irreducibles which are not associates in R since $i \notin R$, and $4 = 2 \cdot 2 = (-2i) \cdot (2i)$ has two distinct factorizations in R. One may also check directly that $2i$ is irreducible but not prime in R (since $R/(2i) \cong \mathbb{Z}/4\mathbb{Z}$). In the larger ring of Gaussian integers, $\mathbb{Z}[i]$, (which is a Unique Factorization Domain) 2 and $2i$ *are* associates since i is a unit in this larger ring. We shall give a slightly different proof that $\mathbb{Z}[2i]$ is not a Unique Factorization Domain at the end of Section 9.3 (one in which we do not have to check that 2 and $2i$ are irreducibles).

(5) The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is another example of an integral domain that is not a Unique Factorization Domain, since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ gives two distinct factorizations of 6 into irreducibles. The principal ideal (6) in $\mathbb{Z}[\sqrt{-5}]$ can be written as a product of 4 nonprincipal prime ideals: $(6) = P_2^2 P_3 P_3'$ and the two distinct factorizations of the element 6 in $\mathbb{Z}[\sqrt{-5}]$ can be interpreted as arising from two rearrangements of this product of ideals into products of principal ideals: the product of $P_2^2 = (2)$ with $P_3 P_3' = (3)$, and the product of $P_2 P_3 = (1 + \sqrt{-5})$ with $P_2 P_3' = (1 - \sqrt{-5})$ (cf. Exercise 8).

While the *elements* of the quadratic integer ring $\mathcal{O}$ need not have unique factorization, it is a theorem (Corollary 16.16) that every *ideal* in $\mathcal{O}$ can be written uniquely as a product of prime *ideals*. The unique factorization of ideals into the product of prime ideals holds in general for rings of integers of algebraic number fields (examples of which are the quadratic integer rings) and leads to the notion of a Dedekind Domain considered in Chapter 16. It was the failure to have unique factorization into irreducibles for elements in algebraic integer rings in number theory that originally led to the definition of an ideal. The resulting uniqueness of the decomposition into prime ideals in these rings gave the elements of the ideals an "ideal" (in the sense of "perfect" or "desirable") behavior that is the basis for the choice of terminology for these (now fundamental) algebraic objects.

The first property of irreducible elements in a Unique Factorization Domain is that they are also primes. One might think that we could deduce Proposition 11 from this proposition together with the previously mentioned theorem (that we shall prove shortly) that every Principal Ideal Domain is a Unique Factorization Domain, however Proposition 11 will be used in the proof of the latter theorem.

Proposition 12. In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.

Proof: Let R be a Unique Factorization Domain. Since by Proposition 10, primes of R are irreducible it remains to prove that each irreducible element is a prime. Let p be an irreducible in R and assume $p \mid ab$ for some $a, b \in R$; we must show that p divides either a or b. To say that p divides ab is to say $ab = pc$ for some c in R. Writing a and b as a product of irreducibles, we see from this last equation and from the *uniqueness* of the decomposition into irreducibles of ab that the irreducible element p must be *associate* to one of the irreducibles occurring either in the factorization of a or in the factorization of b. We may assume that p is associate to one of the irreducibles in the factorization of a, i.e., that a can be written as a product $a = (up)p_2 \cdots p_n$ for u a unit and some (possibly empty set of) irreducibles $p_2, \ldots, p_n$. But then p divides a, since $a = pd$ with $d = up_2 \cdots p_n$, completing the proof.

In a Unique Factorization Domain we shall now use the terms "prime" and "irreducible" interchangeably although we shall usually refer to the "primes" in $\mathbb{Z}$ and the "irreducibles" in $F[x]$.

We shall use the preceding proposition to show that in a Unique Factorization Domain any two nonzero elements a and b have a greatest common divisor:

Proposition 13. Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose

$$a = up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n} \qquad \text{and} \qquad b = vp_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are *distinct* and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\cdots p_n^{\min(e_n,f_n)}$$

(where $d = 1$ if all the exponents are 0) is a greatest common divisor of a and b.

Proof: Since the exponents of each of the primes occurring in d are no larger than the exponents occurring in the factorizations of both a and b, d divides both a and b. To show that d is a greatest common divisor, let c be any common divisor of a and b and let $c = q_1^{g_1}q_2^{g_2}\cdots q_m^{g_m}$ be the prime factorization of c. Since each q_i divides c, hence divides a and b, we see from the preceding proposition that q_i must divide one of the primes p_j. In particular, up to associates (so up to multiplication by a unit) the primes occurring in c must be a subset of the primes occurring in a and b: $\{q_1, q_2, \ldots, q_m\} \subseteq \{p_1, p_2, \ldots, p_n\}$. Similarly, the exponents for the primes occurring in c must be no larger than those occurring in d. This implies that c divides d, completing the proof.

Example

In the example above, where $a = 2210$ and $b = 1131$, we find immediately from their prime factorizations that $(a, b) = 13$. Note that if the prime factorizations for a and b are known, the proposition above gives their greatest common divisor instantly, but that finding these prime factorizations is extremely time-consuming computationally. The Euclidean Algorithm is the fastest method for determining the g.c.d. of two integers but unfortunately it gives almost no information on the prime factorizations of the integers.

We now come to one of the principal results relating some of the rings introduced in this chapter.

Theorem 14. Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

Proof: Note that the second assertion follows from the first since Euclidean Domains are Principal Ideal Domains. To prove the first assertion let R be a Principal Ideal Domain and let r be a nonzero element of R which is not a unit. We must show first that r can be written as a finite product of irreducible elements of R and then we must verify that this decomposition is unique up to units.

The method of proof of the first part is precisely analogous to the determination of the prime factor decomposition of an integer. Assume r is nonzero and is not a unit. If r is itself irreducible, then we are done. If not, then by definition r can be written as a product $r = r_1 r_2$ where neither r_1 nor r_2 is a unit. If both these elements are irreducibles, then again we are done, having written r as a product of irreducible elements. Otherwise, at least one of the two elements, say r_1 is reducible, hence can be written as a product of two nonunit elements $r_1 = r_{11} r_{12}$, and so forth. What we must verify is that this process *terminates*, i.e., that we must necessarily reach a point where all of the elements obtained as factors of r are irreducible. Suppose this is not the case. From the factorization $r = r_1 r_2$ we obtain a *proper* inclusion of ideals: $(r) \subset (r_1) \subset R$. The first inclusion is proper since r_2 is not a unit, and the last inclusion is proper since r_1 is not a unit. From the factorization of r_1 we similarly obtain $(r) \subset (r_1) \subset (r_{11}) \subset R$. If this process of factorization did not terminate after a finite number of steps, then we would obtain an *infinite ascending chain* of ideals:

$$(r) \subset (r_1) \subset (r_{11}) \subset \cdots \subset R$$

where all containments are proper, and the Axiom of Choice ensures that an infinite chain exists (cf. Appendix I).

We now show that any ascending chain $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ of ideals in a Principal Ideal Domain eventually becomes stationary, i.e., there is some positive integer n such that $I_k = I_n$ for all $k \geq n$.[3] In particular, it is not possible to have an infinite ascending chain of ideals where all containments are proper. Let $I = \cup_{i=1}^{\infty} I_i$. It follows easily (as in the proof of Proposition 11 in Section 7.4) that I is an ideal. Since R is a Principal Ideal Domain it is principally generated, say $I = (a)$. Since I is the union of the ideals above, a must be an element of one of the ideals in the chain, say $a \in I_n$. But then we have $I_n \subseteq I = (a) \subseteq I_n$ and so $I = I_n$ and the chain becomes stationary at I_n. This proves that every nonzero element of R which is not a unit has some factorization into irreducibles in R.

It remains to prove that the above decomposition is essentially unique. We proceed by induction on the number, n, of irreducible factors in some factorization of the element r. If $n = 0$, then r is a unit. If we had $r = qc$ (some other factorization) for some irreducible q, then q would divide a unit, hence would itself be a unit, a contradiction. Suppose now that n is at least 1 and that we have two products

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \qquad m \geq n$$

for r where the p_i and q_j are (not necessarily distinct) irreducibles. Since then p_1 divides the product on the right, we see by Proposition 11 that p_1 must divide one of the factors. Renumbering if necessary, we may assume p_1 divides q_1. But then $q_1 = p_1 u$ for some element u of R which must in fact be a unit since q_1 is irreducible. Thus p_1 and q_1 are associates. Cancelling p_1 (recall we are in an integral domain, so this is legitimate), we obtain the equation

$$p_2 \cdots p_n = u q_2 q_3 \cdots q_m = q_2' q_3 \cdots q_m \qquad m \geq n.$$

[3]This same argument can be used to prove the more general statement: an ascending chain of ideals becomes stationary in any commutative ring where all the ideals are *finitely generated*. This result will be needed in Chapter 12 where the details will be repeated.