(ii) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1} \mid a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

5. Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}\,]$. Define the ideals $I_2 = (2, 1 + \sqrt{-5}\,)$, $I_3 = (3, 2 + \sqrt{-5}\,)$, and $I_3' = (3, 2 - \sqrt{-5}\,)$.
   (a) Prove that I_2, I_3, and I_3' are nonprincipal ideals in R. [Note that Example 2 following Proposition 1 proves this for I_3.]
   (b) Prove that the product of two nonprincipal ideals can be principal by showing that I_2^2 is the principal ideal generated by 2, i.e., $I_2^2 = (2)$.
   (c) Prove similarly that $I_2 I_3 = (1-\sqrt{-5}\,)$ and $I_2 I_3' = (1+\sqrt{-5}\,)$ are principal. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.

6. Let R be an integral domain and suppose that every *prime* ideal in R is principal. This exercise proves that every ideal of R is principal, i.e., R is a P.I.D.
   (a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]
   (b) Let I be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let $I_b = (I, b)$ be the ideal generated by I and b, and define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.
   (c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_a J$ is principal, a contradiction, and conclude that R is a P.I.D.

7. An integral domain R in which every ideal generated by two elements is principal (i.e., for every $a, b \in R$, $(a, b) = (d)$ for some $d \in R$) is called a *Bezout Domain*. [cf. also Exercise 11 in Section 3.]
   (a) Prove that the integral domain R is a Bezout Domain if and only if every pair of elements a, b of R has a g.c.d. d in R that can be written as an R-linear combination of a and b, i.e., $d = ax + by$ for some $x, y \in R$.
   (b) Prove that every finitely generated ideal of a Bezout Domain is principal. [cf. the exercises in Sections 9.2 and 9.3 for Bezout Domains in which not every ideal is principal.]
   (c) Let F be the fraction field of the Bezout Domain R. Prove that every element of F can be written in the form a/b with $a, b \in R$ and a and b relatively prime (cf. Exercise 1).

8. Prove that if R is a Principal Ideal Domain and D is a multiplicatively closed subset of R, then $D^{-1}R$ is also a P.I.D. (cf. Section 7.5).

8.3 UNIQUE FACTORIZATION DOMAINS (U.F.D.s)

In the case of the integers $\mathbb{Z}$, there is another method for determining the greatest common divisor of two elements a and b familiar from elementary arithmetic, namely the notion of "factorization into primes" for a and b, from which the greatest common divisor can easily be determined. This can also be extended to a larger class of rings called Unique Factorization Domains (U.F.D.s) — these will be defined shortly. We shall then prove that

every Principal Ideal Domain is a Unique Factorization Domain so that every result about Unique Factorization Domains will automatically hold for both Euclidean Domains and Principal Ideal Domains.

We first introduce some terminology.

Definition. Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and is not a unit. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be *reducible*.

(2) The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.

(3) Two elements a and b of R differing by a unit are said to be *associate* in R (i.e., $a = ub$ for some unit u in R).

Proposition 10. In an integral domain a prime element is always irreducible.

Proof: Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so by definition of prime ideal one of a or b, say a, is in (p). Thus $a = pr$ for some r. This implies $p = ab = prb$ so $rb = 1$ and b is a unit. This shows that p is irreducible.

It is not true in general that an irreducible element is necessarily prime. For example, consider the element 3 in the quadratic integer ring $R = \mathbb{Z}[\sqrt{-5}\,]$. The computations in Section 1 show that 3 is irreducible in R, but 3 is not a prime since $(2+\sqrt{-5}\,)(2-\sqrt{-5}\,) = 3^2$ is divisible by 3, but neither $2+\sqrt{-5}$ nor $2-\sqrt{-5}$ is divisible by 3 in R.

If R is a Principal Ideal Domain however, the notions of prime and irreducible elements are the same. In particular these notions coincide in $\mathbb{Z}$ and in $F[x]$ (where F is a field).

Proposition 11. In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.

Proof: We have shown above that prime implies irreducible. We must show conversely that if p is irreducible, then p is a prime, i.e., the ideal (p) is a prime ideal. If M is any ideal containing (p) then by hypothesis $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = rm$ for some r. But p is irreducible so by definition either r or m is a unit. This means either $(p) = (m)$ or $(m) = (1)$, respectively. Thus the only ideals containing (p) are (p) or (1), i.e., (p) is a maximal ideal. Since maximal ideals are prime ideals, the proof is complete.

Example

Proposition 11 gives another proof that the quadratic integer ring $\mathbb{Z}[\sqrt{-5}\,]$ is not a P.I.D. since 3 is irreducible but not prime in this ring.

The irreducible elements in the integers $\mathbb{Z}$ are the prime numbers (and their negaves) familiar from elementary arithmetic, and two integers a and b are associates of ne another if and only if $a = \pm b$.

In the integers $\mathbb{Z}$ any integer n can be written as a product of primes (not necessarily stinct), as follows. If n is not itself a prime then by definition it is possible to write $= n_1 n_2$ for two other integers n_1 and n_2 neither of which is a unit, i.e., neither of hich is ± 1. Both n_1 and n_2 must be smaller in absolute value than n itself. If they are oth primes, we have already written n as a product of primes. If one of n_1 or n_2 is not ime, then it in turn can be factored into two (smaller) integers. Since integers cannot ecrease in absolute value indefinitely, we must at some point be left only with prime teger factors, and so we have written n as a product of primes. .

For example, if $n = 2210$, the algorithm above proceeds as follows: n is not self prime, since we can write $n = 2 \cdot 1105$. The integer 2 is a prime, but 1105 is not: $105 = 5 \cdot 221$. The integer 5 is prime, but 221 is not: $221 = 13 \cdot 17$. Here the algorithm rminates, since both 13 and 17 are primes. This gives the *prime factorization* of 2210 ; $2210 = 2 \cdot 5 \cdot 13 \cdot 17$. Similarly, we find $1131 = 3 \cdot 13 \cdot 29$. In these examples each ime occurs only to the first power, but of course this need not be the case generally.

In the ring $\mathbb{Z}$ not only is it true that every integer n can be written as a product of imes, but in fact this decomposition is *unique* in the sense that any two prime fac-rizations of the same positive integer n differ only in the order in which the positive ime factors are written. The restriction to positive integers is to avoid considering e factorizations (3)(5) and (−3)(−5) of 15 as essentially distinct. This *unique fac-rization* property of $\mathbb{Z}$ (which we shall prove very shortly) is extremely useful for the ithmetic of the integers. General rings with the analogous property are given a name.

efinition. A *Unique Factorization Domain* (U.F.D.) is an integral domain R in which ery nonzero element $r \in R$ which is not a unit has the following two properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and

(ii) the decomposition in (i) is *unique up to associates*: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \dots, n$.

xamples

(1) A field F is trivially a Unique Factorization Domain since every nonzero element is a unit, so there are no elements for which properties (i) and (ii) must be verified.

(2) As indicated above, we shall prove shortly that every Principal Ideal Domain is a Unique Factorization Domain (so, in particular, $\mathbb{Z}$ and $F[x]$ where F is a field are both Unique Factorization Domains).

(3) We shall also prove in the next chapter that the ring $R[x]$ of polynomials is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain (in contrast to the properties of being a Principal Ideal Domain or being a Euclidean Domain, which do not carry over from a ring R to the polynomial ring $R[x]$). This result together with the preceding example will show that $\mathbb{Z}[x]$ is a Unique Factorization Domain.

(4) The subring of the Gaussian integers $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$, where $i^2 = -1$, is an integral domain but not a Unique Factorization Domain (rings of this nature were introduced in Exercise 23 of Section 7.1). The elements 2 and $2i$ are