16. Find a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not maximal.

17. Find a nontrivial proper ideal of $\mathbb{Z} \times \mathbb{Z}$ that is not prime.

18. Is $\mathbb{Q}[x]/\langle x^2 - 5x + 6\rangle$ a field? Why?

19. Is $\mathbb{Q}[x]/\langle x^2 - 6x + 6\rangle$ a field? Why?

Proof Synopsis

20. Give a one- or two-sentence synopsis of "only if" part of Theorem 31.9.

21. Give a one- or two-sentence synopsis of "if" part of Theorem 31.9.

22. Give a one- or two-sentence synopsis of Theorem 31.24.

23. Give a one- or two-sentence synopsis of the "only if" part of Theorem 31.25.

Theory

24. Give an example of an ideal in $\mathbb{Q}[x, y]$ that is not a principal ideal. Conclude that if R is an integral domain with the property that every ideal in R is principal, it does not follow that every ideal in $R[x]$ is a principal ideal.

25. Prove that if R is a commutative ring with unity and $a \in R$, then $\langle a\rangle = \{ra \mid r \in R\}$ is an ideal in R.

26. Let R be a finite commutative ring with unity. Show that every prime ideal in R is a maximal ideal.

27. Corollary 31.18 tells us that every ring with unity contains a subring isomorphic to either $\mathbb{Z}$ or some $\mathbb{Z}_n$. Is it possible that a ring with unity may simultaneously contain two subrings isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_m$ for $n \neq m$? If it is possible, give an example. If it is impossible, prove it.

28. Continuing Exercise 27, is it possible that a ring with unity may simultaneously contain two subrings isomorphic to the fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for two different primes p and q? Give an example or prove it is impossible.

29. Following the idea of Exercise 28, is it possible for an integral domain to contain two subrings isomorphic to $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for $p \neq q$ and p and q both prime? Give reasons or an illustration.

30. Prove directly from the definitions of maximal and prime ideals that every maximal ideal of a commutative ring R with unity is a prime ideal. [*Hint*: Suppose M is maximal in R, $ab \in M$, and $a \notin M$. Argue that the smallest ideal $\{ra + m \mid r \in R, m \in M\}$ containing a and M must contain 1. Express 1 as $ra + m$ and multiply by b.]

31. Show that N is a maximal ideal in a ring R if and only if R/N is a **simple ring,** that is, it is nontrivial and has no proper nontrivial ideals. (Compare with Theorem 13.20.)

32. Prove that if F is a field, every proper nontrivial prime ideal of $F[x]$ is maximal.

33. Let F be a field and $f(x), g(x) \in F[x]$. Show that $f(x)$ divides $g(x)$ if and only if $g(x) \in \langle f(x)\rangle$.

34. Let F be a field and let $f(x), g(x) \in F[x]$. Show that

$$N = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F[x]\}$$

is an ideal of $F[x]$. Show that if $f(x)$ and $g(x)$ have different degrees and $N \neq F[x]$, then $f(x)$ and $g(x)$ cannot both be irreducible over F.

35. Use Theorem 31.24 to prove the *equivalence* of these two theorems:

Fundamental Theorem of Algebra: Every nonconstant polynomial in $\mathbb{C}[x]$ has a zero in $\mathbb{C}$.

Nullstellensatz for $\mathbb{C}[x]$: Let $f_1(x), \cdots, f_r(x) \in \mathbb{C}[x]$ and suppose that every $\alpha \in \mathbb{C}$ that is a zero of all r of these polynomials is also a zero of a polynomial $g(x)$ in $\mathbb{C}[x]$. Then some power of $g(x)$ is in the smallest ideal of $\mathbb{C}[x]$ that contains the r polynomials $f_1(x), \cdots, f_r(x)$.

There is a sort of arithmetic of ideals in a ring. The next three exercises define sum, product, and quotient of ideals.

36. If A and B are ideals of a ring R, the **sum $A + B$ of A and B** is defined by

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

a. Show that $A + B$ is an ideal.

b. Show that $A \subseteq A + B$ and $B \subseteq A + B$.

37. Let A and B be ideals of a ring R. The **product AB of A and B** is defined by

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

a. Show that AB is an ideal in R. **b.** Show that $AB \subseteq (A \cap B)$.

38. Let A and B be ideals of a *commutative* ring R. The **quotient $A : B$ of A by B** is defined by

$$A : B = \{r \in R \mid rb \in A \text{ for all } b \in B\}.$$

Show that $A : B$ is an ideal of R.

39. Show that for a field F, the set S of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

for $a, b \in F$ is a **right ideal** but not a **left ideal** of $M_2(F)$. That is, show that S is a subring closed under multiplication on the *right* by any element of $M_2(F)$, but is not closed under *left* multiplication.

40. Show that the matrix ring $M_2(\mathbb{Z}_2)$ is a simple ring; that is, $M_2(\mathbb{Z}_2)$ has no proper nontrivial ideals.

SECTION 32 †NONCOMMUTATIVE EXAMPLES

Thus far, the only example we have presented of a ring that is not commutative is the ring $M_n(F)$ of all $n \times n$ matrices with entries in a field F. We shall do almost nothing with noncommutative rings and strictly skew fields. To show that there are other important noncommutative rings occurring very naturally in algebra, we give several examples of such rings.

Rings of Endomorphisms

Let A be any abelian group. A homomorphism of A into itself is an **endomorphism of A**. Let the set of all endomorphisms of A be $\text{End}(A)$. Since the composition of two homomorphisms of A into itself is again such a homomorphism, we define multiplication on $\text{End}(A)$ by function composition, and thus multiplication is associative.

To define addition, for $\phi, \psi \in \text{End}(A)$, we have to describe the value of $(\phi + \psi)$ on each $a \in A$. Define

$$(\phi + \psi)(a) = \phi(a) + \psi(a).$$

Since

$$\begin{aligned}(\phi + \psi)(a + b) &= \phi(a + b) + \psi(a + b) \\ &= [\phi(a) + \phi(b)] + [\psi(a) + \psi(b)] \\ &= [\phi(a) + \psi(a)] + [\phi(b) + \psi(b)] \\ &= (\phi + \psi)(a) + (\phi + \psi)(b)\end{aligned}$$

we see that $\phi + \psi$ is again in $\text{End}(A)$.

Since A is commutative, we have

$$(\phi + \psi)(a) = \phi(a) + \psi(a) = \psi(a) + \phi(a) = (\psi + \phi)(a)$$

† This section is not used in the remainder of the text.

for all $a \in A$, so $\phi + \psi = \psi + \phi$ and addition in End(A) is commutative. The associativity of addition follows from

$$\begin{aligned}[\phi + (\psi + \theta)](a) &= \phi(a) + [(\psi + \theta)(a)] \\ &= \phi(a) + [\psi(a) + \theta(a)] \\ &= [\phi(a) + \psi(a)] + \theta(a) \\ &= (\phi + \psi)(a) + \theta(a) \\ &= [(\phi + \psi) + \theta](a).\end{aligned}$$

If e is the additive identity of A, then the homomorphism 0 defined by

$$0(a) = e$$

for $a \in A$ is an additive identity in End(A). Finally, for

$$\phi \in \text{End}(A),$$

$-\phi$ defined by

$$(-\phi)(a) = -\phi(a)$$

is in End(A), since

$$\begin{aligned}(-\phi)(a + b) &= -\phi(a + b) = -[\phi(a) + \phi(b)] \\ &= -\phi(a) - \phi(b) = (-\phi)(a) + (-\phi)(b),\end{aligned}$$

and $\phi + (-\phi) = 0$. Thus $\langle \text{End}(A), + \rangle$ is an abelian group.

Note that we have not yet used the fact that our functions are *homomorphisms* except to show that $\phi + \psi$ and $-\phi$ are again *homomorphisms*. Thus the set A^A of *all functions* from A into A is an abelian group under exactly the same definition of addition, and, of course, function composition again gives a nice associative multiplication in A^A. However, we do need the fact that these functions in End(A) are homomorphisms now to prove the left distributive law in End(A). Except for this left distributive law, $\langle A^A, +, \cdot \rangle$ satisfies all the axioms for a ring. Let ϕ, ψ, and θ be in End(A), and let $a \in A$. Then

$$(\theta(\phi + \psi))(a) = \theta((\phi + \psi)(a)) = \theta(\phi(a) + \psi(a)).$$

Since θ is a *homomorphism,*

$$\begin{aligned}\theta(\phi(a) + \psi(a)) &= \theta(\phi(a)) + \theta(\psi(a)) \\ &= (\theta\phi)(a) + (\theta\psi)(a) \\ &= (\theta\phi + \theta\psi)(a).\end{aligned}$$

Thus $\theta(\phi + \psi) = \theta\phi + \theta\psi$. The right distributive law causes no trouble, even in A^A, and follows from

$$\begin{aligned}((\psi + \theta)\phi)(a) &= (\psi + \theta)(\phi(a)) = \psi(\phi(a)) + \theta(\phi(a)) \\ &= (\psi\phi)(a) + (\theta\phi)(a) = (\psi\phi + \theta\phi)(a).\end{aligned}$$

Thus we have proved the following theorem.

32.1 Theorem The set End(A) of all endomorphisms of an abelian group A forms a ring under homomorphism addition and homomorphism multiplication (function composition).

Again, to show relevance to this section, we should give an example showing that End(A) need not be commutative. Since function composition is in general not commutative, this seems reasonable to expect. However, End(A) may be commutative in some cases. Indeed, Exercise 15 asks us to show that End($\langle \mathbb{Z}, + \rangle$) is commutative.

32.2 Example Consider the abelian group $\langle \mathbb{Z} \times \mathbb{Z}, + \rangle$ discussed in Section 9. It is straightforward to verify that two elements of End$(\langle \mathbb{Z} \times \mathbb{Z}, + \rangle)$ are ϕ and ψ defined by

$$\phi((m,n)) = (m+n, 0) \qquad \text{and} \qquad \psi((m,n)) = (0,n).$$

Note that ϕ maps everything onto the first factor of $\mathbb{Z} \times \mathbb{Z}$, and ψ collapses the first factor. Thus

$$(\psi\phi)(m,n) = \psi(m+n,0) = (0,0)$$

while

$$(\phi\psi)(m,n) = \phi(0,n) = (n,0).$$

Hence $\phi\psi \neq \psi\phi$. ▲

32.3 Example Let F be a field of characteristic zero, and let $\langle F[x], + \rangle$ be the additive group of the ring $F[x]$ of polynomials with coefficients in F. For this example, let us denote this additive group by $F[x]$, to simplify this notation. We can consider End$(F[x])$. One element of End$(F[x])$ acts on each polynomial in $F[x]$ by multiplying it by x. Let this endomorphism be X, so

$$X\big(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\big) = a_0x + a_1x^2 + a_2x^3 + \cdots + a_nx^{n+1}.$$

Another element of End$(F[x])$ is formal differentiation with respect to x. (The familiar formula "the derivation of a sum is the sum of the derivatives" guarantees that differentiation is an endomorphism of $F[x]$.) Let Y be this endomorphism, so

$$Y\big(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\big) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

Exercise 17 asks us to show that $YX - XY = 1$, where 1 is unity (the identity map) in End$(F[x])$. Thus $XY \neq YX$. Multiplication of polynomials in $F[x]$ by any element of F also gives an element of End $(F[x])$. The subring of End$(F[x])$ generated by X and Y and multiplications by elements of F is the **Weyl algebra** and is important in quantum mechanics. ▲

Group Rings and Group Algebras

Let $G = \{g_i \mid i \in I\}$ be any group written multiplicatively and let R be any commutative ring with nonzero unity. Let RG be the set of all *formal sums*.

$$\sum_{i \in I} a_i g_i$$

for $a_i \in R$ and $g_i \in G$, *where all but a finite number of the* a_i *are 0*. Define the sum of two elements of RG by

$$\left(\sum_{i \in I} a_i g_i\right) + \left(\sum_{i \in I} b_i g_i\right) = \sum_{i \in I} (a_i + b_i) g_i.$$

Observe that $(a_i + b_i) = 0$ except for a finite number of indices i, so $\Sigma_{i \in I}(a_i + b_i)g_i$ is again in RG. It is immediate that $\langle RG, + \rangle$ is an abelian group with additive identity $\Sigma_{i \in I} 0 g_i$.

Multiplication of two elements of RG is defined by the use of the multiplications in G and R as follows:

$$\left(\sum_{i \in I} a_i g_i\right)\left(\sum_{i \in I} b_i g_i\right) = \sum_{i \in I} \left(\sum_{g_j g_k = g_i} a_j b_k\right) g_i.$$

Naively, we formally distribute the sum $\Sigma_{i \in I} a_i g_i$ over the sum $\Sigma_{i \in I} b_i g_i$ and rename a term $a_j g_j b_k g_k$ by $a_j b_k g_i$ where $g_j g_k = g_i$ in G. Since a_i and b_i are 0 for all but a finite

number of i, the sum $\Sigma_{g_jg_k=g_i}a_jb_k$ contains only a finite number of nonzero summands $a_jb_k \in R$ and may thus be viewed as an element of R. Again, at most a finite number of such sums $\Sigma_{g_jg_k=g_i}a_jb_k$ are nonzero. Thus multiplication is closed on RG.

The distributive laws follow at once from the definition of addition and the formal way we used distributivity to define multiplication. For the associativity of multiplication

$$\begin{aligned}\Big(\sum_{i\in I}a_ig_i\Big)\Big[\Big(\sum_{i\in I}b_ig_i\Big)\Big(\sum_{i\in I}c_ig_i\Big)\Big] &= \Big(\sum_{i\in I}a_ig_i\Big)\Big[\sum_{i\in I}\Big(\sum_{g_jg_k=g_i}b_jc_k\Big)g_i\Big]\\ &= \sum_{i\in I}\Big(\sum_{g_hg_jg_k=g_i}a_hb_jc_k\Big)g_i\\ &= \Big[\sum_{i\in I}\Big(\sum_{g_hg_j=g_i}a_hb_j\Big)g_i\Big]\Big(\sum_{i\in I}c_ig_i\Big)\\ &= \Big[\Big(\sum_{i\in I}a_ig_i\Big)\Big(\sum_{i\in I}b_ig_i\Big)\Big]\Big(\sum_{i\in I}c_ig_i\Big).\end{aligned}$$

Thus we have proved the following theorem.

32.4 Theorem If G is any group written multiplicatively and R is a commutative ring with nonzero unity, then $\langle RG, +, \cdot\rangle$ is a ring.

Corresponding to each $g \in G$, we have an element $1g$ in RG. If we identify (rename) $1g$ with g, we see that $\langle RG, \cdot\rangle$ can be considered to contain G naturally as a multiplicative subsystem. Thus, if G is not abelian, RG is not a commutative ring.

32.5 Definition The ring RG defined above is the **group ring of G over R**. If F is a field, then FG is the **group algebra of G over F**. ■

32.6 Example Let us give the addition and multiplication tables for the group algebra $\mathbb{Z}_2G$, where $G = \{e, a\}$ is cyclic of order 2. The elements of Z_2G are

$$0e + 0a, \quad 0e + 1a, \quad 1e + 0a, \quad \text{and} \quad 1e + 1a.$$

If we denote these elements in the obvious, natural way by

$$0, \quad a, \quad e, \quad \text{and} \quad e + a,$$

32.7 Table

$+$	0	a	e	$e+a$
0	0	a	e	$e+a$
a	a	0	$e+a$	e
e	e	$e+a$	0	a
$e+a$	$e+a$	e	a	0

32.8 Table

	0	a	e	$e+a$
0	0	0	0	0
a	0	e	a	$e+a$
e	0	a	e	$e+a$
$e+a$	0	$e+a$	$e+a$	0

respectively, we get Tables 32.7 and 32.8. For example, to see that $(e + a)(e + a) = 0$, we have

$$(1e + 1a)(1e + 1a) = (1 + 1)e + (1 + 1)a = 0e + 0a.$$

This example shows that a group algebra may have 0 divisors. Indeed, this is usually the case. ▲