**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,

*if $R$ 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 $\pm 1$ 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 $\sigma$, 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 $S$.