This shows that **(a)** and **(c)** of Theorem 12.5.2 are equivalent. □

To complete the proof of equivalence of **(i)**–**(iv)** of Theorem 12.5.2**(d)**, it suffices to show that **(ii)** and **(iv)** are equivalent. It is true that -1 is a square modulo 2. We look at the primes different from 2. The next lemma does the job:

Lemma 12.5.5 Let p be an odd prime.

(a) The multiplicative group $\mathbb{F}_p^\times$ contains an element of order 4 if and only if $p \equiv 1$ modulo 4.

(b) The integer a solves the congruence $x^2 \equiv -1$ modulo p if and only if its residue $\overline{a}$ is an element of order 4 in the multiplicative group $\mathbb{F}_p^\times$.

Proof. **(a)** This follows from a fact mentioned before, that the multiplicative group $\mathbb{F}_p^\times$ is a cyclic group (see (15.7.3)). We give an ad hoc proof here. The order of an element divides the order of the group. So if $\bar{a}$ has order 4 in $\mathbb{F}_p^\times$, then the order of $\mathbb{F}_p^\times$, which is $p-1$, is divisible by 4. Conversely, suppose that $p-1$ is divisible by 4. We consider the homomorphism $\varphi: \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ that sends $x \rightsquigarrow x^2$. The only elements of $\mathbb{F}_p^\times$ whose squares are 1 are ± 1 (see (12.2.20)). So the kernel of φ is $\{\pm 1\}$. Therefore its image, call it H, has even order $(p-1)/2$. The first Sylow Theorem shows that H contains an element of order 2. That element is the square of an element x of order 4.

(b) The residue $\bar{a}$ has order 4 if and only if $\bar{a}^2$ has order 2. There is just one element in $\mathbb{F}_p$ of order 2, namely the residue of -1. So $\bar{a}$ has order 4 if and only if $\bar{a}^2 = -\bar{1}$. □

This competes the proof of Theorem 12.5.2. □

You want to hit home run without going into spring training?

—Kenkichi Iwasawa

EXERCISES

Section 1 Factoring Integers

1.1. Prove that a positive integer n that is not an integer square is not the square of a rational number.

1.2. *(partial fractions)*

(a) Write the fraction $7/24$ in the form $a/8 + b/3$.

(b) Prove that if $n = uv$, where u and v are relatively prime, then every fraction $q = m/n$ can be written in the form $q = a/u + b/v$.

1.3. *(Chinese Remainder Theorem)*

(a) Let n and m be relatively prime integers, and let a and b be arbitrary integers. Prove that there is an integer x that solves the simultaneous congruence $x \equiv a$ modulo m and $x \equiv b$ modulo n.

(b) Determine all solutions of these two congruences.

1.4. Solve the following simultaneous congruences:

(a) $x \equiv 3$ modulo 8, $x \equiv 2$ modulo 5,

(b) $x \equiv 3$ modulo 15, $x \equiv 5$ modulo 8, $x \equiv 2$ modulo 7,

(c) $x \equiv 13$ modulo 43, $x \equiv 7$ modulo 71.

1.5. Let a and b be relatively prime integers. Prove that there are integers m and n such that $a^m + b^n \equiv 1$ modulo ab.

Section 2 Unique Factorization Domains

2.1. Factor the following polynomials into irreducible factors in $\mathbb{F}_p[x]$.

(a) x^3+x^2+x+1, $p=2$, **(b)** x^2-3x-3, $p=5$, **(c)** x^2+1, $p=7$

2.2. Compute the greatest common divisor of the polynomials $x^6+x^4+x^3+x^2+x+1$ and $x^5+2x^3+x^2+x+1$ in $\mathbb{Q}[x]$.

2.3. How many roots does the polynomial x^2-2 have, modulo 8?

2.4. Euclid proved that there are infinitely many prime integers in the following way: If $p_1, \ldots, p_k$ are primes, then any prime factor p of $(p_1 \cdots p_k)+1$ must be different from all of the p_i. Adapt this argument to prove that for any field F there are infinitely many monic irreducible polynomials in $F[x]$.

2.5. *(partial fractions for polynomials)*

(a) Prove that every element of $\mathbb{C}(x)$ x can be written as a sum of a polynomial and a linear combination of functions of the form $1/(x-a)^i$.

(b) Exhibit a basis for the field $\mathbb{C}(x)$ of rational functions as vector space over $\mathbb{C}$.

2.6. Prove that the following rings are Euclidean domains.

(a) $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$, **(b)** $\mathbb{Z}[\sqrt{-2}]$.

2.7. Let a and b be integers. Prove that their greatest common divisor in the ring of integers is the same as their greatest common divisor in the ring of Gauss integers.

2.8. Describe a systematic way to do division with remainder in $\mathbb{Z}[i]$. Use it to divide $4+36i$ by $5+i$.

2.9. Let F be a field. Prove that the ring $F[x, x^{-1}]$ of Laurent polynomials (Chapter 11, Exercise 5.7) is a principal ideal domain.

2.10. Prove that the ring $\mathbb{R}[[t]]$ of formal power series (Chapter 11, Exercise 2.2) is a unique factorization domain.

Section 3 Gauss's Lemma

3.1. Let φ denote the homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ defined by

(a) $\varphi(x) = 1+\sqrt{2}$, **(b)** $\varphi(x) = \frac{1}{2}+\sqrt{2}$.

Is the kernel of φ a principal ideal? If so, find a generator.

3.2. Prove that two integer polynomials are relatively prime elements of $\mathbb{Q}[x]$ if and only if the ideal they generate in $\mathbb{Z}[x]$ contains an integer.

3.3. State and prove a version of Gauss's Lemma for Euclidean domains.

3.4. Let x, y, z, w be variables. Prove that $xy-zw$, the determinant of a variable 2×2 matrix, is an irreducible element of the polynomial ring $\mathbb{C}[x, y, z, w]$.

3.5. **(a)** Consider the map $\psi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow f(t^2, t^3)$. Prove that its image is the set of polynomials $p(t)$ such that $\frac{dp}{dt}(0) = 0$.

(b) Consider the map $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $f(x, y) \rightsquigarrow (t^2-t, t^3-t^2)$. Prove that $\ker\varphi$ is a principal ideal, and find a generator $g(x, y)$ for this ideal. Prove that the image of φ is the set of polynomials $p(t)$ such that $p(0) = p(1)$. Give an intuitive explanation in terms of the geometry of the variety $\{g=0\}$ in $\mathbb{C}^2$.

3.6. Let α be a complex number. Prove that the kernel of the substitution map $\mathbb{Z}[x] \to \mathbb{C}$ that sends $x \rightsquigarrow \alpha$ is a principal ideal, and describe its generator.

Section 4 Factoring Integer Polynomials

4.1. **(a)** Factor $x^9 - x$ and $x^9 - 1$ in $\mathbb{F}_3[x]$. **(b)** Factor $x^{16} - x$ in $\mathbb{F}_2[x]$.

4.2. Prove that the following polynomials are irreducible:
(a) $x^2 + 1$, in $\mathbb{F}_7[x]$, **(b)** $x^3 - 9$, in $\mathbb{F}_{31}[x]$.

4.3. Decide whether or not the polynomial $x^4 + 6x^3 + 9x + 3$ generates a maximal ideal in $\mathbb{Q}[x]$.

4.4. Factor the integer polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ modulo 2, modulo 3, and in $\mathbb{Q}$.

4.5. Which of the following polynomials are irreducible in $\mathbb{Q}[x]$?
(a) $x^2 + 27x + 213$, **(b)** $8x^3 - 6x + 1$, **(c)** $x^3 + 6x^2 + 1$, **(d)** $x^5 - 3x^4 + 3$.

4.6. Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and in $\mathbb{F}_2[x]$.

4.7. Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$, when $p = 2, 3$, and 5.

4.8. How might a polynomial $f(x) = x^4 + bx^2 + c$ with coefficients in a field F factor in $F[x]$? Explain with reference to the particular polynomials $x^4 + 4x^2 + 4$ and $x^4 + 3x^2 + 4$.

4.9. For which primes p and which integers n is the polynomial $x^n - p$ irreducible in $\mathbb{Q}[x]$?

4.10. Factor the following polynomials in $\mathbb{Q}[x]$. **(a)** $x^2 + 2351x + 125$, **(b)** $x^3 + 2x^2 + 3x + 1$, **(c)** $x^4 + 2x^3 + 2x^2 + 2x + 2$, **(d)** $x^4 + 2x^3 + 3x^2 + 2x + 1$, **(e)** $x^4 + 2x^3 + x^2 + 2x + 1$, **(f)** $x^4 + 2x^2 + x + 1$, **(g)** $x^8 + x^6 + x^4 + x^2 + 1$, **(h)** $x^6 - 2x^5 - 3x^2 + 9x - 3$, **(j)** $x^4 + x^2 + 1$, **(k)** $3x^5 + 6x^4 + 9x^3 + 3x^2 - 1$, **(l)** $x^5 + x^4 + x^2 + x + 2$.

4.11. Use the sieve method to determine the primes <100, and discuss the efficiency of the sieve: How quickly are the nonprimes filtered out?

4.12. Determine:

(a) the monic irreducible polynomials of degree 3 over $\mathbb{F}_3$,
(b) the monic irreducible polynomials of degree 2 over $\mathbb{F}_5$,
(c) the number of irreducible polynomials of degree 3 over the field $\mathbb{F}_5$.

4.13. *Lagrange interpolation formula*:

(a) Let $a_0, \ldots, a_d$ be distinct complex numbers. Determine a polynomial $p(x)$ of degree n, which has $a_1, \ldots, a_n$ as roots, and such that $p(a_0) = 1$.
(b) Let $a_0, \ldots, a_d$ and $b_0, \ldots, b_d$ be complex numbers, and suppose that the a_i are distinct. There is a unique polynomial g of degree $\leq d$ such that $g(a_i) = b_i$ for each $i = 0, \ldots, d$. Determine the polynomial g explicitly in terms of a_i and b_i.

4.14. By analyzing the locus $x^2 + y^2 = 1$, prove that the polynomial $x^2 + y^2 - 1$ is irreducible in $\mathbb{C}[x, y]$.

4.15. With reference to the Eisenstein criterion, what can one say when
(a) $\overline{f}$ is constant, **(b)** $\overline{f} = x^n + \overline{b}x^{n-1}$?

4.16. Factor $x^{14} + 8x^{13} + 3$ in $\mathbb{Q}[x]$, using reduction modulo 3 as a guide.

4.17. Using congruence modulo 4 as an aid, factor $x^4 + 6x^3 + 7x^2 + 8x + 9$ in $\mathbb{Q}[x]$.

*4.18. Let $q = p^e$ with p prime, and let $r = p^{e-1}$. Prove that the cyclotomic polynomial $(x^q - 1)/(x^r - 1)$ is irreducible.

4.19. Factor $x^5 - x^4 - x^2 - 1$ modulo 2, modulo 16, and over $\mathbb{Q}$.

Section 5 Gauss Primes

5.1. Factor the following into primes in $\mathbb{Z}[i]$: **(a)** $1 - 3i$, **(b)** 10, **(c)** $6 + 9i$, **(d)** $7 + i$.

5.2. Find the greatest common divisor in $\mathbb{Z}[i]$ of **(a)** $11 + 7i, 4 + 7i$, **(b)** $11 + 7i, 8 + i$, **(c)** $3 + 4i, 18 - i$.

5.3. Find a generator for the ideal of $Z[i]$ generated by $3 + 4i$ and $4 + 7i$.

5.4. Make a neat drawing showing the primes in the ring of Gauss integers in a reasonable size range.

5.5. Let π be a Gauss prime. Prove that π and $\overline{\pi}$ are associates if and only if π is an associate of an integer prime, or $\overline{\pi}\pi = 2$.

5.6. Let R be the ring $\mathbb{Z}[\sqrt{-3}]$. Prove that an integer prime p is a prime element of R if and only if the polynomial $x^2 + 3$ is irreducible in $\mathbb{F}_p[x]$.

5.7. Describe the residue ring $\mathbb{Z}[i]/(p)$ for each prime p.

5.8. Let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Make a drawing showing the prime elements of absolute value ≤ 10 in R.

*5.9. Let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Let p be an integer prime $\neq 3$. Adapt the proof of Theorem 12.5.2 to prove the following:

(a) The polynomial $x^2 + x + 1$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1$ modulo 3.

(b) (p) is a maximal ideal of R if and only if $p \equiv -1$ modulo 3.

(c) p factors in R if and only if it can be written in the form $p = a^2 + ab + b^2$, for some integers a and b.

5.10.[1] **(a)** Let α be a Gauss integer. Assume that α has no integer factor, and that $\overline{\alpha}\alpha$ is a square integer. Prove that α is a square in $\mathbb{Z}[i]$.

(b) Let a, b, c be integers such that a and b are relatively prime and $a^2 + b^2 = c^2$. Prove that there are integers m and n such that $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$.

Miscellaneous Problems

M.1. Let S be a commutative semigroup – a set with a commutative and associative law of composition and with an identity element (Chapter 2, Exercise M.4). Suppose the Cancellation Law holds in S: If $ab = ac$ then $b = c$. Make the appropriate definitions and extend Proposition 12.2.14**(a)** to this situation.

M.2. Let $v_1, \ldots, v_n$ be elements of $\mathbb{Z}^2$, and let S be the semigroup of all combinations $a_1v_1 + \cdots + a_nv_n$ with non-negative integer coefficients a_i, the law of composition being *addition* (Chapter 2, Exercise M.4). Determine which of these semigroups has unique factorization **(a)** when the coordinates of the vectors v_i are nonnegative, and **(b)** in general.

Hint: Begin by translating the terminology (12.2.1) into additive notation.

[1] Suggested by Nathaniel Kuhn.

M.3. Let p be an integer prime, and let A be an $n \times n$ integer matrix such that $A^p = I$ but $A \neq I$. Prove that $n \geq p - 1$. Give an example with $n = p - 1$.

***M.4.** **(a)** Let R be the ring of functions that are polynomials in $\cos t$ and $\sin t$, with real coefficients. Prove that R is isomorphic to $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$.

(b) Prove that R is not a unique factorization domain.

(c) Prove that $S = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$ is a principal ideal domain and hence a unique factorization domain.

(d) Determine the units in the rings S and R.

Hint: Show that S is isomorphic to a Laurent polynomial ring $\mathbb{C}[u, u^{-1}]$.

M.5. For which integers n does the circle $x^2 + y^2 = n$ contain a point with integer coordinates?

M.6. Let R be a domain, and let I be an ideal that is a product of distinct maximal ideals in two ways, say $I = P_1 \cdots P_r = Q_1 \cdots Q_s$. Prove that the two factorizations are the same, except for the ordering of the terms.

M.7. Let $R = \mathbb{Z}[x]$.

(a) Prove that every maximal ideal in R has the form (p, f), where p is an integer prime and f is a primitive integer polynomial that is irreducible modulo p.

(b) Let I be an ideal of R generated by two polynomials f and g that have no common factor other than ± 1. Prove that R/I is finite.

M.8. Let u and v be relatively prime integers, and let R' be the ring obtained from $\mathbb{Z}$ by adjoining an element α with the relation $v\alpha = u$. Prove that R' is isomorphic to $\mathbb{Z}[\frac{u}{v}]$ and also to $\mathbb{Z}[\frac{1}{v}]$.

M.9. Let R denote the ring of Gauss integers, and let W be the R-submodule of $V = R^2$ generated by the columns of a 2×2 matrix with coefficients in R. Explain how to determine the index $[V: W]$.

M.10. Let f and g be polynomials in $\mathbb{C}[x, y]$ with no common factor. Prove that the ring $R = \mathbb{C}[x, y]/(f, g)$ is a finite-dimensional vector space over $\mathbb{C}$.

M.11. (*Berlekamp's method*) The problem here is to factor efficiently in $\mathbb{F}_2[x]$. Solving linear equations and finding a greatest common divisor are easy compared with factoring. The derivative f' of a polynomial f is computed using the rule from calculus, but working modulo 2. Prove:

(a) (*square factors*) The derivative f' is a square, and $f' = 0$ if and only if f is a square. Moreover, $\gcd(f, f')$ is the product of powers of the square factors of f.

(b) (*relatively prime factors*) Let n be the degree of f. If $f = uv$, where u and v are relatively prime, the Chinese Remainder Theorem shows that there is a polynomial g of degree at most n such that $g^2 - g \equiv 0$ modulo f, and g can be found by solving a system of linear equations. Either $\gcd(f, g)$ or $\gcd(f, g - 1)$ will be a proper factor of f.

(c) Use this method to factor $x^9 + x^6 + x^4 + 1$.