16

Rings

Up to this point we have studied sets with a single binary operation satisfying certain axioms, but we are often more interested in working with sets that have two binary operations. For example, one of the most natural algebraic structures to study is the integers with the operations of addition and multiplication. These operations are related to one another by the distributive property. If we consider a set with two such related binary operations satisfying certain axioms, we have an algebraic structure called a ring. In a ring we add and multiply elements such as real numbers, complex numbers, matrices, and functions.

16.1 Rings

A nonempty set R is a ***ring*** if it has two closed binary operations, addition and multiplication, satisfying the following conditions.

1. $a + b = b + a$ for $a, b \in R$.
2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.
3. There is an element 0 in R such that $a + 0 = a$ for all $a \in R$.
4. For every element $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0$.
5. $(ab)c = a(bc)$ for $a, b, c \in R$.
6. For $a, b, c \in R$,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

This last condition, the distributive axiom, relates the binary operations of addition and multiplication. Notice that the first four axioms simply require that a ring be an abelian group under addition, so we could also have defined a ring to be an abelian group $(R, +)$ together with a second binary operation satisfying the fifth and sixth conditions given above.

If there is an element $1 \in R$ such that $1 \neq 0$ and $1a = a1 = a$ for each element $a \in R$, we say that R is a ring with ***unity*** or ***identity***. A ring R for which $ab = ba$ for all a, b in R is called a ***commutative ring***. A commutative ring R with identity is called an ***integral domain*** if, for every $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$. A ***division ring*** is a ring R, with an identity, in which every nonzero element in R is a ***unit***; that is, for each $a \in R$ with $a \neq 0$, there exists a unique element a^{-1} such that $a^{-1}a = aa^{-1} = 1$. A commutative division ring is called a ***field***. The relationship among rings, integral domains, division rings, and fields is shown in Figure 16.1.

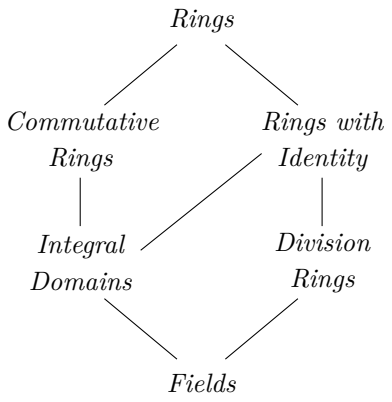

Figure 16.1: Types of rings

Example 16.2. As we have mentioned previously, the integers form a ring. In fact, $\mathbb{Z}$ is an integral domain. Certainly if $ab = 0$ for two integers a and b, either $a = 0$ or $b = 0$. However, $\mathbb{Z}$ is not a field. There is no integer that is the multiplicative inverse of 2, since $1/2$ is not an integer. The only integers with multiplicative inverses are 1 and -1.

Example 16.3. Under the ordinary operations of addition and multiplication, all of the familiar number systems are rings: the rationals, $\mathbb{Q}$; the real numbers, $\mathbb{R}$; and the complex numbers, $\mathbb{C}$. Each of these rings is a field.

Example 16.4. We can define the product of two elements a and b in $\mathbb{Z}_n$ by $ab \pmod{n}$. For instance, in $\mathbb{Z}_{12}$, $5 \cdot 7 \equiv 11 \pmod{12}$. This product makes the abelian group $\mathbb{Z}_n$ into a ring. Certainly $\mathbb{Z}_n$ is a commutative ring; however, it may fail to be an integral domain. If we consider $3 \cdot 4 \equiv 0 \pmod{12}$ in $\mathbb{Z}_{12}$, it is easy to see that a product of two nonzero elements in the ring can be equal to zero.

A nonzero element a in a ring R is called a ***zero divisor*** if there is a nonzero element b in R such that $ab = 0$. In the previous example, 3 and 4 are zero divisors in $\mathbb{Z}_{12}$.

Example 16.5. In calculus the continuous real-valued functions on an interval $[a, b]$ form a commutative ring. We add or multiply two functions by adding or multiplying the values of the functions. If $f(x) = x^2$ and $g(x) = \cos x$, then $(f + g)(x) = f(x) + g(x) = x^2 + \cos x$ and $(fg)(x) = f(x)g(x) = x^2 \cos x$.

Example 16.6. The 2×2 matrices with entries in $\mathbb{R}$ form a ring under the usual operations of matrix addition and multiplication. This ring is noncommutative, since it is usually the case that $AB \neq BA$. Also, notice that we can have $AB = 0$ when neither A nor B is zero.

Example 16.7. For an example of a noncommutative division ring, let

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

where $i^2 = -1$. These elements satisfy the following relations:

$$\begin{aligned} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 &= -1 \\ \mathbf{ij} &= \mathbf{k} \\ \mathbf{jk} &= \mathbf{i} \\ \mathbf{ki} &= \mathbf{j} \\ \mathbf{ji} &= -\mathbf{k} \end{aligned}$$

$$\mathbf{kj} = -\mathbf{i}$$
$$\mathbf{ik} = -\mathbf{j}.$$

Let $\mathbb{H}$ consist of elements of the form $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, where a, b, c, d are real numbers. Equivalently, $\mathbb{H}$ can be considered to be the set of all 2×2 matrices of the form

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix},$$

where $\alpha = a + di$ and $\beta = b + ci$ are complex numbers. We can define addition and multiplication on $\mathbb{H}$ either by the usual matrix operations or in terms of the generators 1, $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$:

$$\begin{aligned}&(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) \\ &= (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k}\end{aligned}$$

and

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k},$$

where

$$\begin{aligned}\alpha &= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\ \beta &= a_1b_2 + a_2b_1 + c_1d_2 - d_1c_2 \\ \gamma &= a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 \\ \delta &= a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2.\end{aligned}$$

Though multiplication looks complicated, it is actually a straightforward computation if we remember that we just add and multiply elements in $\mathbb{H}$ like polynomials and keep in mind the relationships between the generators $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$. The ring $\mathbb{H}$ is called the ring of ***quaternions***.

To show that the quaternions are a division ring, we must be able to find an inverse for each nonzero element. Notice that

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2.$$

This element can be zero only if a, b, c, and d are all zero. So if $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$,

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \left(\frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2} \right) = 1.$$

Proposition 16.8. *Let R be a ring with $a, b \in R$. Then*

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -ab$;
3. $(-a)(-b) = ab$.

Proof. To prove (1), observe that

$$a0 = a(0 + 0) = a0 + a0;$$

hence, $a0 = 0$. Similarly, $0a = 0$. For (2), we have $ab + a(-b) = a(b - b) = a0 = 0$; consequently, $-ab = a(-b)$. Similarly, $-ab = (-a)b$. Part (3) follows directly from (2) since $(-a)(-b) = -(a(-b)) = -(-ab) = ab$. □

Just as we have subgroups of groups, we have an analogous class of substructures for rings. A ***subring*** S of a ring R is a subset S of R such that S is also a ring under the inherited operations from R.

Example 16.9. The ring $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Notice that even though the original ring may have an identity, we do not require that its subring have an identity. We have the following chain of subrings:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

The following proposition gives us some easy criteria for determining whether or not a subset of a ring is indeed a subring. (We will leave the proof of this proposition as an exercise.)

Proposition 16.10. *Let R be a ring and S a subset of R. Then S is a subring of R if and only if the following conditions are satisfied.*

1. $S \neq \emptyset$.
2. $rs \in S$ *for all* $r, s \in S$.
3. $r - s \in S$ *for all* $r, s \in S$.

Example 16.11. Let $R = \mathbb{M}_2(\mathbb{R})$ be the ring of 2×2 matrices with entries in $\mathbb{R}$. If T is the set of upper triangular matrices in R; i.e.,

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\},$$

then T is a subring of R. If

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

are in T, then clearly $A - B$ is also in T. Also,

$$AB = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

is in T.

16.2 Integral Domains and Fields

Let us briefly recall some definitions. If R is a ring and r is a nonzero element in R, then r is said to be a ***zero divisor*** if there is some nonzero element $s \in R$ such that $rs = 0$. A commutative ring with identity is said to be an ***integral domain*** if it has no zero divisors. If an element a in a ring R with identity has a multiplicative inverse, we say that a is a ***unit***. If every nonzero element in a ring R is a unit, then R is called a ***division ring***. A commutative division ring is called a ***field***.

Example 16.12. If $i^2 = -1$, then the set $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$ forms a ring known as the ***Gaussian integers***. It is easily seen that the Gaussian integers are a subring of the complex numbers since they are closed under addition and multiplication. Let $\alpha = a + bi$ be a unit in $\mathbb{Z}[i]$. Then $\overline{\alpha} = a - bi$ is also a unit since if $\alpha\beta = 1$, then $\overline{\alpha}\overline{\beta} = 1$. If $\beta = c + di$, then

$$1 = \alpha\beta\overline{\alpha}\overline{\beta} = (a^2 + b^2)(c^2 + d^2).$$

Therefore, $a^2 + b^2$ must either be 1 or -1; or, equivalently, $a + bi = \pm 1$ or $a + bi = \pm i$. Therefore, units of this ring are ± 1 and $\pm i$; hence, the Gaussian integers are not a field. We will leave it as an exercise to prove that the Gaussian integers are an integral domain.

Example 16.13. The set of matrices

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

with entries in $\mathbb{Z}_2$ forms a field.

Example 16.14. The set $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field. The inverse of an element $a + b\sqrt{2}$ in $\mathbb{Q}(\sqrt{2}\,)$ is

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

We have the following alternative characterization of integral domains.

Proposition 16.15 Cancellation Law. *Let D be a commutative ring with identity. Then D is an integral domain if and only if for all nonzero elements $a \in D$ with $ab = ac$, we have $b = c$.*

Proof. Let D be an integral domain. Then D has no zero divisors. Let $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$. Hence, $b - c = 0$ and $b = c$.

Conversely, let us suppose that cancellation is possible in D. That is, suppose that $ab = ac$ implies $b = c$. Let $ab = 0$. If $a \neq 0$, then $ab = a0$ or $b = 0$. Therefore, a cannot be a zero divisor. □

The following surprising theorem is due to Wedderburn.

Theorem 16.16. *Every finite integral domain is a field.*

Proof. Let D be a finite integral domain and D^* be the set of nonzero elements of D. We must show that every element in D^* has an inverse. For each $a \in D^*$ we can define a map $\lambda_a : D^* \to D^*$ by $\lambda_a(d) = ad$. This map makes sense, because if $a \neq 0$ and $d \neq 0$, then $ad \neq 0$. The map λ_a is one-to-one, since for $d_1, d_2 \in D^*$,

$$ad_1 = \lambda_a(d_1) = \lambda_a(d_2) = ad_2$$

implies $d_1 = d_2$ by left cancellation. Since D^* is a finite set, the map λ_a must also be onto; hence, for some $d \in D^*$, $\lambda_a(d) = ad = 1$. Therefore, a has a left inverse. Since D is commutative, d must also be a right inverse for a. Consequently, D is a field. □

For any nonnegative integer n and any element r in a ring R we write $r + \cdots + r$ (n times) as nr. We define the ***characteristic*** of a ring R to be the least positive integer n such that $nr = 0$ for all $r \in R$. If no such integer exists, then the characteristic of R is defined to be 0. We will denote the characteristic of R by $\operatorname{char} R$.

Example 16.17. For every prime p, $\mathbb{Z}_p$ is a field of characteristic p. By Proposition 3.4, every nonzero element in $\mathbb{Z}_p$ has an inverse; hence, $\mathbb{Z}_p$ is a field. If a is any nonzero element in the field, then $pa = 0$, since the order of any nonzero element in the abelian group $\mathbb{Z}_p$ is p.

Lemma 16.18. *Let R be a ring with identity. If 1 has order n, then the characteristic of R is n.*

Proof. If 1 has order n, then n is the least positive integer such that $n1 = 0$. Thus, for all $r \in R$,

$$nr = n(1r) = (n1)r = 0r = 0.$$

On the other hand, if no positive n exists such that $n1 = 0$, then the characteristic of R is zero. □

Theorem 16.19. *The characteristic of an integral domain is either prime or zero.*

PROOF. Let D be an integral domain and suppose that the characteristic of D is n with $n \neq 0$. If n is not prime, then $n = ab$, where $1 < a < n$ and $1 < b < n$. By Lemma 16.18, we need only consider the case $n1 = 0$. Since $0 = n1 = (ab)1 = (a1)(b1)$ and there are no zero divisors in D, either $a1 = 0$ or $b1 = 0$. Hence, the characteristic of D must be less than n, which is a contradiction. Therefore, n must be prime. □

16.3 Ring Homomorphisms and Ideals

In the study of groups, a homomorphism is a map that preserves the operation of the group. Similarly, a homomorphism between rings preserves the operations of addition and multiplication in the ring. More specifically, if R and S are rings, then a ***ring homomorphism*** is a map $\phi : R \to S$ satisfying

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \end{aligned}$$

for all $a, b \in R$. If $\phi : R \to S$ is a one-to-one and onto homomorphism, then ϕ is called an ***isomorphism*** of rings.

The set of elements that a ring homomorphism maps to 0 plays a fundamental role in the theory of rings. For any ring homomorphism $\phi : R \to S$, we define the ***kernel*** of a ring homomorphism to be the set

$$\ker \phi = \{r \in R : \phi(r) = 0\}.$$

Example 16.20. For any integer n we can define a ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $a \mapsto a \pmod{n}$. This is indeed a ring homomorphism, since

$$\begin{aligned} \phi(a+b) &= (a+b) \pmod{n} \\ &= a \pmod{n} + b \pmod{n} \\ &= \phi(a) + \phi(b) \end{aligned}$$

and

$$\begin{aligned} \phi(ab) &= ab \pmod{n} \\ &= a \pmod{n} \cdot b \pmod{n} \\ &= \phi(a)\phi(b). \end{aligned}$$

The kernel of the homomorphism ϕ is $n\mathbb{Z}$.

Example 16.21. Let $C[a, b]$ be the ring of continuous real-valued functions on an interval $[a, b]$ as in Example 16.5. For a fixed $\alpha \in [a, b]$, we can define a ring homomorphism $\phi_\alpha : C[a, b] \to \mathbb{R}$ by $\phi_\alpha(f) = f(\alpha)$. This is a ring homomorphism since

$$\begin{aligned} \phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g) \\ \phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g). \end{aligned}$$

Ring homomorphisms of the type ϕ_α are called ***evaluation homomorphisms***.

In the next proposition we will examine some fundamental properties of ring homomorphisms. The proof of the proposition is left as an exercise.

Proposition 16.22. *Let $\phi : R \to S$ be a ring homomorphism.*

1. *If R is a commutative ring, then $\phi(R)$ is a commutative ring.*
2. *$\phi(0) = 0$.*
3. *Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.*
4. *If R is a field and $\phi(R) \neq \{0\}$, then $\phi(R)$ is a field.*

In group theory we found that normal subgroups play a special role. These subgroups have nice characteristics that make them more interesting to study than arbitrary subgroups. In ring theory the objects corresponding to normal subgroups are a special class of subrings called ideals. An ***ideal*** in a ring R is a subring I of R such that if a is in I and r is in R, then both ar and ra are in I; that is, $rI \subset I$ and $Ir \subset I$ for all $r \in R$.

Example 16.23. Every ring R has at least two ideals, $\{0\}$ and R. These ideals are called the ***trivial ideals***.

Let R be a ring with identity and suppose that I is an ideal in R such that 1 is in I. Since for any $r \in R$, $r1 = r \in I$ by the definition of an ideal, $I = R$.

Example 16.24. If a is any element in a commutative ring R with identity, then the set

$$\langle a \rangle = \{ar : r \in R\}$$

is an ideal in R. Certainly, $\langle a \rangle$ is nonempty since both $0 = a0$ and $a = a1$ are in $\langle a \rangle$. The sum of two elements in $\langle a \rangle$ is again in $\langle a \rangle$ since $ar + ar' = a(r + r')$. The inverse of ar is $-ar = a(-r) \in \langle a \rangle$. Finally, if we multiply an element $ar \in \langle a \rangle$ by an arbitrary element $s \in R$, we have $s(ar) = a(sr)$. Therefore, $\langle a \rangle$ satisfies the definition of an ideal.

If R is a commutative ring with identity, then an ideal of the form $\langle a \rangle = \{ar : r \in R\}$ is called a ***principal ideal***.

Theorem 16.25. *Every ideal in the ring of integers $\mathbb{Z}$ is a principal ideal.*

PROOF. The zero ideal $\{0\}$ is a principal ideal since $\langle 0 \rangle = \{0\}$. If I is any nonzero ideal in $\mathbb{Z}$, then I must contain some positive integer m. There exists a least positive integer n in I by the Principle of Well-Ordering. Now let a be any element in I. Using the division algorithm, we know that there exist integers q and r such that

$$a = nq + r$$

where $0 \leq r < n$. This equation tells us that $r = a - nq \in I$, but r must be 0 since n is the least positive element in I. Therefore, $a = nq$ and $I = \langle n \rangle$. □

Example 16.26. The set $n\mathbb{Z}$ is ideal in the ring of integers. If na is in $n\mathbb{Z}$ and b is in $\mathbb{Z}$, then nab is in $n\mathbb{Z}$ as required. In fact, by Theorem 16.25, these are the only ideals of $\mathbb{Z}$.

Proposition 16.27. *The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R.*

PROOF. We know from group theory that $\ker \phi$ is an additive subgroup of R. Suppose that $r \in R$ and $a \in \ker \phi$. Then we must show that ar and ra are in $\ker \phi$. However,

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$$

and

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0.$$ □

Remark 16.28. In our definition of an ideal we have required that $rI \subset I$ and $Ir \subset I$ for all $r \in R$. Such ideals are sometimes referred to as ***two-sided ideals***. We can also consider ***one-sided ideals***; that is, we may require only that either $rI \subset I$ or $Ir \subset I$ for $r \in R$ hold but not both. Such ideals are called ***left ideals*** and ***right ideals***, respectively. Of course, in a commutative ring any ideal must be two-sided. In this text we will concentrate on two-sided ideals.

Theorem 16.29. *Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by*

$$(r + I)(s + I) = rs + I.$$

Proof. We already know that R/I is an abelian group under addition. Let $r + I$ and $s + I$ be in R/I. We must show that the product $(r + I)(s + I) = rs + I$ is independent of the choice of coset; that is, if $r' \in r + I$ and $s' \in s + I$, then $r's'$ must be in $rs + I$. Since $r' \in r + I$, there exists an element a in I such that $r' = r + a$. Similarly, there exists a $b \in I$ such that $s' = s + b$. Notice that

$$r's' = (r + a)(s + b) = rs + as + rb + ab$$

and $as + rb + ab \in I$ since I is an ideal; consequently, $r's' \in rs + I$. We will leave as an exercise the verification of the associative law for multiplication and the distributive laws. □

The ring R/I in Theorem 16.29 is called the ***factor*** or ***quotient ring***. Just as with group homomorphisms and normal subgroups, there is a relationship between ring homomorphisms and ideals.

Theorem 16.30. *Let I be an ideal of R. The map $\phi : R \to R/I$ defined by $\phi(r) = r + I$ is a ring homomorphism of R onto R/I with kernel I.*

Proof. Certainly $\phi : R \to R/I$ is a surjective abelian group homomorphism. It remains to show that ϕ works correctly under ring multiplication. Let r and s be in R. Then

$$\phi(r)\phi(s) = (r + I)(s + I) = rs + I = \phi(rs),$$

which completes the proof of the theorem. □

The map $\phi : R \to R/I$ is often called the ***natural*** or ***canonical homomorphism***. In ring theory we have isomorphism theorems relating ideals and ring homomorphisms similar to the isomorphism theorems for groups that relate normal subgroups and homomorphisms in Chapter 11. We will prove only the First Isomorphism Theorem for rings in this chapter and leave the proofs of the other two theorems as exercises. All of the proofs are similar to the proofs of the isomorphism theorems for groups.

Theorem 16.31 First Isomorphism Theorem. *Let $\psi : R \to S$ be a ring homomorphism. Then $\ker \psi$ is an ideal of R. If $\phi : R \to R/\ker \psi$ is the canonical homomorphism, then there exists a unique isomorphism $\eta : R/\ker \psi \to \psi(R)$ such that $\psi = \eta\phi$.*

Proof. Let $K = \ker \psi$. By the First Isomorphism Theorem for groups, there exists a well-defined group homomorphism $\eta : R/K \to \psi(R)$ defined by $\eta(r + K) = \psi(r)$ for the additive abelian groups R and R/K. To show that this is a ring homomorphism, we need only show that $\eta((r + K)(s + K)) = \eta(r + K)\eta(s + K)$; but

$$\begin{aligned} \eta((r + K)(s + K)) &= \eta(rs + K) \\ &= \psi(rs) \\ &= \psi(r)\psi(s) \\ &= \eta(r + K)\eta(s + K). \end{aligned}$$

□

Theorem 16.32 Second Isomorphism Theorem. *Let I be a subring of a ring R and J an ideal of R. Then $I \cap J$ is an ideal of I and*

$$I/I \cap J \cong (I + J)/J.$$

Theorem 16.33 Third Isomorphism Theorem. *Let R be a ring and I and J be ideals of R where $J \subset I$. Then*

$$R/I \cong \frac{R/J}{I/J}.$$

Theorem 16.34 Correspondence Theorem. *Let I be an ideal of a ring R. Then $S \mapsto S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R containing I correspond to ideals of R/I.*

16.4 Maximal and Prime Ideals

In this particular section we are especially interested in certain ideals of commutative rings. These ideals give us special types of factor rings. More specifically, we would like to characterize those ideals I of a commutative ring R such that R/I is an integral domain or a field.

A proper ideal M of a ring R is a ***maximal ideal*** of R if the ideal M is not a proper subset of any ideal of R except R itself. That is, M is a maximal ideal if for any ideal I properly containing M, $I = R$. The following theorem completely characterizes maximal ideals for commutative rings with identity in terms of their corresponding factor rings.

Theorem 16.35. *Let R be a commutative ring with identity and M an ideal in R. Then M is a maximal ideal of R if and only if R/M is a field.*

Proof. Let M be a maximal ideal in R. If R is a commutative ring, then R/M must also be a commutative ring. Clearly, $1 + M$ acts as an identity for R/M. We must also show that every nonzero element in R/M has an inverse. If $a + M$ is a nonzero element in R/M, then $a \notin M$. Define I to be the set $\{ra + m : r \in R \text{ and } m \in M\}$. We will show that I is an ideal in R. The set I is nonempty since $0a + 0 = 0$ is in I. If $r_1a + m_1$ and $r_2a + m_2$ are two elements in I, then

$$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2)$$

is in I. Also, for any $r \in R$ it is true that $rI \subset I$; hence, I is closed under multiplication and satisfies the necessary conditions to be an ideal. Therefore, by Proposition 16.10 and the definition of an ideal, I is an ideal properly containing M. Since M is a maximal ideal, $I = R$; consequently, by the definition of I there must be an m in M and an element b in R such that $1 = ab + m$. Therefore,

$$1 + M = ab + M = ba + M = (a + M)(b + M).$$

Conversely, suppose that M is an ideal and R/M is a field. Since R/M is a field, it must contain at least two elements: $0 + M = M$ and $1 + M$. Hence, M is a proper ideal of R. Let I be any ideal properly containing M. We need to show that $I = R$. Choose a in I but not in M. Since $a + M$ is a nonzero element in a field, there exists an element $b + M$ in R/M such that $(a + M)(b + M) = ab + M = 1 + M$. Consequently, there exists an element $m \in M$ such that $ab + m = 1$ and 1 is in I. Therefore, $r1 = r \in I$ for all $r \in R$. Consequently, $I = R$. □

Example 16.36. Let $p\mathbb{Z}$ be an ideal in $\mathbb{Z}$, where p is prime. Then $p\mathbb{Z}$ is a maximal ideal since $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a field.

A proper ideal P in a commutative ring R is called a ***prime ideal*** if whenever $ab \in P$, then either $a \in P$ or $b \in P$.[1]

Example 16.37. It is easy to check that the set $P = \{0, 2, 4, 6, 8, 10\}$ is an ideal in $\mathbb{Z}_{12}$. This ideal is prime. In fact, it is a maximal ideal.

Proposition 16.38. *Let R be a commutative ring with identity 1, where $1 \neq 0$. Then P is a prime ideal in R if and only if R/P is an integral domain.*

PROOF. First let us assume that P is an ideal in R and R/P is an integral domain. Suppose that $ab \in P$. If $a+P$ and $b+P$ are two elements of R/P such that $(a+P)(b+P) = 0+P = P$, then either $a + P = P$ or $b + P = P$. This means that either a is in P or b is in P, which shows that P must be prime.

Conversely, suppose that P is prime and

$$(a + P)(b + P) = ab + P = 0 + P = P.$$

Then $ab \in P$. If $a \notin P$, then b must be in P by the definition of a prime ideal; hence, $b + P = 0 + P$ and R/P is an integral domain. □

Example 16.39. Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$. The factor ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is an integral domain only when n is prime. It is actually a field. Hence, the nonzero prime ideals in $\mathbb{Z}$ are the ideals $p\mathbb{Z}$, where p is prime. This example really justifies the use of the word "prime" in our definition of prime ideals.

Since every field is an integral domain, we have the following corollary.

Corollary 16.40. *Every maximal ideal in a commutative ring with identity is also a prime ideal.*

Historical Note

Amalie Emmy Noether, one of the outstanding mathematicians of the twentieth century, was born in Erlangen, Germany in 1882. She was the daughter of Max Noether (1844–1921), a distinguished mathematician at the University of Erlangen. Together with Paul Gordon (1837–1912), Emmy Noether's father strongly influenced her early education. She entered the University of Erlangen at the age of 18. Although women had been admitted to universities in England, France, and Italy for decades, there was great resistance to their presence at universities in Germany. Noether was one of only two women among the university's 986 students. After completing her doctorate under Gordon in 1907, she continued to do research at Erlangen, occasionally lecturing when her father was ill.

Noether went to Göttingen to study in 1916. David Hilbert and Felix Klein tried unsuccessfully to secure her an appointment at Göttingen. Some of the faculty objected to women lecturers, saying, "What will our soldiers think when they return to the university and are expected to learn at the feet of a woman?" Hilbert, annoyed at the question, responded, "Meine Herren, I do not see that the sex of a candidate is an argument against her admission as a Privatdozent. After all, the Senate is not a bathhouse." At the end of World War I, attitudes changed and conditions greatly improved for women. After Noether

[1] It is possible to define prime ideals in a noncommutative ring. See [1] or [3].

passed her habilitation examination in 1919, she was given a title and was paid a small sum for her lectures.

In 1922, Noether became a Privatdozent at Göttingen. Over the next 11 years she used axiomatic methods to develop an abstract theory of rings and ideals. Though she was not good at lecturing, Noether was an inspiring teacher. One of her many students was B. L. van der Waerden, author of the first text treating abstract algebra from a modern point of view. Some of the other mathematicians Noether influenced or closely worked with were Alexandroff, Artin, Brauer, Courant, Hasse, Hopf, Pontryagin, von Neumann, and Weyl. One of the high points of her career was an invitation to address the International Congress of Mathematicians in Zurich in 1932. In spite of all the recognition she received from her colleagues, Noether's abilities were never recognized as they should have been during her lifetime. She was never promoted to full professor by the Prussian academic bureaucracy.

In 1933, Noether, a Jew, was banned from participation in all academic activities in Germany. She emigrated to the United States, took a position at Bryn Mawr College, and became a member of the Institute for Advanced Study at Princeton. Noether died suddenly on April 14, 1935. After her death she was eulogized by such notable scientists as Albert Einstein.

16.5 An Application to Software Design

The Chinese Remainder Theorem is a result from elementary number theory about the solution of systems of simultaneous congruences. The Chinese mathematician Sun-tsï wrote about the theorem in the first century A.D. This theorem has some interesting consequences in the design of software for parallel processors.

Lemma 16.41. *Let m and n be positive integers such that $\gcd(m,n) = 1$. Then for $a, b \in \mathbb{Z}$ the system*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a solution. If x_1 and x_2 are two solutions of the system, then $x_1 \equiv x_2 \pmod{mn}$.

Proof. The equation $x \equiv a \pmod{m}$ has a solution since $a + km$ satisfies the equation for all $k \in \mathbb{Z}$. We must show that there exists an integer k_1 such that

$$a + k_1 m \equiv b \pmod{n}.$$

This is equivalent to showing that

$$k_1 m \equiv (b - a) \pmod{n}$$

has a solution for k_1. Since m and n are relatively prime, there exist integers s and t such that $ms + nt = 1$. Consequently,

$$(b - a)ms = (b - a) - (b - a)nt,$$

or

$$[(b - a)s]m \equiv (b - a) \pmod{n}.$$

Now let $k_1 = (b - a)s$.

To show that any two solutions are congruent modulo mn, let c_1 and c_2 be two solutions of the system. That is,

$$c_i \equiv a \pmod{m}$$

$$c_i \equiv b \pmod{n}$$

for $i = 1, 2$. Then

$$\begin{aligned} c_2 &\equiv c_1 \pmod{m} \\ c_2 &\equiv c_1 \pmod{n}. \end{aligned}$$

Therefore, both m and n divide $c_1 - c_2$. Consequently, $c_2 \equiv c_1 \pmod{mn}$. □

Example 16.42. Let us solve the system

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

Using the Euclidean algorithm, we can find integers s and t such that $4s + 5t = 1$. Two such integers are $s = 4$ and $t = -3$. Consequently,

$$x = a + k_1 m = 3 + 4k_1 = 3 + 4[(5 - 4)4] = 19.$$

Theorem 16.43 Chinese Remainder Theorem. *Let $n_1, n_2, \ldots, n_k$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then for any integers $a_1, \ldots, a_k$, the system*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution. Furthermore, any two solutions of the system are congruent modulo $n_1 n_2 \cdots n_k$.

Proof. We will use mathematical induction on the number of equations in the system. If there are $k = 2$ equations, then the theorem is true by Lemma 16.41. Now suppose that the result is true for a system of k equations or less and that we wish to find a solution of

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{k+1} \pmod{n_{k+1}}. \end{aligned}$$

Considering the first k equations, there exists a solution that is unique modulo $n_1 \cdots n_k$, say a. Since $n_1 \cdots n_k$ and n_{k+1} are relatively prime, the system

$$\begin{aligned} x &\equiv a \pmod{n_1 \cdots n_k} \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

has a solution that is unique modulo $n_1 \ldots n_{k+1}$ by the lemma. □

Example 16.44. Let us solve the system

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 1 \pmod{9} \end{aligned}$$

$$x \equiv 5 \pmod 7.$$

From Example 16.42 we know that 19 is a solution of the first two congruences and any other solution of the system is congruent to 19 (mod 20). Hence, we can reduce the system to a system of three congruences:

$$\begin{aligned} x &\equiv 19 \pmod{20} \\ x &\equiv 1 \pmod 9 \\ x &\equiv 5 \pmod 7. \end{aligned}$$

Solving the next two equations, we can reduce the system to

$$\begin{aligned} x &\equiv 19 \pmod{180} \\ x &\equiv 5 \pmod 7. \end{aligned}$$

Solving this last system, we find that 19 is a solution for the system that is unique up to modulo 1260.

One interesting application of the Chinese Remainder Theorem in the design of computer software is that the theorem allows us to break up a calculation involving large integers into several less formidable calculations. A computer will handle integer calculations only up to a certain size due to the size of its processor chip, which is usually a 32 or 64-bit processor chip. For example, the largest integer available on a computer with a 64-bit processor chip is

$$2^{63} - 1 = 9{,}223{,}372{,}036{,}854{,}775{,}807.$$

Larger processors such as 128 or 256-bit have been proposed or are under development. There is even talk of a 512-bit processor chip. The largest integer that such a chip could store with be $2^{511} - 1$, which would be a 154 digit number. However, we would need to deal with much larger numbers to break sophisticated encryption schemes.

Special software is required for calculations involving larger integers which cannot be added directly by the machine. By using the Chinese Remainder Theorem we can break down large integer additions and multiplications into calculations that the computer can handle directly. This is especially useful on parallel processing computers which have the ability to run several programs concurrently.

Most computers have a single central processing unit (CPU) containing one processor chip and can only add two numbers at a time. To add a list of ten numbers, the CPU must do nine additions in sequence. However, a parallel processing computer has more than one CPU. A computer with 10 CPUs, for example, can perform 10 different additions at the same time. If we can take a large integer and break it down into parts, sending each part to a different CPU, then by performing several additions or multiplications simultaneously on those parts, we can work with an integer that the computer would not be able to handle as a whole.

Example 16.45. Suppose that we wish to multiply 2134 by 1531. We will use the integers 95, 97, 98, and 99 because they are relatively prime. We can break down each integer into four parts:

$$\begin{aligned} 2134 &\equiv 44 \pmod{95} \\ 2134 &\equiv 0 \pmod{97} \\ 2134 &\equiv 76 \pmod{98} \\ 2134 &\equiv 55 \pmod{99} \end{aligned}$$

and

$$\begin{aligned} 1531 &\equiv 11 \pmod{95} \\ 1531 &\equiv 76 \pmod{97} \\ 1531 &\equiv 61 \pmod{98} \\ 1531 &\equiv 46 \pmod{99}. \end{aligned}$$

Multiplying the corresponding equations, we obtain

$$\begin{aligned} 2134 \cdot 1531 &\equiv 44 \cdot 11 \equiv 9 \pmod{95} \\ 2134 \cdot 1531 &\equiv 0 \cdot 76 \equiv 0 \pmod{97} \\ 2134 \cdot 1531 &\equiv 76 \cdot 61 \equiv 30 \pmod{98} \\ 2134 \cdot 1531 &\equiv 55 \cdot 46 \equiv 55 \pmod{99}. \end{aligned}$$

Each of these four computations can be sent to a different processor if our computer has several CPUs. By the above calculation, we know that $2134 \cdot 1531$ is a solution of the system

$$\begin{aligned} x &\equiv 9 \pmod{95} \\ x &\equiv 0 \pmod{97} \\ x &\equiv 30 \pmod{98} \\ x &\equiv 55 \pmod{99}. \end{aligned}$$

The Chinese Remainder Theorem tells us that solutions are unique up to modulo $95 \cdot 97 \cdot 98 \cdot 99 = 89{,}403{,}930$. Solving this system of congruences for x tells us that $2134 \cdot 1531 = 3{,}267{,}154$.

The conversion of the computation into the four subcomputations will take some computing time. In addition, solving the system of congruences can also take considerable time. However, if we have many computations to be performed on a particular set of numbers, it makes sense to transform the problem as we have done above and to perform the necessary calculations simultaneously.

Sage Rings are at the heart of Sage's design, so you will find a wide range of possibilities for computing with rings and fields. Ideals, quotients, and homomorphisms are all available.

16.6 Exercises

1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) $7\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

(e) $\mathbb{Z}[\sqrt{3}\,] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

(g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$

(h) $\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

2. Let R be the ring of 2×2 matrices of the form

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

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a subring S of R with an identity.

3. List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$

4. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

(c) $\mathbb{M}_2(\mathbb{R})$, the 2×2 matrices with entries in $\mathbb{R}$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{Q}$

5. For each of the following rings R with ideal I, give an addition table and a multiplication table for R/I.

(a) $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$

(b) $R = \mathbb{Z}_{12}$ and $I = \{0, 3, 6, 9\}$

6. Find all homomorphisms $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

7. Prove that $\mathbb{R}$ is not isomorphic to $\mathbb{C}$.

8. Prove or disprove: The ring $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is isomorphic to the ring $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

9. What is the characteristic of the field formed by the set of matrices

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

with entries in $\mathbb{Z}_2$?

10. Define a map $\phi : \mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Show that ϕ is an isomorphism of $\mathbb{C}$ with its image in $\mathbb{M}_2(\mathbb{R})$.

11. Prove that the Gaussian integers, $\mathbb{Z}[i]$, are an integral domain.

12. Prove that $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ is an integral domain.

13. Solve each of the following systems of congruences.

(a)

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 6 \pmod{11} \end{aligned}$$

(b)

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 5 \pmod{15} \end{aligned}$$

(c)

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 7 \\ x &\equiv 7 \pmod 9 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

(d)

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 1 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

14. Use the method of parallel computation outlined in the text to calculate $2234 + 4121$ by dividing the calculation into four separate additions modulo 95, 97, 98, and 99.

15. Explain why the method of parallel computation outlined in the text fails for $2134 \cdot 1531$ if we attempt to break the calculation down into two smaller calculations modulo 98 and 99.

16. If R is a field, show that the only two ideals of R are $\{0\}$ and R itself.

17. Let a be any element in a ring R with identity. Show that $(-1)a = -a$.

18. Let $\phi : R \to S$ be a ring homomorphism. Prove each of the following statements.

(a) If R is a commutative ring, then $\phi(R)$ is a commutative ring.

(b) $\phi(0) = 0$.

(c) Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.

(d) If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.

19. Prove that the associative law for multiplication and the distributive laws hold in R/I.

20. Prove the Second Isomorphism Theorem for rings: Let I be a subring of a ring R and J an ideal in R. Then $I \cap J$ is an ideal in I and

$$I/I \cap J \cong I + J/J.$$

21. Prove the Third Isomorphism Theorem for rings: Let R be a ring and I and J be ideals of R, where $J \subset I$. Then

$$R/I \cong \frac{R/J}{I/J}.$$

22. Prove the Correspondence Theorem: Let I be an ideal of a ring R. Then $S \to S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R correspond to ideals of R/I.

23. Let R be a ring and S a subset of R. Show that S is a subring of R if and only if each of the following conditions is satisfied.

(a) $S \neq \emptyset$.

(b) $rs \in S$ for all $r, s \in S$.

(c) $r - s \in S$ for all $r, s \in S$.

24. Let R be a ring with a collection of subrings $\{R_\alpha\}$. Prove that $\bigcap R_\alpha$ is a subring of R. Give an example to show that the union of two subrings is not necessarily a subring.

25. Let $\{I_\alpha\}_{\alpha \in A}$ be a collection of ideals in a ring R. Prove that $\bigcap_{\alpha \in A} I_\alpha$ is also an ideal in R. Give an example to show that if I_1 and I_2 are ideals in R, then $I_1 \cup I_2$ may not be an ideal.

26. Let R be an integral domain. Show that if the only ideals in R are $\{0\}$ and R itself, R must be a field.

27. Let R be a commutative ring. An element a in R is ***nilpotent*** if $a^n = 0$ for some positive integer n. Show that the set of all nilpotent elements forms an ideal in R.

28. A ring R is a ***Boolean ring*** if for every $a \in R$, $a^2 = a$. Show that every Boolean ring is a commutative ring.

29. Let R be a ring, where $a^3 = a$ for all $a \in R$. Prove that R must be a commutative ring.

30. Let R be a ring with identity 1_R and S a subring of R with identity 1_S. Prove or disprove that $1_R = 1_S$.

31. If we do not require the identity of a ring to be distinct from 0, we will not have a very interesting mathematical structure. Let R be a ring such that $1 = 0$. Prove that $R = \{0\}$.

32. Let S be a nonempty subset of a ring R. Prove that there is a subring R' of R that contains S.

33. Let R be a ring. Define the ***center*** of R to be

$$Z(R) = \{a \in R : ar = ra \text{ for all } r \in R\}.$$

Prove that $Z(R)$ is a commutative subring of R.

34. Let p be prime. Prove that

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z} \text{ and } \gcd(b, p) = 1\}$$

is a ring. The ring $\mathbb{Z}_{(p)}$ is called the ***ring of integers localized at*** p.

35. Prove or disprove: Every finite integral domain is isomorphic to $\mathbb{Z}_p$.

36. Let R be a ring with identity.

(a) Let u be a unit in R. Define a map $i_u : R \to R$ by $r \mapsto uru^{-1}$. Prove that i_u is an automorphism of R. Such an automorphism of R is called an inner automorphism of R. Denote the set of all inner automorphisms of R by $\text{Inn}(R)$.

(b) Denote the set of all automorphisms of R by $\text{Aut}(R)$. Prove that $\text{Inn}(R)$ is a normal subgroup of $\text{Aut}(R)$.

(c) Let $U(R)$ be the group of units in R. Prove that the map

$$\phi : U(R) \to \text{Inn}(R)$$

defined by $u \mapsto i_u$ is a homomorphism. Determine the kernel of ϕ.

(d) Compute $\text{Aut}(\mathbb{Z})$, $\text{Inn}(\mathbb{Z})$, and $U(\mathbb{Z})$.

37. Let R and S be arbitrary rings. Show that their Cartesian product is a ring if we define addition and multiplication in $R \times S$ by

(a) $(r, s) + (r', s') = (r + r', s + s')$

(b) $(r, s)(r', s') = (rr', ss')$

38. An element x in a ring is called an ***idempotent*** if $x^2 = x$. Prove that the only idempotents in an integral domain are 0 and 1. Find a ring with a idempotent x not equal to 0 or 1.

39. Let $\gcd(a, n) = d$ and $\gcd(b, d) \neq 1$. Prove that $ax \equiv b \pmod{n}$ does not have a solution.

40. **The Chinese Remainder Theorem for Rings.** Let R be a ring and I and J be ideals in R such that $I + J = R$.

(a) Show that for any r and s in R, the system of equations

$$\begin{aligned} x &\equiv r \pmod{I} \\ x &\equiv s \pmod{J} \end{aligned}$$

has a solution.

(b) In addition, prove that any two solutions of the system are congruent modulo $I \cap J$.

(c) Let I and J be ideals in a ring R such that $I + J = R$. Show that there exists a ring isomorphism

$$R/(I \cap J) \cong R/I \times R/J.$$

16.7 Programming Exercise

1. Write a computer program implementing fast addition and multiplication using the Chinese Remainder Theorem and the method outlined in the text.

References and Suggested Readings

[1] Anderson, F. W. and Fuller, K. R. *Rings and Categories of Modules.* 2nd ed. Springer, New York, 1992.

[2] Atiyah, M. F. and MacDonald, I. G. *Introduction to Commutative Algebra.* Westview Press, Boulder, CO, 1994.

[3] Herstein, I. N. *Noncommutative Rings.* Mathematical Association of America, Washington, DC, 1994.

[4] Kaplansky, I. *Commutative Rings.* Revised edition. University of Chicago Press, Chicago, 1974.

[5] Knuth, D. E. *The Art of Computer Programming: Semi-Numerical Algorithms*, vol. 2. 3rd ed. Addison-Wesley Professional, Boston, 1997.

[6] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998. A good source for applications.

[7] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[**8**] McCoy, N. H. *Rings and Ideals*. Carus Monograph Series, No. 8. Mathematical Association of America, Washington, DC, 1968.

[**9**] McCoy, N. H. *The Theory of Rings*. Chelsea, New York, 1972.

[**10**] Zariski, O. and Samuel, P. *Commutative Algebra*, vols. I and II. Springer, New York, 1975, 1960.

17

Polynomials

Most people are fairly familiar with polynomials by the time they begin to study abstract algebra. When we examine polynomial expressions such as

$$p(x) = x^3 - 3x + 2$$
$$q(x) = 3x^2 - 6x + 5,$$

we have a pretty good idea of what $p(x) + q(x)$ and $p(x)q(x)$ mean. We just add and multiply polynomials as functions; that is,

$$\begin{aligned}(p+q)(x) &= p(x) + q(x) \\ &= (x^3 - 3x + 2) + (3x^2 - 6x + 5) \\ &= x^3 + 3x^2 - 9x + 7\end{aligned}$$

and

$$\begin{aligned}(pq)(x) &= p(x)q(x) \\ &= (x^3 - 3x + 2)(3x^2 - 6x + 5) \\ &= 3x^5 - 6x^4 - 4x^3 + 24x^2 - 27x + 10.\end{aligned}$$

It is probably no surprise that polynomials form a ring. In this chapter we shall emphasize the algebraic structure of polynomials by studying polynomial rings. We can prove many results for polynomial rings that are similar to the theorems we proved for the integers. Analogs of prime numbers, the division algorithm, and the Euclidean algorithm exist for polynomials.

17.1 Polynomial Rings

Throughout this chapter we shall assume that R is a commutative ring with identity. Any expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where $a_i \in R$ and $a_n \neq 0$, is called a ***polynomial over*** R with ***indeterminate*** x. The elements $a_0, a_1, \ldots, a_n$ are called the ***coefficients*** of f. The coefficient a_n is called the ***leading coefficient***. A polynomial is called ***monic*** if the leading coefficient is 1. If n is the largest nonnegative number for which $a_n \neq 0$, we say that the ***degree*** of f is n and write $\deg f(x) = n$. If no such n exists—that is, if $f = 0$ is the zero polynomial—then the degree

of f is defined to be $-\infty$. We will denote the set of all polynomials with coefficients in a ring R by $R[x]$. Two polynomials are equal exactly when their corresponding coefficients are equal; that is, if we let

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m,$$

then $p(x) = q(x)$ if and only if $a_i = b_i$ for all $i \geq 0$.

To show that the set of all polynomials forms a ring, we must first define addition and multiplication. We define the sum of two polynomials as follows. Let

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

where $c_i = a_i + b_i$ for each i. We define the product of $p(x)$ and $q(x)$ to be

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$$

for each i. Notice that in each case some of the coefficients may be zero.

Example 17.1. Suppose that

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

and

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

are polynomials in $\mathbb{Z}[x]$. If the coefficient of some term in a polynomial is zero, then we usually just omit that term. In this case we would write $p(x) = 3 + 2x^3$ and $q(x) = 2 - x^2 + 4x^4$. The sum of these two polynomials is

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

The product,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7,$$

can be calculated either by determining the c_is in the definition or by simply multiplying polynomials in the same way as we have always done.

Example 17.2. Let

$$p(x) = 3 + 3x^3 \qquad \text{and} \qquad q(x) = 4 + 4x^2 + 4x^4$$

be polynomials in $\mathbb{Z}_{12}[x]$. The sum of $p(x)$ and $q(x)$ is $7 + 4x^2 + 3x^3 + 4x^4$. The product of the two polynomials is the zero polynomial. This example tells us that we can not expect $R[x]$ to be an integral domain if R is not an integral domain.

Theorem 17.3. *Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.*

PROOF. Our first task is to show that $R[x]$ is an abelian group under polynomial addition. The zero polynomial, $f(x) = 0$, is the additive identity. Given a polynomial $p(x) = \sum_{i=0}^{n} a_i x^i$, the inverse of $p(x)$ is easily verified to be $-p(x) = \sum_{i=0}^{n} (-a_i) x^i = -\sum_{i=0}^{n} a_i x^i$. Commutativity and associativity follow immediately from the definition of polynomial addition and from the fact that addition in R is both commutative and associative.

To show that polynomial multiplication is associative, let

$$\begin{aligned} p(x) &= \sum_{i=0}^{m} a_i x^i, \\ q(x) &= \sum_{i=0}^{n} b_i x^i, \\ r(x) &= \sum_{i=0}^{p} c_i x^i. \end{aligned}$$

Then

$$\begin{aligned} [p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n} b_i x^i \right) \right] \left(\sum_{i=0}^{p} c_i x^i \right) \\ &= \left[\sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \right] \left(\sum_{i=0}^{p} c_i x^i \right) \\ &= \sum_{i=0}^{m+n+p} \left[\sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right] x^i \\ &= \sum_{i=0}^{m+n+p} \left(\sum_{j+k+l=i} a_j b_k c_l \right) x^i \\ &= \sum_{i=0}^{m+n+p} \left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k} \right) \right] x^i \\ &= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\sum_{i=0}^{n+p} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right] \\ &= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\left(\sum_{i=0}^{n} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) \right] \\ &= p(x)[q(x)r(x)] \end{aligned}$$

The commutativity and distribution properties of polynomial multiplication are proved in a similar manner. We shall leave the proofs of these properties as an exercise. □

Proposition 17.4. *Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is an integral domain. Then $\deg p(x) + \deg q(x) = \deg(p(x)q(x))$. Furthermore, $R[x]$ is an integral domain.*

PROOF. Suppose that we have two nonzero polynomials

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

and

$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

with $a_m \neq 0$ and $b_n \neq 0$. The degrees of $p(x)$ and $q(x)$ are m and n, respectively. The leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, which cannot be zero since R is an integral domain; hence, the degree of $p(x)q(x)$ is $m+n$, and $p(x)q(x) \neq 0$. Since $p(x) \neq 0$ and $q(x) \neq 0$ imply that $p(x)q(x) \neq 0$, we know that $R[x]$ must also be an integral domain. □

We also want to consider polynomials in two or more variables, such as $x^2 - 3xy + 2y^3$. Let R be a ring and suppose that we are given two indeterminates x and y. Certainly we can form the ring $(R[x])[y]$. It is straightforward but perhaps tedious to show that $(R[x])[y] \cong R([y])[x]$. We shall identify these two rings by this isomorphism and simply write $R[x, y]$. The ring $R[x, y]$ is called the ***ring of polynomials in two indeterminates*** x ***and*** y ***with coefficients in*** R. We can define the ***ring of polynomials in*** n ***indeterminates with coefficients in*** R similarly. We shall denote this ring by $R[x_1, x_2, \ldots, x_n]$.

Theorem 17.5. *Let R be a commutative ring with identity and $\alpha \in R$. Then we have a ring homomorphism $\phi_\alpha : R[x] \to R$ defined by*

$$\phi_\alpha(p(x)) = p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0,$$

where $p(x) = a_n x^n + \cdots + a_1 x + a_0$.

Proof. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^i$. It is easy to show that $\phi_\alpha(p(x) + q(x)) = \phi_\alpha(p(x)) + \phi_\alpha(q(x))$. To show that multiplication is preserved under the map ϕ_α, observe that

$$\begin{aligned}
\phi_\alpha(p(x))\phi_\alpha(q(x)) &= p(\alpha)q(\alpha) \\
&= \left(\sum_{i=0}^{n} a_i \alpha^i\right)\left(\sum_{i=0}^{m} b_i \alpha^i\right) \\
&= \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) \alpha^i \\
&= \phi_\alpha(p(x)q(x)).
\end{aligned}$$

□

The map $\phi_\alpha : R[x] \to R$ is called the ***evaluation homomorphism*** at α.

17.2 The Division Algorithm

Recall that the division algorithm for integers (Theorem 2.9) says that if a and b are integers with $b > 0$, then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$. The algorithm by which q and r are found is just long division. A similar theorem exists for polynomials. The division algorithm for polynomials has several important consequences. Since its proof is very similar to the corresponding proof for integers, it is worthwhile to review Theorem 2.9 at this point.

Theorem 17.6 Division Algorithm. *Let $f(x)$ and $g(x)$ be polynomials in $F[x]$, where F is a field and $g(x)$ is a nonzero polynomial. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

where either $\deg r(x) < \deg g(x)$ or $r(x)$ is the zero polynomial.

PROOF. We will first consider the existence of $q(x)$ and $r(x)$. If $f(x)$ is the zero polynomial, then

$$0 = 0 \cdot g(x) + 0;$$

hence, both q and r must also be the zero polynomial. Now suppose that $f(x)$ is not the zero polynomial and that $\deg f(x) = n$ and $\deg g(x) = m$. If $m > n$, then we can let $q(x) = 0$ and $r(x) = f(x)$. Hence, we may assume that $m \leq n$ and proceed by induction on n. If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

the polynomial

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

has degree less than n or is the zero polynomial. By induction, there exist polynomials $q'(x)$ and $r(x)$ such that

$$f'(x) = q'(x)g(x) + r(x),$$

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. Now let

$$q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}.$$

Then

$$f(x) = g(x)q(x) + r(x),$$

with $r(x)$ the zero polynomial or $\deg r(x) < \deg g(x)$.

To show that $q(x)$ and $r(x)$ are unique, suppose that there exist two other polynomials $q_1(x)$ and $r_1(x)$ such that $f(x) = g(x)q_1(x) + r_1(x)$ with $\deg r_1(x) < \deg g(x)$ or $r_1(x) = 0$, so that

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

and

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

If $q(x) - q_1(x)$ is not the zero polynomial, then

$$\deg(g(x)[q(x) - q_1(x)]) = \deg(r_1(x) - r(x)) \geq \deg g(x).$$

However, the degrees of both $r(x)$ and $r_1(x)$ are strictly less than the degree of $g(x)$; therefore, $r(x) = r_1(x)$ and $q(x) = q_1(x)$. □

Example 17.7. The division algorithm merely formalizes long division of polynomials, a task we have been familiar with since high school. For example, suppose that we divide $x^3 - x^2 + 2x - 3$ by $x - 2$.

$$\begin{array}{rrrrrrrrrr}
 & & & x^2 & + & x & + & 4 & & \\
\cline{4-10}
x & - & 2 & x^3 & - & x^2 & + & 2x & - & 3 \\
 & & & x^3 & - & 2x^2 & & & & \\
\cline{4-10}
 & & & & & x^2 & + & 2x & - & 3 \\
 & & & & & x^2 & - & 2x & & \\
\cline{5-10}
 & & & & & & & 4x & - & 3 \\
 & & & & & & & 4x & - & 8 \\
\cline{7-10}
 & & & & & & & & & 5
\end{array}$$

Hence, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$.

Let $p(x)$ be a polynomial in $F[x]$ and $\alpha \in F$. We say that α is a ***zero*** or ***root*** of $p(x)$ if $p(x)$ is in the kernel of the evaluation homomorphism ϕ_α. All we are really saying here is that α is a zero of $p(x)$ if $p(\alpha) = 0$.

Corollary 17.8. *Let F be a field. An element $\alpha \in F$ is a zero of $p(x) \in F[x]$ if and only if $x - \alpha$ is a factor of $p(x)$ in $F[x]$.*

PROOF. Suppose that $\alpha \in F$ and $p(\alpha) = 0$. By the division algorithm, there exist polynomials $q(x)$ and $r(x)$ such that

$$p(x) = (x - \alpha)q(x) + r(x)$$

and the degree of $r(x)$ must be less than the degree of $x - \alpha$. Since the degree of $r(x)$ is less than 1, $r(x) = a$ for $a \in F$; therefore,

$$p(x) = (x - \alpha)q(x) + a.$$

But

$$0 = p(\alpha) = 0 \cdot q(\alpha) + a = a;$$

consequently, $p(x) = (x - \alpha)q(x)$, and $x - \alpha$ is a factor of $p(x)$.

Conversely, suppose that $x - \alpha$ is a factor of $p(x)$; say $p(x) = (x - \alpha)q(x)$. Then $p(\alpha) = 0 \cdot q(\alpha) = 0$. □

Corollary 17.9. *Let F be a field. A nonzero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zeros in F.*

PROOF. We will use induction on the degree of $p(x)$. If $\deg p(x) = 0$, then $p(x)$ is a constant polynomial and has no zeros. Let $\deg p(x) = 1$. Then $p(x) = ax + b$ for some a and b in F. If α_1 and α_2 are zeros of $p(x)$, then $a\alpha_1 + b = a\alpha_2 + b$ or $\alpha_1 = \alpha_2$.

Now assume that $\deg p(x) > 1$. If $p(x)$ does not have a zero in F, then we are done. On the other hand, if α is a zero of $p(x)$, then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$ by Corollary 17.8. The degree of $q(x)$ is $n - 1$ by Proposition 17.4. Let β be some other zero of $p(x)$ that is distinct from α. Then $p(\beta) = (\beta - \alpha)q(\beta) = 0$. Since $\alpha \neq \beta$ and F is a field, $q(\beta) = 0$. By our induction hypothesis, $q(x)$ can have at most $n - 1$ zeros in F that are distinct from α. Therefore, $p(x)$ has at most n distinct zeros in F. □

Let F be a field. A monic polynomial $d(x)$ is a ***greatest common divisor*** of polynomials $p(x), q(x) \in F[x]$ if $d(x)$ evenly divides both $p(x)$ and $q(x)$; and, if for any other polynomial $d'(x)$ dividing both $p(x)$ and $q(x)$, $d'(x) \mid d(x)$. We write $d(x) = \gcd(p(x), q(x))$. Two polynomials $p(x)$ and $q(x)$ are ***relatively prime*** if $\gcd(p(x), q(x)) = 1$.

Proposition 17.10. *Let F be a field and suppose that $d(x)$ is a greatest common divisor of two polynomials $p(x)$ and $q(x)$ in $F[x]$. Then there exist polynomials $r(x)$ and $s(x)$ such that*

$$d(x) = r(x)p(x) + s(x)q(x).$$

Furthermore, the greatest common divisor of two polynomials is unique.

PROOF. Let $d(x)$ be the monic polynomial of smallest degree in the set

$$S = \{f(x)p(x) + g(x)q(x) : f(x), g(x) \in F[x]\}.$$

We can write $d(x) = r(x)p(x) + s(x)q(x)$ for two polynomials $r(x)$ and $s(x)$ in $F[x]$. We need to show that $d(x)$ divides both $p(x)$ and $q(x)$. We shall first show that $d(x)$ divides

$p(x)$. By the division algorithm, there exist polynomials $a(x)$ and $b(x)$ such that $p(x) = a(x)d(x) + b(x)$, where $b(x)$ is either the zero polynomial or $\deg b(x) < \deg d(x)$. Therefore,

$$\begin{aligned} b(x) &= p(x) - a(x)d(x) \\ &= p(x) - a(x)(r(x)p(x) + s(x)q(x)) \\ &= p(x) - a(x)r(x)p(x) - a(x)s(x)q(x) \\ &= p(x)(1 - a(x)r(x)) + q(x)(-a(x)s(x)) \end{aligned}$$

is a linear combination of $p(x)$ and $q(x)$ and therefore must be in S. However, $b(x)$ must be the zero polynomial since $d(x)$ was chosen to be of smallest degree; consequently, $d(x)$ divides $p(x)$. A symmetric argument shows that $d(x)$ must also divide $q(x)$; hence, $d(x)$ is a common divisor of $p(x)$ and $q(x)$.

To show that $d(x)$ is a greatest common divisor of $p(x)$ and $q(x)$, suppose that $d'(x)$ is another common divisor of $p(x)$ and $q(x)$. We will show that $d'(x) \mid d(x)$. Since $d'(x)$ is a common divisor of $p(x)$ and $q(x)$, there exist polynomials $u(x)$ and $v(x)$ such that $p(x) = u(x)d'(x)$ and $q(x) = v(x)d'(x)$. Therefore,

$$\begin{aligned} d(x) &= r(x)p(x) + s(x)q(x) \\ &= r(x)u(x)d'(x) + s(x)v(x)d'(x) \\ &= d'(x)[r(x)u(x) + s(x)v(x)]. \end{aligned}$$

Since $d'(x) \mid d(x)$, $d(x)$ is a greatest common divisor of $p(x)$ and $q(x)$.

Finally, we must show that the greatest common divisor of $p(x)$ and $q(x)$ is unique. Suppose that $d'(x)$ is another greatest common divisor of $p(x)$ and $q(x)$. We have just shown that there exist polynomials $u(x)$ and $v(x)$ in $F[x]$ such that $d(x) = d'(x)[r(x)u(x) + s(x)v(x)]$. Since

$$\deg d(x) = \deg d'(x) + \deg[r(x)u(x) + s(x)v(x)]$$

and $d(x)$ and $d'(x)$ are both greatest common divisors, $\deg d(x) = \deg d'(x)$. Since $d(x)$ and $d'(x)$ are both monic polynomials of the same degree, it must be the case that $d(x) = d'(x)$. □

Notice the similarity between the proof of Proposition 17.10 and the proof of Theorem 2.10.

17.3 Irreducible Polynomials

A nonconstant polynomial $f(x) \in F[x]$ is ***irreducible*** over a field F if $f(x)$ cannot be expressed as a product of two polynomials $g(x)$ and $h(x)$ in $F[x]$, where the degrees of $g(x)$ and $h(x)$ are both smaller than the degree of $f(x)$. Irreducible polynomials function as the "prime numbers" of polynomial rings.

Example 17.11. The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible since it cannot be factored any further over the rational numbers. Similarly, $x^2 + 1$ is irreducible over the real numbers.

Example 17.12. The polynomial $p(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{Z}_3[x]$. Suppose that this polynomial was reducible over $\mathbb{Z}_3[x]$. By the division algorithm there would have to be a factor of the form $x - a$, where a is some element in $\mathbb{Z}_3[x]$. Hence, it would have to be true that $p(a) = 0$. However,

$$\begin{aligned} p(0) &= 2 \\ p(1) &= 1 \end{aligned}$$

$$p(2) = 2.$$

Therefore, $p(x)$ has no zeros in $\mathbb{Z}_3$ and must be irreducible.

Lemma 17.13. *Let $p(x) \in \mathbb{Q}[x]$. Then*

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

where $r, s, a_0, \ldots, a_n$ are integers, the a_i's are relatively prime, and r and s are relatively prime.

PROOF. Suppose that

$$p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n,$$

where the b_i's and the c_i's are integers. We can rewrite $p(x)$ as

$$p(x) = \frac{1}{c_0 \cdots c_n}(d_0 + d_1 x + \cdots + d_n x^n),$$

where $d_0, \ldots, d_n$ are integers. Let d be the greatest common divisor of $d_0, \ldots, d_n$. Then

$$p(x) = \frac{d}{c_0 \cdots c_n}(a_0 + a_1 x + \cdots + a_n x^n),$$

where $d_i = da_i$ and the a_i's are relatively prime. Reducing $d/(c_0 \cdots c_n)$ to its lowest terms, we can write

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

where $\gcd(r, s) = 1$. □

Theorem 17.14 Gauss's Lemma. *Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $p(x)$ factors into a product of two polynomials $\alpha(x)$ and $\beta(x)$ in $\mathbb{Q}[x]$, where the degrees of both $\alpha(x)$ and $\beta(x)$ are less than the degree of $p(x)$. Then $p(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are monic polynomials in $\mathbb{Z}[x]$ with $\deg \alpha(x) = \deg a(x)$ and $\deg \beta(x) = \deg b(x)$.*

PROOF. By Lemma 17.13, we can assume that

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1}\alpha_1(x)$$
$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_1(x),$$

where the a_i's are relatively prime and the b_i's are relatively prime. Consequently,

$$p(x) = \alpha(x)\beta(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x),$$

where c/d is the product of c_1/d_1 and c_2/d_2 expressed in lowest terms. Hence, $dp(x) = c\alpha_1(x)\beta_1(x)$.

If $d = 1$, then $ca_m b_n = 1$ since $p(x)$ is a monic polynomial. Hence, either $c = 1$ or $c = -1$. If $c = 1$, then either $a_m = b_n = 1$ or $a_m = b_n = -1$. In the first case $p(x) = \alpha_1(x)\beta_1(x)$, where $\alpha_1(x)$ and $\beta_1(x)$ are monic polynomials with $\deg \alpha(x) = \deg \alpha_1(x)$ and $\deg \beta(x) = \deg \beta_1(x)$. In the second case $a(x) = -\alpha_1(x)$ and $b(x) = -\beta_1(x)$ are the correct monic polynomials since $p(x) = (-\alpha_1(x))(-\beta_1(x)) = a(x)b(x)$. The case in which $c = -1$ can be handled similarly.

Now suppose that $d \neq 1$. Since $\gcd(c, d) = 1$, there exists a prime p such that $p \mid d$ and $p \nmid c$. Also, since the coefficients of $\alpha_1(x)$ are relatively prime, there exists a coefficient a_i

such that $p \nmid a_i$. Similarly, there exists a coefficient b_j of $\beta_1(x)$ such that $p \nmid b_j$. Let $\alpha_1'(x)$ and $\beta_1'(x)$ be the polynomials in $\mathbb{Z}_p[x]$ obtained by reducing the coefficients of $\alpha_1(x)$ and $\beta_1(x)$ modulo p. Since $p \mid d$, $\alpha_1'(x)\beta_1'(x) = 0$ in $\mathbb{Z}_p[x]$. However, this is impossible since neither $\alpha_1'(x)$ nor $\beta_1'(x)$ is the zero polynomial and $\mathbb{Z}_p[x]$ is an integral domain. Therefore, $d = 1$ and the theorem is proven. □

Corollary 17.15. *Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$ and $a_0 \neq 0$. If $p(x)$ has a zero in $\mathbb{Q}$, then $p(x)$ also has a zero α in $\mathbb{Z}$. Furthermore, α divides a_0.*

Proof. Let $p(x)$ have a zero $a \in \mathbb{Q}$. Then $p(x)$ must have a linear factor $x - a$. By Gauss's Lemma, $p(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$. Hence, for some $\alpha \in \mathbb{Z}$

$$p(x) = (x - \alpha)(x^{n-1} + \cdots - a_0/\alpha).$$

Thus $a_0/\alpha \in \mathbb{Z}$ and so $\alpha \mid a_0$. □

Example 17.16. Let $p(x) = x^4 - 2x^3 + x + 1$. We shall show that $p(x)$ is irreducible over $\mathbb{Q}[x]$. Assume that $p(x)$ is reducible. Then either $p(x)$ has a linear factor, say $p(x) = (x - \alpha)q(x)$, where $q(x)$ is a polynomial of degree three, or $p(x)$ has two quadratic factors.

If $p(x)$ has a linear factor in $\mathbb{Q}[x]$, then it has a zero in $\mathbb{Z}$. By Corollary 17.15, any zero must divide 1 and therefore must be ± 1; however, $p(1) = 1$ and $p(-1) = 3$. Consequently, we have eliminated the possibility that $p(x)$ has any linear factors.

Therefore, if $p(x)$ is reducible it must factor into two quadratic polynomials, say

$$\begin{aligned} p(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

where each factor is in $\mathbb{Z}[x]$ by Gauss's Lemma. Hence,

$$\begin{aligned} a + c &= -2 \\ ac + b + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{aligned}$$

Since $bd = 1$, either $b = d = 1$ or $b = d = -1$. In either case $b = d$ and so

$$ad + bc = b(a + c) = 1.$$

Since $a + c = -2$, we know that $-2b = 1$. This is impossible since b is an integer. Therefore, $p(x)$ must be irreducible over $\mathbb{Q}$.

Theorem 17.17 Eisenstein's Criterion. *Let p be a prime and suppose that*

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x].$$

If $p \mid a_i$ for $i = 0, 1, \ldots, n-1$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. By Gauss's Lemma, we need only show that $f(x)$ does not factor into polynomials of lower degree in $\mathbb{Z}[x]$. Let

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

be a factorization in $\mathbb{Z}[x]$, with b_r and c_s not equal to zero and $r, s < n$. Since p^2 does not divide $a_0 = b_0 c_0$, either b_0 or c_0 is not divisible by p. Suppose that $p \nmid b_0$ and $p \mid c_0$. Since

$p \nmid a_n$ and $a_n = b_r c_s$, neither b_r nor c_s is divisible by p. Let m be the smallest value of k such that $p \nmid c_k$. Then

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

is not divisible by p, since each term on the right-hand side of the equation is divisible by p except for $b_0 c_m$. Therefore, $m = n$ since a_i is divisible by p for $m < n$. Hence, $f(x)$ cannot be factored into polynomials of lower degree and therefore must be irreducible. □

Example 17.18. The polynomial

$$f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$$

is easily seen to be irreducible over $\mathbb{Q}$ by Eisenstein's Criterion if we let $p = 3$.

Eisenstein's Criterion is more useful in constructing irreducible polynomials of a certain degree over $\mathbb{Q}$ than in determining the irreducibility of an arbitrary polynomial in $\mathbb{Q}[x]$: given an arbitrary polynomial, it is not very likely that we can apply Eisenstein's Criterion. The real value of Theorem 17.17 is that we now have an easy method of generating irreducible polynomials of any degree.

Ideals in $F[x]$

Let F be a field. Recall that a principal ideal in $F[x]$ is an ideal $\langle p(x) \rangle$ generated by some polynomial $p(x)$; that is,

$$\langle p(x) \rangle = \{p(x)q(x) : q(x) \in F[x]\}.$$

Example 17.19. The polynomial x^2 in $F[x]$ generates the ideal $\langle x^2 \rangle$ consisting of all polynomials with no constant term or term of degree 1.

Theorem 17.20. *If F is a field, then every ideal in $F[x]$ is a principal ideal.*

Proof. Let I be an ideal of $F[x]$. If I is the zero ideal, the theorem is easily true. Suppose that I is a nontrivial ideal in $F[x]$, and let $p(x) \in I$ be a nonzero element of minimal degree. If $\deg p(x) = 0$, then $p(x)$ is a nonzero constant and 1 must be in I. Since 1 generates all of $F[x]$, $\langle 1 \rangle = I = F[x]$ and I is again a principal ideal.

Now assume that $\deg p(x) \geq 1$ and let $f(x)$ be any element in I. By the division algorithm there exist $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = p(x)q(x) + r(x)$ and $\deg r(x) < \deg p(x)$. Since $f(x), p(x) \in I$ and I is an ideal, $r(x) = f(x) - p(x)q(x)$ is also in I. However, since we chose $p(x)$ to be of minimal degree, $r(x)$ must be the zero polynomial. Since we can write any element $f(x)$ in I as $p(x)q(x)$ for some $q(x) \in F[x]$, it must be the case that $I = \langle p(x) \rangle$. □

Example 17.21. It is not the case that every ideal in the ring $F[x, y]$ is a principal ideal. Consider the ideal of $F[x, y]$ generated by the polynomials x and y. This is the ideal of $F[x, y]$ consisting of all polynomials with no constant term. Since both x and y are in the ideal, no single polynomial can generate the entire ideal.

Theorem 17.22. *Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal if and only if $p(x)$ is irreducible.*

Proof. Suppose that $p(x)$ generates a maximal ideal of $F[x]$. Then $\langle p(x) \rangle$ is also a prime ideal of $F[x]$. Since a maximal ideal must be properly contained inside $F[x]$, $p(x)$ cannot be a constant polynomial. Let us assume that $p(x)$ factors into two polynomials of lesser degree, say $p(x) = f(x)g(x)$. Since $\langle p(x) \rangle$ is a prime ideal one of these factors, say $f(x)$, is

in $\langle p(x)\rangle$ and therefore be a multiple of $p(x)$. But this would imply that $\langle p(x)\rangle \subset \langle f(x)\rangle$, which is impossible since $\langle p(x)\rangle$ is maximal.

Conversely, suppose that $p(x)$ is irreducible over $F[x]$. Let I be an ideal in $F[x]$ containing $\langle p(x)\rangle$. By Theorem 17.20, I is a principal ideal; hence, $I = \langle f(x)\rangle$ for some $f(x) \in F[x]$. Since $p(x) \in I$, it must be the case that $p(x) = f(x)g(x)$ for some $g(x) \in F[x]$. However, $p(x)$ is irreducible; hence, either $f(x)$ or $g(x)$ is a constant polynomial. If $f(x)$ is constant, then $I = F[x]$ and we are done. If $g(x)$ is constant, then $f(x)$ is a constant multiple of I and $I = \langle p(x)\rangle$. Thus, there are no proper ideals of $F[x]$ that properly contain $\langle p(x)\rangle$. □

Sage Polynomial rings are very important for computational approaches to algebra, and so Sage makes it very easy to compute with polynomials, over rings, or over fields. And it is trivial to check if a polynomial is irreducible.

Historical Note

Throughout history, the solution of polynomial equations has been a challenging problem. The Babylonians knew how to solve the equation $ax^2 + bx + c = 0$. Omar Khayyam (1048–1131) devised methods of solving cubic equations through the use of geometric constructions and conic sections. The algebraic solution of the general cubic equation $ax^3 + bx^2 + cx + d = 0$ was not discovered until the sixteenth century. An Italian mathematician, Luca Pacioli (ca. 1445–1509), wrote in *Summa de Arithmetica* that the solution of the cubic was impossible. This was taken as a challenge by the rest of the mathematical community.

Scipione del Ferro (1465–1526), of the University of Bologna, solved the "depressed cubic,"

$$ax^3 + cx + d = 0.$$

He kept his solution an absolute secret. This may seem surprising today, when mathematicians are usually very eager to publish their results, but in the days of the Italian Renaissance secrecy was customary. Academic appointments were not easy to secure and depended on the ability to prevail in public contests. Such challenges could be issued at any time. Consequently, any major new discovery was a valuable weapon in such a contest. If an opponent presented a list of problems to be solved, del Ferro could in turn present a list of depressed cubics. He kept the secret of his discovery throughout his life, passing it on only on his deathbed to his student Antonio Fior (ca. 1506–?).

Although Fior was not the equal of his teacher, he immediately issued a challenge to Niccolo Fontana (1499–1557). Fontana was known as Tartaglia (the Stammerer). As a youth he had suffered a blow from the sword of a French soldier during an attack on his village. He survived the savage wound, but his speech was permanently impaired. Tartaglia sent Fior a list of 30 various mathematical problems; Fior countered by sending Tartaglia a list of 30 depressed cubics. Tartaglia would either solve all 30 of the problems or absolutely fail. After much effort Tartaglia finally succeeded in solving the depressed cubic and defeated Fior, who faded into obscurity.

At this point another mathematician, Gerolamo Cardano (1501–1576), entered the story. Cardano wrote to Tartaglia, begging him for the solution to the depressed cubic. Tartaglia refused several of his requests, then finally revealed the solution to Cardano after the latter swore an oath not to publish the secret or to pass it on to anyone else. Using the knowledge that he had obtained from Tartaglia, Cardano eventually solved the general cubic

$$ax^3 + bx^2 + cx + d = 0.$$

Cardano shared the secret with his student, Ludovico Ferrari (1522–1565), who solved the general quartic equation,

$$ax^4 + bx^3 + cx^2 + dx + e = 0.$$

In 1543, Cardano and Ferrari examined del Ferro's papers and discovered that he had also solved the depressed cubic. Cardano felt that this relieved him of his obligation to Tartaglia, so he proceeded to publish the solutions in *Ars Magna* (1545), in which he gave credit to del Ferro for solving the special case of the cubic. This resulted in a bitter dispute between Cardano and Tartaglia, who published the story of the oath a year later.

17.4 Exercises

1. List all of the polynomials of degree 3 or less in $\mathbb{Z}_2[x]$.

2. Compute each of the following.

(a) $(5x^2 + 3x - 4) + (4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(b) $(5x^2 + 3x - 4)(4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(c) $(7x^3 + 3x^2 - x) + (6x^2 - 8x + 4)$ in $\mathbb{Z}_9$

(d) $(3x^2 + 2x - 4) + (4x^2 + 2)$ in $\mathbb{Z}_5$

(e) $(3x^2 + 2x - 4)(4x^2 + 2)$ in $\mathbb{Z}_5$

(f) $(5x^2 + 3x - 2)^2$ in $\mathbb{Z}_{12}$

3. Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$ for each of the following pairs of polynomials.

(a) $a(x) = 5x^3 + 6x^2 - 3x + 4$ and $b(x) = x - 2$ in $\mathbb{Z}_7[x]$

(b) $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_7[x]$

(c) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$

(d) $a(x) = x^5 + x^3 - x^2 - x$ and $b(x) = x^3 + x$ in $\mathbb{Z}_2[x]$

4. Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \gcd(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $a(x)p(x) + b(x)q(x) = d(x)$.

(a) $p(x) = x^3 - 6x^2 + 14x - 15$ and $q(x) = x^3 - 8x^2 + 21x - 18$, where $p(x), q(x) \in \mathbb{Q}[x]$

(b) $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$, where $p(x), q(x) \in \mathbb{Z}_2[x]$

(c) $p(x) = x^3 + x^2 - 4x + 4$ and $q(x) = x^3 + 3x - 2$, where $p(x), q(x) \in \mathbb{Z}_5[x]$

(d) $p(x) = x^3 - 2x + 4$ and $q(x) = 4x^3 + x + 3$, where $p(x), q(x) \in \mathbb{Q}[x]$

5. Find all of the zeros for each of the following polynomials.

(a) $5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}$

(b) $3x^3 - 4x^2 - x + 4$ in $\mathbb{Z}_5$

(c) $5x^4 + 2x^2 - 3$ in $\mathbb{Z}_7$

(d) $x^3 + x + 1$ in $\mathbb{Z}_2$

6. Find all of the units in $\mathbb{Z}[x]$.

7. Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\deg p(x) > 1$.

8. Which of the following polynomials are irreducible over $\mathbb{Q}[x]$?

(a) $x^4 - 2x^3 + 2x^2 + x + 4$

(b) $x^4 - 5x^3 + 3x - 2$

(c) $3x^5 - 4x^3 - 6x^2 + 6$

(d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

9. Find all of the irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$.

10. Give two different factorizations of $x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

11. Prove or disprove: There exists a polynomial $p(x)$ in $\mathbb{Z}_6[x]$ of degree n with more than n distinct zeros.

12. If F is a field, show that $F[x_1, \ldots, x_n]$ is an integral domain.

13. Show that the division algorithm does not hold for $\mathbb{Z}[x]$. Why does it fail?

14. Prove or disprove: $x^p + a$ is irreducible for any $a \in \mathbb{Z}_p$, where p is prime.

15. Let $f(x)$ be irreducible in $F[x]$, where F is a field. If $f(x) \mid p(x)q(x)$, prove that either $f(x) \mid p(x)$ or $f(x) \mid q(x)$.

16. Suppose that R and S are isomorphic rings. Prove that $R[x] \cong S[x]$.

17. Let F be a field and $a \in F$. If $p(x) \in F[x]$, show that $p(a)$ is the remainder obtained when $p(x)$ is divided by $x - a$.

18. **The Rational Root Theorem.** Let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$. Prove that if $p(r/s) = 0$, where $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

19. Let $\mathbb{Q}^*$ be the multiplicative group of positive rational numbers. Prove that $\mathbb{Q}^*$ is isomorphic to $(\mathbb{Z}[x], +)$.

20. **Cyclotomic Polynomials.** The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the ***cyclotomic polynomial.*** Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

21. If F is a field, show that there are infinitely many irreducible polynomials in $F[x]$.

22. Let R be a commutative ring with identity. Prove that multiplication is commutative in $R[x]$.

23. Let R be a commutative ring with identity. Prove that multiplication is distributive in $R[x]$.

24. Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$, for any prime p. Conclude that

$$x^p - x = x(x - 1)(x - 2) \cdots (x - (p - 1)).$$

25. Let F be a field and $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be in $F[x]$. Define $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ to be the ***derivative*** of $f(x)$.

(a) Prove that

$$(f + g)'(x) = f'(x) + g'(x).$$

Conclude that we can define a homomorphism of abelian groups $D : F[x] \to F[x]$ by $D(f(x)) = f'(x)$.

(b) Calculate the kernel of D if $\operatorname{char} F = 0$.

(c) Calculate the kernel of D if $\operatorname{char} F = p$.

(d) Prove that
$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

(e) Suppose that we can factor a polynomial $f(x) \in F[x]$ into linear factors, say
$$f(x) = a(x - a_1)(x - a_2)\cdots(x - a_n).$$
Prove that $f(x)$ has no repeated factors if and only if $f(x)$ and $f'(x)$ are relatively prime.

26. Let F be a field. Show that $F[x]$ is never a field.

27. Let R be an integral domain. Prove that $R[x_1, \ldots, x_n]$ is an integral domain.

28. Let R be a commutative ring with identity. Show that $R[x]$ has a subring R' isomorphic to R.

29. Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is a commutative ring with identity. Prove that $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

17.5 Additional Exercises: Solving the Cubic and Quartic Equations

1. Solve the general quadratic equation
$$ax^2 + bx + c = 0$$
to obtain
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$
The ***discriminant*** of the quadratic equation $\Delta = b^2 - 4ac$ determines the nature of the solutions of the equation. If $\Delta > 0$, the equation has two distinct real solutions. If $\Delta = 0$, the equation has a single repeated real root. If $\Delta < 0$, there are two distinct imaginary solutions.

2. Show that any cubic equation of the form
$$x^3 + bx^2 + cx + d = 0$$
can be reduced to the form $y^3 + py + q = 0$ by making the substitution $x = y - b/3$.

3. Prove that the cube roots of 1 are given by
$$\omega = \frac{-1 + i\sqrt{3}}{2}$$
$$\omega^2 = \frac{-1 - i\sqrt{3}}{2}$$
$$\omega^3 = 1.$$

4. Make the substitution
$$y = z - \frac{p}{3z}$$

for y in the equation $y^3 + py + q = 0$ and obtain two solutions A and B for z^3.

5. Show that the product of the solutions obtained in (4) is $-p^3/27$, deducing that $\sqrt[3]{AB} = -p/3$.

6. Prove that the possible solutions for z in (4) are given by

$$\sqrt[3]{A}, \quad \omega\sqrt[3]{A}, \quad \omega^2\sqrt[3]{A}, \quad \sqrt[3]{B}, \quad \omega\sqrt[3]{B}, \quad \omega^2\sqrt[3]{B}$$

and use this result to show that the three possible solutions for y are

$$\omega^i \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^{2i} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

where $i = 0, 1, 2$.

7. The ***discriminant*** of the cubic equation is

$$\Delta = \frac{p^3}{27} + \frac{q^2}{4}.$$

Show that $y^3 + py + q = 0$

(a) has three real roots, at least two of which are equal, if $\Delta = 0$.

(b) has one real root and two conjugate imaginary roots if $\Delta > 0$.

(c) has three distinct real roots if $\Delta < 0$.

8. Solve the following cubic equations.

(a) $x^3 - 4x^2 + 11x + 30 = 0$

(b) $x^3 - 3x + 5 = 0$

(c) $x^3 - 3x + 2 = 0$

(d) $x^3 + x + 3 = 0$

9. Show that the general quartic equation

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

can be reduced to

$$y^4 + py^2 + qy + r = 0$$

by using the substitution $x = y - a/4$.

10. Show that

$$\left(y^2 + \frac{1}{2}z\right)^2 = (z - p)y^2 - qy + \left(\frac{1}{4}z^2 - r\right).$$

11. Show that the right-hand side of Exercise 17.5.10 can be put in the form $(my + k)^2$ if and only if

$$q^2 - 4(z - p)\left(\frac{1}{4}z^2 - r\right) = 0.$$

12. From Exercise 17.5.11 obtain the ***resolvent cubic equation***

$$z^3 - pz^2 - 4rz + (4pr - q^2) = 0.$$

Solving the resolvent cubic equation, put the equation found in Exercise 17.5.10 in the form

$$\left(y^2 + \frac{1}{2}z\right)^2 = (my + k)^2$$

to obtain the solution of the quartic equation.

13. Use this method to solve the following quartic equations.

(a) $x^4 - x^2 - 3x + 2 = 0$

(b) $x^4 + x^3 - 7x^2 - x + 6 = 0$

(c) $x^4 - 2x^2 + 4x - 3 = 0$

(d) $x^4 - 4x^3 + 3x^2 - 5x + 2 = 0$