Definitions, Theorems and Exercises

Math 332
Abstract Algebra

Ethan D. Bloch

April 20, 2017

Contents

1

Binary Operations

1.1 Binary Operations

Fraleigh, 7th ed. – Section 2
Gallian, 7th ed. – Section 2
Judson, 2016 – Section 3.2

Definition 1.1.1. Let A be a set. A **binary operation** on A is a function $A \times A \to A$. A **unary operation** on A is a function $A \to A$. △

Definition 1.1.2. Let A be a set, let $*$ be a binary operation on A and let $H \subseteq A$. The subset H is **closed** under $*$ if $a * b \in H$ for all $a, b \in H$. △

Definition 1.1.3. Let A be a set, and let $*$ be a binary operation on A. The binary operation $*$ satisfies the **Commutative Law** (an alternative expression is that $*$ is **commutative**) if $a * b = b * a$ for all $a, b \in A$. △

Definition 1.1.4. Let A be a set, and let $*$ be a binary operation on A. The binary operation $*$ satisfies the **Associative Law** (an alternative expression is that $*$ is **associative**) if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$. △

Definition 1.1.5. Let A be a set, and let $*$ be a binary operation on A.

1. Let $e \in A$. The element e is an **identity element** for $*$ if $a * e = a = e * a$ for all $a \in A$.

2. If $*$ has an identity element, the binary operation $*$ satisfies the **Identity Law**. △

Lemma 1.1.6. *Let A be a set, and let $*$ be a binary operation on A. If $*$ has an identity element, the identity element is unique.*

Definition 1.1.7. Let A be a set, and let $*$ be a binary operation of A. Let $e \in A$. Suppose that e is an identity element for $*$.

1. Let $a \in A$. An **inverse** for a is an element $a' \in A$ such that $a * a' = e$ and $a' * a = e$.

2. If every element in A has an inverse, the binary operation $*$ satisfies the **Inverses Law**. △

Exercises

Exercise 1.1.1. Which of the following formulas defines a binary operation on the given set?

(1) Let $*$ be defined by $x * y = xy$ for all $x, y \in \{-1, -2, -3, \dots\}$.

(2) Let $\diamond$ be defined by $x \diamond y = \sqrt{xy}$ for all $x, y \in [2, \infty)$.

(3) Let $\oplus$ be defined by $x \oplus y = x - y$ for all $x, y \in \mathbb{Q}$.

(4) Let $\circ$ be defined by $(x, y) \circ (z, w) = (x + z, y + w)$ for all $(x, y), (z, w) \in \mathbb{R}^2 - \{(0, 0)\}$.

(5) Let $\odot$ be defined by $x \odot y = |x + y|$ for all $x, y \in \mathbb{N}$.

(6) Let $\otimes$ be defined by $x \otimes y = \ln(|xy| - e)$ for all $x, y \in \mathbb{N}$.

Exercise 1.1.2. For each of the following binary operations, state whether the binary operation is associative, whether it is commutative, whether there is an identity element and, if there is an identity element, which elements have inverses.

(1) The binary operation $\oplus$ on $\mathbb{Z}$ defined by $x \oplus y = -xy$ for all $x, y \in \mathbb{Z}$.

(2) The binary operation $\star$ on $\mathbb{R}$ defined by $x \star y = x + 2y$ for all $x, y \in \mathbb{R}$.

(3) The binary operation $\otimes$ on $\mathbb{R}$ defined by $x \otimes y = x + y - 7$ for all $x, y \in \mathbb{R}$.

(4) The binary operation $*$ on $\mathbb{Q}$ defined by $x * y = 3(x + y)$ for all $x, y \in \mathbb{Q}$.

(5) The binary operation $\circ$ on $\mathbb{R}$ defined by $x \circ y = x$ for all $x, y \in \mathbb{R}$.

(6) The binary operation $\diamond$ on $\mathbb{Q}$ defined by $x \diamond y = x + y + xy$ for all $x, y \in \mathbb{Q}$.

(7) The binary operation $\odot$ on $\mathbb{R}^2$ defined by $(x, y) \odot (z, w) = (4xz, y + w)$ for all $(x, y), (z, w) \in \mathbb{R}^2$.

Exercise 1.1.3. For each of the following binary operations given by operation tables, state whether the binary operation is commutative, whether there is an identity element and, if there is an identity element, which elements have inverses. (Do not check for associativity.)

(1)

$\otimes$	1	2	3
1	1	2	1
2	2	3	2
3	1	2	3

.

(2)

$\odot$	j	k	l	m
j	k	j	m	j
k	j	k	l	m
l	k	l	j	l
m	j	m	l	m

.

(3)

$*$	x	y	z	w
x	x	z	w	y
y	z	w	y	x
z	w	y	x	z
w	y	x	z	w

.

(4)

$\star$	a	b	c	d	e
a	d	e	a	b	b
b	e	a	b	a	d
c	a	b	c	d	e
d	b	a	d	e	c
e	b	d	e	c	a

.

(5)

$\diamond$	i	r	s	a	b	c
i	i	r	s	a	b	c
r	r	s	i	c	a	b
s	s	i	r	b	c	a
a	a	b	c	i	s	r
b	b	c	a	r	i	s
c	c	a	b	s	r	i

.

Exercise 1.1.4. Find an example of a set and a binary operation on the set such that the binary operation satisfies the Identity Law and Inverses Law, but not the Associative Law, and for which at least one element of the set has more than one inverse. The simplest way to solve this problem is by constructing an appropriate operation table.

Exercise 1.1.5. Let $n \in \mathbb{N}$. Recall the definition of the set $\mathbb{Z}_n$ and the binary operation $\cdot$ on $\mathbb{Z}_n$. Observe that [1] is the identity element for $\mathbb{Z}_n$ with respect to multiplication. Let $a \in \mathbb{Z}$. Prove that the following are equivalent.

a. The element $[a] \in \mathbb{Z}_n$ has an inverse with respect to multiplication.

b. The equation $ax \equiv 1 \pmod{n}$ has a solution.

c. There exist $p, q \in \mathbb{Z}$ such that $ap + nq = 1$.

(It turns out that the three conditions listed above are equivalent to the fact that a and n are relatively prime.)

Exercise 1.1.6. Let A be a set. A **ternary operation** on A is a function $A \times A \times A \to A$. A ternary operation $\star : A \times A \times A \to A$ is **left-induced** by a binary operation $\diamond : A \times A \to A$ if $\star((a, b, c)) = (a \diamond b) \diamond c$ for all $a, b, c \in A$.

Is every ternary operation on a set left-induced by a binary operation? Give a proof or a counterexample.

Exercise 1.1.7. Let A be a set, and let $*$ be a binary operation on A. Suppose that $*$ satisfies the Associative Law and the Commutative Law. Prove that $(a * b) * (c * d) = b * [(d * a) * c]$ for all $a, b, c, d \in A$.

Exercise 1.1.8. Let B be a set, and let $\diamond$ be a binary operation on B. Suppose that $\diamond$ satisfies the Associative Law. Let

$$P = \{b \in B \mid b \diamond w = w \diamond b \text{ for all } w \in B\}.$$

Prove that P is closed under $\diamond$.

Exercise 1.1.9. Let C be a set, and let $\star$ be a binary operation on C. Suppose that $\star$ satisfies the Associative Law and the Commutative Law. Let

$$Q = \{c \in C \mid c \star c = c\}.$$

Prove that Q is closed under $\star$.

Exercise 1.1.10. Let A be a set, and let $*$ be a binary operation on A. An element $c \in A$ is a **left identity element** for $*$ if $c * a = a$ for all $a \in A$. An element $d \in A$ is a **right identity element** for $*$ if $a * d = a$ for all $a \in A$.

(1) If A has a left identity element, is it unique? Give a proof or a counterexample.

(2) If A has a right identity element, is it unique? Give a proof or a counterexample.

(3) If A has a left identity element and a right identity element, do these elements have to be equal? Give a proof or a counterexample.

1.2 Isomorphic Binary Operations

Fraleigh, 7th ed. – Section 3
Gallian, 7th ed. – Section 6

Definition 1.2.1. Let $(G, *)$ and $(H, \diamond)$ be sets with binary operations, and let $f : G \to H$ be a function. The function f is an **isomorphism** of the binary operations if f is bijective and if $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$. △

Definition 1.2.2. Let $(G, *)$ and $(H, \diamond)$ be sets with binary operations. The binary operations $*$ and $\diamond$ are **isomorphic** if there is an isomorphism $G \to H$. △

Theorem 1.2.3. *Let $(G, *)$ and $(H, \diamond)$ be sets with binary operations. Suppose that $(G, *)$ and $(H, \diamond)$ are isomorphic.*

1. *$(G, *)$ satisfies the Commutative Law if and only if $(H, \diamond)$ satisfies the Commutative Law.*
2. *$(G, *)$ satisfies the Associative Law if and only if $(H, \diamond)$ satisfies the Associative Law.*
3. *$(G, *)$ satisfies the Identity Law if and only if $(H, \diamond)$ satisfies the Identity Law. If $f : G \to H$ is an isomorphism, then $f(e_G) = e_H$.*
4. *$(G, *)$ satisfies the Inverses Law if and only if $(H, \diamond)$ satisfies the Inverses Law.*

Exercises

Exercise 1.2.1. Prove that the two sets with binary operations in each of the following pairs are isomorphic.

(1) $(\mathbb{Z}, +)$ and $(5\mathbb{Z}, +)$, where $5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$.

(2) $(\mathbb{R} - \{0\}, \cdot)$ and $(\mathbb{R} - \{-1\}, *)$, where $x * y = x + y + xy$ for all $x, y \in \mathbb{R} - \{-1\}$.

(3) $(\mathbb{R}^4, +)$ and $(M_{2\times 2}(\mathbb{R}), +)$, where $M_{2\times 2}(\mathbb{R})$ is the set of all 2×2 matrices with real entries.

Exercise 1.2.2. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n + 1$ for all $n \in \mathbb{Z}$.

(1) Define a binary operation $*$ on $\mathbb{Z}$ so that f is an isomorphism of $(\mathbb{Z}, +)$ and $(\mathbb{Z}, *)$, in that order.

(2) Define a binary operation $\diamond$ on $\mathbb{Z}$ so that f is an isomorphism of $(\mathbb{Z}, \diamond)$ and $(\mathbb{Z}, +)$, in that order.

Exercise 1.2.3. Prove Theorem 1.2.3 (2).

Exercise 1.2.4. Prove Theorem 1.2.3 (3).

Exercise 1.2.5. Prove Theorem 1.2.3 (4).

2

Groups

2.1 Groups

Fraleigh, 7th ed. – Section 4
Gallian, 7th ed. – Section 2
Judson, 2016 – Section 3.2

Definition 2.1.1. Let G be a non-empty set, and let $*$ be a binary operation on G. The pair $(G, *)$ is a **group** if $*$ satisfies the Associative Law, the Identity Law and the Inverses Law. △

Definition 2.1.2. Let $(G, *)$ be a group. The group $(G, *)$ is **abelian** if $*$ satisfies the Commutative Law. △

Lemma 2.1.3. *Let $(G, *)$ be a group. If $g \in G$, then g has a unique inverse.*

Definition 2.1.4. Let $(G, *)$ be a group. If G is a finite set, then the **order** of the group, denoted $|G|$, is the cardinality of the set G. △

Definition 2.1.5. Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. The number a is **congruent** to the number b **modulo** n, denoted $a \equiv b \pmod{n}$, if $a - b = kn$ for some $k \in \mathbb{Z}$. △

Theorem 2.1.6. *Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. Then there is a unique $r \in \{0, \ldots, n-1\}$ such that $a \equiv r \pmod{n}$.*

Theorem 2.1.7. *Let $n \in \mathbb{N}$.*

1. *Let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $[a] = [b]$. If $a \not\equiv b \pmod{n}$, then $[a] \cap [b] = \emptyset$.*
2. $[0] \cup [1] \cup \ldots \cup [n-1] = \mathbb{Z}$.

Definition 2.1.8. Let $n \in \mathbb{N}$. The set of **integers modulo** n, denoted $\mathbb{Z}_n$, is the set defined by $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, where the relation classes are for congruence modulo n. △

Definition 2.1.9. Let $n \in \mathbb{N}$. Let $+$ and $\cdot$ be the binary operations on $\mathbb{Z}_n$ defined by $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$. △

Lemma 2.1.10. *Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$. Suppose that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then $a + b \equiv c + d \pmod{n}$ and $ab \equiv cd \pmod{n}$.*

Corollary 2.1.11. *Let $n \in \mathbb{N}$, and let $[a], [b], [c], [d] \in \mathbb{Z}_n$. Suppose that $[a] = [c]$ and $[b] = [d]$. Then $[a + b] = [c + d]$ and $[ab] = [cd]$.*

Lemma 2.1.12. *Let $n \in \mathbb{N}$. Then $(\mathbb{Z}_n, +)$ is an abelian group.*

Exercises

Exercise 2.1.1. For each of the following sets with binary operations, state whether the set with binary operation is a group, and whether it is an abelian group.

(1) The set $(0, 1]$, and the binary operation multiplication.

(2) The set of positive rational numbers, and the binary operation multiplication.

(3) The set of even integers, and the binary operation addition.

(4) The set of even integers, and the binary operation multiplication.

(5) The set $\mathbb{Z}$, and the binary operation $*$ on $\mathbb{Z}$ defined by $a * b = a - b$ for all $a, b \in \mathbb{Z}$.

(6) The set $\mathbb{Z}$, and the binary operation $\star$ on $\mathbb{Z}$ defined by $a \star b = ab + a$ for all $a, b \in \mathbb{Z}$.

(7) The set $\mathbb{Z}$, and the binary operation $\diamond$ on $\mathbb{Z}$ defined by $a \diamond b = a + b + 1$ for all $a, b \in \mathbb{Z}$.

(8) The set $\mathbb{R} - \{-1\}$, and the binary operation $\odot$ on $\mathbb{R} - \{-1\}$ defined by $a \odot b = a + b + ab$ for all $a, b \in \mathbb{R} - \{-1\}$.

Exercise 2.1.2. Let $P = \{a, b, c, d, e\}$. Find a binary operation $*$ on P given by an operation table such that $(P, *)$ is a group.

Exercise 2.1.3. Find an example of a set and a binary operation on the set given by an operation table such that each element of the set appears once and only once in each row of the operation table and once and only once in each column, but the set together with this binary operation is not a group.

Exercise 2.1.4. Let A be a set. Let $\mathcal{P}(A)$ denote the power set of A. Define the binary operation $\triangle$ on $\mathcal{P}(A)$ by $X \triangle Y = (X - Y) \cup (Y - X)$ for all $X, Y \in \mathcal{P}(A)$. (This binary operation is called symmetric difference. Prove that $(\mathcal{P}(A), \triangle)$ is an abelian group.

Exercise 2.1.5. Let $(G, *)$ be a group. Prove that if $x' = x$ for all $x \in G$, then G is abelian. Is the converse to this statement true?

Exercise 2.1.6. Let $(H, \star)$ be a group. Suppose that H is finite, and has an even number of elements. Prove that there is some $h \in H$ such that $h \neq e_H$ and $h \star h = e_H$.

2.2 Isomorphic Groups

Fraleigh, 7th ed. – Section 3
Gallian, 7th ed. – Section 6
Judson, 2016 – Section 9.1

Definition 2.2.1. Let $(G, *)$ and $(H, \diamond)$ be groups, and let $f : G \to H$ be a function. The function f is an **isomorphism** (sometimes called a **group isomorphism**) if f is bijective and if $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$. △

Definition 2.2.2. Let $(G, *)$ and $(H, \diamond)$ be groups. The groups G and H are **isomorphic** if there is an isomorphism $G \to H$. If G and H are isomorphic, it is denoted $G \cong H$. △

Theorem 2.2.3. *Let G and H be groups, and let $f : G \to H$ be an isomorphism.*

1. *$f(e_G) = e_H$.*
2. *If $a \in G$, then $f(a') = [f(a)]'$, where the first inverse is in G, and the second is in H.*

Theorem 2.2.4. *Let G, H and K be groups, and let $f : G \to H$ and $j : H \to K$ be isomorphisms.*

1. *The identity map $1_G : G \to G$ is an isomorphism.*
2. *The function f^{-1} is an isomorphism.*
3. *The function $j \circ f$ is an isomorphism.*

Lemma 2.2.5. *Let G and H be groups. Suppose that G and H are isomorphic. Then G is abelian if and only if H is abelian.*

Lemma 2.2.6. *Let $(G, *)$ be a group, let A be a set, and let $f : A \to G$ be a bijective map. Then there is a unique binary operation $\diamond$ on A such that $(A, \diamond)$ is a group and f is an isomorphism.*

Exercises

Exercise 2.2.1. Which of the following functions are isomorphisms? The groups under consideration are $(\mathbb{R}, +)$, and $(\mathbb{Q}, +)$, and $((0, \infty), \cdot)$.

(1) Let $f : \mathbb{Q} \to (0, \infty)$ be defined by $f(x) = 5^x$ for all $x \in \mathbb{Q}$.

(2) Let $k : (0, \infty) \to (0, \infty)$ be defined by $k(x) = x^{-7}$ for all $x \in (0, \infty)$.

(3) Let $m : \mathbb{R} \to \mathbb{R}$ be defined by $m(x) = x + 3$ for all $x \in \mathbb{R}$.

(4) Let $g : (0, \infty) \to \mathbb{R}$ be defined by $g(x) = \ln x$ for all $x \in (0, \infty)$.

Exercise 2.2.2. Prove Theorem 2.2.3 (1).

Exercise 2.2.3. Prove Theorem 2.2.4 (1) and (2).

Exercise 2.2.4. Prove that up to isomorphism, the only two groups with four elements are $\mathbb{Z}_4$ and the Klein 4-group K. Consider all possible operation tables for the binary operation of a group with four elements; use the fact that each element of a group appears once in each row and once in each column of the operation table for the binary operation of the group, as stated in Remark 2.3.2.

Exercise 2.2.5. Let G be a group, and let $g \in G$. Let $i_g : G \to G$ be defined by $i_g(x) = gxg^{-1}$ for all $x \in G$. Prove that i_g is an isomorphism.

2.3 Basic Properties of Groups

Fraleigh, 7th ed. – Section 4
Gallian, 7th ed. – Section 2
Judson, 2016 – Section 3.2

Theorem 2.3.1. *Let G be a group, and let $a, b, c \in G$.*

1. *$e^{-1} = e$.*

2. *If $ac = bc$, then $a = b$ (Cancelation Law).*

3. *If $ca = cb$, then $a = b$ (Cancelation Law).*

4. *$(a^{-1})^{-1} = a$.*

5. *$(ab)^{-1} = b^{-1}a^{-1}$.*

6. *If $ba = e$, then $b = a^{-1}$.*

7. *If $ab = e$, then $b = a^{-1}$.*

Remark 2.3.2. A useful consequence of Theorem 2.3.1 (2) and (3) is that if the binary operation of a group with finitely many elements is given by an operation table, then each element of the group appears once and only once in each row of the operation table and once and only once in each column (consider what would happen otherwise). On the other hand, just because an operation table does have each element once and only once in each row and once and only once in each column does not guarantee that the operation yields a group; the reader is asked to find such an operation table in Exercise 2.1.3. ◊

Theorem 2.3.3. *Let G be a group. The following are equivalent.*

a. *G is abelian.*

b. *$(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.*

c. *$aba^{-1}b^{-1} = e$ for all $a, b \in G$.*

d. *$(ab)^2 = a^2b^2$ for all $a, b \in G$.*

Theorem 2.3.4 (Definition by Recursion). *Let H be a set, let $e \in H$ and let $k : H \to H$ be a function. Then there is a unique function $f : \mathbb{N} \to H$ such that $f(1) = e$, and that $f(n+1) = k(f(n))$ for all $n \in \mathbb{N}$.*

Definition 2.3.5. Let G be a group and let $a \in G$.

1. The element $a^n \in G$ is defined for all $n \in \mathbb{N}$ by letting $a^1 = a$, and $a^{n+1} = a \cdot a^n$ for all $n \in \mathbb{N}$.

2. The element $a^0 \in G$ is defined by $a^0 = e$. For each $n \in \mathbb{N}$, the element a^{-n} is defined by $a^{-n} = (a^n)^{-1}$. △

Lemma 2.3.6. *Let G be a group, let $a \in G$ and let $n, m \in \mathbb{Z}$.*

1. $a^n a^m = a^{n+m}$.

2. $(a^n)^{-1} = a^{-n}$.

Definition 2.3.7. Let A be a set, and let $*$ be a binary operation on A. An element $e \in A$ is a **left identity element** for $*$ if $e * a = a$ for all $a \in A$. If $*$ has a left identity element, the binary operation $*$ satisfies the **Left Identity Law**. △

Definition 2.3.8. Let A be a set, and let $*$ be a binary operation of A. Let $e \in A$. Suppose that e is a left identity element for $*$. If $a \in A$, a **left inverse** for a is an element $a' \in A$ such that $a' * a = e$. If every element in A has a left inverse, the binary operation $*$ satisfies the **Left Inverses Law**. △

Theorem 2.3.9. *Let G be a set, and let $*$ be a binary operation of A. If the pair $(G, *)$ satisfies the Associative Law, the Left Identity Law and the Left Inverses Law, then $(G, *)$ is a group.*

Exercises

Exercise 2.3.1. Let H be a group, and let $a, b, c \in H$. Prove that if $abc = e_H$, then $bca = e_H$.

Exercise 2.3.2. Let G be a group. An element $g \in G$ is **idempotent** if $g^2 = g$. Prove that G has precisely one idempotent element.

Exercise 2.3.3. Let H be a group. Suppose that $h^2 = e_H$ for all $h \in H$. Prove that H is abelian.

Exercise 2.3.4. Let G be a group, and let $a, b \in G$. Prove that $(ab)^2 = a^2b^2$ if and only if $ab = ba$. (Do not use Theorem 2.3.3.)

Exercise 2.3.5. Let G be a group, and let $a, b \in G$. Prove that $(ab)^{-1} = a^{-1}b^{-1}$ if and only if $ab = ba$. (Do not use Theorem 2.3.3.)

Exercise 2.3.6. Find an example of a group G, and elements $a, b \in G$, such that $(ab)^{-1} \neq a^{-1}b^{-1}$.

Exercise 2.3.7. Let $(H, *)$ be a group. Let $\diamond$ be the binary operation on H defined by $a \diamond b = b * a$ for all $a, b \in H$.

(1) Prove that $(H, \diamond)$ is a group.

(2) Prove that $(H, *)$ and $(H, \diamond)$ are isomorphic.

Exercise 2.3.8. Let G be a group, and let $g \in G$. Suppose that G is finite. Prove that there is some $n \in \mathbb{N}$ such that $g^n = e_G$.

2.4 Subgroups

Fraleigh, 7th ed. – Section 5
Gallian, 7th ed. – Section 3
Judson, 2016 – Section 3.3

Definition 2.4.1. Let $(G, *)$ be a group, and let $H \subseteq G$ be a subset. The subset H is a **subgroup** of G if the following two conditions hold.

(a) H is closed under $*$.

(b) $(H, *)$ is a group.

If H is a subgroup of G, it is denoted $H \leq G$. △

Lemma 2.4.2. *Let G be a group, and let $H \leq G$.*

1. *The identity element of G is in H, and it is the identity element of H.*

2. *The inverse operation in H is the same as the inverse operation in G.*

Theorem 2.4.3. *Let G be a group, and let $H \subseteq G$. Then $H \leq G$ if and only if the following three conditions hold.*

(i) *$e \in H$.*

(ii) *If $a, b \in H$, then $a * b \in H$.*

(iii) *If $a \in H$, then $a^{-1} \in H$.*

Theorem 2.4.4. *Let G be a group, and let $H \subseteq G$. Then $H \leq G$ if and only if the following three conditions hold.*

(i) *$H \neq \emptyset$.*

(ii) *If $a, b \in H$, then $a * b \in H$.*

(iii) *If $a \in H$, then $a^{-1} \in H$.*

Theorem 2.4.5. *Let G be a group, and let $H \subseteq G$. Then $H \leq G$ if and only if the following two conditions hold.*

(i) *$H \neq \emptyset$.*

(ii) *If $a, b \in H$, then $a * b^{-1} \in H$.*

Lemma 2.4.6. *Let G be a group, and let $K \subseteq H \subseteq G$. If $K \leq H$ and $H \leq G$, then $K \leq G$.*

Lemma 2.4.7. *Let G be a group, and let $\{H_i\}_{i \in I}$ be a family of subgroups of G indexed by I. Then $\bigcap_{i \in I} H_i \leq G$.*

Theorem 2.4.8. *Let G and H be groups, and let $f : G \to H$ be an isomorphism.*

1. *If $A \leq G$, then $f(A) \leq H$.*
2. *If $B \leq H$, then $f^{-1}(B) \leq G$.*

Lemma 2.4.9. *Let $(G, *)$ and $(H, \diamond)$ be groups, and let $f : G \to H$ be a function. Suppose that f is injective, and that $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$.*

1. *$f(G) \leq H$.*
2. *The map $f : G \to f(G)$ is an isomorphism.*

Exercises

Exercise 2.4.1. Let $\mathrm{GL}_2(\mathbb{R})$ denote the set of invertible 2×2 matrices with real number entries, and let $\mathrm{SL}_2(\mathbb{R})$ denote the set of all 2×2 matrices with real number entries that have determinant 1. Prove that $\mathrm{SL}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. (This exercise requires familiarity with basic properties of determinants.)

Exercise 2.4.2. Prove Theorem 2.4.5.

Exercise 2.4.3. Let $n \in \mathbb{N}$.

(1) Prove that $(\mathbb{Z}_n, +)$ is an abelian group.

(2) Suppose that n is not a prime number. Then $n = ab$ for some $a, b \in \mathbb{N}$ such that $1 < a < n$ and $1 < b < n$. Prove that the set $\{[0], [a], [2a], \ldots, [(b-1)a]\}$ is a subgroup of $\mathbb{Z}_n$.

(3) Is $(\mathbb{Z}_n - \{[0]\}, \cdot)$ a group for all n? If not, can you find any conditions on n that would guarantee that $(\mathbb{Z}_n - \{[0]\}, \cdot)$ is a group?

Exercise 2.4.4. Find all the subgroups of the symmetry group of the square.

Exercise 2.4.5. Let G be a group, and let $A, B \subseteq G$. Suppose that G is abelian. Let AB denote the subset

$$AB = \{ab \mid a \in A \text{ and } b \in B\}.$$

Prove that if $A, B \leq G$, then $AB \leq G$.

Exercise 2.4.6. Let G be a group, and let $H \subseteq G$. Prove that $H \leq G$ if and only if the following two conditions hold.

(i) $H \neq \emptyset$.

(ii) If $a, b \in H$, then $a * b^{-1} \in H$.

Exercise 2.4.7. Let G be a group. Suppose that G is abelian. Let I denote the subset

$$I = \{g \in G \mid g^2 = e_G\}.$$

Prove that $I \leq G$.

Exercise 2.4.8. Let G be a group, and let $H \subseteq G$. Suppose that the following three conditions hold.

(i) $H \neq \emptyset$.

(ii) H is finite.

(iii) H is closed under $*$.

Prove that $H \leq G$.

Exercise 2.4.9. Let G be a group, and let $s \in G$. Let C_s denote the subset

$$C_s = \{g \in G \mid gs = sg\}.$$

Prove that $C_s \leq G$.

Exercise 2.4.10. Let G be a group, and let $A \subseteq G$. Let C_A denote the subset

$$C_A = \{g \in G \mid ga = ag \text{ for all } a \in A\}.$$

Prove that $C_A \leq G$.

3

Various Types of Groups

3.1 Cyclic Groups

Fraleigh, 7th ed. – Section 6
Gallian, 7th ed. – Section 4
Judson, 2016 – Section 4.1

Lemma 3.1.1. *Let G be a group and let $a \in G$. Then*

$$\{a^n \mid n \in \mathbb{Z}\} = \bigcap \{H \leq G \mid a \in H\}. \tag{3.1.1}$$

Definition 3.1.2. Let G be a group and let $a \in G$. The **cyclic subgroup** of G **generated by** a, denoted $\langle a \rangle$, is the set in Equation 3.1.1. △

Definition 3.1.3. Let G be a group. Then G is a **cyclic group** if $G = \langle a \rangle$ for some $a \in G$; the element a is a **generator** of G. △

Definition 3.1.4. Let G be a group and let $H \leq G$. Then H is a **cyclic subgroup** of G if $H = \langle a \rangle$ for some $a \in G$; the element a is a **generator** of H. △

Definition 3.1.5. Let G be a group and let $a \in G$. If $\langle a \rangle$ is finite, the **order** of a, denoted $|a|$, is the cardinality of $\langle a \rangle$. If $\langle a \rangle$ is infinite, then a has **infinite order**. △

Theorem 3.1.6 (Well-Ordering Principle). *Let $A \subseteq \mathbb{N}$ be a set. If A is non-empty, then there is a unique $m \in A$ such that $m \leq a$ for all $a \in A$.*

Theorem 3.1.7 (Division Algorithm). *Let $a, b \in \mathbb{Z}$. Suppose that $b \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.*

Theorem 3.1.8. *Let G be a group, let $a \in G$ and let $m \in \mathbb{N}$. Then $|a| = m$ if and only if $a^m = e$ and $a^i \neq e$ for all $i \in \{1, \ldots, m-1\}$.*

Lemma 3.1.9. *Let G be a group. If G is cyclic, then G is abelian.*

Theorem 3.1.10. *Let G be a group and let $H \leq G$. If G is cyclic, then H is cyclic.*

Corollary 3.1.11. *Every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{N} \cup \{0\}$.*

Theorem 3.1.12. *Let G be a group. Suppose that G is cyclic.*

1. *If G is infinite, then $G \cong \mathbb{Z}$.*
2. *If $|G| = n$ for some $n \in \mathbb{N}$, then $G \cong \mathbb{Z}_n$.*

Definition 3.1.13. Let $a, b \in \mathbb{Z}$. If at least one of a or b is not zero, the **greatest common divisor** of a and b, denoted (a, b), is the largest integer that divides both a and b. Let $(0, 0) = 0$. △

Lemma 3.1.14. *Let $a, b \in \mathbb{Z}$. Then (a, b) exists and $(a, b) \geq 0$.*

Definition 3.1.15. Let $a, b \in \mathbb{Z}$. The numbers a and b are **relatively prime** if $(a, b) = 1$. △

Lemma 3.1.16. *Let $a, b \in \mathbb{Z}$. Then there are $m, n \in \mathbb{Z}$ such that $(a, b) = ma + nb$.*

Corollary 3.1.17. *Let $a, b \in \mathbb{Z}$. If r is a common divisor of a and b, then $r|(a, b)$.*

Corollary 3.1.18. *Let $a, b \in \mathbb{Z}$. Then $(a, b) = 1$ if and only if there are $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.*

Corollary 3.1.19. *Let $a, b, r \in \mathbb{Z}$. Suppose that $(a, b) = 1$. If $a|br$ then $a|r$.*

Theorem 3.1.20. *Let G be a group. Suppose that $G = \langle a \rangle$ for some $a \in G$, and that $|G| = n$ for some $n \in \mathbb{N}$. Let $s, r \in \mathbb{N}$.*

1. $|a^s| = \frac{n}{(n,s)}$.
2. $\langle a^s \rangle = \langle a^r \rangle$ *if and only if* $(n, s) = (n, r)$.

Corollary 3.1.21. *Let G be a group. Suppose that $G = \langle a \rangle$ for some $a \in G$, and that $|G| = n$ for some $n \in \mathbb{N}$. Let $s \in \mathbb{N}$. Then $G = \langle a^s \rangle$ if and only if $(n, s) = 1$.*

Exercises

Exercise 3.1.1. Let C be a cyclic group of order 60. How many generators does C have?

Exercise 3.1.2. List all orders of subgroups of $\mathbb{Z}_{20}$.

Exercise 3.1.3. Find all the subgroups of $\mathbb{Z}_{36}$.

Exercise 3.1.4. Let $p, q \in \mathbb{N}$ be prime numbers. How many generators does the group $\mathbb{Z}_{pq}$ have?

Exercise 3.1.5. Let G be a group, and let $g, h \in G$. Prove that if gh has order p for some $p \in \mathbb{N}$, then hg has order p.

Exercise 3.1.6. Let G and H be groups, and let $f, k : G \to H$ be isomorphisms. Suppose that $G = \langle a \rangle$ for some $a \in G$. Prove that if $f(a) = k(a)$, then $f = k$.

Exercise 3.1.7. Let G be a group. Prove that if G has a finite number of subgroups, then G is finite.

Exercise 3.1.8. Let G be a group, and let $A, B \leq G$. Suppose that G is abelian, and that A and B are cyclic and finite. Suppose that $|A|$ and $|B|$ are relatively prime. Prove that G has a cyclic subgroup of order $|A| \cdot |B|$

3.2 Finitely Generated Groups

Fraleigh, 7th ed. – Section 7

Lemma 3.2.1. *Let G be a group and let $S \subseteq G$.*

1. $\{H \leq G \mid S \subseteq H\} \neq \emptyset$.
2. $\bigcap\{H \leq G \mid S \subseteq H\} \leq G$.
3. *If $K \leq G$ and $S \subseteq K$, then $\bigcap\{H \leq G \mid S \subseteq H\} \subseteq K$.*

Definition 3.2.2. Let G be a group and let $S \subseteq G$. The **subgroup generated** by S, denoted $\langle S \rangle$, is defined by $\langle S \rangle = \bigcap\{H \leq G \mid S \subseteq H\}$. △

Theorem 3.2.3. *Let G be a group and let $S \subseteq G$. Then*

$$\langle S \rangle = \{(a_1)^{n_1}(a_2)^{n_2} \cdots (a_k)^{n_k} \mid k \in \mathbb{N}, \text{ and } a_1, \ldots, a_k \in S, \text{ and } n_1, \ldots, n_k \in \mathbb{Z}\}.$$

Remark 3.2.4. In an abelian group, using additive notation, we would write the result of Theorem 3.2.3 as

$$\langle S \rangle = \{n_1a_1 + n_2a_2 + \cdots + n_ka_k \mid k \in \mathbb{N}, \text{ and } a_1, \ldots, a_k \in S, \text{ and } n_1, \ldots, n_k \in \mathbb{Z}\}.$$

◊

Definition 3.2.5. Let G be a group and let $S \subseteq G$. Suppose $\langle S \rangle = G$. The set S **generates** G, and the elements of S are **generators** of G. △

Definition 3.2.6. Let G be a group. If $G = \langle S \rangle$ for some finite subset $S \subseteq G$, then G is **finitely generated**. △

3.3 Dihedral Groups

Fraleigh, 7th ed. – Section 8
Gallian, 7th ed. – Section 1
Judson, 2016 – Section 5.2

Theorem 3.3.1. *Let $n \in \mathbb{N}$. Suppose $n \geq 3$. For a regular n-gon, let 1 denote the identity symmetry, let r denote the smallest possible clockwise rotation symmetry, and let m denote a reflection symmetry.*

1. *$r^n = 1$, and $r^k \neq 1$ for $k \in \{1, \ldots, n-1\}$.*

2. *$m^2 = 1$ and $m \neq 1$.*

3. *$rm = mr^{-1}$.*

4. *If $p \in \mathbb{Z}$, then $r^p m = mr^{-p}$.*

5. *If $p \in \mathbb{N}$, then $r^p = r^k$ for a unique $k \in \{0, 1, \ldots, n-1\}$.*

6. *If $p, s \in \{0, 1, \ldots, n-1\}$, then $r^p = r^s$ and $mr^p = mr^s$ if and only if $p = s$.*

7. *If $p \in \{0, 1, \ldots, n-1\}$, then $m \neq r^p$.*

8. *If $p \in \{0, 1, \ldots, n-1\}$, then $(r^p)^{-1} = r^{n-p}$ and $(mr^p)^{-1} = mr^p$.*

Definition 3.3.2. Let $n \in \mathbb{N}$. Suppose $n \geq 3$. For a regular n-gon, let 1 denote the identity symmetry, let r denote the smallest possible clockwise rotation symmetry, and let m denote a reflection symmetry. The ***n*-th dihedral group**, denoted D_n, is the group

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, m, mr, mr^2, \ldots, mr^{n-1}\}. \qquad \triangle$$

Theorem 3.3.3. *Let $n \in \mathbb{N}$. Suppose $n \geq 3$. Then there is a unique group with generators a and b that satisfy the following three conditions.*

(i) *$a^n = 1$, and $a^k \neq 1$ for all $k \in \{1, \ldots, n-1\}$.*

(ii) *$b^2 = 1$ and $b \neq 1$.*

(iii) *$ab = ba^{-1}$.*

3.4 Permutations and Permutation Groups

Fraleigh, 7th ed. – Section 8
Gallian, 7th ed. – Section 5, 6
Judson, 2016 – Section 5.1

Definition 3.4.1. Let A be a non-empty set. A **permutation** of A is a bijective map $A \to A$. The set of all permutations of A is denoted S_A. The identity permutation $A \to A$ is denoted ι. △

Definition 3.4.2. Let A be a non-empty set. The composition of two permutations of A is called **permutation multiplication**. △

Lemma 3.4.3. *Let A be a non-empty set. The pair $(S_A, \circ)$ is a group.*

Remark 3.4.4. In the group S_A, we will usually write $\sigma\tau$ as an abbreviation of $\sigma \circ \tau$. ◊

Lemma 3.4.5. *Let A and B be non-empty sets. Suppose that A and B have the same cardinality. Then $S_A \cong S_B$.*

Definition 3.4.6. Let $n \in \mathbb{N}$, and let $A = \{1, \ldots, n\}$. The group S_A is denoted S_n. The group S_n is the **symmetric group on n letters**. △

Proposition 3.4.7. *Let A be a non-empty set. Then S_A is abelian if and only if A is finite and $|A| \leq 2$.*

Theorem 3.4.8 (Cayley's Theorem). *Let G be a group. Then there is a set A such that G is isomorphic to a subgroup of S_A. If G is finite, a finite set A can be found.*

Exercises

Exercise 3.4.1. Let $\sigma, \tau \in S_5$ be defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}.$$

Compute each of the following.

(1) σ^2.

(2) τ^{-1}.

(3) $\tau\sigma$.

(4) $\sigma\tau$.

Exercise 3.4.2. Find all subgroups of S_3.

Exercise 3.4.3. Let $n \in \mathbb{N}$. Suppose $n \geq 3$. Let $\sigma \in S_n$. Suppose that $\sigma\tau = \tau\sigma$ for all $\tau \in S_n$. Prove that $\sigma = \iota$.

Exercise 3.4.4. Let A be a non-empty set, and let $P \leq S_A$. The subgroup P is **transitive** on A if for each $x, y \in A$, there is some $\sigma \in P$ such that $\sigma(x) = y$.

Prove that if A is finite, then there is a subgroup $Q \leq S_A$ such that Q is cyclic, that $|Q| = |A|$, and that Q is transitive on A.

3.5 Permutations Part II and Alternating Groups

Fraleigh, 7th ed. – Section 9
Gallian, 7th ed. – Section 5
Judson, 2016 – Section 5.1

Definition 3.5.1. Let A be a non-empty set, and let $\sigma \in S_A$. Let $\sim$ be the relation on A defined by $a \sim b$ if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$, for all $a, b \in A$. △

Lemma 3.5.2. *Let A be a non-empty set, and let $\sigma \in S_A$. The relation $\sim$ is an equivalence relation on A.*

Definition 3.5.3. Let A be a set, and let $\sigma \in S_A$. The equivalence classes of $\sim$ are called the **orbits** of σ. △

Definition 3.5.4. Let $n \in \mathbb{N}$, and let $\sigma \in S_n$. The permutation σ is a **cycle** if it has at most one orbit with more than one element. The **length** of a cycle is the number of elements in its largest orbit. A cycle of length 2 is a **transposition**. △

Lemma 3.5.5. *Let $n \in \mathbb{N}$, and let $\sigma \in S_n$. Then σ is the product of disjoint cycles; the cycles of length greater than* 1 *are unique, though not their order.*

Corollary 3.5.6. *Let $n \in \mathbb{N}$, and let $\sigma \in S_n$. Suppose $n \geq 2$. Then σ is the product of transpositions.*

Theorem 3.5.7. *Let $n \in \mathbb{N}$, and let $\sigma \in S_n$. Suppose $n \geq 2$. Then either all representations of σ as a product of transpositions have an even number of transpositions, or all have an odd number of transpositions.*

Definition 3.5.8. Let $n \in \mathbb{N}$, and let $\sigma \in S_n$. Suppose $n \geq 2$. The permutation σ is **even** or **odd**, respectively, if it is the product of an even number or odd number, respectively, of transpositions. △

Definition 3.5.9. Let $n \in \mathbb{N}$. Suppose $n \geq 2$. The set of all even permutations of A is denoted A_n. △

Lemma 3.5.10. *Let $n \in \mathbb{N}$. Suppose $n \geq 2$.*

1. *The set A_n is a subgroup of S_n.*
2. $|A_n| = \frac{n!}{2}$.

Definition 3.5.11. Let $n \in \mathbb{N}$. Suppose $n \geq 2$. The group A_n is the **alternating group on n letters**. △

Exercises

Exercise 3.5.1. Compute the product of cycles $(1,5,2)(3,4)$ as a single permutation in the following groups.

(1) In S_5.

(2) In S_6.

Exercise 3.5.2. Let $\sigma \in S_7$ be defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 1 & 4 & 3 & 6 \end{pmatrix}.$$

(1) Write σ as a product of cycles.

(2) Write σ as a product of transpositions.

Exercise 3.5.3. Let $n \in \mathbb{N}$. Suppose $n \geq 3$. Let $\sigma \in S_n$.

(1) Prove that σ can be written as a product of at most $n-1$ transpositions.

(2) Prove that if σ is not a cycle, it can be written as a product of at most $n-2$ transpositions.

(3) Prove that if σ is odd, it can be written as a product of $2n+3$ transpositions.

(4) Prove that if σ is even, it can be written as a product of $2n+8$ transpositions.

Exercise 3.5.4. Let $n \in \mathbb{N}$. Suppose $n \geq 2$. Let $K \leq S_n$. Prove that either all the permutations in K are even, or exactly half the permutations in K are even.

Exercise 3.5.5. Let $n \in \mathbb{N}$. Suppose $n \geq 2$. Let $\sigma \in S_n$. Suppose that σ is odd. Prove that if $\tau \in S_n$ is odd, then there is some $\eta \in A_n$ such that $\tau = \sigma\eta$.

Exercise 3.5.6. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Prove that if σ is a cycle of odd length, then σ^2 is a cycle.

4

Basic Constructions

4.1 Direct Products

Fraleigh, 7th ed. – Section 11
Gallian, 7th ed. – Section 8
Judson, 2016 – Section 9.2

Definition 4.1.1. Let H and K be groups. The **product binary operation** on $H \times K$ is the binary operation defined by $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$ for all $(h_1, k_1), (h_2, k_2) \in H \times K$. △

Lemma 4.1.2. *Let H and K be groups. The set $H \times K$ with the product binary operation is a group.*

Definition 4.1.3. Let H and K be groups. The set $H \times K$ with the product binary operation is the **direct product** of the groups H and K. △

Lemma 4.1.4. *Let H and K be groups. Then $H \times K \cong K \times H$.*

Lemma 4.1.5. *Let H and K be groups. Suppose that H and K are abelian. Then $H \times K$ is abelian.*

Theorem 4.1.6. *Let $m, n \in \mathbb{N}$. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.*

Definition 4.1.7. Let G be a group, and let $A, B \subseteq G$. Let AB denote the subset $AB = \{ab \mid a \in A \text{ and } b \in B\}$. △

Lemma 4.1.8. *Let H and K be groups. Let $\bar{H} = H \times \{e_K\}$ and $\bar{K} = \{e_H\} \times K$.*

1. *$\bar{H}, \bar{K} \leq H \times K$.*

2. *$\bar{H}\bar{K} = H \times K$.*

3. *$\bar{H} \cap \bar{K} = \{(e_H, e_K)\}$.*

4. *$hk = kh$ for all $h \in \bar{H}$ and $k \in \bar{K}$.*

Lemma 4.1.9. *Let G be a group, and let $H, K \leq G$. Suppose that the following properties hold.*

(i) *$HK = G$.*

(ii) *$H \cap K = \{e\}$.*

(iii) *$hk = kh$ for all $h \in H$ and $k \in K$.*

Then $G \cong H \times K$.

Lemma 4.1.10. *Let* G *be a group, and let* $H, K \leq G$. *Then* $HK = G$ *and* $H \cap K = \{e\}$ *if and only if for every* $g \in G$ *there are unique* $h \in H$ *and* $k \in K$ *such that* $g = hk$.

Theorem 4.1.11. *Let* $m_1, \ldots, m_r \in \mathbb{N}$. *The group* $\prod_{i=1}^{r} \mathbb{Z}_{m_i}$ *is cyclic and is isomorphic to* $\mathbb{Z}_{m_1 m_2 \cdots m_r}$ *if and only if* m_i *and* m_k *are relatively prime for all* $i, k \in \{1, \ldots, r\}$ *such that* $i \neq k$.

Exercises

Exercise 4.1.1. List all the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$, and find the order of each element.

Exercise 4.1.2. Find all the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercise 4.1.3. Prove Lemma 4.1.8.

Exercise 4.1.4. Prove Lemma 4.1.9.

4.2 Finitely Generated Abelian Groups

Fraleigh, 7th ed. – Section 11
Gallian, 7th ed. – Section 11
Judson, 2016 – Section 13.1

Theorem 4.2.1 (**Fundamental Theorem of Finitely Generated Abelian Groups**)**.** *Let G be a finitely generated abelian group. Then*

$$G = \mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbb{Z}_{(p_k)^{n_k}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

for some $k \in \mathbb{N}$, and prime numbers $p_1, \ldots, p_k \in \mathbb{N}$, and $n_1, \ldots, n_k \in \mathbb{N}$. This direct product is unique up to the rearrangement of factors.

Exercises

Exercise 4.2.1. Find, up to isomorphism, all abelian groups of order 16.

Exercise 4.2.2. Find, up to isomorphism, all abelian groups of order 720.

Exercise 4.2.3. How many abelian groups are there, up to isomorphism, of order 24.

Exercise 4.2.4. Let G be a group. Suppose that G is finite and abelian. Prove that G is not cyclic if and only if there is some prime number $p \in \mathbb{N}$ such that G has a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

4.3 Infinite Products of Groups

Definition 4.3.1. Let I be a non-empty set, and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I. The **product** of the family of sets, denoted $\prod_{i\in I} A_i$, is the set defined by

$$\prod_{i\in I} A_i = \{f \in \mathcal{F}(I, \bigcup_{i\in I} A_i) \mid f(i) \in A_i \text{ for all } i \in I\}.$$

If all the sets A_i are equal to a single set A, the product $\prod_{i\in I} A_i$ is denoted by A^I. △

Theorem 4.3.2. *Let I be a non-empty set, and let $\{A_i\}_{i\in I}$ be a family of non-empty sets indexed by I. Then $\prod_{i\in I} A_i \neq \emptyset$.*

Definition 4.3.3. Let I be a non-empty set, and let $\{G_i\}_{i\in I}$ be a family of non-empty groups indexed by I. Let $f, g \in \prod_{i\in I} G_i$.

1. Let $fg : I \to \bigcup_{i\in I} A_i$ be defined by $(fg)(i) = f(i)g(i)$ for all $i \in I$.
2. Let $f' : I \to \bigcup_{i\in I} A_i$ be defined by $(f)(i) = [f(i)]^{-1}$ for all $i \in I$.
3. Let $\bar{e} : I \to \bigcup_{i\in I} A_i$ be defined by $\bar{e}(i) = e_{G_i}$ for all $i \in I$. △

Lemma 4.3.4. *Let I be a non-empty set, and let $\{G_i\}_{i\in I}$ be a family of non-empty groups indexed by I. Let $f, g \in \prod_{i\in I} G_i$.*

1. $fg \in \prod_{i\in I} G_i$.
2. $f' \in \prod_{i\in I} G_i$.
3. $\bar{e} \in \prod_{i\in I} G_i$.

Lemma 4.3.5. *Let I be a non-empty set, and let $\{G_i\}_{i\in I}$ be a family of non-empty groups indexed by I. Then $\prod_{i\in I} G_i$ is group.*

4.4 Cosets

Fraleigh, 7th ed. – Section 10
Gallian, 7th ed. – Section 7
Judson, 2016 – Section 6.1, 6.2

Definition 4.4.1. Let G be a group and let $H \leq G$. Let $\sim_L$ and $\sim_R$ be the relations on G defined by $a \sim_L b$ if and only if $a^{-1}b \in H$ for all $a, b \in G$, and $a \sim_R b$ if and only if $ab^{-1} \in H$ for all $a, b \in G$. △

Lemma 4.4.2. *Let G be a group and let $H \leq G$. The relations $\sim_L$ and $\sim_R$ are equivalence relations on G.*

Definition 4.4.3. Let G be a group, let $H \leq G$ and let $a \in G$. Let aH and Ha be defined by

$$aH = \{ah \mid h \in H\} \quad \text{and} \quad Ha = \{ha \mid h \in H\}. \qquad \triangle$$

Lemma 4.4.4. *Let G be a group, let $H \leq G$ and let $a \in G$.*

1. *The equivalence class of a with respect to $\sim_L$ is aH.*
2. *The equivalence class of a with respect to $\sim_R$ is Ha.*

Definition 4.4.5. Let G be a group, let $H \leq G$ and let $a \in G$. The **left coset** of a (with respect to H) is the set aH. The **right coset** of a (with respect to H) is the set Ha. △

Lemma 4.4.6. *Let G be a group, let $H \leq G$ and let $a, b \in G$.*

1. *$aH = bH$ if and only if $a^{-1}b \in H$.*
2. *$Ha = Hb$ if and only if $ab^{-1} \in H$.*
3. *$aH = H$ if and only if $a \in H$.*
4. *$Ha = H$ if and only if $a \in H$.*

Lemma 4.4.7. *Let G be a group and let $H \leq G$.*

1. *All left cosets of G with respect to H and all right cosets of G with respect to H have the same cardinality as H.*

2. *The family of all left cosets of G with respect to H has the same cardinality as the family of all right cosets of G with respect to H.*

Definition 4.4.8. Let G be a group, let $H \leq G$. The **index** of H in G, denoted $(G : H)$, is the number of left cosets of G with respect to H. △

Theorem 4.4.9. *Let G be a group and let $H \leq G$. Suppose that G is finite. Then $|G| = |H| \cdot (G : H)$.*

Corollary 4.4.10 (Lagrange's Theorem)**.** *Let G be a group and let $H \leq G$. Suppose that G is finite. Then $|H|$ divides $|G|$.*

Corollary 4.4.11. *Let G be a group and let $a \in G$. Suppose that G is finite. Then $|a|$ divides $|G|$.*

Corollary 4.4.12. *Let G be a group. If $|G|$ is a prime number, then G is cyclic.*

Corollary 4.4.13. *Let $p \in \mathbb{N}$ be a prime number. The only group of order p, up to isomorphism, is $\mathbb{Z}_p$.*

Theorem 4.4.14. *Let G be a group and let $K \leq H \leq G$. Suppose that $(G : H)$ and $(H : K)$ are finite. Then $(G : K)$ is finite, and $(G : K) = (G : H) \cdot (H : K)$.*

Exercises

Exercise 4.4.1. Find all cosets of the group $2\mathbb{Z}$ with respect to the subgroup $4\mathbb{Z}$.

Exercise 4.4.2. Find all cosets of the group $\mathbb{Z}_{12}$ with respect to the subgroup $\langle 4 \rangle$.

Exercise 4.4.3. Find $(\mathbb{Z}_{24} : \langle 3 \rangle)$.

Exercise 4.4.4. Let G be a group, and let $p, q \in \mathbb{N}$ be prime numbers. Suppose that $|G| = pq$. Prove that every proper subgroup of G is cyclic.

Exercise 4.4.5. Let G be a group, let $H \leq G$. Prove that there is a bijective map from the set of all left cosets of G with respect to H to the set of all right cosets of G with respect to H. (Note: the group G is not necessarily finite.)

Exercise 4.4.6. Prove Theorem 4.4.14.

Exercise 4.4.7. Let G be a group, let $H \leq G$. Suppose that G is finite, and that $(G : H) = 2$. Prove that every left coset of G with respect to H is a right coset of G with respect to H.

Exercise 4.4.8. Let G be a group. Suppose that G is finite. Let $n = |G|$. Prove that if $g \in G$, then $g^n = e_G$.

4.5 Quotient Groups

Fraleigh, 7th ed. – Section 14, 15
Gallian, 7th ed. – Section 9
Judson, 2016 – Section 10.1

Lemma 4.5.1. *Let G be a group and let $H \leq G$. The formula $(aH)(bH) = (ab)H$ for all $a, b \in G$ gives a well-defined binary operation on the set of all left cosets of G with respect to H if and only if $gH = Hg$ for all $g \in G$.*

Lemma 4.5.2. *Let G be a group and let $H \leq G$. The following are equivalent.*

a. *$gHg^{-1} \subseteq H$ for all $g \in G$.*

b. *$gHg^{-1} = H$ for all $g \in G$.*

c. *$gH = Hg$ for all $g \in G$.*

Definition 4.5.3. Let G be a group and let $H \leq G$. The subgroup H is **normal** if any of the conditions in Lemma 4.5.2 are satisfied. If H is a normal subgroup of G, it is denoted $H \lhd G$. △

Remark 4.5.4. Every subgroup of an abelian group is normal. ◊

Definition 4.5.5. Let G be a group and let $H \lhd G$. The set of all left cosets of G with respect to H is denoted G/H. △

Lemma 4.5.6. *Let G be a group and let $H \lhd G$. The set G/H with the binary operation given by $(aH)(bH) = (ab)H$ for all $a, b \in G$ is a group.*

Definition 4.5.7. Let G be a group and let $H \lhd G$. The set G/H with the binary operation given by $(aH)(bH) = (ab)H$ for all $a, b \in G$ is the **quotient group** (also called **factor group**) of G by H. △

Corollary 4.5.8. *Let G be a group and let $H \lhd G$. Suppose that G is finite. Then $|G/H| = (G : H) = \frac{|G|}{|H|}$.*

Lemma 4.5.9. *Let G be a group and let $H \leq G$. Suppose that G is abelian. Then G/H is abelian.*

Lemma 4.5.10. *Let G be a group and let $H \leq G$. Suppose that G is cyclic. Then G/H is cyclic.*

Lemma 4.5.11. *Let G be a group and let $H \leq G$. If $(G : H) = 2$, then $H \lhd G$.*

Lemma 4.5.12. *Let G be a group and let $H \leq G$. Suppose that G is finite. If $|H| = \frac{1}{2}|G|$, then $H \lhd G$.*

Lemma 4.5.13. *Let H and K be groups. Let $G = H \times K$.*

1. *$H \times \{e_K\} \lhd G$ and $\{e_H\} \times K \lhd G$.*
2. *$G/(H \times \{e_K\}) \cong K$ and $G/(\{e_H\} \times K) \cong H$.*

Lemma 4.5.14. *Let G be a group, and let $H, K \leq G$. Suppose that the following properties hold.*

(i) $HK = G$.

(ii) $H \cap K = \{e\}$.

Then $H, K \lhd G$ if and only if $hk = kh$ for all $h \in H$ and $k \in K$.

Definition 4.5.15. Let G be a group. The group G is **simple** if it has no non-trivial proper normal subgroups. △

Exercises

Exercise 4.5.1. Compute each of the following quotient groups; state what the group is in the form given by the Fundamental Theorem of Finitely Generated Abelian Groups.

(1) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,2)\rangle$.

(2) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle$.

(3) $(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2,4)\rangle$.

(4) $(\mathbb{Z} \times \mathbb{Z})/\langle(0,1)\rangle$.

(5) $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(1,1,1)\rangle$.

Exercise 4.5.2. Let G be a group and let $H \lhd G$. Suppose that $(G : H)$ is finite. Let $m = (G : H)$. Prove that if $g \in G$, then $g^m \in H$.

Exercise 4.5.3. Let G be a group, and let $\{H_i\}_{i \in I}$ be a family of normal subgroups of G indexed by I. Prove that $\bigcap_{i \in I} H_i \lhd G$.

Exercise 4.5.4. Let G be a group and let $S \subseteq G$.

(1) Prove that $\{H \lhd G \mid S \subseteq H\} \neq \emptyset$.

(2) Prove that $\bigcap\{H \lhd G \mid S \subseteq H\} \lhd G$.

(3) Prove that if $K \lhd G$ and $S \subseteq K$, then $\bigcap\{H \lhd G \mid S \subseteq H\} \subseteq K$.

The **normal subgroup generated** by S, which is defined by $\bigcap\{H \leq G \mid S \subseteq H\}$, is the smallest normal subgroup of G that contains S.

Exercise 4.5.5. Let G be a group. A **commutator** in G is an element of G that can be expressed in the form $aba^{-1}b^{-1}$ for some $a, b \in G$. The **commutator subgroup** of G is the smallest normal subgroup of G that contains all the commutators in G; such a subgroup exists by Exercise 4.5.4.

Let C denote the commutator subgroup of G. Prove that G/C is abelian.

Exercise 4.5.6. Let G be a group and let $H \leq G$. Suppose that no other subgroup of G has the same cardinality as H. Prove that $H \lhd G$.

Exercise 4.5.7. Let G be a group, let $H \leq G$, and let $N \lhd G$.

(1) Prove that $H \cap N \lhd H$.

(2) Is $H \cap N$ a normal subgroup of G? Give a proof or a counterexample.

Exercise 4.5.8. Let G be a group, and let $m \in \mathbb{N}$. Suppose that G has a subgroup of order m. Let $K = \bigcap\{H \leq G \mid |H| = m\}$. Prove that $K \lhd G$.

5

Homomorphisms

5.1 Homomorphisms

Fraleigh, 7th ed. – Section 13
Gallian, 7th ed. – Section 10
Judson, 2016 – Section 11.1

Definition 5.1.1. Let $(G, *)$ and $(H, \diamond)$ be groups, and let $f : G \to H$ be a function. The function f is a **homomorphism** (sometimes called a **group homomorphism**) if $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$. △

Theorem 5.1.2. *Let G and H be groups, and let $f : G \to H$ be a homomorphism.*

1. *$f(e_G) = e_H$.*
2. *If $a \in G$, then $f(a^{-1}) = [f(a)]^{-1}$, where the first inverse is in G, and the second is in H.*
3. *If $A \leq G$, then $f(A) \leq H$.*
4. *If $B \leq H$, then $f^{-1}(B) \leq G$.*

Theorem 5.1.3. *Let G, H and K be groups, and let $f : G \to H$ and $j : H \to K$ be homomorphisms. Then $j \circ f$ is a homomorphism.*

Lemma 5.1.4. *Let G and H be groups. Suppose that G is cyclic with generator a. If $b \in H$, there is a unique homomorphism $f : G \to H$ such that $f(a) = b$.*

Definition 5.1.5. Let G be a group. An **endomorphism** of G is a homomorphism $G \to G$. An **automorphism** of G is an isomorphism $G \to G$. △

Definition 5.1.6. Let G be a group. An automorphism $f : G \to G$ is an **inner automorphism** if there is some $g \in G$ such that $f(x) = gxg^{-1}$ for all $x \in G$. △

Lemma 5.1.7. *Let G be a group, and let $H \leq G$. Then $H \lhd G$ if and only if $f(H) = H$ for all inner automorphisms of G.*

Exercises

Exercise 5.1.1. Which of the following functions are homomorphisms? Which of the homomorphisms are isomorphisms? The groups under consideration are $(\mathbb{R}, +)$, and $(\mathbb{Q}, +)$, and $((0, \infty), \cdot)$.

(1) Let $f : \mathbb{Q} \to (0, \infty)$ be defined by $f(x) = 5^x$ for all $x \in \mathbb{Q}$.

(2) Let $k : (0, \infty) \to (0, \infty)$ be defined by $k(x) = x^{-7}$ for all $x \in (0, \infty)$.

(3) Let $m : \mathbb{R} \to \mathbb{R}$ be defined by $m(x) = x + 3$ for all $x \in \mathbb{R}$.

(4) Let $g : (0, \infty) \to \mathbb{R}$ be defined by $g(x) = \ln x$ for all $x \in (0, \infty)$.

(5) Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = |x|$ for all $x \in \mathbb{R}$.

Exercise 5.1.2. Prove that the function $\det : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R} - \{0\}$ is a homomorphism, where the binary operation for both groups is multiplication.

Exercise 5.1.3.

(1) Let $j : \mathbb{Z}_4 \to \mathbb{Z}_3$ be defined by $j([x]) = [x]$ for all $[x] \in \mathbb{Z}_4$, where the two appearances of "$[x]$" in the definition of j refer to elements in different groups. Is this function well-defined? If it is well-defined, is it a homomorphism?

(2) Let $k : \mathbb{Z}_6 \to \mathbb{Z}_3$ be defined by $k([x]) = [x]$ for all $[x] \in \mathbb{Z}_6$. Is this function well-defined? If it is well-defined, is it a homomorphism?

(3) Can you find criteria on $n, m \in \mathbb{N}$ that will determine when the function $r : \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $r([x]) = [x]$ for all $[x] \in \mathbb{Z}_n$ is well-defined and is a homomorphism? Prove your claim.

Exercise 5.1.4. Let G and H be groups. Prove that the projection maps $\pi_1 : G \times H \to G$ and $\pi_2 : G \times H \to H$ are homomorphisms.

Exercise 5.1.5. Let G be a group, and let $f : G \to G$ be defined by $f(x) = x^{-1}$ for all $x \in G$. Is g a homomorphism? Give a proof or a counterexample.

Exercise 5.1.6. Let G and H be groups, and let $f, k : G \to H$ be homomorphisms. Suppose that $G = \langle S \rangle$ for some $S \subseteq G$. Prove that if $f(a) = k(a)$ for all $a \in S$, then $f = k$.

5.2 Kernel and Image

Fraleigh, 7th ed. – Section 13, 14
Gallian, 7th ed. – Section 10
Judson, 2016 – Section 11.1, 11.2

Definition 5.2.1. Let G and H be groups, and let $f : G \to H$ be a homomorphism.

1. The **kernel** of f, denoted $\ker f$, is the set $\ker f = f^{-1}(\{e_H\})$.
2. The **image** of f, denoted $\operatorname{im} f$, is the set $\operatorname{im} f = f(G)$. △

Remark 5.2.2. Observe that

$$\ker f = \{g \in G \mid f(g) = e_H\}$$

and

$$\operatorname{im} f = \{h \in H \mid h = f(g) \text{ for some } g \in G\}.$$ ◇

Lemma 5.2.3. *Let G and H be groups, and let $f : G \to H$ be a homomorphism.*

1. $\ker f \leq G$.
2. $\operatorname{im} f \leq H$.

Lemma 5.2.4. *Let G and H be groups, and let $f : G \to H$ be a homomorphism. Then* $\ker f \lhd G$.

Theorem 5.2.5. *Let G and H be groups, and let $f : G \to H$ be a homomorphism. The function f is injective if and only if* $\ker f = \{e_G\}$.

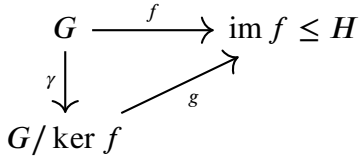
Lemma 5.2.6. *Let G and H be groups, and let $f : G \to H$ be a homomorphism. Let $h \in H$. If $a \in f^{-1}(\{h\})$, then $f^{-1}(\{h\}) = a(\ker f)$.*

Definition 5.2.7. Let G be a group and let $N \lhd G$. The **canonical map** for G and N is the function $\gamma : G \to G/N$ defined by $\gamma(g) = gN$ for all $g \in G$. △

Lemma 5.2.8. *Let G be a group and let $N \lhd G$. The canonical map $\gamma : G \to G/N$ is a surjective homomorphism, and* $\ker \gamma = N$.

Theorem 5.2.9 (**First Isomorphism Theorem**)**.** *Let G and H be groups, and let $f : G \to H$ be a homomorphism. Then there is a a unique isomorphism $g : G/\ker f \to \operatorname{im} f$ such that $f = g \circ \gamma$, where $\gamma : G \to G/\ker f$ is the canonical map.*

Remark 5.2.10. The condition $f = g \circ \gamma$ in the First Isomorphism Theorem is represented by the following commutative diagram (discuss what that means).



$\Diamond$

Corollary 5.2.11. *Let G and H be groups, and let $f : G \to H$ be a homomorphism.*

1. *$G/\ker f \cong \operatorname{im} f$.*
2. *If f is surjective, then $G/\ker f \cong H$.*

Exercises

Exercise 5.2.1. Find the kernel of each of the following homomorphisms.

(1) Let $f : \mathbb{Z} \to \mathbb{Z}_{15}$ be the unique homomorphism determined by $f(1) = [10]$.

(2) Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the unique homomorphism determined by $g((1,0)) = 2$ and $g((0,1)) = 7$.

Exercise 5.2.2. In Exercise 5.1.3, you found criteria on $n, m \in \mathbb{N}$ that determine when the function $r : \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $r([x]) = [x]$ for all $[x] \in \mathbb{Z}_n$ is well-defined and is a homomorphism. Find the kernel for those functions that are well-defined and are homomorphisms.

Exercise 5.2.3. Let G and H be groups, and let $f : G \to H$ be a homomorphism. Prove that $\operatorname{im} f$ is abelian if and only if $aba^{-1}b^{-1} \in \ker f$ for all $a, b \in G$.

Exercise 5.2.4. Let G be a group, and let $g \in G$. Let $f : \mathbb{Z} \to G$ be defined by $f(n) = g^n$ for all $n \in \mathbb{Z}$. Find $\ker f$ and $\operatorname{im} f$.

6
Applications of Groups

6.1 Group Actions

Fraleigh, 7th ed. – Section 16, 17
Gallian, 7th ed. – Section 29
Judson, 2016 – Section 14.1–14.3

Definition 6.1.1. Let X be a set and let G be a group. An **action** of G on X is a function $* : G \times X \to X$ that satisfies the following two conditions.

1. $e_G x = x$ for all $x \in X$.
2. $(ab)x = a(bx)$ for all $x \in X$ and $a, b \in G$. △

Lemma 6.1.2. *Let X be a set and let G be a group.*

1. *Let $* : G \times X \to X$ be an action of G on X. Let $\phi : G \to S_X$ be defined by $\phi(g)(x) = gx$ for all $g \in G$ and $x \in X$. Then ϕ is well-defined and is a homomorphism.*
2. *Let $\psi : G \to S_X$ be a homomorphism. Let $\star : G \times X \to X$ be defined by $\star((g, x)) = \psi(g)(x)$ for all $g \in G$ and $x \in X$. Then $\star$ is an action of G on X.*

Definition 6.1.3. Let X be a set and let G be a group. The set X is a **G-set** if there is an action of G on X. △

Definition 6.1.4. Let X be a set and let G be a group. Suppose that X is a G-set. Let $g \in G$. The **fixed set** of g, denoted X_g, is the set $X_g = \{x \in X \mid gx = x\}$. △

Definition 6.1.5. Let X be a set and let G be a group. Suppose that X is a G-set.

1. The group G **acts faithfully** on X if $X_g \neq X$ for all $g \in G - \{e_G\}$.
2. The group G **acts transitively** on X if for each $x, y \in X$ there is some $g \in G$ such that $gx = y$. △

Definition 6.1.6. Let X be a set and let G be a group. Suppose that X is a G-set. Let $x \in X$. The **isotropy subgroup** of x (also called the **stabilizer** of x), denoted G_x, is the set $G_x = \{g \in G \mid gx = x\}$. △

Lemma 6.1.7. *Let X be a set and let G be a group. Suppose that X is a G-set. Let $x \in X$. Then $G_x \leq G$.*

Definition 6.1.8. Let X be a set and let G be a group. Suppose that X is a G-set. Let $\sim$ be the relation on X defined by $x \sim y$ if and only if there is some $g \in G$ such that $gx = y$ for all $x, y \in X$. △

Lemma 6.1.9. *Let X be a set and let G be a group. Suppose that X is a G-set. The relations $\sim$ is an equivalence relation on X.*

Definition 6.1.10. Let X be a set and let G be a group. Suppose that X is a G-set. Let $x \in X$. The **orbit** of x (with respect to G), denoted Gx, is the set $Gx = \{gx \mid g \in G\}$. △

Lemma 6.1.11. *Let X be a set and let G be a group. Suppose that X is a G-set. Let $x \in X$.*

1. *Suppose Gx is finite. Then $|Gx| = (G : G_x)$.*
2. *Suppose G is finite. Then $|G| = |Gx| \cdot |G_x|$.*

Theorem 6.1.12 (Burnside's Formula). *Let X be a set and let G be a group. Suppose that X and G are finite, and that X is a G-set. Let r be the number of orbits in X with respect to G. Then*

$$r \cdot |G| = \sum_{g \in G} |X_g|.$$

Exercises

Exercise 6.1.1. An action of $(\mathbb{R}, +)$ on the plane $\mathbb{R}^2$ is obtained by assigning to each $\theta \in \mathbb{R}$ the rotation of the $\mathbb{R}^2$ about the origin counterclockwise by angle θ. Let $P \in \mathbb{R}^2$. Suppose that P is not the origin.

(1) Prove that $\mathbb{R}^2$ is a $\mathbb{R}$-set.

(2) Describe the orbit $\mathbb{R}P$ geometrically.

(3) Find the isotropy subgroup $\mathbb{R}_P$.

Exercise 6.1.2. Let X be a set and let G be a group. Suppose that X is a G-set. Prove that G acts faithfully on X if and only if for each $g, h \in G$ such that $g \neq h$, there is some $x \in X$ such that $gx \neq hx$.

Exercise 6.1.3. Let X be a set, let $Y \subseteq X$, and let G be a group. Suppose that X is a G-set. Let $G_Y = \{g \in G \mid gy = y \text{ for all } y \in Y\}$. Prove that $G_Y \leq G$.

Exercise 6.1.4. A five-pointed crown is to have each of it's five points painted with one of three available colors. How many different ways can that be done?

Exercise 6.1.5. The four faces of a tetrahedral die are labeled with 1, 2, 3 and 4 dots, respectively. How many different tetrahedral dice can be made?

Exercise 6.1.6. Each face of a cube is painted with one of eight colors; no two faces can have the same color. How many different cubes can be made?

Exercise 6.1.7. Each corner of a cube is painted with one of four colors; different corners may have the same color. How many different cubes can be made?

7

Rings and Fields

7.1 Rings

Fraleigh, 7th ed. – Section 18
Gallian, 7th ed. – Section 12
Judson, 2016 – Section 16.1

Definition 7.1.1. Let A be a set, and let $+$ and $\cdot$ be binary operations on A.

1. The binary operations $+$ and $\cdot$ satisfy the **Left Distributive Law** (an alternative expression is that $\cdot$ is **left distributive over** $+$) if $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ for all $a, b, c \in A$.

2. The binary operations $+$ and $\cdot$ satisfy the **Right Distributive Law** (an alternative expression is that $\cdot$ is **right distributive over** $+$) if $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in A$. △

Definition 7.1.2. Let R be a non-empty set, and let and let $+$ and $\cdot$ be binary operations on R. The triple $(R, +, \cdot)$ is a **ring** if the following three properties hold.

(i) $(R, +)$ is an abelian group.

(ii) The binary operation $\cdot$ is associative.

(iii) The binary operation $\cdot$ is left distributive and right distributive over $+$. △

Lemma 7.1.3. *Let $(R, +, \cdot)$ be a ring, and let $a, b \in R$.*

1. *$0 \cdot a = 0$ and $a \cdot 0 = 0$.*

2. *$a(-b) = (-a)b = -(ab)$.*

3. *$(-a)(-b) = ab$.*

Definition 7.1.4. Let $(R, +, \cdot)$ be a ring, and let $S \subseteq R$ be a subset. The subset S is a **subring** of R if the following two conditions hold.

(a) S is closed under $+$ and $\cdot$.

(b) $(S, +, \cdot)$ is a ring.

If S is a subring of R, it is denoted $S \leq R$. △

Remark 7.1.5. Let $(R, +, \cdot)$ be a ring, and let $S \subseteq R$ be a subset.

1. If S is a subring of R, then S is an additive subgroup of R.
2. If S is an additive subgroup of R, it is not necessarily the case that S is a subring of R. See Exercise 7.1.3.

$\Diamond$

Lemma 7.1.6. *Let R be a ring, and let $S \leq R$.*

1. *The additive identity element of R is in S, and it is the additive identity element of S.*
2. *The additive inverse operation in S is the same as the additive inverse operation in R.*

Theorem 7.1.7. *Let R be a ring, and let $S \subseteq R$. Then $S \leq R$ if and only if the following four conditions hold.*

(i) $0 \in S$.

(ii) *If $a, b \in S$, then $a + b \in S$.*

(iii) *If $a \in S$, then $-a \in S$.*

(iv) *If $a, b \in S$, then $ab \in S$.*

Theorem 7.1.8. *Let R be a ring, and let $S \subseteq R$. Then $S \leq R$ if and only if the following four conditions hold.*

(i) $S \neq \emptyset$.

(ii) *If $a, b \in S$, then $a + b \in S$.*

(iii) *If $a \in S$, then $-a \in S$.*

(iv) *If $a, b \in S$, then $ab \in S$.*

Theorem 7.1.9. *Let R be a ring, and let $S \subseteq R$. Then $S \leq R$ if and only if the following three conditions hold.*

(i) $S \neq \emptyset$.

(ii) *If $a, b \in S$, then $a + (-b) \in S$.*

(iii) *If $a, b \in S$, then $ab \in S$.*

Lemma 7.1.10. *Let R be a ring, and let $T \subseteq S \subseteq R$. If $T \leq S$ and $S \leq R$, then $T \leq R$.*

Lemma 7.1.11. *Let R be a ring, and let $\{S_i\}_{i \in I}$ be a family of subrings of R indexed by I. Then $\bigcap_{i \in I} S_i \leq R$.*

Definition 7.1.12. Let R and S be rings. The **product binary operations** on $R \times S$ are the binary operations $+$ and $\cdot$ defined by $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$ for all $(r_1, s_1), (r_2, s_2) \in S \times R$. △

Lemma 7.1.13. *Let R and S be rings. The set $R \times S$ with the product binary operations is a ring.*

Definition 7.1.14. Let R and S be rings. The set $R \times S$ with the product binary operations is the **direct product** of the rings R and S. △

Exercises

Exercise 7.1.1. For each of the following sets with two binary operations, state whether the set with the binary operations is a ring.

(1) The set $\mathbb{N}$, with the standard addition and multiplication.

(2) Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$, with the standard addition and multiplication.

(3) The set $\mathbb{Z} \times \mathbb{Z}$, with the standard addition and multiplication on each component.

(4) The set $2\mathbb{Z} \times \mathbb{Z}$, with the standard addition and multiplication on each component.

(5) The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, with the standard addition and multiplication.

(6) The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, with the standard addition and multiplication.

Exercise 7.1.2. Let $(G, +)$ be an abelian group. Let a binary operation $\cdot$ on G be defined by $a \cdot b = 0$ for all $a, b \in G$, where 0 is the identity element for $+$. Prove that $(G, +, \cdot)$ is a ring.

Exercise 7.1.3. Find a ring R and a subset $S \subseteq R$ such that S is a subgroup of R, but S is not a subring of R. [Hint: Try $R = \mathbb{R}$, and find a subset $S \subseteq \mathbb{R}$ that is nonempty, closed under addition and negation, but not closed under multiplication.]

Exercise 7.1.4. Let R be a ring, and let $a \in R$. An element $a \in R$ is **idempotent** if $a^2 = a$.

Find all the idempotent elements of $\mathbb{Z}_6 \times \mathbb{Z}_1 2$.

Exercise 7.1.5. Let R be a ring, and let $a \in R$. Let $S_a = \{r \in R \mid ar = 0\}$. Prove that S_a is a subring of R.

Exercise 7.1.6. Prove Theorem 7.1.9.

7.2 Various Types of Rings

Fraleigh, 7th ed. – Section 18
Gallian, 7th ed. – Section 12, 13
Judson, 2016 – Section 16.1, 16.2

Definition 7.2.1. Let $(R, +, \cdot)$ be a ring.

1. The ring R is **commutative** if the binary operation $\cdot$ satisfies the Commutative Law.
2. The ring R is a **ring with unity** if the binary operation $\cdot$ has an identity element (usually denoted 1). △

Lemma 7.2.2. *Let $(R, +, \cdot)$ be a ring with unity. Then $0 = 1$ if and only if $R = \{0\}$.*

Definition 7.2.3. Let $(R, +, \cdot)$ be a ring with unity, and let $a \in R$. Then a is a **unit** if there is some $b \in R$ such that $ab = 1$ and $ba = 1$. △

Lemma 7.2.4. *Let $(R, +, \cdot)$ be a ring with unity.*

1. *The unity is unique.*
2. *Let $a \in R$. If there is some $b \in R$ such that $ab = 1$ and $ba = 1$, then b is unique.*

Definition 7.2.5. Let $(R, +, \cdot)$ be a ring with unity, and let $a \in R$. Suppose a is a unit. The **multiplicative inverse** of a is the element $b \in R$ such that $ab = 1$ and $ba = 1$. The multiplicative inverse of a is denoted a^{-1}. △

Lemma 7.2.6. *Let $(R, +, \cdot)$ be a ring with unity, and let $a, b, c \in R$.*

1. *If $0 \neq 1$, then 0 is not a unit.*
2. *If a is a unit and $ab = ac$, then $b = c$.*
3. *If a is a unit and $ba = ca$, then $b = c$.*
4. *If a is a unit, then a^{-1} is a unit and $(a^{-1})^{-1} = a$.*
5. *If a and b are units, then ab is a unit and $(ab)^{-1} = b^{-1}a^{-1}$.*
6. *Suppose R is commutative. If a or b is not a unit, then ab and ba are not units.*

Definition 7.2.7. Let $(R, +, \cdot)$ be a ring.

1. The ring R is a **division ring** (also called a **skew field**) if it is a ring with unity, if $0 \neq 1$, and if every non-zero element is a unit.

2. The ring R is a **field** if it is a commutative ring with unity, if $0 \neq 1$, if every non-zero element is a unit, and if the binary operation $\cdot$ satisfies the Commutative Law. △

Lemma 7.2.8. *Let $(R, +, \cdot)$ be a ring. If R is a field, it is a division ring.*

Exercises

Exercise 7.2.1. Let R be a ring, and let $\{S_i\}_{i \in I}$ be a family of subrings of R indexed by I. We saw in Lemma 7.1.11 that $\bigcap_{i \in I} S_i$ is a subring of R.

(1) Suppose that S_i is a commutative ring for all $i \in I$. Prove that $\bigcap_{i \in I} S_i$ is a commutative ring.

(2) Suppose that S_i is a ring with unity for all $i \in I$. Suppose further that $\bigcap_{i \in I} S_i$ has at least one element that is a unit in R. Prove that $\bigcap_{i \in I} S_i$ is a ring with unity.

(3) Suppose that S_i is a field for all $i \in I$. Prove that $\bigcap_{i \in I} S_i$ is a field.

Exercise 7.2.2. Let R and S be rings.

(1) Suppose that R and S are commutative rings with unity. Prove that $R \times S$ is a commutative ring with unity.

(2) Suppose that R and S are fields. Prove that $R \times S$ is a field.

Exercise 7.2.3. Let $(R, +, \cdot)$ be a ring with unity. Let U be the set of all the units of R. Prove that $(U, \cdot)$ is a group.

Exercise 7.2.4. Let $(R, +, \cdot)$ be a ring. Prove that $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$ if and only if R is commutative.

Exercise 7.2.5. Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is **idempotent** if $a^2 = a$.

Suppose that R is commutative. Let P be the set of all the idempotent elements of R. Prove that P is closed under multiplication.

Exercise 7.2.6. Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$.

Suppose that R is commutative. Let $c, d \in R$. Prove that if c and d are nilpotent, then $c + d$ is nilpotent.

Exercise 7.2.7. Let $(R, +, \cdot)$ be a ring. The ring R is a **Boolean Ring** if $a^2 = a$ for all $a \in R$ (that is, if every element of R is idempotent). Prove that if R is a Boolean ring, then R is commutative.

Exercise 7.2.8. Let A be a set. Let $\mathcal{P}(A)$ denote the power set of A. Let binary operations $+$ and $\cdot$ on $\mathcal{P}(A)$ be defined by

$$X + Y = (X \cup Y) - (X \cap Y) \quad \text{and} \quad X \cdot Y = X \cap Y$$

for all $X, Y \in \mathcal{P}(A)$. Prove that $(\mathcal{P}(A), +, \cdot)$ is a Boolean ring (as defined in Exercise 7.2.7); make sure to prove first that it is a ring.

7.3 Integral Domains

Fraleigh, 7th ed. – Section 19
Gallian, 7th ed. – Section 13
Judson, 2016 – Section 16.2

Definition 7.3.1. Let $(R, +, \cdot)$ be a ring, and let $a \in R$. The element a is a **zero divisor** if $a \neq 0$ and if there is some $b \in R$ such that $b \neq 0$ and $ab = 0$. △

Lemma 7.3.2. *Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}_n$. Then a is a zero divisor if and only if $a \neq 0$ and $(a, n) \neq 1$.*

Corollary 7.3.3. *Let $p \in \mathbb{N}$. If p is a prime number, then $\mathbb{Z}_p$ has no zero divisors.*

Lemma 7.3.4. *Let $(R, +, \cdot)$ be a ring. The following are equivalent.*

a. *The ring R has no zero divisors.*

b. *$ab = 0$ implies $a = 0$ or $b = 0$, for all $a, b \in R$.*

c. *$a \neq 0$ and $ab = ac$ imply $b = c$, for all $a, b, c \in R$.*

d. *$a \neq 0$ and $ba = ca$ imply $b = c$, for all $a, b, c \in R$.*

Definition 7.3.5. Let $(R, +, \cdot)$ be a ring. The ring R is an **integral domain** if it is a commutative ring with unity, if it has no zero divisors, and if $0 \neq 1$. △

Lemma 7.3.6. *Let $(R, +, \cdot)$ be a ring. If R is a division ring (and in particular if R is a field), then it is an integral domain.*

Lemma 7.3.7. *Let $n \in \mathbb{N}$. Then $\mathbb{Z}_n$ is an integral domain if and only if n is a prime number.*

Theorem 7.3.8. *Let $(R, +, \cdot)$ be a ring. If R is finite and an integral domain, then it is a field.*

Corollary 7.3.9. *Let $n \in \mathbb{N}$. Then $\mathbb{Z}_n$ is a field if and only if n is a prime number.*

Lemma 7.3.10. *Let $(R, +, \cdot)$ be a ring with unity. Suppose R is finite. Let*

$$G = \{a \in R \mid a \text{ is not a zero divisor}\}.$$

Then G is a group under multiplication.

Definition 7.3.11. Let $(R, +, \cdot)$ be a ring. The **characteristic** of R is a number in $\mathbb{N} \cup \{0\}$ that is defined as follows. If there exists some $n \in \mathbb{N}$ such that $n \cdot a = 0$ for all $a \in R$, then the **characteristic** of R is the least such n; if there is no such n, then **characteristic** of R is 0. △

Lemma 7.3.12. *Let $(R, +, \cdot)$ be a ring with unity.*

1. *Suppose that $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$. Then the characteristic of R is 0.*
2. *Suppose that $n \cdot 1 = 0$ for some $n \in \mathbb{N}$. Then the characteristic of R is the smallest $m \in \mathbb{N}$ such that $m \cdot 1 = 0$.*

Exercises

Exercise 7.3.1. Let $R = \mathsf{M}_{2\times 2}(\mathbb{Z})$, and let $A = \left[\begin{smallmatrix} 1 & 2 \\ 2 & 4 \end{smallmatrix}\right]$. Show that A is a zero divisor in R.

Exercise 7.3.2. Let R be a ring. Suppose that R has at least two elements. Suppose that for each $a \in R$, there is a unique $b \in R$ such that $aba = a$.

(1) Prove that R has no zero divisors.

(2) Let $a \in R$, and let $b \in R$ be the unique element of R such that $aba = a$. Prove that $bab = b$.

(3) Prove that R is a ring with unity.

(4) Prove that R is a division ring.

Exercise 7.3.3. Let D be an integral domain. Let $S = \{n \cdot 1 \mid z \in \mathbb{Z}\}$.

(1) Prove that $S \leq D$.

(2) Prove that if $T \leq D$, then $S \subseteq T$.

Exercise 7.3.4. Prove Lemma 7.3.10

7.4 More on $\mathbb{Z}_n$

Fraleigh, 7th ed. – Section 20

Lemma 7.4.1. *Let $(F, +, \cdot)$ be a field. Let F^* be the set of all non-zero elements of F. Then $(F^*, \cdot)$ is a group.*

Theorem 7.4.2 (Fermat's Little Theorem)**.** *Let $p \in \mathbb{N}$ be a prime number. Let $a \in \mathbb{Z}$. Suppose $a \not\equiv 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Corollary 7.4.3. *Let $p \in \mathbb{N}$ be a prime number. Let $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.*

Corollary 7.4.4. *Let $a \in \mathbb{Z}$. Then $a^{33} - a$ is divisible by* 15.

Definition 7.4.5. The **Euler phi-function** is the function $\varphi : \mathbb{N} \to \mathbb{N}$ defined as follows. Let $n \in \mathbb{N}$. Then let $\varphi(n)$ be the cardinality of the set $\{x \in \mathbb{N} \mid x < n \text{ and } (x, n) = 1\}$. △

Theorem 7.4.6 (Euler's Theorem)**.** *Let $n \in \mathbb{N}$. Let $a \in \mathbb{Z}$. Suppose $(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Exercises

Exercise 7.4.1. Use Fermat's Little Theorem to find the remainder of 3^{47} when it is divided by 23.

Exercise 7.4.2. Use Fermat's Little Theorem to find the remainder of 37^{49} when it is divided by 7.

Exercise 7.4.3. Let $p \in \mathbb{N}$ be a prime number. Find $\varphi(p^2)$.

Exercise 7.4.4. Let $p, q \in \mathbb{N}$ be prime numbers. Find $\varphi(pq)$.

7.5 Ring Homomorphisms

Fraleigh, 7th ed. – Section 26
Gallian, 7th ed. – Section 15
Judson, 2016 – Section 16.3

Definition 7.5.1. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings, and let $f : R \to S$ be a function.

1. The function f is a **ring homomorphism** (sometimes called a **homomorphism**) if $f(a+b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$.
2. The function f is a **ring isomorphism** (sometimes called an **isomorphism**) if it is a ring homomorphism and bijective.
3. The rings $(R, +, \cdot)$ and $(S, +, \cdot)$ are **isomorphic** if there is a ring isomorphism $R \to S$. △

Theorem 7.5.2. *Let R and S be rings, and let $f : R \to S$ be a ring homomorphism.*

1. *$f(0) = 0$.*
2. *If $a \in R$, then $f(-a) = -f(a)$.*
3. *If $A \leq R$, then $f(A) \leq S$.*
4. *If $B \leq S$, then $f^{-1}(B) \leq R$.*
5. *If R is a ring with unity, where the unity is denoted 1, then $f(R)$ is a ring with unity, where the unity is $f(1)$.*

Theorem 7.5.3. *Let R, S and T be rings, and let $f : R \to S$ and $j : S \to T$ be ring homomorphisms. Then $j \circ f$ is a ring homomorphism.*

Theorem 7.5.4. *Let R, S and T be rings, and let $f : R \to S$ and $j : S \to T$ be ring isomorphisms.*

1. *The identity map $1_R : R \to R$ is a ring isomorphism.*
2. *The function f^{-1} is a ring isomorphism.*
3. *The function $j \circ f$ is a ring isomorphism.*

Lemma 7.5.5. *Let R and S be rings. Suppose that R and S are isomorphic.*

1. *The ring R is commutative if and only if the ring S is commutative.*
2. *The ring R is a ring with unity if and only if the ring S is a ring with unity.*
3. *The ring R is an integral domain if and only if the ring S is an integral domain.*

Theorem 7.5.6. *Let $m, n \in \mathbb{N}$. The ring $\mathbb{Z}_m \times \mathbb{Z}_n$ is ring isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime.*

Definition 7.5.7. Let R and S be rings, and let $f : R \to S$ be a ring homomorphism.

1. The **kernel** of f, denoted $\ker f$, is the set $\ker f = f^{-1}(\{0\})$.
2. The **image** of f, denoted $\operatorname{im} f$, is the set $\operatorname{im} f = f(R)$. △

Remark 7.5.8. Observe that

$$\ker f = \{r \in R \mid f(r) = 0\}$$

and

$$\operatorname{im} f = \{s \in S \mid s = f(r) \text{ for some } r \in R\}. \qquad \Diamond$$

Lemma 7.5.9. *Let R and S be rings, and let $f : R \to S$ be a ring homomorphism.*

1. $\ker f \leq R$.
2. $\operatorname{im} f \leq S$.

Theorem 7.5.10. *Let R and S be rings, and let $f : R \to S$ be a ring homomorphism. The function f is injective if and only if* $\ker f = \{0\}$.

Lemma 7.5.11. *Let R and S be rings, and let $f : R \to S$ be a ring homomorphism. Let $s \in S$. If $r \in f^{-1}(\{s\})$, then $f^{-1}(\{s\}) = r + \ker f$.*

Exercises

Exercise 7.5.1. Prove Lemma 7.5.5 (1) and (3).

Exercise 7.5.2. Let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, and let $S = \{\left[\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right] \in \mathsf{M}_{2\times 2}(\mathbb{Z}) \mid a, b \in \mathbb{Z}\}$.

(1) Prove that R is a subring of $\mathbb{R}$.

(2) Prove that S is a subring of $\mathsf{M}_{2\times 2}(\mathbb{Z})$.

Prove that R and S are isomorphic.

Exercise 7.5.3. Let $T = \{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid a, b \in \mathbb{R}\}$

(1) Prove that T is a subring of $\mathsf{M}_{2\times 2}(\mathbb{R})$.

(2) Let $\phi : \mathbb{C} \to T$ be defined by $\phi(a + bi) = \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]$ for all $a + bi \in \mathbb{C}$. Prove that ϕ is a ring isomorphism.

Exercise 7.5.4. Let R and S be ring, and let $f : R \to S$ be a ring homomorphism. Suppose that R is a ring with unity, that $S \neq \{0\}$ and that f is surjective. Let $u \in R$ be a unit. Prove that $f(u)$ is a unit of S.

7.6 Ideals and Quotient Rings

Fraleigh, 7th ed. – Section 26
Gallian, 7th ed. – Section 14
Judson, 2016 – Section 16.3

Definition 7.6.1. Let R be a ring, and let $S \leq R$. The subring S is an **ideal** if $rS \subseteq S$ and $Sr \subseteq S$ for all $r \in R$. △

Theorem 7.6.2. *Let R be a ring, and let $S \subseteq R$. Then S is an ideal if and only if the following three conditions hold.*

(i) *$S \neq \emptyset$.*

(ii) *If $a, b \in S$, then $a + (-b) \in S$.*

(iii) *If $a \in S$ and $r \in R$, then $ar \in S$ and $ra \in S$.*

Definition 7.6.3. Let R be a ring, and let S be an ideal of R. The ideal S is the **trivial ideal** if $S = \{0\}$; the ideal S is the **improper ideal** if $S = R$; the ideal S is a **proper nontrivial ideal** if $\{0\} \subsetneqq S \subsetneqq R$. △

Lemma 7.6.4. *Let R be a ring with unity, and let S be an ideal of R. If S contains a unit, then $S = R$.*

Corollary 7.6.5. *Let F be a field. The only ideals of F are $\{0\}$ and F.*

Theorem 7.6.6. *Let R and S be rings, and let $f : R \to S$ be a ring homomorphism.*

1. *If A is an ideal of R, then $f(A)$ is an ideal of $f(R)$.*

2. *If B is an ideal of $f(R)$ or of S, then $f^{-1}(B)$ is an ideal of R.*

Lemma 7.6.7. *Let R and S be rings, and let $f : R \to S$ be a homomorphism. Then* $\ker f$ *is an ideal of R.*

Lemma 7.6.8. *Let R be a group and let S be a subring of R. The formulas $(a + S) + (b + S) = (a + b) + S$ and $(a + S)(b + S) = ab + S$ for all $a, b \in R$ give well-defined binary operations on the set of all additive cosets of R with respect to S if and only if S is an ideal of R.*

Lemma 7.6.9. *Let R be a ring and let S be an ideal of R. The set of additive cosets R/S with binary operations given by $(a + S) + (b + S) = (a + b) + S$ and $(a + S)(b + S) = ab + S$ for all $a, b \in R$ for all $a, b \in R$ is a ring.*

Definition 7.6.10. Let R be a group and let S be an ideal of R. The set of additive cosets R/S with binary operations given by $(a + S) + (b + S) = (a + b) + S$ and $(a + S)(b + S) = ab + S$ for all $a, b \in R$ is the **quotient ring** (also called **factor ring**) of R by S. △

Lemma 7.6.11. *Let R be a ring and let S be an ideal of R.*

1. *If R is commutative, then R/S is commutative.*
2. *If R is a ring with unity, then R/S is a ring with unity.*

Definition 7.6.12. Let R be a ring and let S be an ideal of R. The **canonical map** for R and S is the function $\gamma : R \to R/S$ defined by $\gamma(r) = rS$ for all $r \in R$. △

Lemma 7.6.13. *Let R be a ring and let S be an ideal of R. The canonical map $\gamma : R \to R/S$ is a surjective ring homomorphism, and* $\ker \gamma = S$.

Theorem 7.6.14 (First Isomorphism Theorem). *Let R and S be rings, and let $f : R \to S$ be a homomorphism. Then there is a a unique isomorphism $g : R/\ker f \to \operatorname{im} f$ such that $f = g \circ \gamma$, where $\gamma : R \to R/\ker f$ is the canonical map.*

Exercises

Exercise 7.6.1. Find all the ideals of $\mathbb{Z}_{12}$.

Exercise 7.6.2. Let R be a group, and let $\{S_i\}_{i \in I}$ be a family of ideals of R indexed by I. Prove that $\bigcap_{i \in I} S_i$ is an ideal of R.

Exercise 7.6.3. Let R be a commutative ring, and let $a \in R$. Let $S_a = \{r \in R \mid ar = 0\}$. Prove that S_a is an ideal of R.

Exercise 7.6.4. Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$.

Suppose that R is commutative. Let $N = \{c \in R \mid c \text{ is nilpotent}\}$. Prove that N is an ideal of R.

Exercise 7.6.5. Prove Theorem 7.6.6.

Exercise 7.6.6. Find an example of rings R and S, a ring homomorphism $f : R \to S$, and an ideal N of R, such that $f(N)$ is not an ideal of S.

Exercise 7.6.7. All parts of this exercise are about the quotient ring $2\mathbb{Z}/8\mathbb{Z}$.

(1) List the elements of $2\mathbb{Z}/8\mathbb{Z}$.

(2) Make an addition table and a multiplication table for $2\mathbb{Z}/8\mathbb{Z}$.

(3) Are $2\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}_4$ ring isomorphic?

7.7 Polynomials

Fraleigh, 7th ed. – Section 22
Gallian, 7th ed. – Section 16
Judson, 2016 – Section 17.1

Definition 7.7.1. Let R be a ring. The **set of polynomials over** R, denoted $R[x]$, is the set

$$R[x] = \{ f : \mathbb{N} \cup \{0\} \to R \mid \text{ there is some } N \in \mathbb{N} \cup \{0\} \text{ such that } f(i) = 0 \text{ for all } i \in \mathbb{N} \cup \{0\} \text{ such that } i > N \}. \quad \triangle$$

Definition 7.7.2. Let R be a ring.

1. Let $\mathbf{0} : \mathbb{N} \cup \{0\} \to R$ be defined by $\mathbf{0}(i) = 0$ for all $i \in \mathbb{N} \cup \{0\}$.
2. Suppose that R has a unity. Let $\mathbf{1} : \mathbb{N} \cup \{0\} \to R$ be defined by $\mathbf{1}(0) = 1$ and $\mathbf{1}(i) = 0$ for all $i \in \mathbb{N}$. $\triangle$

Definition 7.7.3. Let R be a ring, and let $f \in R[x]$. Suppose that $f \neq \mathbf{0}$. The **degree** of f, denoted $\deg f$, is the smallest $N \in \mathbb{N} \cup \{0\}$ such that $f(i) = 0$ for all $i \in \mathbb{N} \cup \{0\}$ such that $i > N$. $\triangle$

Definition 7.7.4. Let R be a ring, and let $f, g \in R[x]$. Let $f + g, fg, -f : \mathbb{N} \cup \{0\} \to R$ be defined by $(f + g)(i) = f(i) + g(i)$, and $(fg)(i) = \sum_{k=0}^{i} f(k)g(i-k)$, and $(-f)(i) = -f(i)$ for all $i \in \mathbb{N} \cup \{0\}$. $\triangle$

Lemma 7.7.5. *Let R be a ring, and let $f, g \in R[x]$. Suppose $f \neq \mathbf{0}$ and $g \neq \mathbf{0}$.*

1. *$-f \in R[x]$. If $f \neq \mathbf{0}$, then $\deg(-f) = \deg f$.*
2. *$f + g \in R[x]$. If $f \neq \mathbf{0}$, and $g \neq \mathbf{0}$ and $f + g \neq \mathbf{0}$, then $\deg(f + g) \leq \max\{\deg f, \deg g\}$.*
3. *$fg \in R[x]$. If $f \neq \mathbf{0}$, and $g \neq \mathbf{0}$ and $fg \neq \mathbf{0}$, then $\deg(fg) \leq \deg f + \deg g$; if R is an integral domain, and if $f \neq \mathbf{0}$ and $g \neq \mathbf{0}$, then $\deg(fg) = \deg f + \deg g$.*

Lemma 7.7.6. *Let R be a ring.*

1. *$(R[x], +, \cdot)$ is a ring.*
2. *If R is commutative, then $R[x]$ is commutative.*

3. *If R has a unity, then $R[x]$ has a unity.*

4. *If R is an integral domain, then $R[x]$ is an integral domain.*

Remark 7.7.7.

1. Let R be an integral domain. Then the formula $\deg(fg) = \deg f + \deg g$ tell us that polynomials of degree greater than 0 cannot have multiplicative inverses. Hence, the units in $R[x]$ are precisely the polynomials of degree zero, meaning the constant polynomials other than the zero polynomial.

2. Even if F is a field, then the units in $F[x]$ are still the constant polynomials other than the zero polynomial, and hence $F[x]$ is not a field (though it is still an integral domain).

$\Diamond$

Definition 7.7.8. Let R be a ring, let $f \in R[x]$ and let $r \in R$. Let $rf : \mathbb{N} \cup \{0\} \to R$ be defined by $(rf)(i) = rf(i)$ for all $i \in \mathbb{N} \cup \{0\}$. $\triangle$

Lemma 7.7.9. *Let R be a ring, let $f \in R[x]$ and let $r \in R$. Then $rf \in R[x]$.*

Definition 7.7.10. Let R be a ring, and let $n \in \mathbb{N} \cup \{0\}$. Let

$$R_n[x] = \{f \in R[x] \mid \deg f \leq n\}. \qquad \triangle$$

Lemma 7.7.11. *Let R be a ring, and let $n \in \mathbb{N} \cup \{0\}$.*

1. *The set $(R_n[x], +)$ is a subgroup of $(R[x], +)$.*

2. *The set $(R_0[x], +, \cdot)$ is a subring of $(R[x], +, \cdot)$.*

Lemma 7.7.12. *Let R be a ring. Then there is a ring isomorphism $\psi : R \to R_0[x]$.*

Definition 7.7.13. Let R be an integral domain. Let $x : \mathbb{N} \cup \{0\} \to R$ be defined by $x(1) = 1$ and $x(i) = 0$ for all $i \in \mathbb{N} \cup \{0\} - \{1\}$. $\triangle$

Lemma 7.7.14. *Let R be an integral domain, and let $n \in \mathbb{N}$. Then $x^n(n) = 1$ and $x(i) = 0$ for all $i \in \mathbb{N} \cup \{0\} - \{n\}$, for all $n \in \mathbb{N}$.*

Definition 7.7.15. Let R be an integral domain. Let x^0 be defined by $x^0 = \mathbf{1}$. $\triangle$

Lemma 7.7.16. *Let R be a commutative ring with unity, let $f \in R[x]$, and let $n \in \mathbb{N} \cup \{0\}$. If $f \neq \mathbf{0}$, suppose that $n \geq \deg f$. Then there are unique $a_0, a_1, \ldots, a_n \in R$ such that $f = a_0\mathbf{1} + a_1 x + \cdots + a_n x^n$.*

Definition 7.7.17. Let R be a commutative ring with unity, let $S \subseteq R$ be a commutative subring with unity, and let $\alpha \in R$. The **evaluation map** with respect to α is the function $\Phi_\alpha : S[x] \to R$ defined by $\Phi_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ for all $a_0 + a_1x + \cdots + a_nx^n \in S[x]$. △

Lemma 7.7.18. *Let R be a commutative ring with unity, let $S \subseteq R$ be a commutative subring with unity, and let $\alpha \in R$.*

1. *The evaluation map $\Phi_\alpha : S[x] \to R$ is a ring homomorphism.*
2. *$\Phi_\alpha(x) = \alpha$.*
3. *The function $\Phi_\alpha|_S$ is the inclusion map $S \to R$.*

Definition 7.7.19. Let R be a commutative ring with unity, let $S \subseteq R$ be a commutative subring with identity, and let $f \in S[x]$. The **polynomial function induced** by f is the function $\hat{f} : R \to R$ defined by $\hat{f}(\alpha) = \Phi_\alpha(f)$ for all $\alpha \in R$. △

Definition 7.7.20. Let R be a commutative ring with unity, let $S \subseteq R$ be a commutative subring with identity, and let $f \in S[x]$. A **zero** of f is any $\alpha \in R$ such that $\hat{f}(\alpha) = 0$. △

Exercises

Exercise 7.7.1. List all the polynomials in $\mathbb{Z}_3[x]$ that have degree less than or equal to 2.

Exercise 7.7.2. Let $f \in \mathbb{Z}_6[x]$ be $f = x^2 + [3]x + [2]$. Find all the zeros of f.

Exercise 7.7.3. Let $g \in \mathbb{Z}_4[x]$ be $g = [2]x + [1]$. Show that g is a unit in $\mathbb{Z}_4$.

Exercise 7.7.4. Find the units in each of the following rings.

(1) $\mathbb{Z}[x]$.

(2) $\mathbb{Z}_5[x]$.

Exercise 7.7.5. Let D be an integral domain. Describe the units in $D[x]$.

Exercise 7.7.6. Let F be a field. A function $\phi \in \mathcal{F}(F, F)$ is a **polynomial function** if there is some $f \in F[x]$ such that $\phi(a) = f(a)$ for all $a \in F$. Let $\mathcal{F}_P = \{g \in \mathcal{F}(F, F) \mid g \text{ is a polynomial function}\}$.

(1) Prove that $\mathcal{F}_P$ is a subring of $\mathcal{F}(F, F)$.

(2) Find an example of a field F such that $\mathcal{F}_P$ is not isomorphic to $F[x]$. [Hint: look at finite fields, and find an example where $\mathcal{F}_P$ and $F[x]$ do not have the same cardinality.

8

Unique Factorization Domains, Principal Ideal Domains and Euclidean Domains

8.1 Unique Factorization Domains

Fraleigh, 7th ed. – Section 45
Gallian, 7th ed. – Section 18
Judson, 2016 – Section 18.2

Definition 8.1.1. Let D be an integral domain, and let $a, b \in D$. The element a **divides** the element b, written $a|b$, if there is some $q \in D$ such that $aq = b$. If a divides b, we also say that b is **divisible** by a. △

Remark 8.1.2. Let D be an integral domain, and let $a \in D$. Then a is a unit if and only if $a|1$. ◊

Definition 8.1.3. Let D be an integral domain, and let $a, b \in D$. The elements a and b are **associates** if there is some unit $u \in D$ such that $au = b$. △

Remark 8.1.4. Let D be an integral domain, and let $a, b \in D$. Suppose a and b are associates.

1. Observe in Definition 8.1.3 that if $au = b$, then $a = bu^{-1}$, and so it doesn't matter which of a and b is the one multiplied by the unit.

   Because integral domains are commutative, we can write $au = b$ or $ua = b$, whichever is more convenient.

◊

Lemma 8.1.5. *Let D be an integral domain, and let $a, b \in D$. Suppose $a \neq 0$ and $b \neq 0$. Then $a|b$ and $b|a$ if and only if a and b are associates.*

Definition 8.1.6. Let $p \in \mathbb{N}$. Suppose $p > 1$.

1. The number p is a **prime number** if the only positive integers that divide p are 1 and p.

2. The number p is a **composite number** if it is not a prime number. △

Definition 8.1.7. Let D be an integral domain, and let $p \in D$. Suppose that p is not a unit. The element p is **irreducible** if $p = ab$ for some $a, b \in D$ implies that a or b is a unit. △

Lemma 8.1.8. *Let D be an integral domain, and let $p \in D$. If p is irreducible, then any associate of p is irreducible.*

Definition 8.1.9. Let D be an integral domain, and let $p \in D$. Suppose that p is not a unit. The element p is **prime** if $p|(ab)$ for some $a, b \in D$ implies that $p|a$ or $p|b$. △

Lemma 8.1.10. *Let D be an integral domain, and let $p \in D$. If p is prime, then p is irreducible.*

Definition 8.1.11. Let $d \in \mathbb{Z}$. Suppose that $d \neq 1$, and that d is not divisible by p^2 for any prime $p \in \mathbb{Z}$. The set $\mathbb{Z}[d]$ is defined by

$$\mathbb{Z}[d] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$ △

Definition 8.1.12. Let $d \in \mathbb{Z}$. Suppose that $d \neq 1$, and that d is not divisible by p^2 for any prime $p \in \mathbb{Z}$. The **norm** of $\mathbb{Z}[d]$ is the function $N : \mathbb{Z}[d] \to \mathbb{N} \cup \{0\}$ defined by

$$N(a + b\sqrt{d}) = |a^2 - b^2 d|$$

for all $a + b\sqrt{d} \in \mathbb{Z}[d]$. △

Lemma 8.1.13. *Let $d \in \mathbb{Z}$. Suppose that $d \neq 1$, and that d is not divisible by p^2 for any prime $p \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}[d]$.*

1. *$N(x) = 0$ if and only if $x = 0$.*
2. *$N(xy) = N(x)N(y)$.*
3. *$N(x) = 1$ if and only if x is a unit.*
4. *If $N(x)$ is prime in $\mathbb{Z}$, then x is irreducible in $\mathbb{Z}[d]$.*

Lemma 8.1.14. *Let $d \in \mathbb{Z}$. Suppose that $d \neq 1$, and that d is not divisible by p^2 for any prime $p \in \mathbb{Z}$. Then $\mathbb{Z}[d]$ is an integral domain.*

Definition 8.1.15. Let D be an integral domain. The integral domain D is a **unique factorization domain** (abbreviated **UFD**) if the following holds. Let $a \in D$. Suppose a is not 0 and is not a unit. Then a can be uniquely factored into irreducible, as follows.

1. The element a can be written as the product of finitely many irreducibles of D.
2. If $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where $p_1, p_2, \ldots p_r, q_1, q_2, \ldots q_s$ are irreducibles, then $r = s$, and the order of $q_1, q_2, \ldots q_s$ can be rewritten so that q_i is an associate of p_i for all $i \in \{1, 2, \ldots, r\}$. △

Exercises

Exercise 8.1.1. Prove Lemma 8.1.13 (1), (2) and (4). The proof of each part can use any of the previous parts of the lemma.

Exercise 8.1.2. All parts of this exercise are about $\mathbb{Z}[-1]$.

(1) Show that $1 - i$ is irreducible.

(2) Show that 3 is irreducible.

(3) Show that 2 is not irreducible.

Exercise 8.1.3. In $\mathbb{Z}[-5]$, find two different ways to factor 21 into a product of irreducibles. You must show that the irreducibles you use are actually irreducible.

Exercise 8.1.4. Let $a + bi \in \mathbb{Z}[-1]$, Suppose that $a^2 + b^2$ is a prime number. Prove that $a + bi$ is irreducible.

8.2 Principal Ideal Domains

Fraleigh, 7th ed. – Section 45
Gallian, 7th ed. – Section 16
Judson, 2016 – Section 18.2

Lemma 8.2.1. *Let R be a commutative ring with unity, and let $a \in R$.*

1. *The set $\{ar \mid r \in R\}$ is an ideal of R.*

2. *The set $\{ar \mid r \in R\}$ contains a.*

Definition 8.2.2. Let R be a commutative ring with unity.

1. Let $a \in R$. The **principal ideal generated by** a, denoted $\langle a \rangle$, is the ideal

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

2. Let S be an ideal of R. The ideal S is a **principal ideal** if $S = \langle c \rangle$ for some $c \in R$. △

Lemma 8.2.3. *Let D be an integral domain, and let $a, b \in D$.*

1. *Prove that $\langle a \rangle \subseteq \langle b \rangle$ if and only if $b|a$.*

2. *Prove that $\langle a \rangle = \langle b \rangle$ if and only if a and b are associates.*

Lemma 8.2.4. *Let S be an ideal of $\mathbb{Z}$. Then there is some $m \in \mathbb{Z}$ such that $S = m\mathbb{Z} = \langle m \rangle$.*

Definition 8.2.5. Let D be an integral domain. The integral domain D is a **principal ideal domain** (abbreviated **PID**) if every ideal in D is a principal ideal. △

Lemma 8.2.6. *Let D be a PID, and let $p \in D$. Then p is prime if and only if p is irreducible.*

Corollary 8.2.7. *Let D be a PID, and let $p, a_1, \ldots, a_n \in D$, for some $n \in \mathbb{N}$. Suppose p is irreducible. If $p|(a_1 a_2 \cdots a_n)$ then there is some $i \in \{1, 2, \ldots, n\}$ such that $p|a_i$.*

Lemma 8.2.8. *Let R be a commutative ring, and let $S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$ of R be an ascending chain of ideals. Then $\bigcup_{i=1}^{\infty} S_i$ is an ideal of R.*

Definition 8.2.9. Let R be a ring. The ring R is satisfies the **ascending chain condition** (abbreviated **ACC**) if every ascending chain of ideals $S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$ of R, there is some $p \in \mathbb{N}$ such that $t \in \mathbb{N}$ and $t \geq p$ imply $S_t = S_p$. △

Lemma 8.2.10. *Let D be a PID. Then D satisfies ACC.*

Theorem 8.2.11. *Let D be a PID, and let $d \in D$. Suppose that $d \neq 0$ and that d is not a unit. Then there are $a_1, \ldots, a_n \in D$ such that $a_1, \ldots, a_n$ are irreducible and $d = a_1 a_2 \cdots a_n$.*

Theorem 8.2.12. *Let D be a PID. Then D is a UFD.*

Corollary 8.2.13 (Fundamental Theorem of Arithmetic)**.** *The ring $\mathbb{Z}$ is a UFD.*

Exercises

Exercise 8.2.1. Prove Lemma 8.2.1.

Exercise 8.2.2. Prove Lemma 8.2.3.

8.3 Euclidean Domains

Fraleigh, 7th ed. – Section 46
Gallian, 7th ed. – Section 18
Judson, 2016 – Section 18.2

Definition 8.3.1. Let R be a ring. The set R^* is defined to be $R^* = R - \{0\}$. △

Definition 8.3.2. Let D be an integral domain. A **Euclidean norm** (also called **Euclidean valuation**) on D is a function $\nu : D^* \to \mathbb{N} \cup \{0\}$ that satisfies the following two conditions. Let $a, b \in D$.

1. Suppose $b \neq 0$. Then there are $q, r \in D$ such that $a = bq + r$ and that $r = 0$ or $\nu(r) < \nu(b)$.
2. Suppose $a \neq 0$ and $b \neq 0$. Then $\nu(a) \leq \nu(ab)$. △

Definition 8.3.3. Let D be an integral domain. The integral domain D is a **Euclidean domain** (abbreviated **ED**) if D has a Euclidean norm. △

Corollary 8.3.4. *Let D be a ED. Then D is a PID.*

Corollary 8.3.5. *Let D be a ED. Then D is a UFD.*

Exercises

Exercise 8.3.1. Let $\mu : \mathbb{Z}^* \to \mathbb{N} \cup \{0\}$ defined by $\mu(a) = a^2$ for all $a \in \mathbb{Z}^*$. Prove that μ is a Euclidean norm.

Exercise 8.3.2. Let $\delta : \mathbb{Q}^* \to \mathbb{N} \cup \{0\}$ defined by $\delta(a) = 17$ for all $a \in \mathbb{Q}^*$. Prove that δ is a Euclidean norm.

Exercise 8.3.3. Let D be a ED with Euclidean norm ν, and let $a, b \in D$. Suppose that a and b are associates. Prove that $\nu(a) = \nu(b)$.

Exercise 8.3.4. Let F be a field. Prove that F is a ED.

Exercise 8.3.5. Let D be a ED with Euclidean norm ν, and let $e \in \mathbb{Z}$. Suppose that $\nu(1) + e > 0$. Let $\mu : D^* \to \mathbb{N} \cup \{0\}$ be defined by $\mu(a) = \nu(a) + e$ for all $a \in D^*$. Prove that μ is a Euclidean norm on D.

9

Applications of Rings to Polynomials

9.2 Factorization of Polynomials over a Field

Fraleigh, 7th ed. – Section 23
Gallian, 7th ed. – Section 18
Judson, 2016 – Section 18.2

Theorem 9.2.1. *Let F be a field. Then then the function $\nu : F[x]^* \to \mathbb{N} \cup \{0\}$ defined by $\nu(f) = \deg f$ for all $f \in F[x]^*$ is a Euclidean norm.*

Corollary 9.2.2. *Let F be a field. Then $F[x]$ is a PID.*

Corollary 9.2.3. *Let F be a field. Then $F[x]$ is a UFD.*

Theorem 9.2.4. *Let F be a field, let $f \in F[x]$ and let $r \in F$. Then r is a zero of f if and only if $x - r$ is a factor of f.*

Corollary 9.2.5. *Let F be a field, let $f \in F[x]$. Suppose $f \neq 0$. Let $n = \deg f$. Then f has at most n zeros.*

Exercises

Exercise 9.2.1. Let $a, b \in \mathbb{Z}_7[x]$ be $a = x^6 + [3]x^5 + [4]x^2 - [3]x + [2]$ and $b = x^2 + [2]x - [3]$. Find $q, r \in \mathbb{Z}_7[x]$ such that $a = bq + r$, and $r = 0$ or $\deg r < \deg b$.

Exercise 9.2.2. Let $f \in \mathbb{Z}_{11}[x]$ be $f = [2]x^3 + [3]x^2 - [7]x - [5]$. Factor f into irreducibles.

9.3 Prime Ideals and Maximal Ideals

Fraleigh, 7th ed. – Section 27
Gallian, 7th ed. – Section 14
Judson, 2016 – Section 16.4

Definition 9.3.1. Let R be a ring, and let M be an ideal of R. The ideal M is a **maximal ideal** if $M \subsetneqq R$, and if there is no ideal S of R such that $M \subsetneqq S \subsetneqq R$. △

Theorem 9.3.2. *Let R be a commutative ring with unity, let S be an ideal of R. Then R/S is a field if and only if S is a maximal ideal.*

Corollary 9.3.3. *Let R be a commutative ring with unity. Then R is a field if and only if the only ideals of R are $\{0\}$ and R.*

Lemma 9.3.4. *Let D be a PID, and let $n \in D$. Then $\langle n \rangle$ is a maximal ideal if and only if n is irreducible.*

Definition 9.3.5. Let R be a ring, and let P be an ideal of R. The ideal P is a **prime ideal** if $P \subsetneqq R$, and if $ab \in P$ implies $a \in P$ or $b \in P$ for all $a, b \in R$. △

Theorem 9.3.6. *Let R be a commutative ring with unity, let S be an ideal of R. Then R/S is an integral domain if and only if S is a prime ideal.*

Corollary 9.3.7. *Let R be a commutative ring with unity, and let S be an ideal of R. If S is a maximal ideal, then S is a prime ideal.*

Corollary 9.3.8. *Let R be a commutative ring with unity, and let S be an ideal of R. Suppose R is finite. Then S is a maximal ideal if and only if S is a prime ideal.*

Lemma 9.3.9. *Let R be a ring with unity, and let $\phi : \mathbb{Z} \to R$ be defined by $\phi(m) = m \cdot 1$ for all $m \in \mathbb{Z}$. Then ϕ is a ring homomorphism.*

Corollary 9.3.10. *Let R be a ring with unity.*

1. *If R has positive characteristic n, then R contains a subring isomorphic to $\mathbb{Z}_n$.*
2. *If R has characteristic 0, then R contains a subring isomorphic to $\mathbb{Z}$.*

Corollary 9.3.11. *Let F be a field.*

1. *If F has positive characteristic, then the characteristic is a prime number p, and F contains a subfield isomorphic to $\mathbb{Z}_n$.*

2. *If F has characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$.*

Exercises

Exercise 9.3.1. Find all the maximal ideals and all the prime ideals of $\mathbb{Z}_6$.

Exercise 9.3.2. Prove Corollary 9.3.8.

Exercise 9.3.3. Let F be a field. Let S be an ideal of $F[x]$. Prove that if S is non-trivial and a prime ideal, then S is a maximal ideal.

Exercise 9.3.4. Let $R = \mathcal{F}(\mathbb{R}, \mathbb{R})$. Then R is a ring. Let $S = \{f \in R \mid f(2) = 0\}$. Prove that S is a maximal ideal of R.

Exercise 9.3.5. Let $S = 2\mathbb{Z}$. Observe that S is a maximal ideal of $\mathbb{Z}$. Prove that $S[x]$ is not a maximal ideal of $\mathbb{Z}[x]$.

Exercise 9.3.6. Let R be a commutative ring with unity, and let S be an ideal of R. Suppose that $a^2 = a$ for all $a \in R$. Suppose that S is a prime ideal. Prove that R/S has two elements.

Exercise 9.3.7. Let R be a commutative ring with unity, and let S be an ideal of R. Suppose that $S \neq R$. Suppose that if $a \in R - S$, then a is a unit. Prove that S is the unique maximal ideal of R.

9.4 Extension Fields

Fraleigh, 7th ed. – Section 29
Gallian, 7th ed. – Section 20
Judson, 2016 – Section 21.1

Definition 9.4.1. Let F be a field. An **extension field** of F is any field E such that $F \subseteq E$. △

Theorem 9.4.2. *Let F be a field, let $f \in F[x]$. Suppose* $\deg f \geq 1$. *Then there is an extension field E of F such that f has a zero in E.*

Definition 9.4.3. Let F be a field, let E be an extension field of F, and let $\alpha \in E$. The **extension field obtained by adjoining α to F**, denoted $F(\alpha)$, is defined by

$$F(\alpha) = \{S \subseteq E \mid S \text{ is a subfield of } E \text{ and } F \subseteq S \text{ and } \alpha \in S\}. \qquad \triangle$$

Lemma 9.4.4. *Let F be a field, let E be an extension field of F, and let $\alpha \in E$.*

1. *$\{S \subseteq E \mid S$ is a subfield of E and $F \subseteq S$ and $\alpha \in S\} \neq \emptyset$.*
2. *$F(\alpha)$ is a subfield of E.*
3. *$F \subseteq F(\alpha)$ and $\alpha \in F(\alpha)$.*
4. *If K is a subfield of E such that $F \subseteq K$ and $\alpha \in K$, then $F(\alpha) \subseteq K$.*

Definition 9.4.5. Let F be a field, let E be an extension field of F, and let $\alpha \in E$.

1. The element α is **algebraic** over F if there is some $f \in F[x]$ such that α is a zero of f.
2. The element α is **transcendental** over F if it is not algebraic. △

Theorem 9.4.6. *Let F be a field, let E be an extension field of F, and let $\alpha \in E$. Suppose α is algebraic over F.*

1. *There is irreducible polynomial $p \in F[x]$ such that α is a zero of p.*
2. *The polynomial p is unique up to multiplication by elements of F.*
3. *If $h \in F[x]$ and α is a zero of h, then $p|h$.*

4. *The polynomial p has minimal degree among all polynomials in $F[x]$ that have α as a zero.*

Theorem 9.4.7. *Let F be a field, let E be an extension field of F, and let $\alpha \in E$. Suppose α is algebraic over F. Let $p \in F[x]$ be an irreducible polynomial such that α is a zero of p.*

1. *The field $F(\alpha)$ is isomorphic to $F[x]/\langle p(x)\rangle$.*

2. *Let $n = \deg p$. If $d \in F(\alpha)$, then there are unique $c_0, c_1, \ldots, c_{n-1} \in F$ such that*

$$d = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

Corollary 9.4.8. *Let F be a field, let E be an extension field of F, and let $\alpha \in E$. Suppose α is algebraic over F. Let $p \in F[x]$ be an irreducible polynomial such that α is a zero of p. Let $n = \deg p$. Then*

$$F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_0, c_1, \ldots, c_{n-1}\}.$$

Exercises

Exercise 9.4.1. Show that each of the following numbers in $\mathbb{R}$ are algebraic over $\mathbb{Q}$.

(1) $1 + \sqrt{2}$.

(2) $\sqrt{2} + \sqrt{3}$.

Exercise 9.4.2. Describe the elements of each of the following extension fields over $\mathbb{Q}$.

(1) $\mathbb{Q}(1 + i)$.

(2) $\mathbb{Q}(\sqrt{1 + \sqrt[3]{2}})$.

Exercise 9.4.3. Let F be a field, let E be an extension field of F, and let $\alpha, \beta \in E$. Prove that $[F(\beta)](\alpha) = [F(\alpha)](\beta)$.

Exercise 9.4.4. Are $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ isomorphic? Prove your claim.