36. Show that if I is the ideal of all polynomials in $\mathbb{Z}[x]$ with zero constant term then $I^n = \{a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{n+m}x^{n+m} \mid a_i \in \mathbb{Z},\ m \geq 0\}$ is the set of polynomials whose first nonzero term has degree at least n.

37. An ideal N is called *nilpotent* if N^n is the zero ideal for some $n \geq 1$. Prove that the ideal $p\mathbb{Z}/p^m\mathbb{Z}$ is a nilpotent ideal in the ring $\mathbb{Z}/p^m\mathbb{Z}$.

7.4 PROPERTIES OF IDEALS

Throughout this section R is a ring with identity $1 \neq 0$.

Definition. Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called *the ideal generated by* A.

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$).
Similarly, $AR = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$ and $RAR = \{r_1a_1r_1' + r_2a_2r_2' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}^+\}$.

(3) An ideal generated by a single element is called a *principal ideal.*

(4) An ideal generated by a finite set is called a *finitely generated ideal.*

When $A = \{a\}$ or $\{a_1, a_2, \ldots\}$, etc., we shall drop the set brackets and simply write (a), $(a_1, a_2, \ldots)$ for (A), respectively.

The notion of ideals generated by subsets of a ring is analogous to that of subgroups generated by subsets of a group (Section 2.4). Since the intersection of any nonempty collection of ideals of R is also an ideal (cf. Exercise 18, Section 3) and A is always contained in at least one ideal (namely R), we have

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I\ ,$$

i.e., (A) is the intersection of all ideals of R that contain the set A.

The *left ideal generated by* A is the intersection of all left ideals of R that contain A. This left ideal is obtained from A by closing A under all the operations that define a left ideal. It is immediate from the definition that RA is closed under addition and under left multiplication by any ring element. Since R has an identity, RA contains A. Thus RA is a left ideal of R which contains A. Conversely, any left ideal which contains A must contain all finite sums of elements of the form ra, $r \in R$ and $a \in A$ and so must contain RA. Thus *RA is precisely the left ideal generated by A.* Similarly, *AR is the right ideal generated by A* and *RAR is the (two-sided) ideal generated by A.* In particular,

$$\textit{if } R \textit{ is commutative then } RA = AR = RAR = (A).$$

When R is a commutative ring and $a \in R$, the principal ideal (a) generated by a is just the set of all R-multiples of a. If R is not commutative, however, the set

$\{ras \mid r, s \in R\}$ is not necessarily the two-sided ideal generated by a since it need not be closed under addition (in this case the ideal generated by a is the ideal RaR, which consists of all *finite sums* of elements of the form ras, $r, s \in R$).

The formation of principal ideals in a commutative ring is a particularly simple way of creating ideals, similar to generating cyclic subgroups of a group. Notice that the element $b \in R$ belongs to the ideal (a) if and only if $b = ra$ for some $r \in R$, i.e., if and only if *b is a multiple of a* or, put another way, *a divides b in R*. Also, $b \in (a)$ if and only if $(b) \subseteq (a)$. Thus containment relations between ideals, in particular between principal ideals, is seen to capture some of the arithmetic of general commutative rings. Commutative rings in which all ideals are principal are among the easiest to study and these will play an important role in Chapters 8 and 9.

Examples

(1) The trivial ideal 0 and the ideal R are both principal: $0 = (0)$ and $R = (1)$.

(2) In $\mathbb{Z}$ we have $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$ for all integers n. Thus our notation for aR is consistent with the definition of $n\mathbb{Z}$ we have been using. As noted in the preceding section, these are all the ideals of $\mathbb{Z}$ so *every* ideal of $\mathbb{Z}$ is principal. For positive integers n and m, $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if m divides n in $\mathbb{Z}$, so the lattice of ideals containing $n\mathbb{Z}$ is the same as the lattice of divisors of n. Furthermore, the ideal generated by two nonzero integers n and m is the principal ideal generated by their greatest common divisor, d: $(n, m) = (d)$. The notation for (n, m) as the greatest common divisor of n and m is thus consistent with the same notation for the ideal generated by n and m (although a principal generator for the ideal generated by n and m is determined only up to a $\pm$ sign — we could make it unique by choosing a nonnegative generator). In particular, n and m are relatively prime if and only if $(n, m) = (1)$.

(3) We show that the ideal $(2, x)$ generated by 2 and x in $\mathbb{Z}[x]$ is *not* a principal ideal. Observe that $(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$ and so this ideal consists precisely of the polynomials with integer coefficients whose constant term is even (as discussed in Example 5 in the preceding section) — in particular, this is a proper ideal. Assume by way of contradiction that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Since $2 \in (a(x))$ there must be some $p(x)$ such that $2 = p(x)a(x)$. The degree of $p(x)a(x)$ equals degree $p(x)$ + degree $a(x)$, hence both $p(x)$ and $a(x)$ must be constant polynomials, i.e., integers. Since 2 is a prime number, $a(x)$, $p(x) \in \{\pm 1, \pm 2\}$. If $a(x)$ were ± 1 then every polynomial would be a multiple of $a(x)$, contrary to $(a(x))$ being a proper ideal. The only possibility is $a(x) = \pm 2$. But now $x \in (a(x)) = (2) = (-2)$ and so $x = 2q(x)$ for some polynomial $q(x)$ with integer coefficients, clearly impossible. This contradiction proves that $(2, x)$ is not principal.

Note that the symbol (A) is ambiguous if the ring is not specified: the ideal generated by 2 and x in $\mathbb{Q}[x]$ is the entire ring (1) since it contains the element $\frac{1}{2}2 = 1$.

We shall see in Chapter 9 that for any *field* F, all ideals of $F[x]$ *are* principal.

(4) If R is the ring of all functions from the closed interval $[0,1]$ into $\mathbb{R}$ let M be the ideal $\{f \mid f(\frac{1}{2}) = 0\}$ (the kernel of evaluation at $\frac{1}{2}$). Let $g(x)$ be the function which is zero at $x = \frac{1}{2}$ and 1 at all other points. Then $f = fg$ for all $f \in M$ so M is a principal ideal with generator g. In fact, *any* function which is zero at $\frac{1}{2}$ and nonzero at all other points is another generator for the same ideal M.

On the other hand, if R is the ring of all *continuous* functions from $[0,1]$ to $\mathbb{R}$ then $\{f \mid f(\frac{1}{2}) = 0\}$ is *not* principal nor is it even finitely generated (cf. the exercises).

(5) If G is a finite group and R is a commutative ring with 1 then the augmentation ideal is generated by the set $\{g - 1 \mid g \in G\}$, although this need not be a minimal set of generators. For example, if G is a cyclic group with generator σ, then the augmentation ideal is a principal ideal with generator $\sigma - 1$.

Proposition 9. Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Proof: (1) If $I = R$ then I contains the unit 1. Conversely, if u is a unit in I with inverse v, then for any $r \in R$

$$r = r \cdot 1 = r(vu) = (rv)u \in I$$

hence $R = I$.

(2) The ring R is a field if and only if every nonzero element is a unit. If R is a field every nonzero ideal contains a unit, so by the first part R is the only nonzero ideal. Conversely, if 0 and R are the only ideals of R let u be any nonzero element of R. By hypothesis $(u) = R$ and so $1 \in (u)$. Thus there is some $v \in R$ such that $1 = vu$, i.e., u is a unit. Every nonzero element of R is therefore a unit and so R is a field.

Corollary 10. If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Proof: The kernel of a ring homomorphism is an ideal. The kernel of a nonzero homomorphism is a proper ideal hence is 0 by the proposition.

These results show that the ideal structure of fields is trivial. Our approach to studying an algebraic structure through its homomorphisms will still play a fundamental role in field theory (Part IV) when we study injective homomorphisms (embeddings) of one field into another and automorphisms of fields (isomorphisms of a field to itself).

If D is a ring with identity $1 \neq 0$ in which the only left ideals and the only right ideals are 0 and D, then D is a division ring. Conversely, the only (left, right or two-sided) ideals in a division ring D are 0 and D, which gives an analogue of Proposition 9(2) if R is not commutative (see the exercises). However, if F is a field, then for any $n \geq 2$ the only two-sided ideals in the matrix ring $M_n(F)$ are 0 and $M_n(F)$, even though this is not a division ring (it does have proper, nontrivial, left and right ideals: cf. Section 3), which shows that Proposition 9(2) does not hold for noncommutative rings. Rings whose only two-sided ideals are 0 and the whole ring (which are called *simple rings*) will be studied in Chapter 18.

One important class of ideals are those which are not contained in any other proper ideal:

Definition. An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

A general ring need not have maximal ideals. For example, take any abelian group which has no maximal subgroups (for example, $\mathbb{Q}$ — cf. Exercise 16, Section 6.1) and make it into a trivial ring by defining $ab = 0$ for all a, b. In such a ring the ideals are simply the subgroups and so there are no maximal ideals. The zero ring has no maximal ideals, hence any result involving maximal ideals forces a ring to be nonzero. The next proposition shows that rings with an identity $1 \neq 0$ always possess maximal ideals. Like many such general existence theorems (e.g., the result that a finitely generated group has maximal subgroups or that every vector space has a basis) the proof relies on Zorn's Lemma (see Appendix I). In many specific rings, however, the presence of maximal ideals is often obvious, independent of Zorn's Lemma.

Proposition 11. In a ring with identity every proper ideal is contained in a maximal ideal.

Proof: Let R be a ring with identity and let I be a proper ideal (so R cannot be the zero ring, i.e., $1 \neq 0$). Let $\mathcal{S}$ be the set of all proper ideals of R which contain I. Then $\mathcal{S}$ is nonempty ($I \in \mathcal{S}$) and is partially ordered by inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, define J to be the union of all ideals in $\mathcal{C}$:

$$J = \bigcup_{A \in \mathcal{C}} A.$$

We first show that J is an ideal. Certainly J is nonempty because $\mathcal{C}$ is nonempty — specifically, $0 \in J$ since 0 is in every ideal A. If $a, b \in J$, then there are ideals $A, B \in \mathcal{C}$ such that $a \in A$ and $b \in B$. By definition of a chain either $A \subseteq B$ or $B \subseteq A$. In either case $a - b \in J$, so J is closed under subtraction. Since each $A \in \mathcal{C}$ is closed under left and right multiplication by elements of R, so is J. This proves J is an ideal.

If J is not a proper ideal then $1 \in J$. In this case, by definition of J we must have $1 \in A$ for some $A \in \mathcal{C}$. This is a contradiction because each A is a proper ideal ($A \in \mathcal{C} \subseteq \mathcal{S}$). This proves that each chain has an upper bound in $\mathcal{S}$. By Zorn's Lemma $\mathcal{S}$ has a maximal element which is therefore a maximal (proper) ideal containing I.

For commutative rings the next result characterizes maximal ideals by the structure of their quotient rings.

Proposition 12. Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof: This follows from the Lattice Isomorphism Theorem together with Proposition 9(2). The ideal M is maximal if and only if there are no ideals I with $M \subset I \subset R$. By the Lattice Isomorphism Theorem the ideals of R containing M correspond bijectively with the ideals of R/M, so M is maximal if and only if the only ideals of R/M are 0 and R/M. By Proposition 9(2) we see that M is maximal if and only if R/M is a field.

The proposition above indicates how to *construct* some fields: take the quotient of any commutative ring R with identity by a maximal ideal in R. We shall use this in Part IV to construct all finite fields by taking quotients of the ring $\mathbb{Z}[x]$ by maximal ideals.

Examples

(1) Let n be a nonnegative integer. The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is a maximal ideal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. We saw in Section 3 that this is the case if and only if n is a prime number. This also follows directly from the containment of ideals of $\mathbb{Z}$ described in Example 2 above.

(2) The ideal $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$ because its quotient ring is the field $\mathbb{Z}/2\mathbb{Z}$ — cf. Example 3 above and Example 5 at the end of Section 3.

(3) The ideal (x) in $\mathbb{Z}[x]$ is not a maximal ideal because $(x) \subset (2, x) \subset \mathbb{Z}[x]$. The quotient ring $\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}$ (the ideal (x) in $\mathbb{Z}[x]$ is the kernel of the surjective ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}$ given by evaluation at 0). Since $\mathbb{Z}$ is not a field, we see again that (x) is not a maximal ideal in $\mathbb{Z}[x]$.

(4) Let R be the ring of all functions from [0,1] to $\mathbb{R}$ and for each $a \in [0, 1]$ let M_a be the kernel of evaluation at a. Since evaluation is a surjective homomorphism from R to $\mathbb{R}$, we see that $R/M_a \cong \mathbb{R}$ and hence M_a is a maximal ideal. Similarly, the kernel of evaluation at any fixed point is a maximal ideal in the ring of continuous real valued functions on [0, 1].

(5) If F is a field and G is a finite group, then the augmentation ideal I is a maximal ideal of the group ring FG (cf. Example 7 at the end of the preceding section). The augmentation ideal is the kernel of the augmentation map which is a surjective homomorphism onto the field F (i.e., $FG/I \cong F$, a field). Note that Proposition 12 does not apply directly since FG need not be commutative, however, the implication in Proposition 12 that I is a maximal ideal if R/I is a field holds for arbitrary rings.

Definition. Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

The notion of a maximal ideal is fairly intuitive but the definition of a prime ideal may seem a little strange. It is, however, a natural generalization of the notion of a "prime" in the integers $\mathbb{Z}$. Let n be a nonnegative integer. According to the above definition the ideal $n\mathbb{Z}$ is a *prime* ideal provided $n \neq 1$ (to ensure that the ideal is proper) and provided every time the product ab of two integers is an element of $n\mathbb{Z}$, at least one of a, b is an element of $n\mathbb{Z}$. Put another way, if $n \neq 0$, it must have the property that whenever n divides ab, n must divide a or divide b. This is equivalent to the usual definition that n is a prime number. Thus *the prime ideals of $\mathbb{Z}$ are just the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ generated by prime numbers p together with the ideal 0.*

For the integers $\mathbb{Z}$ there is no difference between the maximal ideals and the nonzero prime ideals. This is not true in general, but we shall see shortly that every maximal ideal is a prime ideal. First we translate the notion of prime ideals into properties of quotient rings as we did for maximal ideals in Proposition 12. Recall that an integral domain is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

Proposition 13. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Proof: This proof is simply a matter of translating the definition of a prime ideal into the language of quotients. The ideal P is prime if and only if $P \neq R$ and whenever

$ab \in P$, then either $a \in P$ or $b \in P$. Use the bar notation for elements of R/P: $\bar{r} = r + P$. Note that $r \in P$ if and only if the element $\bar{r}$ is zero in the quotient ring R/P. Thus in the terminology of quotients P is a prime ideal if and only if $\bar{R} \neq \bar{0}$ and whenever $\overline{ab} = \bar{a}\bar{b} = \bar{0}$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$, i.e., R/P is an integral domain.

It follows in particular that a commutative ring with identity is an integral domain if and only if 0 is a prime ideal.

Corollary 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: If M is a maximal ideal then R/M is a field by Proposition 12. A field is an integral domain so the corollary follows from Proposition 13.

Examples

(1) The principal ideals generated by primes in $\mathbb{Z}$ are both prime and maximal ideals. The zero ideal in $\mathbb{Z}$ is prime but not maximal.

(2) The ideal (x) is a prime ideal in $\mathbb{Z}[x]$ since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. This ideal is not a maximal ideal. The ideal 0 is a prime ideal in $\mathbb{Z}[x]$, but is not a maximal ideal.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary entries in the j^{th} column and zero in all other entries and let E_{ij} be the element of $M_n(R)$ whose i, j entry is 1 and whose other entries are all 0. Prove that $L_j = M_n(R)E_{ij}$ for any i. [See Exercise 6, Section 2.]

2. Assume R is commutative. Prove that the augmentation ideal in the group ring RG is generated by $\{g - 1 \mid g \in G\}$. Prove that if $G = \langle \sigma \rangle$ is cyclic then the augmentation ideal is generated by $\sigma - 1$.

3. **(a)** Let p be a prime and let G be an abelian group of order p^n. Prove that the nilradical of the group ring $\mathbb{F}_p G$ is the augmentation ideal (cf. Exercise 29, Section 3). [Use the preceding exercise.]

(b) Let $G = \{g_1, \ldots, g_n\}$ be a finite group and assume R is commutative. Prove that if r is any element of the augmentation ideal of RG then $r(g_1 + \cdots + g_n) = 0$. [Use the preceding exercise.]

4. Assume R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

5. Prove that if M is an ideal such that R/M is a field then M is a maximal ideal (do not assume R is commutative).

6. Prove that R is a division ring if and only if its only left ideals are (0) and R. (The analogous result holds when "left" is replaced by "right.")

7. Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is a maximal ideal if and only if R is a field.

8. Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$, if and only if $a = ub$ for some unit u of R.

9. Let R be the ring of all continuous functions on $[0, 1]$ and let I be the collection of functions $f(x)$ in R with $f(1/3) = f(1/2) = 0$. Prove that I is an ideal of R but is not a prime ideal.

10. Assume R is commutative. Prove that if P is a prime ideal of R and P contains no zero divisors then R is an integral domain.

11. Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.

12. Assume R is commutative and suppose $I = (a_1, a_2, \ldots, a_n)$ and $J = (b_1, b_2, \ldots, b_m)$ are two finitely generated ideals in R. Prove that the product ideal IJ is finitely generated by the elements $a_i b_j$ for $i = 1, 2, \ldots, n$, and $j = 1, 2, \ldots, m$.

13. Let $\varphi : R \to S$ be a homomorphism of commutative rings.

(a) Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R.

(b) Prove that if M is a maximal ideal of S and φ is surjective then $\varphi^{-1}(M)$ is a maximal ideal of R. Give an example to show that this need not be the case if φ is not surjective.

14. Assume R is commutative. Let x be an indeterminate, let $f(x)$ be a monic polynomial in $R[x]$ of degree $n \geq 1$ and use the bar notation to denote passage to the quotient ring $R[x]/(f(x))$.

(a) Show that every element of $R[x]/(f(x))$ is of the form $\overline{p(x)}$ for some polynomial $p(x) \in R[x]$ of degree less than n, i.e.,

$$R[x]/(f(x)) = \{\overline{a_0} + \overline{a_1}\overline{x} + \cdots + \overline{a_{n-1}x^{n-1}} \mid a_0, a_1, \ldots, a_{n-1} \in R\}.$$

[If $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ then $\overline{x^n} = \overline{-(b_{n-1}x^{n-1} + \cdots + b_0)}$. Use this to reduce powers of $\overline{x}$ in the quotient ring.]

(b) Prove that if $p(x)$ and $q(x)$ are distinct polynomials in $R[x]$ which are both of degree less than n, then $\overline{p(x)} \neq \overline{q(x)}$. [Otherwise $p(x) - q(x)$ is an $R[x]$-multiple of the monic polynomial $f(x)$.]

(c) If $f(x) = a(x)b(x)$ where both $a(x)$ and $b(x)$ have degree less than n, prove that $\overline{a(x)}$ is a zero divisor in $R[x]/(f(x))$.

(d) If $f(x) = x^n - a$ for some nilpotent element $a \in R$, prove that $\overline{x}$ is nilpotent in $R[x]/(f(x))$.

(e) Let p be a prime, assume $R = \mathbb{F}_p$ and $f(x) = x^p - a$ for some $a \in \mathbb{F}_p$. Prove that $\overline{x - a}$ is nilpotent in $R[x]/(f(x))$. [Use Exercise 26(c) of Section 3.]

15. Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.

(a) Prove that $\overline{E}$ has 4 elements: $\overline{0}$, $\overline{1}$, $\overline{x}$ and $\overline{x+1}$.

(b) Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.

(c) Write out the 4×4 multiplication table for $\overline{E}$ and prove that $\overline{E}^\times$ is isomorphic to the cyclic group of order 3. Deduce that $\overline{E}$ is a field.

16. Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^4 - 16)$.

(a) Find a polynomial of degree ≤ 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $(x^4 - 16)$.

(b) Prove that $\overline{x - 2}$ and $\overline{x + 2}$ are zero divisors in $\overline{E}$.

17. Let $x^3 - 2x + 1$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^3 - 2x + 1)$. Let $p(x) = 2x^7 - 7x^5 + 4x^3 - 9x + 1$ and let $q(x) = (x - 1)^4$.

(a) Express each of the following elements of $\overline{E}$ in the form $\overline{f(x)}$ for some polynomial $f(x)$ of degree ≤ 2: $\overline{p(x)}$, $\overline{q(x)}$, $\overline{p(x)+q(x)}$ and $\overline{p(x)q(x)}$.
(b) Prove that $\overline{E}$ is not an integral domain.
(c) Prove that $\bar{x}$ is a unit in $\overline{E}$.

18. Prove that if R is an integral domain and $R[[x]]$ is the ring of formal power series in the indeterminate x then the principal ideal generated by x is a prime ideal (cf. Exercise 3, Section 2). Prove that the principal ideal generated by x is a maximal ideal if and only if R is a field.

19. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal.

20. Prove that a nonzero finite commutative ring that has no zero divisors is a field (if the ring has an identity, this is Corollary 3, so do not assume the ring has a 1).

21. Prove that a finite ring with identity $1 \neq 0$ that has no zero divisors is a field (you may quote Wedderburn's Theorem).

22. Let $p \in \mathbb{Z}^+$ be a prime and let the $\mathbb{F}_p$ Quaternions be defined by

$$a + bi + cj + dk \qquad a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$$

where addition is componentwise and multiplication is defined using the same relations on i, j, k as for the real Quaternions.
(a) Prove that the $\mathbb{F}_p$ Quaternions are a homomorphic image of the integral Quaternions (cf. Section 1).
(b) Prove that the $\mathbb{F}_p$ Quaternions contain zero divisors (and so they cannot be a division ring). [Use the preceding exercise.]

23. Prove that in a Boolean ring (cf. Exercise 15, Section 1) every prime ideal is a maximal ideal.

24. Prove that in a Boolean ring every finitely generated ideal is principal.

25. Assume R is commutative and for each $a \in R$ there is an integer $n > 1$ (depending on a) such that $a^n = a$. Prove that every prime ideal of R is a maximal ideal.

26. Prove that a prime ideal in a commutative ring R contains every nilpotent element (cf. Exercise 13, Section 1). Deduce that the nilradical of R (cf. Exercise 29, Section 3) is contained in the intersection of all the prime ideals of R. (It is shown in Section 15.2 that the nilradical of R is equal to the intersection of all prime ideals of R.)

27. Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

28. Prove that if R is a commutative ring and $N = (a_1, a_2, \ldots, a_m)$ where each a_i is a nilpotent element, then N is a nilpotent ideal (cf. Exercise 37, Section 3). Deduce that if the nilradical of R is finitely generated then it is a nilpotent ideal.

29. Let p be a prime and let G be a finite group of order a power of p (i.e., a p-group). Prove that the augmentation ideal in the group ring $\mathbb{Z}/p\mathbb{Z}G$ is a nilpotent ideal. (Note that this ring may be noncommutative.) [Use Exercise 2.]

30. Let I be an ideal of the commutative ring R and define

$$\text{rad } I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$$

called the *radical* of I. Prove that rad I is an ideal containing I and that $(\text{rad } I)/I$ is the nilradical of the quotient ring R/I, i.e., $(\text{rad } I)/I = \mathfrak{N}(R/I)$ (cf. Exercise 29, Section 3).

31. An ideal I of the commutative ring R is called a *radical ideal* if rad $I = I$.

(a) Prove that every prime ideal of R is a radical ideal.

(b) Let $n > 1$ be an integer. Prove that 0 is a radical ideal in $\mathbb{Z}/n\mathbb{Z}$ if and only if n is a product of distinct primes to the first power (i.e., n is square free). Deduce that (n) is a radical ideal of $\mathbb{Z}$ if and only if n is a product of distinct primes in $\mathbb{Z}$.

32. Let I be an ideal of the commutative ring R and define

$$\text{Jac } I \text{ to be the intersection of all maximal ideals of } R \text{ that contain } I$$

where the convention is that Jac $R = R$. (If I is the zero ideal, Jac 0 is called the *Jacobson radical* of the ring R, so Jac I is the preimage in R of the Jacobson radical of R/I.)

(a) Prove that Jac I is an ideal of R containing I.

(b) Prove that rad $I \subseteq$ Jac I, where rad I is the radical of I defined in Exercise 30.

(c) Let $n > 1$ be an integer. Describe Jac $n\mathbb{Z}$ in terms of the prime factorization of n.

33. Let R be the ring of all continuous functions from the closed interval [0,1] to $\mathbb{R}$ and for each $c \in [0, 1]$ let $M_c = \{f \in R \mid f(c) = 0\}$ (recall that M_c was shown to be a maximal ideal of R).

(a) Prove that if M is *any* maximal ideal of R then there is a real number $c \in [0, 1]$ such that $M = M_c$.

(b) Prove that if b and c are distinct points in [0,1] then $M_b \neq M_c$.

(c) Prove that M_c is not equal to the principal ideal generated by $x - c$.

(d) Prove that M_c is not a finitely generated ideal.

The preceding exercise shows that there is a bijection between the *points* of the closed interval [0,1] and the set of *maximal ideals* in the ring R of all of continuous functions on [0,1] given by $c \leftrightarrow M_c$. For any subset X of $\mathbb{R}$ or, more generally, for any completely regular topological space X, the map $c \mapsto M_c$ is an *injection* from X to the set of maximal ideals of R, where R is the ring of all bounded continuous real valued functions on X and M_c is the maximal ideal of functions that vanish at c. Let $\beta(X)$ be the set of maximal ideals of R. One can put a topology on $\beta(X)$ in such a way that if we identify X with its image in $\beta(X)$ then X (in its given topology) becomes a subspace of $\beta(X)$. Moreover, $\beta(X)$ is a compact space under this topology and is called the *Stone-Čech compactification* of X.

34. Let R be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ and for each $c \in \mathbb{R}$ let M_c be the maximal ideal $\{f \in R \mid f(c) = 0\}$.

(a) Let I be the collection of functions $f(x)$ in R with *compact support* (i.e., $f(x) = 0$ for $|x|$ sufficiently large). Prove that I is an ideal of R that is not a prime ideal.

(b) Let M be a maximal ideal of R containing I (properly, by (a)). Prove that $M \neq M_c$ for any $c \in \mathbb{R}$ (cf. the preceding exercise).

35. Let $A = (a_1, a_2, \ldots, a_n)$ be a nonzero finitely generated ideal of R. Prove that there is an ideal B which is maximal with respect to the property that it does not contain A. [Use Zorn's Lemma.]

36. Assume R is commutative. Prove that the set of prime ideals in R has a minimal element with respect to inclusion (possibly the zero ideal). [Use Zorn's Lemma.]

37. A commutative ring R is called a *local ring* if it has a unique maximal ideal. Prove that if R is a local ring with maximal ideal M then every element of $R - M$ is a unit. Prove conversely that if R is a commutative ring with 1 in which the set of nonunits forms an ideal M, then R is a local ring with unique maximal ideal M.

38. Prove that the ring of all rational numbers whose denominators is odd is a local ring whose unique maximal ideal is the principal ideal generated by 2.

39. Following the notation of Exercise 26 in Section 1, let K be a field, let v be a discrete

valuation on K and let R be the valuation ring of v. For each integer $k \geq 0$ define $A_k = \{r \in R \mid v(r) \geq k\} \cup \{0\}$.

(a) Prove that A_k is a principal ideal and that $A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots$.

(b) Prove that if I is any nonzero ideal of R, then $I = A_k$ for some $k \geq 0$. Deduce that R is a local ring with unique maximal ideal A_1.

40. Assume R is commutative. Prove that the following are equivalent: (see also Exercises 13 and 14 in Section 1)

(i) R has exactly one prime ideal

(ii) every element of R is either nilpotent or a unit

(iii) $R/\eta(R)$ is a field (cf. Exercise 29, Section 3).

41. A proper ideal Q of the commutative ring R is called *primary* if whenever $ab \in Q$ and $a \notin Q$ then $b^n \in Q$ for some positive integer n. (Note that the symmetry between a and b in this definition implies that if Q is a primary ideal and $ab \in Q$ with *neither* a nor b in Q, then a positive power of a and a positive power of b both lie in Q.) Establish the following facts about primary ideals.

(a) The primary ideals of $\mathbb{Z}$ are 0 and (p^n), where p is a prime and n is a positive integer.

(b) Every prime ideal of R is a primary ideal.

(c) An ideal Q of R is primary if and only if every zero divisor in R/Q is a nilpotent element of R/Q.

(d) If Q is a primary ideal then $\text{rad}(Q)$ is a prime ideal (cf. Exercise 30).

7.5 RINGS OF FRACTIONS

Throughout this section R is a commutative ring. Proposition 2 shows that if a is not zero nor a zero divisor and $ab = ac$ in R then $b = c$. Thus a nonzero element that is not a zero divisor enjoys some of the properties of a unit without necessarily possessing a multiplicative inverse in R. On the other hand, we saw in Section 1 that a zero divisor a cannot be a unit in R and, by definition, if a is a zero divisor we cannot always cancel the a's in the equation $ab = ac$ to obtain $b = c$ (take $c = 0$ for example). The aim of this section is to prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q. The principal application of this will be to integral domains, in which case this ring Q will be a field — called its *field of fractions* or *quotient field*. Indeed, the paradigm for the construction of Q from R is the one offered by the construction of the field of rational numbers from the integral domain $\mathbb{Z}$.

In order to see the essential features of the construction of the field $\mathbb{Q}$ from the integral domain $\mathbb{Z}$ we review the basic properties of fractions. Each rational number may be represented in many different ways as the quotient of two integers (for example, $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$, etc.). These representations are related by

$$\frac{a}{b} = \frac{c}{d} \qquad \text{if and only if} \qquad ad = bc.$$

In more precise terms, the fraction $\frac{a}{b}$ is the equivalence class of ordered pairs (a, b) of integers with $b \neq 0$ under the equivalence relation: $(a, b) \sim (c, d)$ if and only if

$ad = bc$. The arithmetic operations on fractions are given by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

These are well defined (independent of choice of representatives of the equivalence classes) and make the set of fractions into a commutative ring (in fact, a field), $\mathbb{Q}$. The integers $\mathbb{Z}$ are identified with the subring $\{\frac{a}{1} \mid a \in \mathbb{Z}\}$ of $\mathbb{Q}$ and every nonzero integer a has an inverse $\frac{1}{a}$ in $\mathbb{Q}$.

It seems reasonable to attempt to follow the same steps for any commutative ring R, allowing arbitrary denominators. If, however, b is zero or a zero divisor in R, say $bd = 0$, and if we allow b as a denominator, then we should expect to have

$$d = \frac{d}{1} = \frac{bd}{b} = \frac{0}{b} = 0$$

in the "ring of fractions" (where, for convenience, we have assumed R has a 1). Thus if we allow zero or zero divisors as denominators there must be some collapsing in the sense that we cannot expect R to appear naturally as a subring of this "ring of fractions." A second restriction is more obviously imposed by the laws of addition and multiplication: if ring elements b and d are allowed as denominators, then bd must also be a denominator, i.e., the set of denominators must be closed under multiplication in R. The main result of this section shows that these two restrictions are sufficient to construct a ring of fractions for R. Note that this theorem includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case.

Theorem 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

(1) every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field.

(2) (uniqueness of Q) The ring Q is the *"smallest"* ring containing R in which all elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Remark: In Section 15.4 a more general construction is given. The proof of the general result is more technical but relies on the same basic rationale and steps as the proof of Theorem 15. Readers wishing greater generality may read the proof below and the beginning of Section 15.4 in concert.

Proof: Let $\mathcal{F} = \{(r, d) \mid r \in R,\ d \in D\}$ and define the relation $\sim$ on $\mathcal{F}$ by

$$(r, d) \sim (s, e) \qquad \text{if and only if} \qquad re = sd.$$

It is immediate that this relation is reflexive and symmetric. Suppose $(r, d) \sim (s, e)$ and $(s, e) \sim (t, f)$. Then $re - sd = 0$ and $sf - te = 0$. Multiplying the first of these equations by f and the second by d and adding them gives $(rf - td)e = 0$. Since $e \in D$ is neither zero nor a zero divisor we must have $rf - td = 0$, i.e., $(r, d) \sim (t, f)$. This proves $\sim$ is transitive, hence an equivalence relation. Denote the equivalence class of (r, d) by $\frac{r}{d}$:

$$\frac{r}{d} = \{(a, b) \mid a \in R,\ b \in D \text{ and } rb = ad\}.$$

Let Q be the set of equivalence classes under $\sim$. Note that $\frac{r}{d} = \frac{re}{de}$ in Q for all $e \in D$, since D is closed under multiplication.

We now define an additive and multiplicative structure on Q:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

In order to prove that Q is a commutative ring with identity there are a number of things to check:

(1) these operations are well defined (i.e., do not depend on the choice of representatives for the equivalence classes),

(2) Q is an abelian group under addition, where the additive identity is $\frac{0}{d}$ for any $d \in D$ and the additive inverse of $\frac{a}{d}$ is $\frac{-a}{d}$,

(3) multiplication is associative, distributive and commutative, and

(4) Q has an identity ($= \frac{d}{d}$ for any $d \in D$).

These are all completely straightforward calculations involving only arithmetic in R and the definition of $\sim$. Again we need D to be closed under multiplication for addition and multiplication to be defined.

For example, to check that addition is well defined assume $\frac{a}{b} = \frac{a'}{b'}$ (i.e., $ab' = a'b$) and $\frac{c}{d} = \frac{c'}{d'}$ (i.e., $cd' = c'd$). We must show that $\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$, i.e.,

$$(ad + bc)(b'd') = (a'd' + b'c')(bd).$$

The left hand side of this equation is $ab'dd' + cd'bb'$ substituting $a'b$ for ab' and $c'd$ for cd' gives $a'bdd' + c'dbb'$, which is the right hand side. Hence addition of fractions is well defined. Checking the details in the other parts of (1) to (4) involves even easier manipulations and so is left as an exercise.

Next we embed R into Q by defining

$$\iota : R \to Q \qquad \text{by} \qquad \iota : r \mapsto \frac{rd}{d} \quad \text{where } d \text{ is any element of } D.$$

Since $\frac{rd}{d} = \frac{re}{e}$ for all $d, e \in D$, $\iota(r)$ does not depend on the choice of $d \in D$. Since D is closed under multiplication, one checks directly that ι is a ring homomorphism.

Furthermore, ι is injective because

$$\iota(r) = 0 \Leftrightarrow \frac{rd}{d} = \frac{0}{d} \Leftrightarrow rd^2 = 0 \Leftrightarrow r = 0$$

because d (hence also d^2) is neither zero nor a zero divisor. The subring $\iota(R)$ of Q is therefore isomorphic to R. We henceforth identify each $r \in R$ with $\iota(r)$ and so consider R as a subring of Q.

Next note that each $d \in D$ has a multiplicative inverse in Q: namely, if d is represented by the fraction $\frac{de}{e}$ then its multiplicative inverse is $\frac{e}{de}$. One then sees that every element of Q may be written as $r \cdot d^{-1}$ for some $r \in R$ and some $d \in D$. In particular, if $D = R - \{0\}$, every nonzero element of Q has a multiplicative inverse and Q is a field.

It remains to establish the uniqueness property of Q. Assume $\varphi : R \to S$ is an injective ring homomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$. Extend φ to a map $\Phi : Q \to S$ by defining $\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1}$ for all $r \in R$, $d \in D$. This map is well defined, since $rd^{-1} = se^{-1}$ implies $re = sd$, so $\varphi(r)\varphi(e) = \varphi(s)\varphi(d)$, and then

$$\Phi(rd^{-1}) = \varphi(r)\varphi(d)^{-1} = \varphi(s)\varphi(e)^{-1} = \Phi(se^{-1}).$$

It is straightforward to check that Φ is a ring homomorphism — the details are left as an exercise. Finally, Φ is injective because $rd^{-1} \in \ker \Phi$ implies $r \in \ker \Phi \cap R = \ker \varphi$; since φ is injective this forces r and hence also rd^{-1} to be zero. This completes the proof.

Definition. Let R, D and Q be as in Theorem 15.

(1) The ring Q is called the *ring of fractions* of D with respect to R and is denoted $D^{-1}R$.

(2) If R is an integral domain and $D = R - \{0\}$, Q is called the *field of fractions* or *quotient field* of R.

If A is a subset of a field F (for example, if A is a subring of F), then the intersection of all the subfields of F containing A is a subfield of F and is called the subfield *generated* by A. This subfield is the smallest subfield of F containing A (namely, any subfield of F containing A contains the subfield generated by A).

The next corollary shows that the smallest field containing an integral domain R is its field of fractions.

Corollary 16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Proof: Let $\varphi : R \cong R' \subseteq F$ be a (ring) isomorphism of R to R'. In particular, $\varphi : R \to F$ is an injective homomorphism from R into the field F. Let $\Phi : Q \to F$ be the extension of φ to Q as in the theorem. By Theorem 15, Φ is injective, so $\Phi(Q)$ is an isomorphic copy of Q in F containing $\varphi(R) = R'$. Now, any subfield of F containing $R' = \varphi(R)$ contains the elements $\varphi(r_1)\varphi(r_2)^{-1} = \varphi(r_1 r_2^{-1})$ for all $r_1, r_2 \in R$. Since

every element of Q is of the form $r_1 r_2^{-1}$ for some $r_1, r_2 \in R$, it follows that any subfield of F containing R' contains the field $\Phi(Q)$, so that $\Phi(Q)$ is the subfield of F generated by R', proving the corollary.

Examples

(1) If R is a field then its field of fractions is just R itself.

(2) The integers $\mathbb{Z}$ are an integral domain whose field of fractions is the field $\mathbb{Q}$ of rational numbers. The quadratic integer ring $\mathcal{O}$ of Section 1 is an integral domain whose field of fractions is the quadratic field $\mathbb{Q}(\sqrt{D})$.

(3) The subring $2\mathbb{Z}$ of $\mathbb{Z}$ also has no zero divisors (but has no identity). Its field of fractions is also $\mathbb{Q}$. Note how an identity "appears" in the field of fractions.

(4) If R is any integral domain, then the polynomial ring $R[x]$ is also an integral domain. The associated field of fractions is the field of *rational functions* in the variable x over R. The elements of this field are of the form $\dfrac{p(x)}{q(x)}$, where $p(x)$ and $q(x)$ are polynomials with coefficients in R with $q(x)$ not the zero polynomial. In particular, $p(x)$ and $q(x)$ may both be constant polynomials, so the field of rational functions contains the field of fractions of R: elements of the form $\dfrac{a}{b}$ such that $a, b \in R$ and $b \neq 0$. If F is a field, we shall denote the field of rational functions by $F(x)$. Thus if F is the field of fractions of the integral domain R then the field of rational functions over R is the same as the field of rational functions over F, namely $F(x)$.

For example, suppose $R = \mathbb{Z}$, so $F = \mathbb{Q}$. If $p(x), q(x)$ are polynomials in $\mathbb{Q}[x]$ then for some integer N, $Np(x), Nq(x)$ have integer coefficients (let N be a common denominator for all the coefficients in $p(x)$ and $q(x)$, for example). Then $\dfrac{p(x)}{q(x)} = \dfrac{Np(x)}{Nq(x)}$ can be written as the quotient of two polynomials with integer coefficients, so the field of fractions of $\mathbb{Q}[x]$ is the same as the field of fractions of $\mathbb{Z}[x]$.

(5) If R is any commutative ring with identity and d is neither zero nor a zero divisor in R we may form the ring $R[1/d]$ by setting $D = \{1, d, d^2, d^3, \dots\}$ and defining $R[1/d]$ to be the ring of fractions $D^{-1}R$. Note that R is the subring of elements of the form $\dfrac{r}{1}$. In this way any nonzero element of R that is not a zero divisor can be inverted in a larger ring containing R. Note that the elements of $R[1/d]$ look like polynomials in $1/d$ with coefficients in R, which explains the notation.

EXERCISES

Let R be a commutative ring with identity $1 \neq 0$.

1. Fill in all the details in the proof of Theorem 15.

2. Let R be an integral domain and let D be a nonempty subset of R that is closed under multiplication. Prove that the ring of fractions $D^{-1}R$ is isomorphic to a subring of the quotient field of R (hence is also an integral domain).

3. Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (F_0 is called the *prime subfield* of F). [See Exercise 26, Section 3.]

4. Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

5. If F is a field, prove that the field of fractions of $F[[x]]$ (the ring of formal power series in the indeterminate x with coefficients in F) is the ring $F((x))$ of formal Laurent series (cf. Exercises 3 and 5 of Section 2). Show the field of fractions of the power series ring $\mathbb{Z}[[x]]$ is *properly* contained in the field of Laurent series $\mathbb{Q}((x))$. [Consider the series for e^x.]

6. Prove that the real numbers, $\mathbb{R}$, contain a subring A with $1 \in A$ and A maximal (under inclusion) with respect to the property that $\frac{1}{2} \notin A$. [Use Zorn's Lemma.] (Exercise 13 in Section 15.3 shows $\mathbb{R}$ is the quotient field of A, so $\mathbb{R}$ is the quotient field of a proper subring.)

7.6 THE CHINESE REMAINDER THEOREM

Throughout this section we shall assume unless otherwise stated that all rings are commutative with an identity $1 \neq 0$.

Given an arbitrary collection of rings (not necessarily satisfying the conventions above), their *(ring) direct product* is defined to be their direct product as (abelian) groups made into a ring by defining multiplication componentwise. In particular, if R_1 and R_2 are two rings, we shall denote by $R_1 \times R_2$ their direct product (as rings), that is, the set of ordered pairs (r_1, r_2) with $r_1 \in R_1$ and $r_2 \in R_2$ where addition and multiplication are performed componentwise:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \qquad \text{and} \qquad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

We note that a map φ from a ring R into a direct product ring is a homomorphism if and only if the induced maps into each of the components are homomorphisms.

There is a generalization to arbitrary rings of the notion in $\mathbb{Z}$ of two integers n and m being relatively prime (even to rings where the notion of greatest common divisor is not defined). In $\mathbb{Z}$ this is equivalent to being able to solve the equation $nx + my = 1$ in integers x and y (this fact was stated in Chapter 0 and will be proved in Chapter 8). This in turn is equivalent to $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ as ideals (in general, $n\mathbb{Z} + m\mathbb{Z} = (m, n)\mathbb{Z}$). This motivates the following definition:

Definition. The ideals A and B of the ring R are said to be *comaximal* if $A + B = R$.

Recall that the *product*, AB, of the ideals A and B of R is the ideal consisting of all finite sums of elements of the form xy, $x \in A$ and $y \in B$ (cf. Exercise 34, Section 3). If $A = (a)$ and $B = (b)$, then $AB = (ab)$. More generally, the product of the ideals $A_1, A_2, \ldots, A_k$ is the ideal of all finite sums of elements of the form $x_1 x_2 \cdots x_k$ such that $x_i \in A_i$ for all i. If $A_i = (a_i)$, then $A_1 \cdots A_k = (a_1 \cdots a_k)$.

Theorem 17. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \qquad \text{defined by} \qquad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Proof: We first prove this for $k = 2$; the general case will follow by induction. Let $A = A_1$ and $B = A_2$. Consider the map $\varphi : R \to R/A \times R/B$ defined by $\varphi(r) = (r \bmod A, r \bmod B)$, where mod A means the class in R/A containing r (that is, $r + A$). This map is a ring homomorphism because φ is just the natural projection of R into R/A and R/B for the two components. The kernel of φ consists of all the elements $r \in R$ that are in A and in B, i.e., $A \cap B$. To complete the proof in this case it remains to show that when A and B are comaximal, φ is surjective and $A \cap B = AB$. Since $A + B = R$, there are elements $x \in A$ and $y \in B$ such that $x + y = 1$. This equation shows that $\varphi(x) = (0, 1)$ and $\varphi(y) = (1, 0)$ since, for example, x is an element of A and $x = 1 - y \in 1 + B$. If now $(r_1 \bmod A, r_2 \bmod B)$ is an arbitrary element in $R/A \times R/B$, then the element $r_2x + r_1y$ maps to this element since

$$\begin{aligned}\varphi(r_2x + r_1y) &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y)\\ &= (r_2 \bmod A, r_2 \bmod B)(0, 1) + (r_1 \bmod A, r_1 \bmod B)(1, 0)\\ &= (0, r_2 \bmod B) + (r_1 \bmod A, 0)\\ &= (r_1 \bmod A, r_2 \bmod B).\end{aligned}$$

This shows that φ is indeed surjective. Finally, the ideal AB is always contained in $A \cap B$. If A and B are comaximal and x and y are as above, then for any $c \in A \cap B$, $c = c1 = cx + cy \in AB$. This establishes the reverse inclusion $A \cap B \subseteq AB$ and completes the proof when $k = 2$.

The general case follows easily by induction from the case of two ideals using $A = A_1$ and $B = A_2 \cdots A_k$ once we show that A_1 and $A_2 \cdots A_k$ are comaximal. By hypothesis, for each $i \in \{2, 3, \ldots, k\}$ there are elements $x_i \in A_1$ and $y_i \in A_i$ such that $x_i + y_i = 1$. Since $x_i + y_i \equiv y_i \bmod A_1$, it follows that $1 = (x_2 + y_2) \cdots (x_k + y_k)$ is an element in $A_1 + (A_2 \cdots A_k)$. This completes the proof.

This theorem obtained its name from the special case $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ *as rings* when m and n are relatively prime integers. We proved this isomorphism just for the additive groups earlier. This isomorphism, phrased in number-theoretic terms, relates to simultaneously solving two congruences modulo relatively prime integers (and states that such congruences can always be solved, and uniquely). Such problems were considered by the ancient Chinese, hence the name. Some examples are provided in the exercises.

Since the isomorphism in the Chinese Remainder Theorem is an isomorphism of *rings*, in particular the groups of *units* on both sides must be isomorphic. It is easy to see that the units in any direct product of rings are the elements that have units in each of the coordinates. In the case of $\mathbb{Z}/mn\mathbb{Z}$ the Chinese Remainder Theorem gives the following isomorphism on the groups of units:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

More generally we have the following result.

Corollary 18. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

If we compare orders on the two sides of this last isomorphism, we obtain the formula

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k})$$

for the Euler φ-function. This in turn implies that φ is what in elementary number theory is termed a *multiplicative function*, namely that $\varphi(ab) = \varphi(a)\varphi(b)$ whenever a and b are relatively prime positive integers. The value of φ on prime powers p^α is easily seen to be $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (cf. Chapter 0). From this and the multiplicativity of φ we obtain its value on all positive integers.

Corollary 18 is also a step toward a determination of the decomposition of the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$ into a direct product of cyclic groups. The complete structure is derived at the end of Section 9.5.

EXERCISES

Let R be a ring with identity $1 \neq 0$.

1. An element $e \in R$ is called an *idempotent* if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$. Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.
2. Let R be a finite Boolean ring with identity $1 \neq 0$ (cf. Exercise 15 of Section 1). Prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$. [Use the preceding exercise.]
3. Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.
4. Prove that if R and S are nonzero rings then $R \times S$ is never a field.
5. Let $n_1, n_2, \dots, n_k$ be integers which are relatively prime in pairs: $(n_i, n_j) = 1$ for all $i \neq j$.
   (a) Show that the Chinese Remainder Theorem implies that for any $a_1, \dots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the simultaneous congruences
   $$x \equiv a_1 \bmod n_1\,, \qquad x \equiv a_2 \bmod n_2\,, \quad \dots, \quad x \equiv a_k \bmod n_k$$
   and that the solution x is unique mod $n = n_1 n_2 \dots n_k$.
   (b) Let $n_i' = n/n_i$ be the quotient of n by n_i, which is relatively prime to n_i by assumption. Let t_i be the inverse of n_i' mod n_i. Prove that the solution x in (a) is given by
   $$x = a_1 t_1 n_1' + a_2 t_2 n_2' + \cdots + a_k t_k n_k' \bmod n.$$
   Note that the elements t_i can be quickly found by the Euclidean Algorithm as described in Section 2 of the Preliminaries chapter (writing $an_i + bn_i' = (n_i, n_i') = 1$ gives $t_i = b$) and that these then quickly give the solutions to the system of congruences above for any choice of $a_1, a_2, \dots, a_k$.

(c) Solve the simultaneous system of congruences

$$x \equiv 1 \bmod 8\,, \qquad x \equiv 2 \bmod 25\,, \quad \text{and} \quad x \equiv 3 \bmod 81$$

and the simultaneous system

$$y \equiv 5 \bmod 8\,, \qquad y \equiv 12 \bmod 25\,, \quad \text{and} \quad y \equiv 47 \bmod 81.$$

6. Let $f_1(x), f_2(x), \ldots, f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs (i.e., $(n_i, n_j) = 1$ for all $i \neq j$). Use the Chinese Remainder Theorem to prove there exists a polynomial $f(x)$ with integer coefficients and of degree d with

$$f(x) \equiv f_1(x) \bmod n_1\,, \qquad f(x) \equiv f_2(x) \bmod n_2\,, \quad \ldots, \quad f(x) \equiv f_k(x) \bmod n_k$$

i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \bmod n_i$. Show that if all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic. [Apply the Chinese Remainder Theorem in $\mathbb{Z}$ to each of the coefficients separately.]

7. Let m and n be positive integers with n dividing m. Prove that the natural surjective ring projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is also surjective on the units: $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$.

The next four exercises develop the concept of *direct limits* and the "dual" notion of *inverse limits*. In these exercises I is a nonempty index set with a partial order $\leq$ (cf. Appendix I). For each $i \in I$ let A_i be an additive abelian group. In Exercise 8 assume also that I is a *directed set*: for every $i, j \in I$ there is some $k \in I$ with $i \leq k$ and $j \leq k$.

8. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\rho_{ij} : A_i \to A_j$ such that the following hold:

i. $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ whenever $i \leq j \leq k$, and
ii. $\rho_{ii} = 1$ for all $i \in I$.

Let B be the disjoint union of all the A_i. Define a relation $\sim$ on B by

$$a \sim b \text{ if and only if there exists } k \text{ with } i, j \leq k \text{ and } \rho_{ik}(a) = \rho_{jk}(b),$$

for $a \in A_i$ and $b \in A_j$.

(a) Show that $\sim$ is an equivalence relation on B. (The set of equivalence classes is called the *direct* or *inductive limit* of the directed system $\{A_i\}$, and is denoted $\varinjlim A_i$. In the remaining parts of this exercise let $A = \varinjlim A_i$.)

(b) Let $\overline{x}$ denote the class of x in A and define $\rho_i : A_i \to A$ by $\rho_i(a) = \overline{a}$. Show that if each ρ_{ij} is injective, then so is ρ_i for all i (so we may then identify each A_i as a subset of A).

(c) Assume all ρ_{ij} are group homomorphisms. For $a \in A_i, b \in A_j$ show that the operation

$$\overline{a} + \overline{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$$

where k is any index with $i, j \leq k$, is well defined and makes A into an abelian group. Deduce that the maps ρ_i in (b) are group homomorphisms from A_i to A.

(d) Show that if all A_i are commutative rings with 1 and all ρ_{ij} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all ρ_i are ring homomorphisms.

(e) Under the hypotheses in (c) prove that the direct limit has the following *universal property*: if C is any abelian group such that for each $i \in I$ there is a homomorphism $\varphi_i : A_i \to C$ with $\varphi_i = \varphi_j \circ \rho_{ij}$ whenever $i \leq j$, then there is a unique homomorphism $\varphi : A \to C$ such that $\varphi \circ \rho_i = \varphi_i$ for all i.

9. Let I be the collection of open intervals $U = (a, b)$ on the real line containing a fixed real number p. Order these by reverse inclusion: $U \leq V$ if $V \subseteq U$ (note that I is a directed set). For each U let A_U be the ring of continuous real valued functions on U. For $V \subseteq U$ define the *restriction maps* $\rho_{UV} : A_U \to A_V$ by $f \mapsto f|_V$, the usual restriction of a function on U to a function on the subset V (which is easily seen to be a ring homomorphism). Let $A = \varinjlim A_U$ be the direct limit. In the notation of the preceding exercise, show that the maps $\rho_U : A_U \to A$ are *not* injective but are all surjective (A is called the ring of *germs of continuous functions* at p).

We now develop the notion of *inverse limits*. Continue to assume I is a partially ordered set (but not necessarily directed), and A_i is a group for all $i \in I$.

10. Suppose for every pair of indices i, j with $i \leq j$ there is a map $\mu_{ji} : A_j \to A_i$ such that the following hold:

i. $\mu_{ji} \circ \mu_{kj} = \mu_{ki}$ whenever $i \leq j \leq k$, and
ii. $\mu_{ii} = 1$ for all $i \in I$.

Let P be the subset of elements $(a_i)_{i \in I}$ in the direct product $\prod_{i \in I} A_i$ such that $\mu_{ji}(a_j) = a_i$ whenever $i \leq j$ (here a_i and a_j are the i^{th} and j^{th} components respectively of the element in the direct product). The set P is called the *inverse* or *projective limit* of the system $\{A_i\}$, and is denoted $\varprojlim A_i$.)

(a) Assume all μ_{ji} are group homomorphisms. Show that P is a subgroup of the direct product group (cf. Exercise 15, Section 5.1).
(b) Assume the hypotheses in (a), and let $I = \mathbb{Z}^+$ (usual ordering). For each $i \in I$ let $\mu_i : P \to A_i$ be the projection of P onto its i^{th} component. Show that if each μ_{ji} is surjective, then so is μ_i for all i (so each A_i is a quotient group of P).
(c) Show that if all A_i are commutative rings with 1 and all μ_{ji} are ring homomorphisms that send 1 to 1, then A may likewise be given the structure of a commutative ring with 1 such that all μ_i are ring homomorphisms.
(d) Under the hypotheses in (a) prove that the inverse limit has the following *universal property*: if D is any group such that for each $i \in I$ there is a homomorphism $\pi_i : D \to A_i$ with $\pi_i = \mu_{ji} \circ \pi_j$ whenever $i \leq j$, then there is a unique homomorphism $\pi : D \to P$ such that $\mu_i \circ \pi = \pi_i$ for all i.

11. Let p be a prime let $I = \mathbb{Z}^+$, let $A_i = \mathbb{Z}/p^i\mathbb{Z}$ and let μ_{ji} be the natural projection maps

$$\mu_{ji} : a \pmod{p^j} \longmapsto a \pmod{p^i}.$$

The inverse limit $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ is called the ring of *p-adic integers*, and is denoted by $\mathbb{Z}_p$.

(a) Show that every element of $\mathbb{Z}_p$ may be written uniquely as an infinite formal sum $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ with each $b_i \in \{0, 1, \ldots, p-1\}$. Describe the rules for adding and multiplying such formal sums corresponding to addition and multiplication in the ring $\mathbb{Z}_p$. [Write a least residue in each $\mathbb{Z}/p^i\mathbb{Z}$ in its base p expansion and then describe the maps μ_{ji}.] (Note in particular that $\mathbb{Z}_p$ is uncountable.)
(b) Prove that $\mathbb{Z}_p$ is an integral domain that contains a copy of the integers.
(c) Prove that $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ as in (a) is a unit in $\mathbb{Z}_p$ if and only if $b_0 \neq 0$.
(d) Prove that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (where $p = 0 + 1p + 0p^2 + 0p^3 + \cdots$). Prove that every ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for some integer $n \geq 0$.
(e) Show that if $a_1 \not\equiv 0 \pmod{p}$ then there is an element $a = (a_i)$ in the direct limit $\mathbb{Z}_p$ satisfying $a_j^p \equiv 1 \pmod{p^j}$ and $\mu_{j1}(a_j) = a_1$ for all j. Deduce that $\mathbb{Z}_p$ contains $p - 1$ distinct $(p-1)^{\text{st}}$ roots of 1.