11. If N is the ideal of all nilpotent elements in a commutative ring R (see Exercise 1), then R/N is a ring with no nonzero nilpotent elements.

12. Let R be a ring without identity and with no zero divisors. Let S be the ring whose additive group is $R \times \mathbf{Z}$ as in the proof of Theorem 1.10. Let $A = \{(r,n) \in S \mid rx + nx = 0 \text{ for every } x \in R\}$.
    (a) A is an ideal in S.
    (b) S/A has an identity and contains a subring isomorphic to R.
    (c) S/A has no zero divisors.

13. Let $f : R \to S$ be a homomorphism of rings, I an ideal in R, and J an ideal in S.
    (a) $f^{-1}(J)$ is an ideal in R that contains $\operatorname{Ker} f$.
    (b) If f is an epimorphism, then $f(I)$ is an ideal in S. If f is not surjective, $f(I)$ need not be an ideal in S.

14. If P is an ideal in a not necessarily commutative ring R, then the following conditions are equivalent.
    (a) P is a prime ideal.
    (b) If $r,s \in R$ are such that $rRs \subset P$, then $r \in P$ or $s \in P$. [*Hint:* If (a) holds and $rRs \subset P$, then $(RrR)(RsR) \subset P$, whence $RrR \subset P$ or $RsR \subset P$, say $RrR \subset P$. If $A = (r)$, then $A^3 \subset RrR \subset P$, whence $r \in A \subset P$.]
    (c) If (r) and (s) are principal ideals of R such that $(r)(s) \subset P$, then $r \in P$ or $s \in P$.
    (d) If U and V are right ideals in R such that $UV \subset P$, then $U \subset P$ or $V \subset P$.
    (e) If U and V are left ideals in R such that $UV \subset P$, then $U \subset P$ or $V \subset P$.

15. The set consisting of zero and all zero divisors in a commutative ring with identity contains at least one prime ideal.

16. Let R be a commutative ring with identity and suppose that the ideal A of R is contained in a finite union of prime ideals $P_1 \cup \cdots \cup P_n$. Show that $A \subset P_i$ for some i. [*Hint:* otherwise one may assume that $A \cap P_j \not\subset \bigcup_{i \neq j} P_i$ for all j. Let $a_j \in (A \cap P_j) - (\bigcup_{i \neq j} P_i)$. Then $a_1 + a_2a_3 \cdots a_n$ is in A but not in $P_1 \cup \cdots \cup P_n$.]

17. Let $f : R \to S$ be an epimorphism of rings with kernel K.
    (a) If P is a prime ideal in R that contains K, then $f(P)$ is a prime ideal in S [see Exercise 13].
    (b) If Q is a prime ideal in S, then $f^{-1}(Q)$ is a prime ideal in R that contains K.
    (c) There is a one-to-one correspondence between the set of all prime ideals in R that contain K and the set of all prime ideals in S, given by $P \mapsto f(P)$.
    (d) If I is an ideal in a ring R, then every prime ideal in R/I is of the form P/I, where P is a prime ideal in R that contains I.

18. An ideal $M \neq R$ in a commutative ring R with identity is maximal if and only if for every $r \in R - M$, there exists $x \in R$ such that $1_R - rx \in M$.

19. The ring E of even integers contains a maximal ideal M such that E/M is *not* a field.

20. In the ring $\mathbf{Z}$ the following conditions on a nonzero ideal I are equivalent: (i) I is prime; (ii) I is maximal; (iii) $I = (p)$ with p prime.

21. Determine all prime and maximal ideals in the ring Z_m.

22. (a) If $R_1, \ldots, R_n$ are rings with identity and I is an ideal in $R_1 \times \cdots \times R_n$, then $I = A_1 \times \cdots \times A_m$, where each A_i is an ideal in R_i. [*Hint:* Given I let $A_k = \pi_k(I)$, where $\pi_k : R_1 \times \cdots \times R_n \to R_k$ is the canonical epimorphism.]
    (b) Show that the conclusion of (a) need not hold if the rings R_i do not have identities.

23. An element e in a ring R is said to be **idempotent** if $e^2 = e$. An element of the center of the ring R is said to be **central.** If e is a central idempotent in a ring R with identity, then
    (a) $1_R - e$ is a central idempotent;
    (b) eR and $(1_R - e)R$ are ideals in R such that $R = eR \times (1_R - e)R$.

24. Idempotent elements $e_1, \ldots, e_n$ in a ring R [see Exercise 23] are said to be **orthogonal** if $e_ie_j = 0$ for $i \neq j$. If $R, R_1, \ldots, R_n$ are rings with identity, then the following conditions are equivalent:
    (a) $R \cong R_1 \times \cdots \times R_n$.
    (b) R contains a set of orthogonal central idempotents [Exercise 23] $\{e_1, \ldots, e_n\}$ such that $e_1 + e_2 + \cdots + e_n = 1_R$ and $e_iR \cong R_i$ for each i.
    (c) R is the internal direct product $R = A_1 \times \cdots \times A_n$ where each A_i is an ideal of R such that $A_i \cong R_i$.
    [*Hint:* (a) $\Rightarrow$ (b) The elements $\bar{e}_1 = (1_{R_1}, 0, \ldots, 0)$, $\bar{e}_2 = (0, 1_{R_2}, 0, \ldots, 0), \ldots, \bar{e}_n = (0, \ldots, 0, 1_{R_n})$ are orthogonal central idempotents in $S = R_1 \times \cdots \times R_n$ such that $\bar{e}_1 + \cdots + \bar{e}_n = 1_S$ and $\bar{e}_iS \cong R_i$. (b) $\Rightarrow$ (c) Note that $A_k = e_kR$ is the principal ideal (e_k) in R and that e_kR is itself a ring with identity e_k.]

25. If $m \in \mathbf{Z}$ has a prime decomposition $m = p_1^{k_1} \cdots p_t^{k_t}$ ($k_i > 0$; p_i distinct primes), then there is an isomorphism of rings $Z_m \cong Z_{p_1^{k_1}} \times \cdots \times Z_{p_t^{k_t}}$. [*Hint:* Corollary 2.27.]

26. If $R = \mathbf{Z}$, $A_1 = (6)$ and $A_2 = (4)$, then the map $\theta : R/A_1 \cap A_2 \to R/A_1 \times R/A_2$ of Corollary 2.27 is not surjective.

3. FACTORIZATION IN COMMUTATIVE RINGS

In this section we extend the concepts of divisibility, greatest common divisor and prime in the ring of integers to arbitrary commutative rings and study those integral domains in which an analogue of the Fundamental Theorem of Arithmetic (Introduction, Theorem 6.7) holds. The chief result is that every principal ideal domain is such a unique factorization domain. In addition we study those commutative rings in which an analogue of the division algorithm is valid (Euclidean rings).

Definition 3.1. *A nonzero element* a *of a commutative ring* R *is said to* **divide** *an element* b ∈ R (*notation:* a | b) *if there exists* x ∈ R *such that* ax = b. *Elements* a,b *of* R *are said to be* **associates** *if* a | b *and* b | a.

Virtually all statements about divisibility may be phrased in terms of principal ideals as we now see.

Theorem 3.2. *Let* a,b *and* u *be elements of a commutative ring* R *with identity.*

(i) a | b *if and only if* (b) $\subset$ (a).
(ii) a *and* b *are associates if and only if* (a) = (b).
(iii) u *is a unit if and only if* u | r *for all* r $\in$ R.
(iv) u *is a unit if and only if* (u) = R.
(v) *The relation* "a *is an associate of b*" *is an equivalence relation on* R.
(vi) *If* a = br *with* r $\in$ R *a unit, then* a *and* b *are associates. If* R *is an integral domain, the converse is true.*

PROOF. Exercise; Theorem 2.5(v) may be helpful for (i) and (ii). ■

Definition 3.3. *Let* R *be a commutative ring with identity. An element* c *of* R *is* **irreducible** *provided that:*

(i) c *is a nonzero nonunit;*
(ii) c = ab $\Rightarrow$ a *or* b *is a unit.*

An element p *of* R *is* **prime** *provided that:*

(i) p *is a nonzero nonunit;*
(ii) p | ab $\Rightarrow$ p | a *or* p | b.

EXAMPLES. If p is an ordinary prime integer, then both p and $-p$ are irreducible and prime in **Z** in the sense of Definition 3.3. In the ring Z_6, 2 is easily seen to be a prime. However $2 \in Z_6$ is not irreducible since $2 = 2 \cdot 4$ and neither 2 nor 4 are units in Z_6 (indeed they are zero divisors). For an example of an irreducible element which is not prime, see Exercise 3.

There is a close connection between prime [resp. irreducible] elements in a ring R and prime [resp. maximal] principal ideals in R.

Theorem 3.4. *Let* p *and* c *be nonzero elements in an integral domain* R.

(i) p *is prime if and only if* (p) *is nonzero prime ideal;*
(ii) c *is irreducible if and only if* (c) *is maximal in the set* S *of all proper principal ideals of R.*
(iii) *Every prime element of* R *is irreducible.*
(iv) *If* R *is a principal ideal domain, then* p *is prime if and only if* p *is irreducible.*
(v) *Every associate of an irreducible* [*resp. prime*] *element of* R *is irreducible* [*resp. prime*].
(vi) *The only divisors of an irreducible element of* R *are its associates and the units of* R.

REMARK. Several parts of Theorem 3.4 are true for any commutative ring with identity, as is seen in the following proof.

SKETCH OF PROOF OF 3.4. (i) Use Definition 3.3 and Theorem 2.15. (ii) If c is irreducible then (c) is a proper ideal of R by Theorem 3.2. If $(c) \subset (d)$, then $c = dx$. Since c is irreducible either d is a unit (whence $(d) = R$) or x is a unit (whence $(c) = (d)$ by Theorem 3.2). Hence (c) is maximal in S. Conversely if (c) is maximal in S, then c is a (nonzero) nonunit in R by Theorem 3.2. If $c = ab$, then $(c) \subset (a)$, whence $(c) = (a)$ or $(a) = R$. If $(a) = R$, then a is a unit (Theorem 3.2). If $(c) = (a)$, then $a = cy$ and hence $c = ab = cyb$. Since R is an integral domain $1 = yb$, whence b is a unit. Therefore, c is irreducible. (iii) If $p = ab$, then $p \mid a$ or $p \mid b$; say $p \mid a$. Then $px = a$ and $p = ab = pxb$, which implies that $1 = xb$. Therefore, b is a unit. (iv) If p is irreducible, use (ii), Theorem 2.19 and (i) to show that p is prime. (v) If c is irreducible and d is an associate of c, then $c = du$ with $u \in R$ a unit (Theorem 3.2). If $d = ab$, then $c = abu$, whence a is a unit or bu is a unit. But if bu is a unit, so is b. Hence d is irreducible. (vi) If c is irreducible and $a \mid c$, then $(c) \subset (a)$, whence $(c) = (a)$ or $(a) = R$ by (ii). Therefore, a is either an associate of c or a unit by Theorem 3.2. ■

We have now developed the analogues in an arbitrary integral domain of the concepts of divisibility and prime integers in the ring **Z**. Recall that every element in **Z** is a product of a finite number of irreducible elements (prime integers or their negatives) according to the Fundamental Theorem of Arithmetic (Introduction, Theorem 6.7). Furthermore this factorization is essentially unique (except for the order of the irreducible factors). Consequently, **Z** is an example of:

Definition 3.5. *An integral domain* R *is a* **unique factorization domain** *provided that:*

(i) *every nonzero nonunit element* a *of* R *can be written* $a = c_1c_2 \cdots c_n$, *with* $c_1, \ldots, c_n$ *irreducible.*
(ii) *If* $a = c_1c_2 \cdots c_n$ *and* $a = d_1d_2 \cdots d_m$ (c_i, d_i *irreducible*), *then* n = m *and for some permutation* σ *of* $\{1,2, \ldots, n\}$, c_i *and* $d_{\sigma(i)}$ *are associates for every* i.

REMARK. Every irreducible element in a unique factorization domain is necessarily prime by (ii). Consequently, irreducible and prime elements coincide by Theorem 3.4 (iii).

Definition 3.5 is nontrivial in the sense that there are integral domains in which every element is a finite product of irreducible elements, but this factorization is not unique (that is, Definition 3.5 (ii) fails to hold); see Exercise 4. Indeed one of the historical reasons for introducing the concept of *ideal* was to obtain some sort of unique factorization theorems (for ideals) in rings of algebraic integers in which factorization of elements was not necessarily unique; see Chapter VIII.

In view of the relationship between irreducible elements and principal ideals (Theorem 3.4) and the example of the integers, it seems plausible that every principal ideal domain is a unique factorization domain. In order to prove that this is indeed the case we need:

Lemma 3.6. *If* R *is a principal ideal ring and* $(a_1) \subset (a_2) \subset \cdots$ *is a chain of ideals in* R, *then for some positive integer* n, $(a_j) = (a_n)$ *for all* $j \geq n$.

Theorem 3.2. *Let* a,b *and* u *be elements of a commutative ring* R *with identity.*

(i) a | b *if and only if* (b) $\subset$ (a).
(ii) a *and* b *are associates if and only if* (a) = (b).
(iii) u *is a unit if and only if* u | r *for all* r $\in$ R.
(iv) u *is a unit if and only if* (u) = R.
(v) *The relation* "a *is an associate of b*" *is an equivalence relation on* R.
(vi) *If* a = br *with* r $\in$ R *a unit, then* a *and* b *are associates. If* R *is an integral domain, the converse is true.*

PROOF. Exercise; Theorem 2.5(v) may be helpful for (i) and (ii). ■

Definition 3.3. *Let* R *be a commutative ring with identity. An element* c *of* R *is* **irreducible** *provided that:*

(i) c *is a nonzero nonunit;*
(ii) c = ab $\Rightarrow$ a *or* b *is a unit.*

An element p *of* R *is* **prime** *provided that:*

(i) p *is a nonzero nonunit;*
(ii) p | ab $\Rightarrow$ p | a *or* p | b.

EXAMPLES. If p is an ordinary prime integer, then both p and $-p$ are irreducible and prime in **Z** in the sense of Definition 3.3. In the ring Z_6, 2 is easily seen to be a prime. However $2 \in Z_6$ is not irreducible since $2 = 2 \cdot 4$ and neither 2 nor 4 are units in Z_6 (indeed they are zero divisors). For an example of an irreducible element which is not prime, see Exercise 3.

There is a close connection between prime [resp. irreducible] elements in a ring R and prime [resp. maximal] principal ideals in R.

Theorem 3.4. *Let* p *and* c *be nonzero elements in an integral domain* R.

(i) p *is prime if and only if* (p) *is nonzero prime ideal;*
(ii) c *is irreducible if and only if* (c) *is maximal in the set* S *of all proper principal ideals of R.*
(iii) *Every prime element of* R *is irreducible.*
(iv) *If* R *is a principal ideal domain, then* p *is prime if and only if* p *is irreducible.*
(v) *Every associate of an irreducible* [*resp. prime*] *element of* R *is irreducible* [*resp. prime*].
(vi) *The only divisors of an irreducible element of* R *are its associates and the units of* R.

REMARK. Several parts of Theorem 3.4 are true for any commutative ring with identity, as is seen in the following proof.

SKETCH OF PROOF OF 3.4. (i) Use Definition 3.3 and Theorem 2.15. (ii) If c is irreducible then (c) is a proper ideal of R by Theorem 3.2. If $(c) \subset (d)$, then $c = dx$. Since c is irreducible either d is a unit (whence $(d) = R$) or x is a unit (whence $(c) = (d)$ by Theorem 3.2). Hence (c) is maximal in S. Conversely if (c) is maximal in S, then c is a (nonzero) nonunit in R by Theorem 3.2. If $c = ab$, then $(c) \subset (a)$, whence $(c) = (a)$ or $(a) = R$. If $(a) = R$, then a is a unit (Theorem 3.2). If $(c) = (a)$, then $a = cy$ and hence $c = ab = cyb$. Since R is an integral domain $1 = yb$, whence b is a unit. Therefore, c is irreducible. (iii) If $p = ab$, then $p \mid a$ or $p \mid b$; say $p \mid a$. Then $px = a$ and $p = ab = pxb$, which implies that $1 = xb$. Therefore, b is a unit. (iv) If p is irreducible, use (ii), Theorem 2.19 and (i) to show that p is prime. (v) If c is irreducible and d is an associate of c, then $c = du$ with $u \in R$ a unit (Theorem 3.2). If $d = ab$, then $c = abu$, whence a is a unit or bu is a unit. But if bu is a unit, so is b. Hence d is irreducible. (vi) If c is irreducible and $a \mid c$, then $(c) \subset (a)$, whence $(c) = (a)$ or $(a) = R$ by (ii). Therefore, a is either an associate of c or a unit by Theorem 3.2. ■

We have now developed the analogues in an arbitrary integral domain of the concepts of divisibility and prime integers in the ring **Z**. Recall that every element in **Z** is a product of a finite number of irreducible elements (prime integers or their negatives) according to the Fundamental Theorem of Arithmetic (Introduction, Theorem 6.7). Furthermore this factorization is essentially unique (except for the order of the irreducible factors). Consequently, **Z** is an example of:

Definition 3.5. *An integral domain* R *is a* **unique factorization domain** *provided that:*

(i) *every nonzero nonunit element* a *of* R *can be written* $a = c_1c_2 \cdots c_n$, *with* $c_1, \ldots, c_n$ *irreducible.*
(ii) *If* $a = c_1c_2 \cdots c_n$ *and* $a = d_1d_2 \cdots d_m$ (c_i, d_i *irreducible*), *then* n = m *and for some permutation* σ *of* $\{1,2, \ldots, n\}$, c_i *and* $d_{\sigma(i)}$ *are associates for every* i.

REMARK. Every irreducible element in a unique factorization domain is necessarily prime by (ii). Consequently, irreducible and prime elements coincide by Theorem 3.4 (iii).

Definition 3.5 is nontrivial in the sense that there are integral domains in which every element is a finite product of irreducible elements, but this factorization is not unique (that is, Definition 3.5 (ii) fails to hold); see Exercise 4. Indeed one of the historical reasons for introducing the concept of *ideal* was to obtain some sort of unique factorization theorems (for ideals) in rings of algebraic integers in which factorization of elements was not necessarily unique; see Chapter VIII.

In view of the relationship between irreducible elements and principal ideals (Theorem 3.4) and the example of the integers, it seems plausible that every principal ideal domain is a unique factorization domain. In order to prove that this is indeed the case we need:

Lemma 3.6. *If* R *is a principal ideal ring and* $(a_1) \subset (a_2) \subset \cdots$ *is a chain of ideals in* R, *then for some positive integer* n, $(a_j) = (a_n)$ *for all* $j \geq n$.

PROOF. Let $A = \bigcup_{i\geq 1} (a_i)$. We claim that A is an ideal. If $b,c \in A$, then $b \in (a_i)$ and $c \in (a_j)$. Either $i \leq j$ or $i \geq j$; say $i \geq j$. Consequently $(a_j) \subset (a_i)$ and $b,c \in (a_i)$. Since (a_i) is an ideal $b - c \in (a_i) \subset A$. Similarly if $r \in R$ and $b \in A$, then $b \in (a_i)$, whence $rb \in (a_i) \subset A$ and $br \in (a_i) \subset A$. Therefore, A is an ideal by Theorem 2.2. By hypothesis A is principal, say $A = (a)$. Since $a \in A = \bigcup(a_i)$, $a \in (a_n)$ for some n. By Definition 2.4 $(a) \subset (a_n)$. Therefore, for every $j \geq n$, $(a) \subset (a_n) \subset (a_j) \subset A = (a)$, whence $(a_j) = (a_n)$. ■

Theorem 3.7. *Every principal ideal domain* R *is a unique factorization domain.*

REMARK. The converse of Theorem 3.7 is false. For example the polynomial ring $\mathbf{Z}[x]$ can be shown to be a unique factorization domain (Theorem 6.14 below), but $\mathbf{Z}[x]$ is not a principal ideal domain (Exercise 6.1).

SKETCH OF PROOF OF 3.7. Let S be the set of all nonzero nonunit elements of R which cannot be factored as a finite product of irreducible elements. We shall first show that S is empty, whence every nonzero nonunit element of R has at least one factorization as a finite product of irreducibles. Suppose S is not empty and $a \in S$. Then (a) is a proper ideal by Theorem 3.2(iv) and is contained in a maximal ideal (c) by Theorem 2.18. The element $c \in R$ is irreducible by Theorem 3.4(ii). Since $(a) \subset (c)$, c divides a. Therefore, it is possible to choose for each $a \in S$ an irreducible divisor c_a of a (Axiom of Choice). Since R is an integral domain, c_a uniquely determines a nonzero $x_a \in R$ such that $c_a x_a = a$. We claim that $x_a \in S$. For if x_a were a unit, then $a = c_a x_a$ would be irreducible by Theorems 3.2(vi) and 3.4(v). If x_a is a nonunit and not in S, then x_a has a factorization as a product of irreducibles, whence a also does. Since $a \in S$ this is a contradiction. Hence $x_a \in S$. Furthermore, we claim that the ideal (a) is properly contained in the ideal (x_a). Since $x_a \mid a$, $(a) \subset (x_a)$ by Theorem 3.2(i). But $(a) = (x_a)$ implies that $x_a = ay$ for some $y \in R$, whence $a = x_a c_a = ayc_a$ and $1 = yc_a$. This contradicts the fact that c_a is irreducible (and hence a nonunit). Therefore $(a) \subsetneq (x_a)$.

The preceding remarks show that the function $f : S \to S$ given by $f(a) = x_a$ is well defined. By the Recursion Theorem 6.2 of the Introduction (with $f = f_n$ for all n) there exists a function $\varphi : \mathbf{N} \to S$ such that

$$\varphi(0) = a \quad \text{and} \quad \varphi(n+1) = f(\varphi(n)) = x_{\varphi(n)} \ (n \geq 0).$$

If we denote $\varphi(n)$ by a_n, we thus have a sequence of elements of S: $a, a_1, a_2, \ldots$ such that

$$a_1 = x_a;\ a_2 = x_{a_1};\ \cdots;\ a_{n+1} = x_{a_n};\ \cdots.$$

Consequently, the preceding paragraph shows that there is an ascending chain of ideals

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots,$$

contradicting Lemma 3.6. Therefore, the set S must be empty, whence every nonzero nonunit element in R has a factorization as a finite product of irreducibles.

Finally if $c_1 c_2 \cdots c_n = a = d_1 d_2 \cdots d_m$ (c_i, d_i irreducible), then c_1 divides some d_i by Theorem 3.4(iv). Since c_1 is a nonunit, it must be an associate of d_i by Theorem 3.4 (vi). The proof of uniqueness is now completed by a routine inductive argument. ■

Several important integral domains that we shall meet frequently have certain properties not shared by all integral domains.

Definition 3.8. *Let* N *be the set of nonnegative integers and* R *a commutative ring.* R *is a* **Euclidean ring** *if there is a function* $\varphi : \mathrm{R} - \{0\} \to \mathbf{N}$ *such that:*

(i) *if* $\mathrm{a,b} \in \mathrm{R}$ *and* $\mathrm{ab} \neq 0$, *then* $\varphi(\mathrm{a}) \leq \varphi(\mathrm{ab})$;
(ii) *if* $\mathrm{a,b} \in \mathrm{R}$ *and* $\mathrm{b} \neq 0$, *then there exist* $\mathrm{q,r} \in \mathrm{R}$ *such that* $\mathrm{a} = \mathrm{qb} + \mathrm{r}$ *with* $\mathrm{r} = 0$, *or* $\mathrm{r} \neq 0$ *and* $\varphi(\mathrm{r}) < \varphi(\mathrm{b})$.

A Euclidean ring which is an integral domain is called a **Euclidean domain.**

EXAMPLE. The ring $\mathbf{Z}$ of integers with $\varphi(x) = |x|$ is a Euclidean domain.

EXAMPLE. If F is a field, let $\varphi(x) = 1$ for all $x \in F$, $x \neq 0$. Then F is a Euclidean domain.

EXAMPLE. If F is a field, then the ring of polynomials in one variable $F[x]$ is a Euclidean domain with $\varphi(f) =$ degree of f; see Corollary 6.4 below.

EXAMPLE. Let $\mathbf{Z}[i]$ be the following subset of the complex numbers $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$. $\mathbf{Z}[i]$ is an integral domain called the domain of **Gaussian integers.** Define $\varphi(a + bi) = a^2 + b^2$. Clearly $\varphi(a + bi) \neq 0$ if $a + bi \neq 0$; it is also easy to show that condition (i) of the definition is satisfied. The proof that φ satisfies condition (ii) is left to the reader (Exercise 6).

Theorem 3.9. *Every Euclidean ring* R *is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.*

REMARK. The converse of Theorem 3.9 is false since there are principal ideal domains that are not Euclidean domains (Exercise 8).

PROOF OF 3.9. If I is a nonzero ideal in R, choose $a \in I$ such that $\varphi(a)$ is the least integer in the set of nonnegative integers $\{\varphi(x) \mid x \neq 0;\ x \in I\}$. If $b \in I$, then $b = qa + r$ with $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(a)$. Since $b \in I$ and $qa \in I$, r is necessarily in I. Since $\varphi(r) < \varphi(a)$ would contradict the choice of a, we must have $r = 0$, whence $b = qa$. Consequently, by Theorem 2.5 $I \subset Ra \subset (a) \subset I$. Therefore $I = Ra = (a)$ and R is a principal ideal ring.

Since R itself is an ideal, $R = Ra$ for some $a \in R$. Consequently, $a = ea = ae$ for some $e \in R$. If $b \in R = Ra$, then $b = xa$ for some $x \in R$. Therefore, $be = (xa)e = x(ae) = xa = b$, whence e is a multiplicative identity element for R. The last statement of the theorem is now an immediate consequence of Theorem 3.7. ■

We close this section with some further observations on divisibility that will be used occasionally in the sequel (Sections 5, 6 and IV.6).

Definition 3.10. *Let* X *be a nonempty subset of a commutative ring* R. *An element* d ∈ R *is a* **greatest common divisor** *of* X *provided:*

(i) d | a *for all* a ∈ X;
(ii) c | a *for all* a ∈ X ⇒ c | d.

Greatest common divisors do not always exist. For example, in the ring E of even integers 2 has no divisors at all, whence 2 and 4 have no (greatest) common divisor. Even when a greatest common divisor of $a_1, \ldots, a_n$ exists, it need not be unique. However, any two greatest common divisors of X are clearly associates by (ii). Furthermore any associate of a greatest common divisor of X is easily seen to be a greatest common divisor of X. If R has an identity and $a_1, a_2, \ldots, a_n$ have 1_R as a greatest common divisor, then $a_1, a_2, \ldots a_n$ are said to be **relatively prime.**

Theorem 3.11. *Let* $a_1, \ldots, a_n$ *be elements of a commutative ring* R *with identity.*

(i) d ∈ R *is a greatest common divisor of* $\{a_1, \ldots, a_n\}$ *such that* $d = r_1a_1 + \cdots + r_na_n$ *for some* $r_i \in R$ *if and only if* $(d) = (a_1) + (a_2) + \cdots + (a_n)$;

(ii) *if* R *is a principal ideal ring, then a greatest common divisor of* $a_1, \ldots, a_n$ *exists and every one is of the form* $r_1a_1 + \cdots + r_na_n$ $(r_i \in R)$;

(iii) *if* R *is a unique factorization domain, then there exists a greatest common divisor of* $a_1, \ldots, a_n$.

REMARK. Theorem 3.11(i) does *not* state that every greatest common divisor of $a_1, \ldots, a_n$ is expressible as a linear combination of $a_1, \ldots, a_n$. In general this is not the case (Exercise 6.15). See also Exercise 12.

SKETCH OF PROOF OF 3.11. (i) Use Definition 3.10 and Theorem 2.5. (ii) follows from (i). (iii) Each a_i has a factorization: $a_i = c_1^{m_{i1}}c_2^{m_{i2}} \cdots c_t^{m_{it}}$ with $c_1, \ldots, c_t$ distinct irreducible elements and each $m_{ij} \geq 0$. Show that $d = c_1^{k_1}c_2^{k_2} \cdots c_t^{k_t}$ is a greatest common divisor of $a_1, \ldots, a_n$, where $k_j = \min\{m_{1j}, m_{2j}, m_{3j}, \ldots, m_{nj}\}$. ∎

EXERCISES

1. A nonzero ideal in a principal ideal domain is maximal if and only if it is prime.

2. An integral domain R is a unique factorization domain if and only if every nonzero prime ideal in R contains a nonzero principal ideal that is prime.

3. Let R be the subring $\{a + b\sqrt{10} \mid a,b \in \mathbf{Z}\}$ of the field of real numbers.
   (a) The map $N : R \to \mathbf{Z}$ given by $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ is such that $N(uv) = N(u)N(v)$ for all $u,v \in R$ and $N(u) = 0$ if and only if $u = 0$.
   (b) u is a unit in R if and only if $N(u) = \pm 1$.
   (c) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are irreducible elements of R.
   (d) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are not prime elements of R. [*Hint:* $3 \cdot 2 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$.]

4. Show that in the integral domain of Exercise 3 every element can be factored into a product of irreducibles, but this factorization need not be unique (in the sense of Definition 3.5 (ii)).

5. Let R be a principal ideal domain.
   (a) Every proper ideal is a product $P_1P_2 \cdots P_n$ of maximal ideals, which are uniquely determined up to order.
   (b) An ideal P in R is said to be primary if $ab \in P$ and $a \notin P$ imply $b^n \in P$ for some n. Show that P is primary if and only if for some n, $P = (p^n)$, where $p \in R$ is prime (= irreducible) or $p = 0$.
   (c) If $P_1, P_2, \ldots, P_n$ are primary ideals such that $P_i = (p_i^{n_i})$ and the p_i are distinct primes, then $P_1P_2 \cdots P_n = P_1 \cap P_2 \cap \cdots \cap P_n$.
   (d) Every proper ideal in R can be expressed (uniquely up to order) as the intersection of a finite number of primary ideals.

6. (a) If a and n are integers, $n > 0$, then there exist integers q and r such that $a = qn + r$, where $|r| \leq n/2$.
   (b) The Gaussian integers $\mathbf{Z}[i]$ form a Euclidean domain with $\varphi(a + bi) = a^2 + b^2$. [*Hint:* to show that Definition 3.8(ii) holds, first let $y = a + bi$ and assume x is a positive integer. By part (a) there are integers such that $a = q_1x + r_1$ and $b = q_2x + r_2$, with $|r_1| \leq x/2$, $|r_2| \leq x/2$. Let $q = q_1 + q_2i$ and $r = r_1 + r_2i$; then $y = qx + r$, with $r = 0$ or $\varphi(r) < \varphi(x)$. In the general case, observe that for $x = c + di \neq 0$ and $\bar{x} = c - di$, $x\bar{x} > 0$. There are $q, r_0 \in \mathbf{Z}[i]$ such that $y\bar{x} = q(x\bar{x}) + r_0$, with $r_0 = 0$ or $\varphi(r_0) < \varphi(x\bar{x})$. Let $r = y - qx$; then $y = qx + r$ and $r = 0$ or $\varphi(r) < \varphi(x)$.]

7. What are the units in the ring of Gaussian integers $\mathbf{Z}[i]$?

8. Let R be the following subring of the complex numbers: $R = \{a + b(1 + \sqrt{19}\, i)/2 \mid a,b \in \mathbf{Z}\}$. Then R is a principal ideal domain that is not a Euclidean domain.

9. Let R be a unique factorization domain and d a nonzero element of R. There are only a finite number of distinct principal ideals that contain the ideal (d). [*Hint:* $(d) \subset (k) \Rightarrow k \mid d$.]

10. If R is a unique factorization domain and $a,b \in R$ are relatively prime and $a \mid bc$, then $a \mid c$.

11. Let R be a Euclidean ring and $a \in R$. Then a is a unit in R if and only if $\varphi(a) = \varphi(1_R)$.

12. Every nonempty set of elements (possibly infinite) in a commutative principal ideal ring with identity has a greatest common divisor.

13. (Euclidean algorithm). Let R be a Euclidean domain with associated function $\varphi : R - \{0\} \to \mathbf{N}$. If $a,b \in R$ and $b \neq 0$, here is a method for finding the greatest common divisor of a and b. By repeated use of Definition 3.8(ii) we have:

$$\begin{aligned}
a &= q_0b + r_1, && \text{with } r_1 = 0 \text{ or } \varphi(r_1) < \varphi(b);\\
b &= q_1r_1 + r_2, && \text{with } r_2 = 0 \text{ or } \varphi(r_2) < \varphi(r_1);\\
r_1 &= q_2r_2 + r_3, && \text{with } r_3 = 0 \text{ or } \varphi(r_3) < \varphi(r_2);\\
&\vdots\\
r_k &= q_{k+1}r_{k+1} + r_{k+2}, && \text{with } r_{k+2} = 0 \text{ or } \varphi(r_{k+2}) < \varphi(r_{k+1});\\
&\vdots
\end{aligned}$$

Let $r_0 = b$ and let n be the least integer such that $r_{n+1} = 0$ (such an n exists since the $\varphi(r_k)$ form a strictly decreasing sequence of nonnegative integers). Show that r_n is the greatest common divisor a and b.

4. RINGS OF QUOTIENTS AND LOCALIZATION

In the first part of this section the familiar construction of the field of rational numbers from the ring of integers is considerably generalized. The rings of quotients so constructed from any commutative ring are characterized by a universal mapping property (Theorem 4.5). The last part of this section, which is referred to only occasionally in the sequel, deals with the (prime) ideal structure of rings of quotients and introduces localization at a prime ideal.

Definition 4.1. *A nonempty subset* S *of a ring* R *is* **multiplicative** *provided that*

$$a,b \in S \Rightarrow ab \in S.$$

EXAMPLES. The set S of all elements in a nonzero ring with identity that are not zero divisors is multiplicative. In particular, the set of all nonzero elements in an integral domain is multiplicative. The set of units in any ring with identity is a multiplicative set. If P is a prime ideal in a commutative ring R, then both P and $S = R - P$ are multiplicative sets by Theorem 2.15.

The motivation for what follows may be seen most easily in the ring $\mathbf{Z}$ of integers and the field $\mathbf{Q}$ of rational numbers. The set S of all nonzero integers is clearly a multiplicative subset of $\mathbf{Z}$. Intuitively the field $\mathbf{Q}$ is thought of as consisting of all fractions a/b with $a \in \mathbf{Z}$ and $b \in S$, subject to the requirement

$$a/b = c/d \Leftrightarrow ad = bc \text{ (or } ad - bc = 0).$$

More precisely, $\mathbf{Q}$ may be constructed as follows (details of the proof will be supplied later). The relation on the set $\mathbf{Z} \times S$ defined by

$$(a,b) \sim (c,d) \Leftrightarrow ad - bc = 0$$

is easily seen to be an equivalence relation. $\mathbf{Q}$ is defined to be the set of equivalence classes of $\mathbf{Z} \times S$ under this equivalence relation. The equivalence class of (a,b) is denoted a/b and addition and multiplication are defined in the usual way. One verifies that these operations are well defined and that $\mathbf{Q}$ is a field. The map $\mathbf{Z} \to \mathbf{Q}$ given by $a \mapsto a/1$ is easily seen to be a monomorphism (embedding).

We shall now extend the construction just outlined to an arbitrary multiplicative subset of any commutative ring R (possibly without identity). We shall construct a commutative ring $S^{-1}R$ with identity and a homomorphism $\varphi_S : R \to S^{-1}R$. If S is the set of all nonzero elements in an integral domain R, then $S^{-1}R$ will be a field ($S^{-1}R = \mathbf{Q}$ if $R = \mathbf{Z}$) and φ_S will be a monomorphism embedding R in $S^{-1}R$.

Theorem 4.2. *Let* S *be a multiplicative subset of a commutative ring* R. *The relation defined on the set* $R \times S$ *by*

$$(r,s) \sim (r',s') \Leftrightarrow s_1(rs' - r's) = 0 \text{ for some } s_1 \in S$$

is an equivalence relation. Furthermore if R *has no zero divisors and* $0 \notin S$, *then*

$$(r,s) \sim (r',s') \Leftrightarrow rs' - r's = 0.$$

PROOF. Exercise. ■

Let S be a multiplicative subset of a commutative ring R and $\sim$ the equivalence relation of Theorem 4.2. The equivalence class of $(r,s) \in R \times S$ will be denoted r/s. The set of all equivalence classes of $R \times S$ under $\sim$ will be denoted by $S^{-1}R$. Verify that

(i) $r/s = r'/s' \Leftrightarrow s_1(rs' - r's) = 0$ for some $s_1 \in S$;
(ii) $tr/ts = r/s$ for all $r \in R$ and $s,t \in S$;
(iii) If $0 \in S$, then $S^{-1}R$ consists of a single equivalence class.

Theorem 4.3. *Let* S *be a multiplicative subset of a commutative ring* R *and let* $S^{-1}R$ *be the set of equivalence classes of* $R \times S$ *under the equivalence relation of Theorem* 4.2.

(i) $S^{-1}R$ *is a commutative ring with identity, where addition and multiplication are defined by*

$$r/s + r'/s' = (rs' + r's)/ss' \quad \text{and} \quad (r/s)(r'/s') = rr'/ss'.$$

(ii) *If* R *is a nonzero ring with no zero divisors and* $0 \notin S$, *then* $S^{-1}R$ *is an integral domain.*

(iii) *If* R *is a nonzero ring with no zero divisors and* S *is the set of all nonzero elements of* R, *then* $S^{-1}R$ *is a field.*

SKETCH OF PROOF. (i) Once we know that addition and multiplication in $S^{-1}R$ are well-defined binary operations (independent of the choice of r,s,r',s'), the rest of the proof of (i) is routine. In particular, for all $s,s' \in S$, $0/s = 0/s'$ and $0/s$ is the additive identity. The additive inverse of r/s is $-r/s$. For any $s,s' \in S$, $s/s = s'/s'$ and s/s is the multiplicative identity in $S^{-1}R$.

To show that addition is well defined, observe first that since S is multiplicative $(rs' + r's)/ss'$ is an element of $S^{-1}R$. If $r/s = r_1/s_1$ and $r'/s' = r_1'/s_1'$, we must show that $(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s_1'$. By hypothesis there exist $s_2,s_3 \in S$ such that

$$s_2(rs_1 - r_1s) = 0,$$
$$s_3(r's_1' - r_1's') = 0.$$

Multiply the first equation by $s_3s's_1'$ and the second by s_2ss_1. Add the resulting equations to obtain

$$s_2s_3[(rs' + r's)s_1s_1' - (r_1s_1' + r_1's_1)ss'] = 0.$$

Therefore, $(rs' + r's)/ss' = (r_1s_1' + r_1's_1)/s_1s_1'$ (since $s_2s_3 \in S$). The proof that multiplication is independent of the choice of r,s,r',s' is similar.

(ii) If R has no zero divisors and $0 \notin S$, then $r/s = 0/s$ if and only if $r = 0$ in R. Consequently, $(r/s)(r'/s') = 0$ in $S^{-1}R$ if and only if $rr' = 0$ in R. Since $rr' = 0$ if and only if $r = 0$ or $r' = 0$, it follows that $S^{-1}R$ is an integral domain. (iii) If $r \neq 0$, then the multiplicative inverse of $r/s \in S^{-1}R$ is $s/r \in S^{-1}R$. ■

The ring $S^{-1}R$ in Theorem 4.3 is called the **ring of quotients** or **ring of fractions** or **quotient ring** of R by S. An important special case occurs when S is the set of all nonzero elements in an integral domain R. Then $S^{-1}R$ is a field (Theorem 4.3(iii)) which is called the **quotient field of the integral domain** R. Thus if $R = \mathbf{Z}$, the quotient field is precisely the field $\mathbf{Q}$ of rational numbers. More generally suppose R is any nonzero commutative ring and S is the set of all nonzero elements of R that are *not* zero divisors. If S is nonempty (as is always the case if R has an identity), then $S^{-1}R$ is called the **complete** (or full) **ring of quotients** (or fractions) of the ring R.[3] Theorem 4.3 (iii) may be rephrased: if a nonzero ring R has no zero divisors, then the complete ring of quotients of R is a field. Clearly the complete ring of quotients of an integral domain is just its quotient field.

If $\varphi : \mathbf{Z} \to \mathbf{Q}$ is the map given by $n \mapsto n/1$, then φ is clearly a monomorphism that embeds $\mathbf{Z}$ in $\mathbf{Q}$. Furthermore, for every nonzero n, $\varphi(n)$ is a unit in $\mathbf{Q}$. More generally, we have:

Theorem 4.4. *Let* S *be a multiplicative subset of a commutative ring* R.

(i) *The map* $\varphi_S : R \to S^{-1}R$ *given by* $r \mapsto rs/s$ (*for any* $s \in S$) *is a well-defined homomorphism of rings such that* $\varphi_S(s)$ *is a unit in* $S^{-1}R$ *for every* $s \in S$.

(ii) *If* $0 \notin S$ *and* S *contains no zero divisors, then* φ_S *is a monomorphism. In particular, any integral domain may be embedded in its quotient field.*

(iii) *If* R *has an identity and* S *consists of units, then* φ_S *is an isomorphism. In particular, the complete ring of quotients* (= *quotient field*) *of a field* F *is isomorphic to* F.

SKETCH OF PROOF. (i) If $s,s' \in S$, then $rs/s = rs'/s'$, whence φ_S is well defined. Verify that φ_S is a ring homomorphism and that for each $s \in S$, $s/s^2 \in S^{-1}R$ is the multiplicative inverse of $s^2/s = \varphi_S(s)$. (ii) If $\varphi_S(r) = rs/s = 0$ in $S^{-1}R$, then $rs/s = 0/s$, whence $rs^2s_1 = 0$ for some $s_1 \in S$. Since $s^2s_1 \in S$, $s^2s_1 \neq 0$. Since S has no zero divisors, we must have $r = 0$. (iii) φ_S is a monomorphism by (ii). If $r/s \in S^{-1}R$ with s a unit in R, then $r/s = \varphi_S(rs^{-1})$, whence φ_S is an epimorphism. ■

In view of Theorem 4.4 (ii) it is customary to identify an integral domain R with its image under φ_S and to consider R as a subring of its quotient field. Since $1_R \in S$ in this case, $r \in R$ is thus identified with $r/1_R \in S^{-1}R$.

The next theorem shows that rings of quotients may be completely characterized by a universal mapping property. This theorem is sometimes used as a definition of the ring of quotients.

Theorem 4.5. *Let* S *be a multiplicative subset of a commutative ring* R *and let* T *be any commutative ring with identity. If* $f : R \to T$ *is a homomorphism of rings such that* f(s) *is a unit in* T *for all* $s \in S$, *then there exists a unique homomorphism of rings* $\bar{f} : S^{-1}R \to T$ *such that* $\bar{f}\varphi_S = f$. *The ring* $S^{-1}R$ *is completely determined* (*up to isomorphism*) *by this property.*

SKETCH OF PROOF. Verify that the map $\bar{f} : S^{-1}R \to T$ given by $\bar{f}(r/s) = f(r)f(s)^{-1}$ is a well-defined homomorphism of rings such that $\bar{f}\varphi_S = f$. If

[3]For the noncommutative analogue, see Definition IX.4.7.

$g : S^{-1}R \to T$ is another homomorphism such that $g\varphi_S = f$, then for every $s \in S$, $g(\varphi_S(s))$ is a unit in T. Consequently, $g(\varphi_S(s)^{-1}) = g(\varphi_S(s))^{-1}$ for every $s \in S$ by Exercise 1.15. Now for each $s \in S$, $\varphi_S(s) = s^2/s$, whence $\varphi_S(s)^{-1} = s/s^2 \in S^{-1}R$. Thus for each $r/s \in S^{-1}R$:

$$g(r/s) = g(\varphi_S(r)\varphi_S(s)^{-1}) = g(\varphi_S(r))g(\varphi_S(s)^{-1}) = g(\varphi_S(r))g(\varphi_S(s))^{-1}$$
$$= f(r)f(s)^{-1} = \bar{f}(r/s).$$

Therefore, $\bar{f} = g$.

To prove the last statement of the theorem let $\mathcal{C}$ be the category whose objects are all (f,T), where T is a commutative ring with identity and $f : R \to T$ a homomorphism of rings such that $f(s)$ is a unit in T for every $s \in S$. Define a morphism in $\mathcal{C}$ from (f_1,T_1) to (f_2,T_2) to be a homomorphism of rings $g : T_1 \to T_2$ such that $gf_1 = f_2$. Verify that $\mathcal{C}$ is a category and that a morphism g in $\mathcal{C}$ $(f_1,T_1) \to (f_2,T_2)$ is an equivalence if and only if $g : T_1 \to T_2$ is an isomorphism of rings. The preceding paragraph shows that $(\varphi_S, S^{-1}R)$ is a universal object in the category $\mathcal{C}$, whence $S^{-1}R$ is completely determined up to isomorphism by Theorem I.7.10. ■

Corollary 4.6. *Let* R *be an integral domain considered as a subring of its quotient field* F. *If* E *is a field and* $f : R \to E$ *a monomorphism of rings, then there is a unique monomorphism of fields* $\bar{f} : F \to E$ *such that* $\bar{f} \mid R = f$. *In particular any field* E_1 *containing* R *contains an isomorphic copy* F_1 *of* F *with* $R \subset F_1 \subset E_1$.

SKETCH OF PROOF. Let S be the set of all nonzero elements of R and apply Theorem 4.5 to $f : R \to E$. Then there is a homomorphism $\bar{f} : S^{-1}R = F \to E$ such that $\bar{f}\varphi_S = f$. Verify that $\bar{f}$ is a monomorphism. Since R is identified with $\varphi_S(R)$, this means that $\bar{f} \mid R = f$. The last statement of the theorem is the special case when $f : R \to E_1$ is the inclusion map. ■

Theorems 4.7-4.11 deal with the ideal structure of rings of quotients. This material will be used only in Section VIII.6. Theorem 4.13, which does not depend on Theorems 4.7-4.11, will be referred to in the sequel.

Theorem 4.7. *Let* S *be a multiplicative subset of a commutative ring* R.

(i) *If* I *is an ideal in* R, *then* $S^{-1}I = \{a/s \mid a \in I; s \in S\}$ *is an ideal in* $S^{-1}R$.

(ii) *If* J *is another ideal in* R, *then*

$$S^{-1}(I + J) = S^{-1}I + S^{-1}J;$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J);$$
$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J.$$

REMARKS. $S^{-1}I$ is called the **extension** of I in $S^{-1}R$. Note that $r/s \in S^{-1}I$ need not imply that $r \in I$ since it is possible to have $a/s = r/s$ with $a \in I$, $r \notin I$.

SKETCH OF PROOF OF 4.7. Use the facts that in $S^{-1}R$, $\sum_{i=1}^{n} (c_i/s) = \left(\sum_{i=1}^{n} c_i\right)/s$; $\sum_{j=1}^{m} (a_jb_j/s) = \sum_{j=1}^{m} (a_j/s)(b_js/s)$; and

$$\sum_{k=1}^{t}(c_k/s_k) = \left(\sum_{k=1}^{t} c_k s_1 s_2 \cdots s_{k-1} s_{k+1} \cdots s_t\right)/s_1 s_2 \cdots s_t. \quad \blacksquare$$

Theorem 4.8. *Let* S *be a multiplicative subset of a commutative ring* R *with identity and let* I *be an ideal of* R. *Then* $S^{-1}I = S^{-1}R$ *if and only if* $S \cap I \neq \varnothing$.

PROOF. If $s \in S \cap I$, then $1_{S^{-1}R} = s/s \in S^{-1}I$ and hence $S^{-1}I = S^{-1}R$. Conversely, if $S^{-1}I = S^{-1}R$, then $\varphi_S^{-1}(S^{-1}I) = R$ whence $\varphi_S(1_R) = a/s$ for some $a \in I$, $s \in S$. Since $\varphi_S(1_R) = 1_R s/s$ we have $s^2 s_1 = a s s_1$ for some $s_1 \in S$. But $s^2 s_1 \in S$ and $a s s_1 \in I$ imply $S \cap I \neq \varnothing$. $\blacksquare$

In order to characterize the prime ideals in a ring of quotients we need a lemma. Recall that if J is an ideal in a ring of quotients $S^{-1}R$, then $\varphi_S^{-1}(J)$ is an ideal in R (Exercise 2.13). $\varphi_S^{-1}(J)$ is sometimes called the **contraction** of J in R.

Lemma 4.9. *Let* S *be a multiplicative subset of a commutative ring* R *with identity and let* I *be an ideal in* R.

(i) $I \subset \varphi_S^{-1}(S^{-1}I)$.

(ii) *If* $I = \varphi_S^{-1}(J)$ *for some ideal* J *in* $S^{-1}R$, *then* $S^{-1}I = J$. *In other words every ideal in* $S^{-1}R$ *is of the form* $S^{-1}I$ *for some ideal* I *in* R.

(iii) *If* P *is a prime ideal in* R *and* $S \cap P = \varnothing$, *then* $S^{-1}P$ *is a prime ideal in* $S^{-1}R$ *and* $\varphi_S^{-1}(S^{-1}P) = P$.

PROOF. (i) If $a \in I$, then $as \in I$ for every $s \in S$. Consequently, $\varphi_S(a) = as/s \in S^{-1}I$, whence $a \in \varphi_S^{-1}(S^{-1}I)$. Therefore, $I \subset \varphi_S^{-1}(S^{-1}I)$. (ii) Since $I = \varphi_S^{-1}(J)$ every element of $S^{-1}I$ is of the form r/s with $\varphi_S(r) \in J$. Therefore, $r/s = (1_R/s)(rs/s) = (1_R/s)\varphi_S(r) \in J$, whence $S^{-1}I \subset J$. Conversely, if $r/s \in J$, then $\varphi_S(r) = rs/s = (r/s)(s^2/s) \in J$, whence $r \in \varphi_S^{-1}(J) = I$. Thus $r/s \in S^{-1}I$ and hence $J \subset S^{-1}I$. (iii) $S^{-1}P$ is an ideal such that $S^{-1}P \neq S^{-1}R$ by Theorem 4.8. If $(r/s)(r'/s') \in S^{-1}P$, then $rr'/ss' = a/t$ with $a \in P$, $t \in S$. Consequently, $s_1 t r r' = s_1 s s' a \in P$ for some $s_1 \in S$. Since $s_1 t \in S$ and $S \cap P = \varnothing$, Theorem 2.15 implies that $rr' \in P$, whence $r \in P$ or $r' \in P$. Thus $r/s \in S^{-1}P$ or $r'/s' \in S^{-1}P$. Therefore, $S^{-1}P$ is prime by Theorem 2.15. Finally $P \subset \varphi_S^{-1}(S^{-1}P)$ by (i). Conversely if $r \in \varphi_S^{-1}(S^{-1}P)$, then $\varphi_S(r) \in S^{-1}P$. Thus $\varphi_S(r) = rs/s = a/t$ with $a \in P$ and $s, t \in S$. Consequently, $s_1 s t r = s_1 s a \in P$ for some $s_1 \in S$. Since $s_1 s t \in S$ and $S \cap P = \varnothing$, $r \in P$ by Theorem 2.15. Therefore, $\varphi_S^{-1}(S^{-1}P) \subset P$. $\blacksquare$

Theorem 4.10. *Let* S *be a multiplicative subset of a commutative ring* R *with identity. Then there is a one-to-one correspondence between the set* $\mathfrak{U}$ *of prime ideals of* R *which are disjoint from* S *and the set* $\mathfrak{V}$ *of prime ideals of* $S^{-1}R$, *given by* $P \mapsto S^{-1}P$.

PROOF. By Lemma 4.9(iii) the assignment $P \mapsto S^{-1}P$ defines an injective map $\mathfrak{U} \to \mathfrak{V}$. We need only show that it is surjective as well. Let J be a prime ideal of $S^{-1}R$ and let $P = \varphi_S^{-1}(J)$. Since $S^{-1}P = J$ by Lemma 4.9(ii), it suffices to show that P is prime. If $ab \in P$, then $\varphi_S(a)\varphi_S(b) = \varphi_S(ab) \in J$ since $P = \varphi_S^{-1}(J)$. Since J is prime

in $S^{-1}R$, either $\varphi_S(a) \in J$ or $\varphi_S(b) \in J$ by Theorem 2.15. Consequently, either $a \in \varphi_S^{-1}(J) = P$ or $b \in P$. Therefore, P is prime by Theorem 2.15. $\blacksquare$

Let R be a commutative ring with identity and P a prime ideal of R. Then $S = R - P$ is a multiplicative subset of R by Theorem 2.15. The ring of quotients $S^{-1}R$ is called the **localization of R at P** and is denoted R_P. If I is an ideal in R, then the ideal $S^{-1}I$ in R_P is denoted I_P.

Theorem 4.11. *Let* P *be a prime ideal in a commutative ring* R *with identity.*

(i) *There is a one-to-one correspondence between the set of prime ideals of* R *which are contained in* P *and the set of prime ideals of* R_P, *given by* $Q \mapsto Q_P$;

(ii) *the ideal* P_P *in* R_P *is the unique maximal ideal of* R_P.

PROOF. Since the prime ideals of R contained in P are precisely those which are disjoint from $S = R - P$, (i) is an immediate consequence of Theorem 4.10. If M is a maximal ideal of R_P, then M is prime by Theorem 2.19, whence $M = Q_P$ for some prime ideal Q of R with $Q \subset P$. But $Q \subset P$ implies $Q_P \subset P_P$. Since $P_P \neq R_P$ by Theorem 4.8, we must have $Q_P = P_P$. Therefore, P_P is the unique maximal ideal in R_P. $\blacksquare$

Rings with a unique maximal ideal, such as R_P in Theorem 4.11, are of some interest in their own right.

Definition 4.12. *A* **local ring** *is a commutative ring with identity which has a unique maximal ideal.*

REMARK. Since every ideal in a ring with identity is contained in some maximal ideal (Theorem 2.18), the unique maximal ideal of a local ring R must contain every ideal of R (except of course R itself).

EXAMPLE. If p is prime and $n \geq 1$, then Z_{p^n} is a local ring with unique maximal ideal (p).

Theorem 4.13. *If* R *is a commutative ring with identity then the following conditions are equivalent.*

(i) R *is a local ring;*

(ii) *all nonunits of* R *are contained in some ideal* $M \neq R$;

(iii) *the nonunits of* R *form an ideal.*

SKETCH OF PROOF. If I is an ideal of R and $a \in I$, then $(a) \subset I$ by Theorem 2.5. Consequently, $I \neq R$ if and only if I consists only of nonunits (Theorem 3.2(iv)). (ii) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (i) follow from this fact. (i) $\Rightarrow$ (ii) If $a \in R$ is a nonunit, then $(a) \neq R$. Therefore, (a) (and hence a) is contained in the unique maximal ideal of R by the remark after Definition 4.12. $\blacksquare$

EXERCISES

1. Determine the complete ring of quotients of the ring Z_n for each $n \geq 2$.

2. Let S be a multiplicative subset of a commutative ring R with identity and let T be a multiplicative subset of the ring $S^{-1}R$. Let $S_* = \{r \in R \mid r/s \in T \text{ for some } s \in S\}$. Then S_* is a multiplicative subset of R and there is a ring isomorphism $S_*^{-1}R \cong T^{-1}(S^{-1}R)$.

3. (a) The set E of positive even integers is a multiplicative subset of $\mathbf{Z}$ such that $E^{-1}(\mathbf{Z})$ is the field of rational numbers.
(b) State and prove condition(s) on a multiplicative subset S of $\mathbf{Z}$ which insure that $S^{-1}\mathbf{Z}$ is the field of rationals.

4. If $S = \{2,4\}$ and $R = Z_6$, then $S^{-1}R$ is isomorphic to the field Z_3. Consequently, the converse of Theorem 4.3(ii) is false.

5. Let R be an integral domain with quotient field F. If T is an integral domain such that $R \subset T \subset F$, then F is (isomorphic to) the quotient field of T.

6. Let S be a multiplicative subset of an integral domain R such that $0 \notin S$. If R is a principal ideal domain [resp. unique factorization domain], then so is $S^{-1}R$.

7. Let R_1 and R_2 be integral domains with quotient fields F_1 and F_2 respectively. If $f : R_1 \to R_2$ is an isomorphism, then f extends to an isomorphism $F_1 \cong F_2$. [*Hint:* Corollary 4.6.]

8. Let R be a commutative ring with identity, I an ideal of R and $\pi : R \to R/I$ the canonical projection.
(a) If S is a multiplicative subset of R, then $\pi S = \pi(S)$ is a multiplicative subset of R/I.
(b) The mapping $\theta : S^{-1}R \to (\pi S)^{-1}(R/I)$ given by $r/s \mapsto \pi(r)/\pi(s)$ is a well-defined function.
(c) θ is a ring epimorphism with kernel $S^{-1}I$ and hence induces a ring isomorphism $S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I)$.

9. Let S be a multiplicative subset of a commutative ring R with identity. If I is an ideal in R, then $S^{-1}(\text{Rad } I) = \text{Rad } (S^{-1}I)$. [See Exercise 2.2.]

10. Let R be an integral domain and for each maximal ideal M (which is also prime, of course), consider R_M as a subring of the quotient field of R. Show that $\bigcap R_M = R$, where the intersection is taken over all maximal ideals M of R.

11. Let p be a prime in $\mathbf{Z}$; then (p) is a prime ideal. What can be said about the relationship of Z_p and the localization $\mathbf{Z}_{(p)}$?

12. A commutative ring with identity is local if and only if for all $r, s \in R$, $r + s = 1_R$ implies r or s is a unit.

13. The ring R consisting of all rational numbers with denominators not divisible by some (fixed) prime p is a local ring.

14. If M is a maximal ideal in a commutative ring R with identity and n is a positive integer, then the ring R/M^n has a unique prime ideal and therefore is local.

15. In a commutative ring R with identity the following conditions are equivalent: (i) R has a unique prime ideal; (ii) every nonunit is nilpotent (see Exercise 1.12); (iii) R has a minimal prime ideal which contains all zero divisors, and all nonunits of R are zero divisors.

16. Every nonzero homomorphic image of a local ring is local.

5. RINGS OF POLYNOMIALS AND FORMAL POWER SERIES

We begin by defining and developing notation for polynomials in one indeterminate over a ring R. Next the ring of polynomials in n indeterminates over R is defined and its basic properties are developed. The last part of the section, which is not needed in the sequel, is a brief introduction to the ring of formal power series in one indeterminate over R.

Theorem 5.1. *Let* R *be a ring and let* R[x] *denote the set of all sequences of elements of* R $(a_0,a_1, \ldots)$ *such that* $a_i = 0$ *for all but a finite number of indices* i.

(i) R[x] *is a ring with addition and multiplication defined by:*

$$(a_0,a_1, \ldots) + (b_0,b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

and

$$(a_0,a_1, \ldots)(b_0,b_1, \ldots) = (c_0,c_1, \ldots),$$

where

$$c_n = \sum_{i=0}^{n} a_{n-i}b_i = a_nb_0 + a_{n-1}b_1 + \cdots + a_1b_{n-1} + a_0b_n = \sum_{k+j=n} a_kb_j.$$

(ii) *If* R *is commutative* [*resp. a ring with identity or a ring with no zero divisors or an integral domain*], *then so is* R[x].

(iii) *The map* $R \to R[x]$ *given by* $r \mapsto (r,0,0, \ldots)$ *is a monomorphism of rings.*

PROOF. Exercise. If R has an identity 1_R, then $(1_R,0,0, \ldots)$ is an identity in $R[x]$. Observe that if $(a_0,a_1, \ldots), (b_0,b_1, \ldots) \in R[x]$ and k [resp. j] is the smallest index such that $a_k \neq 0$ [resp. $b_j \neq 0$], then

$$(a_0,a_1, \ldots)(b_0,b_1, \ldots) = (0, \ldots,0,a_kb_j,a_{k+1}b_j + a_kb_{j+1}, \ldots). \quad \blacksquare$$

The ring $R[x]$ of Theorem 5.1 is called the **ring of polynomials** over R. Its elements are called polynomials. The notation $R[x]$ is explained below. In view of Theorem 5.1(iii) we shall identify R with its isomorphic image in $R[x]$ and write $(r,0,0, \ldots)$ simply as r. Note that $r(a_0,a_1, \ldots) = (ra_0,ra_1, \ldots)$. We now develop a more familiar notation for polynomials.

Theorem 5.2. *Let* R *be a ring with identity and denote by* x *the element* $(0,1_R,0,0, \ldots)$ *of* R[x].

(i) $x^n = (0,0, \ldots,0,1_R,0, \ldots)$, *where* 1_R *is the* (n + 1)st *coordinate.*

(ii) *If* $r \in R$, *then for each* $n \geq 0$, $rx^n = x^nr = (0, \ldots,0,r,0, \ldots)$, *where* r *is the* (n + 1)st *coordinate.*