A Semester Course in Basic Abstract Algebra

Marcel B. Finan
Arkansas Tech University

December 29, 2011

PREFACE

This book is an introduction to abstract algebra course for undergraduates either at the junior or senior level. The course is usually taken by Mathematics, Physics, Chemistry, and Engineering majors. The content of the book can be covered in a one semester time period. The chapters presented here represent the core of the subject, the basic idea of groups, rings, and fields. This book has the additional goal of introducing the axiomatic method and the construction of proofs.
This book has been designed for use either as a supplement of standard textbooks or as a textbook for a formal course in an introductory abstract algebra.

Marcel B. Finan,
Arkansas Tech University
January, 2004.

Contents

0 Preliminary Notions

Throughout this book, we assume that the reader is familiar with the following number systems:

- The set of all positive integers

$$\mathbb{N} = \{1, 2, 3, \cdots\}.$$

- The set of all integers

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

- The set of all rational numbers

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \; with \; b \neq 0\}.$$

- The set $\mathbb{R}$ of all real numbers.
- The set of all complex numbers

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

where $i = \sqrt{-1}$.

We start with this introductory section to present the fundamentals of mathematical logic, mathematical proofs, and set theory.

Fundamentals of Mathematical Logic

Logic is commonly known as the science of reasoning. We will develop some of the symbolic techniques required later in the book.

Definition 0.1

A **proposition** is any meaningful statement that is either true or false, but not both.

We will use lowercase letters, such as $p, q, r, \cdots$, to represent propositions. We will also use the notation

$$p : 1 + 1 = 3$$

to define p to be the proposition $1 + 1 = 3$.

Definition 0.2
The **truth value** of a proposition is true, denoted by T, if it is a true statement and false, denoted by F, if it is a false statement.

Statements that are not propositions include questions and commands.

Example 0.1
Which of the following are propositions? Give the truth value of the propositions.
a. $2 + 3 = 7$.
b. Julius Ceasar was president of the United States.
c. What time is it?
d. Be quiet !

Solution.
a. A proposition with truth value (F).
b. A proposition wiht truth value (F).
c. Not a proposition since no truth value can be assigned to this statement.
d. Not a proposition. ■

Definition 0.3
Let p and q be propositions. The **conjunction** of p and q, denoted $p \wedge q$, is the proposition: p *and* q. This proposition is defined to be true only when both p and q are true and it is false otherwise. The **disjunction** of p and q, denoted $p \vee q$, is the proposition: p *or* q. The 'or' is used in an inclusive way. This proposition is false only when both p and q are false, otherwise it is true.

Example 0.2
Let

$$p: \quad 5 < 9$$
$$q: \quad 9 < 7.$$

Construct the propositions $p \wedge q$ and $p \vee q$.

Solution.
The conjunction of the propositions p and q is the proposition

$$p \wedge q : 5 < 9 \text{ and } 9 < 7.$$

The disjunction of the propositions p and q is the proposition

$$p \vee q : 5 < 9 \text{ or } 9 < 7.\blacksquare$$

Definition 0.4
A **truth table** displays the relationships between the truth values of propositions.

Below, we display the truth tables of $p \wedge q$ and $p \vee q$.

p	q	p $\wedge$ q
T	T	T
T	F	F
F	T	F
F	F	F

p	q	p $\vee$ q
T	T	T
T	F	T
F	T	T
F	F	F

Definition 0.5
The **negation** of p, denoted $\sim p$, is the proposition not p.

The truth table of $\sim p$ is displayed below

p	$\sim p$
T	F
F	T

Example 0.3
Find the negation of the proposition $p : -5 < x \leq 0$.

Solution.
The negation of p is the proposition $\sim p : x > 0$ *or* $x \leq -5$ ■

Definition 0.6
Two propositions are **equivalent** if they have exactly the same truth values under all circumstances. We write $p \equiv q$.

Example 0.4
a. Show that $\sim (p \vee q) \equiv \sim p \wedge \sim q$.
b. Show that $\sim (p \wedge q) \equiv \sim p \vee \sim q$.
c. Show that $\sim (\sim p) \equiv p$.

a. and b. are known as DeMorgan's laws.

Solution.

a.

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim (p \vee q)$	$\sim p \wedge \sim q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

b.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim (p \wedge q)$	$\sim p \vee \sim q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

c.

p	$\sim p$	$\sim (\sim p)$
T	F	T
F	T	F

■

Definition 0.7
Let p and q be propositions. The implication $p \Longrightarrow q$ is the the proposition that is false only when p is true and q is false; otherwise it is true. p is called the **hypothesis** and q is called the **conclusion.** The connective $\Longrightarrow$ is called the **conditional** connective.

Example 0.5
Construct the truth table of the implication $p \Longrightarrow q$.

Solution.
The truth table is

p	q	$p \Longrightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

■

Example 0.6
Show that $p \Longrightarrow q \equiv \sim p \vee q$.

Solution.

p	q	$\sim p$	$p \Longrightarrow q$	$\sim p \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

■

It follows from the previous exercise that the proposition $p \Longrightarrow q$ is always true if the hypothesis p is false, regardless of the truth value of q. We say that $p \Longrightarrow q$ is **true by default** or **vacuously true**.
In terms of words the proposition $p \Longrightarrow q$ also reads:
(a) if p then q.
(b) p implies q.
(c) p is a sufficient condition for q.
(d) q is a necessary condition for p.
(e) p only if q.

Definition 0.8
The **converse** of $p \Longrightarrow q$ is the proposition $q \Longrightarrow p$. The **opposite** or **inverse** of $p \Longrightarrow q$ is the proposition $\sim p \Longrightarrow \sim q$. The **contrapositive** of $p \Longrightarrow q$ is the proposition $\sim q \Longrightarrow \sim p$.

Example 0.7
Show that $p \Longrightarrow q \equiv \sim q \Longrightarrow \sim p$.

Solution.
We use De Morgan's laws as follows.

$$\begin{aligned} p \Longrightarrow q &\equiv \sim p \vee q \\ &\equiv \sim (p \wedge \sim q) \\ &\equiv \sim (\sim q \wedge p) \\ &\equiv \sim\sim q \vee \sim p \\ &\equiv q \vee \sim p \\ &\equiv \sim q \Longrightarrow \sim p \end{aligned}$$

■

Example 0.8
Using truth tables show the following:
a. $p \Longrightarrow q \not\equiv q \Longrightarrow p$
b. $p \Longrightarrow q \not\equiv \sim p \Longrightarrow \sim q$

Solution.
a. It suffices to show that $\sim p \vee q \not\equiv \sim q \vee p$.

p	q	$\sim p$	$\sim q$	$\sim p \vee q$		$\sim q \vee p$
T	T	F	F	T		T
T	F	F	T	F	$\neq$	T
F	T	T	F	T	$\neq$	F
F	F	T	T	T		T

b. We will show that $\sim p \vee q \not\equiv p \vee \sim q$.

p	q	$\sim p$	$\sim q$	$\sim p \vee q$		$p \vee \sim q$
T	T	F	F	T		T
T	F	F	T	F	$\neq$	T
F	T	T	F	T	$\neq$	F
F	F	T	T	T		T

■

Definition 0.9
The **biconditional** proposition of p and q, denoted by $p \iff q$, is the propositional function that is true when both p and q have the same truth values and false if p and q have opposite truth values. Also reads, "p if and only if q" or "p is a necessary and sufficient condition for q."

Example 0.9
Construct the truth table for $p \iff q$.

Solution.

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

■

Example 0.10
Show that the biconditional proposition of p and q is logically equivalent to the conjunction of the conditional propositions $p \Longrightarrow q$ and $q \Longrightarrow p$.

Solution.

p	q	$p \Longrightarrow q$	$q \Longrightarrow p$	$p \Longleftrightarrow q$	$(p \Longrightarrow q) \wedge (q \Longrightarrow p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

■

Propositions and Quantifiers

Another way to generate propositions is by means of quantifiers. Let $P(x)$ be a statement that depends on a variable x and which is defined on some set D. "If $P(x)$ is true for all values of $x \in D$" then such a statement defines a proposition. For example, suppose that $P(n) : 2n \; is \; even$ where $n \in \mathbb{N}$. Then the statement "For all $n \in \mathbb{N}, P(n)$" is always true and thus defines a proposition. Such a statement can be written as

$$\forall n \in \mathbb{N}, \{2n \; is \; even\}.$$

The symbol $\forall$ is called the **universal quantifier.**

Example 0.11
Write in the form $\forall x \in D, P(x)$ the proposition :" every real number is either positive, negative or 0."

Solution.
$\forall x \in \mathbb{R}, x > 0, x < 0, or \; x = 0.$■

The proposition $\forall x \in D, P(x)$ is false if $P(x)$ is false for at least one value of x. In this case x is called a **counterexample**.

Example 0.12
Show that the proposition $\forall x \in \mathbb{R}, x > \frac{1}{x}$ is false.

Solution.
A counterexample is $x = \frac{1}{2}$. Clearly, $\frac{1}{2} < 2 = \frac{1}{\frac{1}{2}}$. ■

The notation $\exists x \in D, P(x)$ is a proposition that is true if there is at least one value of $x \in D$ where $P(x)$ is true; otherwise it is false. The symbol $\exists$ is called the **existential** quantifier.

Example 0.13
Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the proposition $\exists x \in \mathbb{R}, P(x)$.

Solution.
Since $4 \in \mathbb{R}$ and $4 > 3$ then the given proposition is true.■

Example 0.14
Write the sets $\cap_{i \in I} S_i$ and $\cup_{i \in I} S_i$ using quantifiers.

Solution.
Recall that $\cap_{i \in I} S_i = \{$x|x is an element of S_i for all i in I$\}$. Using the universal quantifier we obtain $\cap_{i \in I} S_i = \{x | \forall i \in I, x \in S_i\}$. Similarly, since $\cup_{i \in I} S_i = \{$x|x is in S_i for some i $\in$ I$\}$ then using the existential quantifier we can write $\cup_{i \in I} S_i = \{x | \exists i \in I, x \in S_i\}$.■

Example 0.15
a. What is the negation of the proposition $\forall x \in D, P(x)$?
b. What is the negation of the proposition $\exists x \in D, P(x)$?

Solution.
a. $\exists x \in D, \sim P(x)$.
b. $\forall x \in D, \sim P(x)$.■

Example 0.16
Write the negation of each of the following propositions:

a. Every polynomial function is continuous.
b. There exists a triangle with the property that the sum of angles is greater than 180°.

Solution.
a. There exists a polynomial that is not continuous everywhere.
b. For any triangle, the sum of the angles is less than or equal to 180°. ■

Next we discuss statements that contain multiple quantifiers. A typical example is the definition of a limit. We say that $L = \lim_{x \to a} f(x)$ if and only if $\forall \epsilon > 0, \exists$ a positive number δ such that if $|x - a| \leq \delta$ then $|f(x) - L| < \epsilon$.

Example 0.17
a. Let $P(x, y)$ denote the statement "$x + y = y + x$." What is the truth value of the proposition $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}), P(x, y)$?
b. Let $Q(x, y)$ denote the statement "$x + y = 0$." What is the truth value of the proposition $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R}), Q(x, y)$?

Solution.
a. The given proposition is always true.
b. The proposition is false. For otherwise, one can choose $x \neq -y$ to obtain $0 \neq x + y = 0$ which is impossible ■

Example 0.18
Find the negation of the following propositions:
a. $\forall x \exists y, P(x, y)$.
b. $\exists x \forall y, P(x, y)$.

Solution.
a. $\exists x \forall y, \sim P(x, y)$.
b. $\forall x \exists y, \sim P(x, y)$ ■

Example 0.19
The symbol $\exists\,!$ stands for the phrase "there exists a unique". Which of the following statements are true and which are false.

a. $\exists\,!\; x \in \mathbb{R}, \forall y \in \mathbb{R}, xy = y$.
b. $\exists\,!$ integer x such that $\frac{1}{x}$ is an integer.

Solution.
a. True. Let $x = 1$.
b. False since 1 and -1 are both integers with integer reciprocals ■

As a final application of quantifiers we prove the following result known as DeMorgan's laws for sets.

Theorem 0.1
Let $\{A_i\}_{i \in I}$ be a collection of sets. Then

(a) $(\cup_{i \in I} A_i)^c = \cap_{i \in I} A_i^c$.
(b) $(\cap_{i \in I} A_i)^c = \cup_{i \in I} A_i^c$.

Proof.
(a) Let $x \in (\cup_{i\in I} A_i)^c$. Then by the definition of complement we have $x \in U$ and $x \notin \cup_{i\in I} A_i$. Thus, $x \notin A_i, \forall i \in I$. Hence, we have $x \in U$ and $x \notin A_i, \forall i \in I$ and this means that $x \in A_i^c, \forall i \in I$. Therefore, $x \in \cap_{i\in I} A_i^c$. This proves that $(\cup_{i\in I} A_i)^c \subseteq \cap_{i\in I} A_i^c$.
Now, let $x \in \cap_{i\in I} A_i^c$. Then $x \notin A_i, \forall i \in I$. Hence, $x \notin \cup_{i\in I} A_i$. Since $x \in U$ and $x \notin \cup_{i\in I} A_i$ then $x \in (\cup_{i\in I} A_i)^c$. This shows that $\cap_{i\in I} A_i^c \subseteq (\cup_{i\in I} A_i)^c$.
(b) Similar to (a) and is left for the reader. ■

Methods of Mathematical Proofs
Mathematical proofs can be classified as either a direct proof or an indirect proof. In a direct proof one starts with the hypothesis of an implication $p \Longrightarrow q$ and then prove that the conclusion is true. Any other method of proof will be referred to as an indirect proof. In this section we study two methods of indirect proofs, namely, the proof by contradiction and the proof by contrapositive.

• **Proof by contradiction**: With this method, a conditional statement "$p \Longrightarrow q$" is proved by showing that if p were true and q were not true, then some contradiction (absurdity) would result. We give a couple of problems where we use this method.

Example 0.20
Show that if n^2 is an even integer then so is n.

Solution.
Suppose the contrary. That is suppose that n is odd. Then there is an integer k such that $n = 2k + 1$. In this case, $n^2 = 2(2k^2 + 2k) + 1$ is odd and this contradicts the assumption that n^2 is even. Hence, n must be even ■

Example 0.21
Show tthat the number $\sqrt{2}$ is irrational.

Solution.
Suppose not. That is, suppose that $\sqrt{2}$ is rational. Then there exist two integers m and n with no common divisors such that $\sqrt{2} = \frac{m}{n}$. Squaring both sides of this equality we find that $2n^2 = m^2$. Thus, m^2 is even. By Problem 0.20, m is even. That is, 2 divides m. But then $m = 2k$ for some integer k.

Taking the square we find that $2n^2 = m^2 = 4k^2$, that is $n^2 = 2k^2$. This says that n^2 is even and by Example 0.20, n is even. We conclude that 2 divides both m and n and this contradcits our assumption that m and n have no common divisors. Hence, $\sqrt{2}$ must be irrational ■

• **Proof by contrapositive**: We already know that $p \Longrightarrow q \equiv \sim q \Longrightarrow \sim p$. So to prove $p \Longrightarrow q$ we sometimes instead prove $\sim q \Longrightarrow \sim p$.

Example 0.22
Show that if n is an integer such that n^2 is odd then n is also odd.

Proof.
Suppose that n is an integer that is even. Then there exists an integer k such that $n = 2k$. But then $n^2 = 2(2k^2)$ which is even. ■

Method of Proof by Induction
We want to prove that some predicate $P(n)$ is true for any nonnegative integer $n \geq n_0$. This is acheived by using the method of mathematical induction. The steps of this method are as follows:

(i) (Basis of induction) Show that $P(n_0)$ is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true.
(iii) (Induction step) Show that $P(n+1)$ is true.

Example 0.23
Use the technique of mathematical induction to show that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Solution.
Let $S(n) = 1 + 2 + \cdots + n$. Then
(i) (Basis of induction) $S(1) = 1 = \frac{1(1+1)}{2}$. That is, $S(1)$is true.
(ii) (Induction hypothesis) Assume $S(n)$ is true. That is, $S(n) = \frac{n(n+1)}{2}$.
(iii) (Induction step) We must show that $S(n+1) = \frac{(n+1)(n+2)}{2}$. Indeed,

$$\begin{aligned} S(n+1) &= 1 + 2 + \cdots + n + (n+1) \\ &= S(n) + (n+1) \\ &= \tfrac{n(n+1)}{2} + (n+1) \\ &= \tfrac{(n+1)(n+2)}{2} \quad ■ \end{aligned}$$

Example 0.24
a. Use induction to prove that $n < 2^n$ for all non-negative integers n.
b. Use induction to prove that $2^n < n!$ for all non-negative integers $n \geq 4$.

Solution.
a. Let $S(n) = 2^n - n, n \geq 0$. We want to show that $S(n) > 0$ is valid for all $n \geq 0$. By the method of mathematical induction we have
(i) (Basis of induction) $S(0) = 2^0 - 0 = 1 > 0$. That is, $S(0)$is true.
(ii) (Induction hypothesis) Assume $S(n)$ is true. That is, $S(n) > 0$.
(iii) (Induction step) We must show that $S(n+1) > 0$. Indeed,

$$\begin{aligned} S(n+1) &= 2^{n+1} - (n+1) \\ &= 2^n.2 - n - 1 \\ &= 2^n(1+1) - n - 1 \\ &= 2^n - n + 2^n - 1 \\ &= (2^n - 1) + S(n) \\ &> 2^n - 1 > 0 \end{aligned}$$

since the smallest value of n is 0 and in this case $2^0 - 1 = 0$.
b. Let $S(n) = n! - 2^n,\ n \geq 4$. We want to show that $S(n) > 0$ for all $n \geq 4$. By the method of mathematical induction we have
(i) (Basis of induction) $S(4) = 4! - 2^4 = 8 > 0$. That is, $S(4)$is true.
(ii) (Induction hypothesis) Assume $S(n)$ is true. That is, $S(n) > 0,\ n \geq 4$.
(iii) (Induction step) We must show that $S(n+1) > 0$. Indeed,

$$\begin{aligned} S(n+1) &= (n+1)! - 2^{n+1} \\ &= (n+1)n! - 2^n(1+1) \\ &= n! - 2^n + nn! - 2^n \\ &> 2(n! - 2^n) = 2S(n) > 0. \end{aligned}$$

where we have used the fact that if $n \geq 1$ then $nn! \geq n!$ ■

Example 0.25 *(Bernoulli's inequality)*
Let $h > -1$. Use induction to show that

$$(1 + nh) \leq (1 + h)^n, \quad n \geq 0.$$

Solution.
Let $S(n) = (1+h)^n - (1+nh)$. We want to show that $S(n) \geq 0$ for all $n \geq 0$.

We use mathematical induction as follows.
(i) (Basis of induction) $S(0) = (1+h)^0 - (1+0h) = 0$. That is, $S(0)$is true.
(ii) (Induction hypothesis) Assume $S(n)$ is true. That is, $S(n) \geq 0,\ n \geq 0$.
(iii) (Induction step) We must show that $S(n+1) \geq 0$. Indeed,

$$\begin{aligned} S(n+1) &= (1+h)^{n+1} - (1+(n+1)h) \\ &= (1+h)(1+h)^n - nh - 1 - h \\ &\geq (1+h)(1+nh) - nh - 1 - h \\ &= nh^2 \geq 0. \quad \blacksquare \end{aligned}$$

Fundamentals of Set Theory

Set is the most basic term in mathematics. In this section we introduce the concept of sets and its various operations and then study the properties of these operations.

Definition 0.10
We define a **set** A as a collection of well-defined objects (called **elements** or **members** of A) such that for any given object x either one (but not both) of the following holds:

- x belongs to A and we write $x \in A$.
- x does not belong to A, and in this case we write $x \notin A$.

We denote sets by capital letters $A, B, C, \cdots$ and elements by lowercase letters $a, b, c, \cdots$. Sets consisting of sets will be denoted by script letters.
There are two different ways to represent a set. The first one is to list, without repetition, the elements of the set. The other way is to describe a property that characterizes the elements of the set. This is also known as the **set-builder** notation.
We define the **empty** set, denoted by $\emptyset$, to be the set with no elements.

Example 0.26
List the elements of the following sets.
a. $\{x | x$ is a real number such that $x^2 = 1\}$.
b. $\{x | x$ is an integer such that $x^2 - 3 = 0\}$.

Solution.
a. $\{-1, 1\}$.
b. $\emptyset$ $\blacksquare$

Example 0.27
Use a property to give a description of each of the following sets.
a. $\{a, e, i, o, u\}$.
b. $\{1, 3, 5, 7, 9\}$.

Solution.
a. $\{x|x \text{ is a vowel}\}$.
b. $\{n \in \mathbb{N}|n \text{ is odd and less than } 10\}$ ■

Definition 0.11
Let A and B be two sets. We say that A is a **subset** of B, denoted by $A \subseteq B$, if and only if every element of A is also an element of B.

If there exists an element of A which is not in B then we write $A \nsubseteq B$.

Example 0.28
Suppose that $A = \{2, 4, 6\}$, $B = \{2, 6\}$, and $C = \{4, 6\}$. Determine which of these sets are subsets of which other of these sets.

Solution.
$B \subseteq A$ and $C \subseteq A$ ■

If sets A and B are represented as regions in the plane, relationships between A and B can be represented by pictures, called **Venn diagrams.**

Example 0.29
Represent $A \subseteq B$ using Venn diagram.

Solution.
The Venn diagram is given in Figure 0.1■

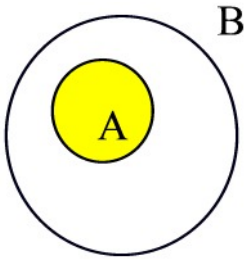


Fig. 1

Figure 0.1

Definition 0.12
Two sets A and B are said to be **equal** if and only if $A \subseteq B$ and $B \subseteq A$. We write $A = B$.

It follows from the above definition that in order to show $A = B$ it suffices to show the double inclusions mentioned in the definition. For non-equal sets we write $A \neq B$.

Example 0.30
Determine whether each of the following pairs of sets are equal.
(a) $\{1, 3, 5\}$ and $\{5, 3, 1\}$.
(b) $\{\{1\}\}$ and $\{1, \{1\}\}$.

Solution.
(a) $\{1, 3, 5\} = \{5, 3, 1\}$.
(b) $\{\{1\}\} \neq \{1, \{1\}\}$ since $1 \notin \{\{1\}\}$ ■

Definition 0.13
Let A and B be two sets. We say that A is a **proper** subset of B, denoted by $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Thus, to show that A is a proper subset of B we must show that every element of A is an element of B and there is an element of B which is not in A.

Example 0.31
Order the sets of numbers: $\mathbb{C}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{N}$ using $\subset$.

Solution.
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. ■

Example 0.32
Determine whether each of the following statements is true or false.
(a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{x\} \in \{x\}$
(d) $\{x\} \in \{\{x\}\}$ (e) $\emptyset \subseteq \{x\}$ (f) $\emptyset \in \{x\}$

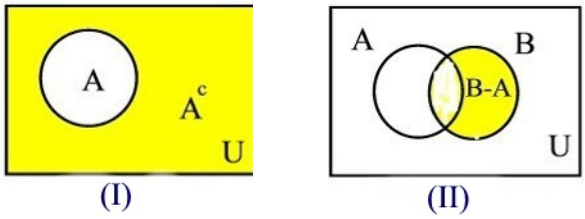
Solution.
(a) True (b) True (c) False, since only $x \in \{x\}$ (d) True (e) True (f) False, since $\emptyset$ is a set and $\{x\}$ has an element which is not a set. ■

Definition 0.14
If U is a given set whose subsets are under consideration, then we call U a **universal set.** Let U be a universal set and A, B be two subsets of U. The **absolute complement** of A (See Figure 0.2) is the set

$$A^c = \{x \in U | x \notin A\}.$$

The **relative complement** of A with respect to B (See Figure 0.3) is the set

$$B - A = \{x \in U | x \in B \text{ and } x \notin A\}.$$



Example 0.33
Let $U = \mathbb{R}$. Consider the sets $A = \{x \in \mathbb{R} | x < -1 \text{ or } x > 1\}$ and $B = \{x \in \mathbb{R} | x \leq 0\}$. Find

a. A^c.
b. $B - A$.

Solution.
a. $A^c = [-1, 1]$.
b. $B - A = [-1, 0]$ ■

Definition 0.15
Let A and B be two sets. The **union** of A and B is the set

$$A \cup B = \{x | x \in A \text{ or } x \in B\}$$

where the 'or' is inclusive.(See Figure 0.4)

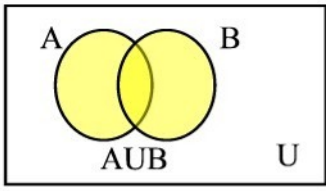


Figure 0.4

The above definition can be extended to more than two sets. More precisely, if $A_1, A_2, \cdots$, are sets then

$$\cup_{n=1}^{\infty} A_n = \{x | x \in A_i \ for \ some \ i \in \mathbb{N}\}.$$

Definition 0.16
Let A and B be two sets. The **intersection** of A and B is the set

$$A \cap B = \{x | x \in A \ and \ x \in B\}.$$

(See Figure 0.5).

If $A \cap B = \emptyset$ we say that A and B are **disjoint** sets.

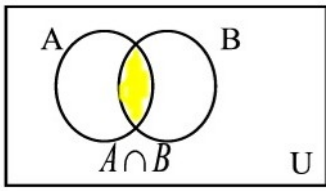


Figure 0.5

Given the sets $A_1, A_2, \cdots$, we define

$$\cap_{n=1}^{\infty} A_n = \{x | x \in A_i \ for \ all \ i \in \mathbb{N}\}.$$

Example 0.34
Let $A = \{a, b, c\}, B = \{b, c, d\}$, and $C = \{b, c, e\}$.

a. Find $A \cup (B \cap C), (A \cup B) \cap C$, and $(A \cup B) \cap (A \cup C)$. Which of these sets are equal?
b. Find $A \cap (B \cup C), (A \cap B) \cup C$, and $(A \cap B) \cup (A \cap C)$. Which of these sets are equal?
c. Find $A - (B - C)$ and $(A - B) - C$. Are these sets equal?

Solution.
a. $A \cup (B \cap C) = A, (A \cup B) \cap C = \{b, c\}, (A \cup B) \cap (A \cup C) = \{a, b, c\} = A \cup (B \cap C)$.
b. $A \cap (B \cup C) = \{b, c\}, (A \cap B) \cup C = C, (A \cap B) \cup (A \cap C) = \{b, c\}. = A \cap (B \cup C)$.
c. $A - (B - C) = A$ and $(A - B) - C = \{a\} \neq A - (B - C)$. ■

Example 0.35
For each $n \geq 1$, let $A_n = \{x \in \mathbb{R} : x < 1 + \frac{1}{n}\}$. Show that

$$\cap_{n=1}^{\infty} A_n = \{x \in \mathbb{R} : x \leq 1\}.$$

Solution.
The proof is by double inclusions method. Let $y \in \{x \in \mathbb{R} : x \leq 1\}$. Then for all positive integer n we have $y \leq 1 < 1 + \frac{1}{n}$. That is, $y \in \cap_{n=1}^{\infty} A_n$. This shows that $\{x \in \mathbb{R} : x \leq 1\} \subseteq \cap_{n=1}^{\infty} A_n$.
Conversely, let $y \in \cap_{n=1}^{\infty} A_n$. Then $y < 1 + \frac{1}{n}$ for all $n \geq 1$. Now take the limit of both sides as $n \to \infty$ to obtain $y \leq 1$. That is, $y \in \{x \in \mathbb{R} : x \leq 1\}$. This shows that $\cap_{n=1}^{\infty} A_n \subseteq \{x \in \mathbb{R} : x \leq 1\}$. ■

Definition 0.17
The notation $(a_1, a_2, \cdots, a_n)$ is called an **ordered n-tuples**. We say that two n-tuples $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ are equal if and only if $a_1 = b_1, a_2 = b_2, \cdots, a_n = b_n$.
Given n sets $A_1, A_2, \cdots, A_n$ the **Cartesian product** of these sets is the set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) : a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}$$

Example 0.36
Let $A = \{x, y\}, B = \{1, 2, 3\}$, and $C = \{a, b\}$. Find $A \times B \times C$.

Solution.

$$\begin{aligned} A \times B \times C = \quad & \{(x,1,a),(x,2,a),(x,3,a),(y,1,a),(y,2,a), \\ & (y,3,a),(x,1,b),(x,2,b),(x,3,b),(y,1,b) \\ & (y,2,b),(y,3,b)\} \blacksquare \end{aligned}$$

We end this section by discussing some basic properties of sets.
The following problem shows that the operation $\subseteq$ is reflexive and transitive, concepts that will be discussed in Section 9.

Example 0.37
a. Show that $A \subseteq A$.
b. Suppose that A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.
c. Find two sets A and B such that $A \in B$ and $A \subseteq B$.

Solution.
a. The proposition if $x \in A$ then $x \in A$ is always true. Thus, $A \subseteq A$.
b. We need to show that every element of A is an element of C. Let $x \in A$. Since $A \subseteq B$ then $x \in B$. But $B \subseteq C$ so $x \in C$.
c. $A = \{x\}$ and $B = \{x, \{x\}\}$.■

Theorem 0.2
Let A and B be two sets. Then
a. $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
b. $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

Proof.
a. If $x \in A \cap B$ then $x \in A$ and $x \in B$. This still imply that $x \in A$. Hence, $A \cap B \subseteq A$. A similar argument holds for $A \cap B \subseteq B$.
b. The proposition "if $x \in A$ then $x \in A \cup B$" is always true. Hence, $A \subseteq A \cup B$. A similar argument holds for $B \subseteq A \cup B$■

Theorem 0.3
If A and B are subsets of U then
a. $A \cup U = U$.
b. $A \cup A = A$.
c. $A \cup \emptyset = A$.
d. $A \cup B = B \cup A$.
e. $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof.
a. Clearly, $A \cup U \subseteq U$. Conversely, let $x \in U$. Then definitely, $x \in A \cup U$. That is, $U \subseteq A \cup U$.
b. If $x \in A$ then $x \in A$ or $x \in A$. That is, $x \in A \cup A$ and consequently $A \subseteq A \cup A$. Conversely, if $x \in A \cup A$ then $x \in A$. Hence, $A \cup A \subseteq A$.
c. If $x \in A \cup \emptyset$ then $x \in A$ since $x \notin \emptyset$. Thus, $A \cup \emptyset \subseteq A$. Conversely, if $x \in A$ then $x \in A$ or $x \in \emptyset$. Hence, $A \subseteq A \cup \emptyset$.
d. If $x \in A \cup B$ then $x \in A$ or $x \in B$. But this is the same thing as saying $x \in B$ or $x \in A$. That is, $x \in B \cup A$. Now interchange the roles of A and B to show that $B \cup A \subseteq A \cup B$.
e. Let $x \in (A \cup B) \cup C$. Then $x \in (A \cup B)$ or $x \in C$. Thus, ($x \in A$ or $x \in B$) or $x \in C$. This implies $x \in A$ or ($x \in B$ or $x \in C$). Hence, $x \in A \cup (B \cup C)$. The converse is similar ■

Theorem 0.4
Let A and B be subsets of U. Then
a. $A \cap U = A$.
b. $A \cap A = A$.
c. $A \cap \emptyset = \emptyset$.
d. $A \cap B = B \cap A$.
e. $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof.
a. If $x \in A \cap U$ then $x \in A$. That is , $A \cap U \subseteq A$. Conversely, let $x \in A$. Then definitely, $x \in A$ and $x \in U$. That is, $x \in A \cap U$. Hence, $A \subseteq A \cap U$.
b. If $x \in A$ then $x \in A$ and $x \in A$. That is, $A \subseteq A \cap A$. Conversely, if $x \in A \cap A$ then $x \in A$. Hence, $A \cap A \subseteq A$.
c. Clearly $\emptyset \subseteq A \cap \emptyset$. Conversely, if $x \in A \cap \emptyset$ then $x \in \emptyset$. Hence, $A \cap \emptyset \subseteq \emptyset$.
d. If $x \in A \cap B$ then $x \in A$ and $x \in B$. But this is the same thing as saying $x \in B$ and $x \in A$. That is, $x \in B \cap A$. Now interchange the roles of A and B to show that $B \cap A \subseteq A \cap B$.
e. Let $x \in (A \cap B) \cap C$. Then $x \in (A \cap B)$ and $x \in C$. Thus, ($x \in A$ and $x \in B$) and $x \in C$. This implies $x \in A$ and ($x \in B$ and $x \in C$). Hence, $x \in A \cap (B \cap C)$. The converse is similar ■

Theorem 0.5
If A, B, and C are subsets of U then
a. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
b. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof.
a. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Thus, $x \in A$ and ($x \in B$ or $x \in C$). This implies that ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$). Hence, $x \in A \cap B$ or $x \in A \cap C$, i.e. $x \in (A \cap B) \cup (A \cap C)$. The converse is similar.
b. Let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. Thus, $x \in A$ or ($x \in B$ and $x \in C$). This implies that ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$). Hence, $x \in A \cup B$ and $x \in A \cup C$, i.e. $x \in (A \cup B) \cap (A \cup C)$. The converse is similar ■

Theorem 0.6 *(De Morgan's Laws)*
Let A and B be subsets of U then

a. $(A \cup B)^c = A^c \cap B^c$.
b. $(A \cap B)^c = A^c \cup B^c$.

Proof.
a. Let $x \in (A \cup B)^c$. Then $x \in U$ and $x \notin A \cup B$. Hence, $x \in U$ and ($x \notin A$ and $x \notin B$). This implies that ($x \in U$ and $x \notin A$) and ($x \in U$ and $x \notin B$). It follows that $x \in A^c \cap B^c$. Now, go backward for the converse.
b. Let $x \in (A \cap B)^c$. Then $x \in U$ and $x \notin A \cap B$. Hence, $x \in U$ and ($x \notin A$ or $x \notin B$). This implies that ($x \in U$ and $x \notin B$) or ($x \in U$ and $x \notin A$). It follows that $x \in A^c \cup B^c$. The converse is similar ■

Definition 0.18
A collection of nonempty subsets $\{A_1, A_2, \cdots, A_n\}$ of A is said to be a **partition** of A if and only if

(i) $A = \cup_{k=1}^{n} A_k$.
(ii) $A_i \cap A_j = \emptyset$ for all $i \neq j, 1 \leq i, j \leq n$.

Example 0.38
Let $A = \{1, 2, 3, 4, 5, 6\}, A_1 = \{1, 2\}, A_2 = \{3, 4\}, A_3 = \{5, 6\}$. Show that $\{A_1, A_2, A_3\}$ is a partition of A.

Solution.
(i) $A_1 \cup A_2 \cup A_3 = A$.
(ii) $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$.■

Definition 0.19
The number of elements of a set is called the **cardinality** of the set. We write $|A|$ to denote the cardinality of the set A. If A has a finite cardinality we say that A is a **finite** set. Otherwise, it is called **infinite**.

Example 0.39
What is the cardinality of each of the following sets.
(a) $\emptyset$.
(b) $\{\emptyset\}$.
(c) $\{a, \{a\}, \{a, \{a\}\}\}$.

Solution.
(a) $|\emptyset| = 0$
(b) $|\{\emptyset\}| = 1$
(c) $|\{a, \{a\}, \{a, \{a\}\}\}| = 3$ ■

Definition 0.20
Let A be a set. The **power set** of A, denoted by $\mathcal{P}(\mathrm{A})$, is the set of all possible subsets of A.

Example 0.40
Find the power set of $A = \{a, b, c\}$.

Solution.

$$\begin{aligned}\mathcal{P}(\mathrm{A}) &= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \\ &\qquad \{b, c\}, \{a, b, c\}\} \quad \blacksquare\end{aligned}$$

Example 0.41
If $A \subseteq B$ then $\mathcal{P}(\mathrm{A}) \subseteq \mathcal{P}(\mathrm{B})$.

Solution.
Let $X \in \mathcal{P}(\mathrm{A})$. Then $X \subseteq A$. Since $A \subseteq B$ then $X \subseteq B$. Hence, $X \in \mathcal{P}(\mathrm{B})$ $\blacksquare$

Example 0.42
Let A be a non-empty set with n elements. Prove that $|\mathcal{P}(A)| = 2^n$.

Solution.
If $n = 0$ then $A = \emptyset$ and in this case $\mathcal{P}(\mathrm{A}) = \{\emptyset\}$. Thus $|\mathcal{P}(\mathrm{A})| = 1$. As induction hypothesis, suppose that if $|A| = n$ then $|\mathcal{P}(\mathrm{A})| = 2^n$. Let $B = A \cup \{a_{n+1}\}$. Then $\mathcal{P}(\mathrm{B})$ consists of all subsets of A and all subsets of A with the element a_{n+1} added to them. Hence, $|\mathcal{P}(\mathrm{B})| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.$\blacksquare$

Review Problems

Exercise 0.1
a. Show that $p \wedge q \equiv q \wedge p$ and $p \vee q \equiv q \vee p$.
b. Show that $(p \vee q) \vee r \equiv p \vee (q \vee r)$ and $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.
c. Show that $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ and $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$.

Exercise 0.2
Construct the truth table for the proposition: $\sim p \vee q \Longrightarrow r$.

Exercise 0.3
Construct the truth table for the proposition: $(p \Longrightarrow r) \Longleftrightarrow (q \Longrightarrow r)$.

Exercise 0.4
Write negations for each of the following propositions. (Assume that all variables represent fixed quantities or entities, as appropriate.)

a. If P is a square, then P is a rectangle.
b. If today is Thanksgiving, then tomorrow is Friday.
c. If r is rational, then the decimal expansion of r is repeating.
d. If n is prime, then n is odd or n is 2.
e. If Tom is Ann's father, then Jim is her uncle and Sue is her aunt.
f. If n is divisible by 6, then n is divisible by 2 and n is divisible by 3.

Exercise 0.5
Write the contrapositives for the propositions of Exercise 0.4.

Exercise 0.6
Write the converse and inverse for the propositions of Exercise 0.4.

Exercise 0.7
Use the proof by contradiction to prove the proposition "There is no greatest even integer."

Exercise 0.8
Prove by contradiction that the difference of any rational number and any irrational number is irrational.

Exercise 0.9
Use the proof by contraposition to show that if a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Exercise 0.10
Use the proof by contradiction to show that the product of any nonzero rational number and any irrational number is irrational.

Exercise 0.11
Use the method of induction to show that

$$2 + 4 + 6 + \cdots + 2n = n^2 + n$$

for all integers $n \geq 1$.

Exercise 0.12
Use mathematical induction to prove that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all integers $n \geq 0$.

Exercise 0.13
Use mathematical induction to show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for all integers $n \geq 1$.

Exercise 0.14
Use mathematical induction to show that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

for all integers $n \geq 1$.

Exercise 0.15
Use mathematical induction to show that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for all integers $n \geq 1$.

Exercise 0.16
Let $S(n) = \sum_{k=1}^{n} \frac{k}{(k+1)!}$. Evaluate $S(1), S(2), S(3), S(4)$, and $S(5)$. Make a conjecture about a formula for this sum for general n, and prove your conjecture by mathematical induction.

Exercise 0.17
Show that $2^n < (n+2)!$ for all integers $n \geq 0$.

Exercise 0.18
a. Use mathematical induction to show that $n^3 > 2n + 1$ for all integers $n \geq 2$.
b. Use mathematical induction to show that $n! > n^2$ for all integers $n \geq 4$.

Exercise 0.19
Which of the following sets are equal?
a. $\{a, b, c, d\}$
b. $\{d, e, a, c\}$
c. $\{d, b, a, c\}$
d. $\{a, a, d, e, c, e\}$

Exercise 0.20
Let $A = \{c, d, f, g\}, B = \{f, j\}$, and $C = \{d, g\}$. Answer each of the following questions. Give reasons for your answers.
a. Is $B \subseteq A$?
b. Is $C \subseteq A$?
c. Is $C \subseteq C$?
d. Is C a proper subset of A?

Exercise 0.21
a. Is $3 \in \{1, 2, 3\}$?
b. Is $1 \subseteq \{1\}$?
c. Is $\{2\} \in \{1, 2\}$?
d. Is $\{3\} \in \{1, \{2\}, \{3\}\}$?
e. Is $1 \in \{1\}$?
f. Is $\{2\} \subseteq \{1, \{2\}, \{3\}\}$?
g. Is $\{1\} \subseteq \{1, 2\}$?
h. Is $1 \in \{\{1\}, 2\}$?
i. Is $\{1\} \subseteq \{1, \{2\}\}$?
j. Is $\{1\} \subseteq \{1\}$?

Exercise 0.22
Let $A = \{b, c, d, f, g\}$ and $B = \{a, b, c\}$. Find each of the following:
a. $A \cup B$.
b. $A \cap B$.
c. $A - B$.
d. $B - A$.

Exercise 0.23
Indicate which of the following relationships are true and which are false:
a. $\mathbb{Z}^+ \subseteq \mathbb{Q}$.
b. $\mathbb{R}^- \subset \mathbb{Q}$.
c. $\mathbb{Q} \subset \mathbb{Z}$.
d. $\mathbb{Z}^+ \cup \mathbb{Z}^- = \mathbb{Z}$.
e. $\mathbb{Q} \cap \mathbb{R} = \mathbb{Q}$.
f. $\mathbb{Q} \cup \mathbb{Z} = \mathbb{Z}$.
g. $\mathbb{Z}^+ \cap \mathbb{R} = \mathbb{Z}^+$
h. $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$.

Exercise 0.24
Let $A = \{x, y, z, w\}$ and $B = \{a, b\}$. List the elements of each of the following sets:
a. $A \times B$
b. $B \times A$
c. $A \times A$
d. $B \times B$.

Exercise 0.25
Let A, B, and C be sets. Prove that if $A \subseteq B$ then $A \cap C \subseteq B \cap C$.

Exercise 0.26
Find sets A, B, and C such that $A \cap C = B \cap C$ but $A \neq B$.

Exercise 0.27
Find sets A, B, and C such that $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$ but $A \neq B$.

Exercise 0.28
Let A and B be two sets. Prove that if $A \subseteq B$ then $B^c \subseteq A^c$.

Exercise 0.29
Let A, B, and C be sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Exercise 0.30
Let A, B, and C be sets. Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Exercise 0.31
Let A, B, and C be sets. Show that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Exercise 0.32
a. Is the number 0 in $\emptyset$? Why?
b. Is $\emptyset = \{\emptyset\}$? Why?
c. Is $\emptyset \in \{\emptyset\}$? Why?

Exercise 0.33
Let A and B be two sets. Prove that $(A - B) \cap (A \cap B) = \emptyset$.

Exercise 0.34
Let A and B be two sets. Show that if $A \subseteq B$ then $A \cap B^c = \emptyset$.

Exercise 0.35
Let A, B and C be three sets. Prove that if $A \subseteq B$ and $B \cap C = \emptyset$ then $A \cap C = \emptyset$.

Exercise 0.36
Find two sets A and B such that $A \cap B = \emptyset$ but $A \times B \neq \emptyset$.

Exercise 0.37
Suppose that $A = \{1, 2\}$ and $B = \{2, 3\}$. Find each of the following:
a. $\mathcal{P}(\mathrm{A} \cap \mathrm{B})$.
b. $\mathcal{P}(\mathrm{A})$.
c. $\mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
d. $\mathcal{P}(\mathrm{A} \times \mathrm{B})$.

Exercise 0.38
a. Find $\mathcal{P}(\emptyset)$.
b. Find $\mathcal{P}(\mathcal{P}(\emptyset))$.
c. Find $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

Exercise 0.39
Determine which of the following statements are true and which are false. Prove each statement that is true and give a counterexample for each statement that is false.
a. $\mathcal{P}(\mathrm{A} \cup \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B})$.
b. $\mathcal{P}(\mathrm{A} \cap \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cap \mathcal{P}(\mathrm{B})$.
c. $\mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B}) \subseteq \mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
d. $\mathcal{P}(\mathrm{A} \times \mathrm{B}) = \mathcal{P}(\mathrm{A}) \times \mathcal{P}(\mathrm{B})$.

1 The Concept of a Mapping

The concept of a mapping (aka function) is important throughout mathematics. We have been dealing with functions for a long time. You recall from calculus that a function is a rule which assigns with each real number in the domain a unique real number in the codomain. So both the domain and codomain are subsets of the real numbers system. In this section, we would like to define functions on domains and codomains other than the set of real numbers.

Definition 1.1
If S and T are nonempty sets, then a **mapping** (or a function) from S into T is a rule which assigns to each member of S a unique member in T. We call S the **domain** and T the **codomain** of the mapping.

In what follows, we will use the terms function and mapping interchangeably. If α is a function from S to T we shall adopt the notation:

$$\alpha : S \longrightarrow T.$$

Note that every member x in the domain S is associated to a unique member y of the codomain T. In function notation, we write $y = \alpha(x)$. However, not every element in the codomain need be associated to an element in the domain.

Example 1.1
If α is a mapping from S to S and A is a subset of S then the rule $\iota_A(x) = x$ defines a mapping from A into A. We call ι_A the **identity mapping** on A.■

Example 1.2
Assume that S and T are finite sets containing m and n elements, respectively. How many mappings are there from S to T?

Solution.
The problem of finding the number of mappings from S to T is the same as that of computing the number of different ways each element of S can be assigned an image in T. For the first element, there are m possibilities, for the second element there are also m possibilitites, etc, for the nth element there are m possibilities. By the Principle of Counting, there are m^n mappings from S to T.■

Remark 1.1
In the notation $y = \alpha(x)$, x is sometimes referred to as the **preimage** of y with respect to α. ■

Sometimes it is necessary to identify the elements of T which can be associated to some elements in the domain S. This subset of the codomain is called the **image** or **range** of α (denoted $\alpha(S)$).

Definition 1.2
If $\alpha : S \longrightarrow T$ is a mapping and A is a subset of S then the set of all images of the members of A will be denoted by $\alpha(A)$.(See Figure 1.1). In set-builder notation

$$\alpha(A) = \{\alpha(x) : x \in A\}.$$

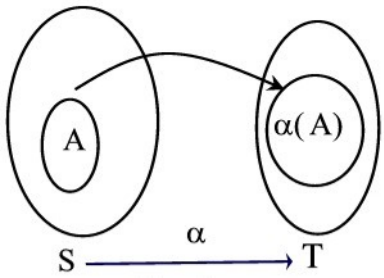
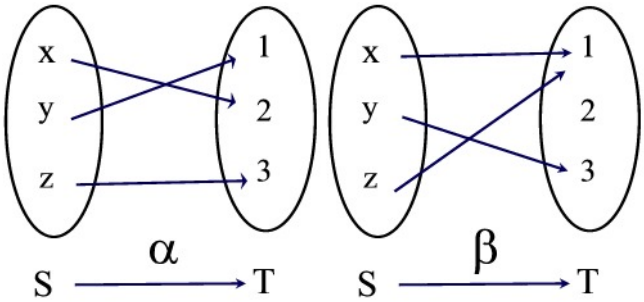


Figure 1.1

Example 1.3
The rules α and β defined from the set $S = \{x, y, z\}$ to $T = \{1, 2, 3\}$ represent mappings with $\alpha(S) = T$ and $\beta(S) = \{1, 3\}$, respectively.(See Figure 1.2) On the other hand, the rule γ does not define a mapping for two reasons: first, the member y has no image, and second, the member x is associated to two members 1 and 3 of T.■



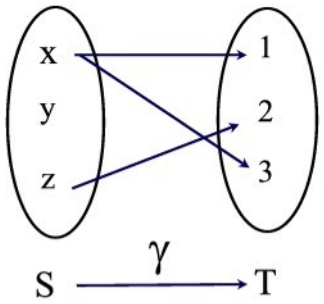


Figure 1.2

Example 1.4
With α and β as in Example 1.3

$$\alpha(\{x,z\}) = \{2,3\} \quad and \quad \beta(\{x,z\}) = \{1\}. \blacksquare$$

The first operation of mappings that we consider is the equality of two mappings.

Example 1.5 *(Equality of two mappings)*
We say that two mappings α and β from S into T are *equal* if and only if $\alpha(x) = \beta(x)$ for all $x \in S$, i.e. the range of α is equal to the range of β. We write $\alpha = \beta$. When two functions are not equal we write $\alpha \neq \beta$. This occurs, when there is a member in the common domain such that $\alpha(x) \neq \beta(x)$. For example, the mappings α and β of Example 1.3 are different since $\alpha(y) \neq \beta(y)$. On the other hand, the mappings $\alpha : \mathbb{R} \longrightarrow \mathbb{R}$ and $\beta : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $\alpha(x) = (x+1)^2$ and $\beta(x) = x^2 + 2x + 1$ are equal.■

Next, we introduce a family of mappings with the property that the range is the whole codomain.

Definition 1.3
A mapping $\alpha : S \longrightarrow T$ is called **onto** (or **surjective**) if and only if $\alpha(S) = T$. That is, if and only if for every member in the codomain there is a member in the domain associated to it. Using quantifiers, α is onto if and only if $\forall y \in T$, $\exists x \in S$ such that $\alpha(x) = y$.

Example 1.6
In terms of a Venn diagram, a mapping is onto if and only if each element in the codomain has at least one arrow pointed to it. Thus, since $\alpha(S) = T$ in Example 1.3 then α is onto whereas β is not since $\beta(S) \neq T$. ■

Example 1.7
The functions $f(x) = x^2$ and $g(x) = \sin x$ are not onto as functions from $\mathbb{R}$ to $\mathbb{R}$. However, if the codomain is restricted to $\mathbb{R}^+$ then f is onto. Also, if the codomain of g is restricted to $[-1, 1]$ then g is onto.■

Example 1.8
Let $\alpha : S \to T$ be a mapping between finite sets such that the number of elements of S is less than that of T. Can α be onto? Explain.

Solution.
If T has more elements than S and since each element of S is associated to exactly one element in T then some elements in T has no preimages in S. Thus, α can not be onto.■

Next, you recall from calculus that a function α from $\mathbb{R}$ to $\mathbb{R}$ is one-to-one if and only if its graph satisfies the horizontal line test, i.e. every horizontal line crosses the graph of α at most once. That is, no two different members of the domain of α share the same member in the range. This concept can be generalized to any sets.

Definition 1.4
A mapping $\alpha : S \longrightarrow T$ is called **one-to-one** (or **injective**) if and only if for any $x_1, x_2 \in S$

$$x_1 \neq x_2 \ \ \textit{implies} \ \ \alpha(x_1) \neq \alpha(x_2)$$

that is, unequal elements in the domain of α have unequal images in the range.

Example 1.9
In terms of a Venn diagram, a mapping is one-to-one if and only if no two arrows point to a same member in the codomain. The function α in Example 1.3 is one-to-one whereas β is not since $x \neq z$ but $\beta(x) = \beta(z)$. ■

Example 1.10
Show that the functions $\alpha(x) = x^2$ and $\beta(x) = \sin x$ defined on the set $\mathbb{R}$ are not one-to-one functions. Modify the domain of each so that they become one-to-one functions.

Solution.
The domain of α is the set of all real numbers. Since $\alpha(-1) = \alpha(1) = 1$ then α is not one-to-one on its domain. Similarly, β is defined for all real numbers. Since $\beta(\frac{\pi}{2}) = \beta(\frac{5\pi}{2}) = 1$ then β is not one-to-one. These functions become one-to-one if α is restricted to either the interval $[0, \infty)$ or the interval $(-\infty, 0]$ whereas β can be restricted to intervals of the form $\left[(2k-1)\frac{\pi}{2}, (2k+1)\frac{\pi}{2}\right]$, where k is an integer.■

Example 1.11
Let $\alpha : S \to T$ be a mapping between two finite sets such that S has more elements than its range. Can α be one-to-one? Explain.

Solution.
If S has more elements than $\alpha(S)$ then there must exist at least two distinct members of S with the same image in $\alpha(S)$. Thus, by Definition 1.4, α can not be one-to-one.■

An equivalent statement to

$$x_1 \neq x_2 \ \ \textit{implies} \ \ \alpha(x_1) \neq \alpha(x_2) \ \ (x_1, x_2 \in S)$$

is its contrapositive, i.e. the statement

$$\alpha(x_1) = \alpha(x_2) \ \ \textit{implies} \ \ x_1 = x_2.$$

This latter condition is usually much easier to work with than the one given in the definition of one-to-one as shown in the next example.

Example 1.12
The mapping $\alpha(x) = 2x - 1$ defined on $\mathbb{R}$ is a one-to-one function. To see this, suppose that $x_1 = x_2$. Then multiplying both sides of this equality by 2 to obtain $2x_1 = 2x_2$. Finally, subtract 1 from both sides to obtain $2x_1 - 1 = 2x_2 - 1$. That is, $\alpha(x_1) = \alpha(x_2)$. Hence, α is one-to-one. ■

A mapping can be one-to-one but not onto, onto but not one-one, neither one-to-one nor onto, or both one-to-one and onto. See Example 1.13. We single out the last case in the next definition.

Definition 1.5
A mapping $\alpha : S \longrightarrow T$ is called a **one-to-one correspondence** (or **bijective**) if and only if α is both one-to-one and onto.

Example 1.13
(a) The mapping $\alpha : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $\alpha(x) = x^3$ is a one-to-one correspondence. To see this, for any $y \in \mathbb{R}$ we can find an $x \in \mathbb{R}$ such that $\alpha(x) = y$. Indeed, let $x = \sqrt[3]{y}$. Hence, α is onto. Now, if $x_1^3 = x_2^3$ then taking the cube root of both sides to obtain $x_1 = x_2$. That is, α is one-to-one.
(b) The function $\beta : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $\beta(n) = 2n$ is one-to-one but not onto. Indeed, $\beta(n_1) = \beta(n_2)$ implies $n_1 = n_2$ so that β is one-to-one. The fact that β is not onto follows from the fact that no arrow is pointed to the numbers 1, 3, 5, etc.
(c) The function $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$\beta(n) = \begin{cases} \frac{n+1}{2} & \text{if n is odd} \\ \frac{n}{2} & \text{if n is even} \end{cases}$$

is onto. To see this, let n be a positive integer. If n is odd then $m = 2n-1 \in \mathbb{N}$ is also odd. Moreover, $\beta(m) = \frac{m+1}{2} = n$. Now, if n is even then $m = 2n \in \mathbb{N}$ is also even and $\beta m = \frac{m}{2} = n$. β is not one-to-one since $\beta 3 = \beta 4 = 2$.
(d) The Ceiling function $\alpha(x) = \lceil x \rceil$ is the piecewise defined function given by

$$\lceil x \rceil = \text{smallest integer greater than or equal to x.}$$

α is neither one-to-one nor onto as seen in Figure 1.3.■

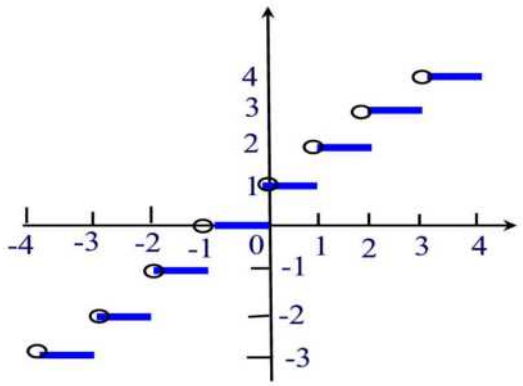


Figure 1.3

Review Problems

Exercise 1.1
A Sequence of real numbers $\{a_n\}_{n=1}^{\infty}$ can be viewed as a function α. Find the domain and the codomain of α.

Exercise 1.2
Determine whether $\alpha : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ given by

$$\alpha\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{a+c}{b+d}$$

is a mapping.

Exercise 1.3
Find an example of a function familiar to you from calculus that satisfies the eqution $\alpha(x+y) = \alpha(x) \cdot \alpha(y)$. Such a function will be called a **homomorphism.**

Exercise 1.4
Define a mapping $\alpha : \mathbb{N} \to \mathbb{N}$ such that the equation $\alpha(x) = n$ has two solutions for each $n \in \mathbb{N}$.

Exercise 1.5
Consider the functions $\alpha : \mathbb{R} \to \mathbb{R}$ defined by $\alpha(x) = x + 1$, $\beta : \mathbb{R} - \{1\} \to \mathbb{R}$ defined by $\beta(x) = \frac{x^2-1}{x-1}$, and $\gamma : \mathbb{R} \to \mathbb{R}$ defined by $\gamma(x) = \frac{2x+2}{2}$. Which are equal?

Exercise 1.6
A function can be defined in terms of a subset of a Cartesian product of two sets. More precisely, if S and T are two nonempty sets and G is a subset of the Cartesian product $S \times T = \{(a, b) : a \in S \text{ and } b \in T\}$ such that each first component of an element of G is associated to exactly one second component then G defines a function from S to T.
Let $S = \{1, 2, 3\}$ and $T = \{u, v, w\}$. Consider the subsets $\alpha = \{(1, u), (2, v), (3, w)\}$, $\beta = \{(1, u), (2, u), (3, u)\}$, $\gamma = \{(1, u), (3, w)\}$, and $\delta = \{(1, u), (2, u), (2, v), (3, w)\}$ of $S \times T$. Determine those who are functions and those who are not.

Exercise 1.7
Let $S = \{w, x, y, z\}$ and $T = \{1, 2, 3, 4\}$, and define $\alpha : S \to T$ by $\alpha(w) = 2, \alpha(x) = 4, \alpha(y) = 2, \alpha(z) = 2$ and $\beta(w) = 4, \beta(x) = 2, \beta(y) = 3, \beta(z) = 1$.

(a) Is α one-to-one? Is β one-to-one?Is α onto? Is β onto?
(b) Let $A = \{w, y\}$ and $B = \{x, y, z\}$. Determine each of the following subsets of $T : \alpha(A), \beta(B), \alpha(A \cap B), \beta(A \cup B)$.

Exercise 1.8
Assume that S and T are finite sets containing m and n elements, respectively.

(a) How many mappings are there from S to T?
(b) How many one-to-one mappings are there from S to T?

Exercise 1.9
A mapping $f : \mathbb{R} \to \mathbb{R}$ is one-to-one iff each horizontal line intersects the graph of f at most once.

(a) Formulate a similar condition for $f : \mathbb{R} \to \mathbb{R}$ to be onto.
(b) Formulate a similar condition for $f : \mathbb{R} \to \mathbb{R}$ to be one-to-one and onto.

Exercise 1.10
Suppose X is a set with 6 elements and Y is a finite set with n elements. Complete the following.

1) There exists an injective $\alpha : X \to Y$ if and only if n_____.
2) There exists surjective $\alpha : X \to Y$ iff n_____.
3) There exists a bijective $\alpha : X \to Y$ iff n_____.

Exercise 1.11
(a) What does it mean for a function not to be one-to-one?
(b) What does it mean for a function not to be onto?

Exercise 1.12
Let α, β, γ be mappings from $\mathbb{Z}$ to $\mathbb{Z}$ defined by $\alpha(n) = 2n, \beta(n) = n + 1$ and $\gamma(n) = n^3$ for each $n \in \mathbb{Z}$.

(a) Which of the three mappings are onto?

(b) Which of the three mappings are one-to-one?
(c) Determine $\alpha(\mathbb{N}), \beta(\mathbb{N})$, and $\gamma(\mathbb{N})$.

Exercise 1.13
For each ordered pairs (a, b) of integers define a mapping $\alpha_{a,b} : \mathbb{Z} \to \mathbb{Z}$ by $\alpha_{a,b}(n) = an + b$.

1. For which pairs (a, b) is $\alpha_{a,b}$ onto?
2. For which pairs (a, b) is $\alpha_{a,b}$ one-to-one?

Exercise 1.14
For each $n \in \mathbb{Z}$, define the mapping $f_n : \mathbb{Z} \to \mathbb{Z}$ by $f_n(x) = nx$.

(a) For which values of n is f_n onto ?
(b) For which values of n is f_n one-to-one ?

Exercise 1.15
Prove that if A and B are finite sets and $f : A \to B$ is a one-to-one correspondence then A and B have the same number of elements.

Exercise 1.16
Let $\alpha : S \to T$ be a function. Suppose that S and T are finite sets with the same number of elements. Show that α is one-to-one if and only if it is onto.

Exercise 1.17
Let S and T be two nonempty sets. Prove that there is a one-to-one correspondence between $S \times T$ and $T \times S$.

Exercise 1.18
Let S be a nonempty set. Show that the identity mapping ι_S is one-to-one and onto.

Exercise 1.19
(a) Show that $\alpha : \mathbb{R} \to [-1, 1]$ defined by $\alpha(x) = \sin x$ is surjective but not injective.
(b) Show that $\beta : [0, \frac{\pi}{2}] \to \mathbb{R}$ defined by $\beta(x) = \sin x$ is injective but not surjective.
(c) Show that $\gamma : [0, \frac{\pi}{2}] \to [0, 1]$ defined by $\gamma(x) = \sin x$ is bijective.

Exercise 1.20
A small town has only 500 residents. Must there be 2 residents with the same birthday (month and day)? Why?

Exercise 1.21
Let $f : A \to B$ and let $\{E_\alpha\}_{\alpha\in\Lambda}$ be a collection of subsets of A. The union of $E_\alpha s$ is defined by $\cup_\alpha E_\alpha = \{x \in E_\alpha : for\ some\ \alpha \in \Lambda\}$. Similarly, the intersection is defined by $\cap_\alpha E_\alpha = \{x \in E_\alpha : \forall\alpha \in \Lambda\}$. Prove that

1. $f[\cup_\alpha E_\alpha] = \cup_\alpha f[E_\alpha]$,
2. $f[\cap_\alpha E_\alpha] \subseteq \cap_\alpha f[E_\alpha]$.

Exercise 1.22
Construct an example of a mapping $\alpha : S \to T$ such that

(1) $\alpha[E \cap F] \neq \alpha[E] \cap \alpha[F]$, where $E, F \subseteq S$.
(2) Show that equality in (1) holds only if α is one-to-one.

Exercise 1.23
Let A_1, A_2, B_1, and B_2 be nonempty sets such that $A_1 \cap A_2 = \emptyset$ and $B_1 \cap B_2 = \emptyset$. Suppose that $f_i : A_i \to B_i$, $(i = 1, 2)$, are given functions. Define $f : A_1 \cup A_2 \to B_1 \cup B_2$ by

$$f(x) = \begin{cases} f_1(x) & \text{if } x \in A_1 \\ f_2(x) & \text{if } x \in A_2 \end{cases}$$

Prove:
(a) f is one-to-one if and only if f_1 and f_2 are one-to-one.
(b) f is onto if and only if f_1 and f_2 are onto.

2 Composition. Invertible Mappings

In this section we discuss two procedures for creating new mappings from old ones, namely, the composition of mappings and invertible mappings.

Composition of Two Mappings

Composition is the combination of two or more mappings to form a single new mapping.

Definition 2.1

Let $\alpha : S \longrightarrow T$ and $\beta : T \longrightarrow U$ be two mappings. We define the **composition** of α followed by β, denoted by $\beta \circ \alpha$, to be the mapping

$$(\beta \circ \alpha)(x) = \beta(\alpha(x))$$

for all $x \in \alpha$.

Note carefully that in the notation $\beta \circ \alpha$ the mapping on the right is applied first. See Figure 2.1

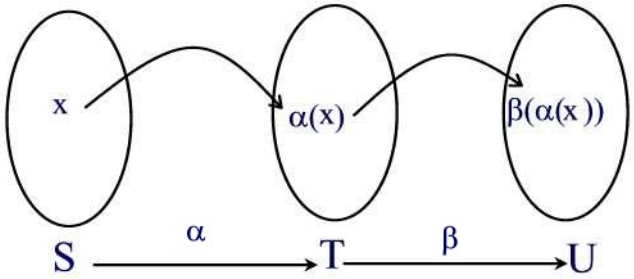


Figure 2.1

Example 2.1

Let α and β be given by the Venn diagram of Figure 2.2.

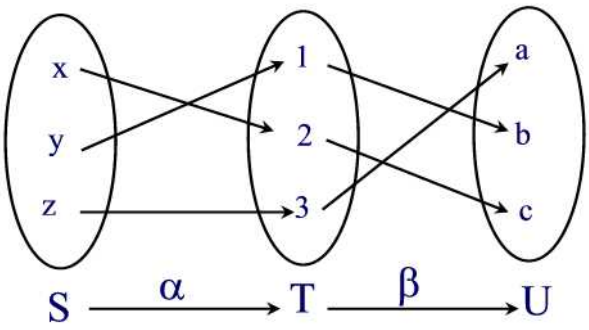


Figure 2.2

Then

$$\begin{array}{rcccccl} (\beta \circ \alpha)(x) & = & \beta(\alpha(x)) & = & \beta(2) & = & c \\ (\beta \circ \alpha)(y) & = & \beta(\alpha(y)) & = & \beta(1) & = & b \\ (\beta \circ \alpha)(z) & = & \beta(\alpha(z)) & = & \beta(3) & = & a \end{array}$$ ■

Example 2.2
Let f and g be two functions given as sets of (x, y) points:

$f = \{(-2, 3), (-1, 1), (0, 0), (1, -1), (2, -3)\}$, $g = \{(-3, 1), (-1, -2), (0, 2), (2, 2), (3, 1)\}$.

Find $(f \circ g)(0)$.

Solution.
Since $g(0) = 2$ and $f(2) = -3$ then $(f \circ g)(0) = f(g(0)) = f(2) = -3$.■

Example 2.3
The following example shows how to find the formula of the composition mapping given the formulas for both α and β. Let $\alpha : \mathbb{R} \longrightarrow \mathbb{R}$ and $\beta : \mathbb{R} \longrightarrow \mathbb{R}$ be defined by $\alpha(x) = x^2 + 2$ and $\beta(x) = x - 1$ respectively. Find $\beta \circ \alpha$ and $\alpha \circ \beta$.

Solution.
Using the definition of composition we have

$$\begin{array}{rcc} (\beta \circ \alpha)(x) & = & \beta(\alpha(x)) \\ & = & \beta(x^2 + 2) \\ & = & (x^2 + 2) - 1 = x^2 + 1 \end{array}$$

while

$$\begin{aligned}(\alpha \circ \beta)(x) &= \alpha(\beta(x)) \\ &= \alpha(x-1) \\ &= (x-1)^2 + 2 \\ &= x^2 - 2x + 3\end{aligned}$$

This example, shows that, in general, $\alpha \circ \beta$ and $\beta \circ \alpha$ need not be equal. ■

In the following two theorems, we discuss the question of either composing two onto mappings or two one-to-one mappings.

Theorem 2.1
Assume that $\alpha : S \longrightarrow T$ and $\beta : T \longrightarrow U$ are two mappings.

(a) If α and β are onto then the composition $\beta \circ \alpha$ is also onto.
(b) If $\beta \circ \alpha$ is onto then β is onto.

Proof.
(a) The mapping $\beta \circ \alpha$ is a mapping from S to U. So, let $u \in U$. Since β is onto then there is a $t \in T$ such that $\beta(t) = u$. Now, since α is onto then there is an $s \in S$ such that $\alpha(s) = t$. Thus, given $u \in U$ we can find an $s \in S$ such that $(\beta \circ \alpha)(s) = \beta(\alpha(s)) = \beta(t) = u$. This says that $\beta \circ \alpha$ is onto.

(b) Suppose now that $\beta \circ \alpha$ is onto. Pick an arbitrary element $u \in U$. Since $\beta \circ \alpha$ is onto then there is an $s \in S$ such that $\beta(\alpha(s)) = u$. Let $t = \alpha(s) \in T$. Then $\beta(t) = u$. This shows that β is onto. ■

Example 2.4
Consider the two mappings $\alpha : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $\alpha(n) = 2n$ and $\beta : \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$\beta(n) = \begin{cases} \frac{n+1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even} \end{cases}$$

Show that β and $\beta \circ \alpha$ are onto but α is not.

Solution.
First, we show that β is onto. Let $n \in \mathbb{N}$. If n is even then $2n$ is even and $\beta(2n) = n$. If n is odd then $2n - 1$ is odd and $\beta(2n - 1) = n$. Thus, β is onto. One can easily check that $\beta \circ \alpha = \iota_{\mathbb{N}}$. Since the identity map is onto then $\beta \circ \alpha$ is onto. The mapping α is not onto since odd positive integers do not have preimages.■

Theorem 2.2
Assume that $\alpha : S \longrightarrow T$ and $\beta : T \longrightarrow U$ are two mappings.

(a) If α and β are one-to-one then $\beta \circ \alpha$ is also one-to-one.
(b) If $\beta \circ \alpha$ is one-to-one then α is one-to-one.

Proof.
(a) Suppose that α and β are one-to-one. Suppose that $(\beta \circ \alpha)(s_1) = (\beta \circ \alpha)(s_2)$ for some $s_1, s_2 \in S$. This implies that $\beta(\alpha(s_1)) = \beta(\alpha(s_2))$. Since β is one-to-one then $\alpha(s_1) = \alpha(s_2)$. Now since α is one-to-one then $s_1 = s_2$. Thus, $\beta \circ \alpha$ is one-to-one.

(b) Assume that $\beta \circ \alpha$ is one-to-one. Suppose that $\alpha(s_1) = \alpha(s_2)$. Since β is a well-defined mapping then $\beta(\alpha(s_1)) = \beta(\alpha(s_2))$. Since $\beta \circ \alpha$ is one-to-one then $s_1 = s_2$. This shows that α is one-to-one. ■

Example 2.5
Consider the two mappings $\alpha : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $\alpha(n) = 2n$ and $\beta : \mathbb{N} \longrightarrow \mathbb{N}$ defined by

$$\beta(n) = \begin{cases} \frac{n+1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even} \end{cases}$$

Show that α and $\beta \circ \alpha$ are one-to-one but β is not.

Solution.
Since $\alpha(n_1) = \alpha(n_2)$ implies $2n_1 = 2n_2$ and this in turns implies that $n_1 = n_2$ then α is one-to-one. Since $\beta \circ \alpha = \iota_{\mathbb{N}}$ and $\iota_{\mathbb{N}}$ is one-to-one then $\beta \circ \alpha$ is one-to-one. The mapping β is not one-to-one since $\beta(1) = \beta(2)$ with $1 \neq 2$.■

Example 2.6
Let $\alpha : S \longrightarrow T, \beta : T \longrightarrow U$, and $\gamma : U \longrightarrow V$ be three mappings such that $\gamma \circ (\beta \circ \alpha)$ and $(\gamma \circ \beta) \circ \alpha$ are well defined. Show that

$$\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$$

Solution.
Note first that the mappings $\gamma \circ (\beta \circ \alpha)$ and $(\gamma \circ \beta) \circ \alpha$ have the same codomain V. The following argument shows that $\gamma \circ (\beta \circ \alpha)$ and $(\gamma \circ \beta) \circ \alpha$ have the

same range.
Let s be in S then

$$\begin{aligned}[\gamma \circ (\beta \circ \alpha)](s) &= \gamma((\beta \circ \alpha)(s)) \\ &= \gamma(\beta(\alpha(s))) \\ &= (\gamma \circ \beta)(\alpha(s)) \\ &= [(\gamma \circ \beta) \circ \alpha](s)\end{aligned}$$ ■

Invertible Mappings

In this section we consider special kind of mappings which have the property that for each output value we can work our way backwards to find the unique input that produced it.

Let $\alpha : S \longrightarrow T$ and $\beta : T \longrightarrow S$ be two given mappings.

Definition 2.2
We say that β is an **inverse** of α if and only if $\beta \circ \alpha = \iota_S$ and $\alpha \circ \beta = \iota_T$. In this case we say that α is **invertible.**

An invertible mapping has a unique inverse as shown in the next theorem.

Theorem 2.3
If $\alpha : S \to T$ is invertible then its inverse is unique.

Proof.
Suppose that $\alpha_1 : T \longrightarrow S$ and $\alpha_2 : T \longrightarrow S$ are two inverses of α. Then from Definition 2.2 we have $\alpha_1 \circ \alpha = \alpha_2 \circ \alpha = \iota_S$ and $\alpha \circ \alpha_1 = \alpha \circ \alpha_2 = \iota_T$. We want to show that the mappings α_1 and α_2 are equal. That is, we must show that $\alpha_1(t) = \alpha_2(t)$ for each $t \in T$. Indeed,

$$\begin{aligned}\alpha_1(t) &= \iota_S(\alpha_1(t)) \\ &= (\alpha_2 \circ \alpha)((\alpha_1(t)) \\ &= \alpha_2((\alpha \circ \alpha_1)(t)) \\ &= \alpha_2(\iota_T(t)) \\ &= \alpha_2(t)\end{aligned}$$

Thus, $\alpha_1 = \alpha_2$. ■

Definition 2.3
We denote the unique inverse of a mapping α by α^{-1}.

Example 2.7
Show that the mapping α in Example 2.1 is invertible and find its inverse.

Solution
The inverse of α is defined by

$$\alpha^{-1}(1) = y, \quad \alpha^{-1}(2) = x, \quad \alpha^{-1}(3) = z.$$

One can easily check that $\alpha \circ \alpha^{-1} = \iota_T$ and $\alpha^{-1} \circ \alpha = \iota_S$ where $S = \{x, y, z\}$ and $T = \{1, 2, 3\}$. Looking closely at the Venn diagram we see that α^{-1} is gotten by reversing the direction of the arrows under α. ■

The following theorem characterizes those mappings that are invertible.

Theorem 2.4
A mapping $\alpha : S \longrightarrow T$ is invertible if and only if α is one-to-one and onto.

Proof.
Suppose first that α is invertible with inverse $\alpha^{-1} : T \longrightarrow S$. We will show that α is both one-to-one and onto. To see that α is one-to-one, we assume that $\alpha(s_1) = \alpha(s_2)$, where $s_1, s_2 \in S$, and show that $s_1 = s_2$. Indeed,

$$\begin{aligned} s_1 &= \iota_S(s_1) = (\alpha^{-1} \circ \alpha)(s_1) \\ &= \alpha^{-1}(\alpha(s_1)) = \alpha^{-1}(\alpha(s_2)) \\ &= (\alpha^{-1} \circ \alpha)(s_2) = \iota_S(s_2) = s_2 \end{aligned}$$

Next, to show that α is onto we pick an arbitrary member t in T and show that there is an s in S such that $\alpha(s) = t$. Indeed, since t is in T then $t = \iota_T(t) = (\alpha \circ \alpha^{-1})(t) = \alpha(\alpha^{-1}(t)) = \alpha(s)$ where $s = \alpha^{-1}(t) \in S$. This shows that α is onto.
Conversely, suppose that α is one-to-one and onto. We will find a mapping $\beta : T \longrightarrow S$ such that $\alpha \circ \beta = \iota_T$ and $\beta \circ \alpha = \iota_S$. Let $t \in T$. Since α is onto then there is an element $s \in S$ such that $\alpha(s) = t$. s is unique, for if $s' \in S$ is such that $\alpha(s') = t$ then $\alpha(s) = \alpha(s')$. But α is one-to-one so that $s = s'$. Hence, for each $t \in T$ there is a unique $s \in S$ such that $\alpha(s) = t$. Define $\beta : T \longrightarrow S$ by $\beta(t) = s$. Then β satisfies the following properties:

$$(\alpha \circ \beta)(t) = \alpha(\beta(t)) = \alpha(s) = t, \quad t \in T$$

and

$$(\beta \circ \alpha)(s) = \beta(\alpha(s)) = \beta(t) = s, \quad s \in S.$$

That is, $\alpha \circ \beta = \iota_T$ and $\beta \circ \alpha = \iota_S$. According to Definition 2.2, α is invertible■

Example 2.8
Show that the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = x^2$ is not invertible.

Solution.
Indeed, since $f(-1) = f(1)$ and $1 \neq -1$ then f is not one-to-one. By Theorem 2.4, f can't be invertible.■

Example 2.9
Show that the function $f(x) = x^3$ is invertible and find a formula for the inverse.

Solution.
We have seen (See Example 1.13(a), Sec. 1.1) that $f(x) = x^3$ is one-to-one and onto so that it has an inverse. To find the inverse we proceed as follows:

1. Replace $f(x)$ by y to obtain $y = x^3$.
2. Switch the letters x and y to obtain $x = y^3$.
3. Solve for y in terms of x to obtain $y = \sqrt[3]{x}$.
4. Replace y by $f^{-1}(x)$ to obtain $f^{-1}(x) = \sqrt[3]{x}$.■

Theorem 2.5
Let $\alpha : S \longrightarrow T$ and $\beta : T \longrightarrow U$ be two given mappings.

(a) If α is invertible then α^{-1} is also invertible with $(\alpha^{-1})^{-1} = \alpha$.
(b) If α and β are both invertible then $\beta \circ \alpha$ is invertible with inverse $(\beta \circ \alpha)^{-1} = \alpha^{-1} \circ \beta^{-1}$.

Proof.
(a) Suppose α is invertible with inverse $\alpha^{-1} : T \longrightarrow S$. Since $\alpha^{-1} \circ \alpha = \iota_S$ and $\alpha \circ \alpha^{-1} = \iota_T$ then by Definition 2.2, α^{-1} is invertible with inverse α.

(b) Suppose α and β are invertible. Then $\alpha^{-1} \circ \alpha = \iota_S, \beta^{-1} \circ \beta = \alpha \circ \alpha^{-1} = \iota_T$, and $\beta \circ \beta^{-1} = \iota_U$. Thus, for any $u \in U$ we have

$$\begin{aligned}
[(\beta \circ \alpha) \circ (\alpha^{-1} \circ \beta^{-1})](u) &= [\beta \circ (\alpha \circ \alpha^{-1}) \circ \beta^{-1}](u) \\
&= \beta \circ (\iota_T(\beta^{-1}(u)) \\
&= (\beta \circ \beta^{-1})(u) \\
&= \iota_U(u) = u
\end{aligned}$$

It follows that $(\beta \circ \alpha) \circ (\alpha^{-1} \circ \beta^{-1}) = \iota_U$. Similarly, one can show that $(\alpha^{-1} \circ \beta^{-1}) \circ (\beta \circ \alpha) = \iota_S$. By Definition 2.2, $\beta \circ \alpha$ is invertible with inverse $\alpha^{-1} \circ \beta^{-1}$.■

Review Problems

Exercise 2.1
Let f and g be two functions given as sets of (x, y) points:

$f = \{(-2, 3), (-1, 1), (0, 0), (1, -1), (2, -3)\}$, $g = \{(-3, 1), (-1, -2), (0, 2), (2, 2), (3, 1)\}$.

Find $(g \circ f)(1)$.

Exercise 2.2
Let $f(x) = \log_5(x + 1)$ and $g(x) = x^2 + 1$.

(a) Find $(g \circ f)(x)$.
(b) Find the domain and range of $g \circ f$.
(c) Evaluate $(g \circ f)(4)$.

Exercise 2.3
Given $h(x) = (x+1)^2 + 2(x+1) - 3$. Determine two functions $f(x)$ and $g(x)$ such that $h(x) = f(g(x))$.

Exercise 2.4
You work 40 hours a week at a furniture store. You receive a \$220 weekly salary, plus a 3% commision on sales over \$5000. Assume that you sell enough this week to get the commission. Given the functions $f(x) = 0.03x$ and $g(x) = x - 5000$, which of $(f \circ g)(x)$ and $(g \circ f)(x)$ represents your commission?

Exercise 2.5
Let α, β, and γ be mappings from $\mathbb{Z}$ to $\mathbb{Z}$ defined by $\alpha(n) = 2n, \beta(n) = n+1$, and $\gamma(n) = n^2$. Write a formula for each of the composition below. Also, determine the range in each case.

(i) $\alpha \circ \alpha$
(ii) $\alpha \circ \beta$
(iii) $\beta \circ \gamma$.

Exercise 2.6
Prove that if $\alpha : S \to T$ then $\alpha \circ \iota_S = \alpha$ and $\iota_T \circ \alpha = \alpha$.

Exercise 2.7
Consider f and g, mappings $\mathbb{R}$ to $\mathbb{R}$, defined by $f(x) = \sin x$ and $g(x) = 2x$. Is $f \circ g$ equal to $g \circ f$?

Exercise 2.8
(a) Prove that if $\alpha : S \to T, \beta : T \to U, \gamma : T \to U$, α is onto, and $\beta \circ \alpha = \gamma \circ \alpha$, then $\beta = \gamma$.
(b) Give an example to show that the condition "α is onto" cannot be omitted from Part (a).

Exercise 2.9
(a) Prove that if $\beta : S \to T, \gamma : S \to T, \alpha : T \to U$, α is one-to-one, and $\alpha \circ \beta = \alpha \circ \gamma$, then $\beta = \gamma$.
(b) Give an example to show that the condition "α is one-to-one" cannot be omitted from Part (a).

Exercise 2.10
Let $f : \mathbb{R} \to \mathbb{R}$ be the map given by $f(x) = x^2$. Let

$$A = [1, 2] = \{x \in \mathbb{R} |\ 1 \leq x \leq 2\},$$

$$B = (-1, 1) = \{x \in \mathbb{R} |\ -1 < x < 1\},$$

$$C = (4, 9) = \{x \in \mathbb{R} |\ 4 < x < 9\},$$

$$D = [0, 9] = \{x \in \mathbb{R} |\ 0 \leq x \leq 9\}.$$

Find

(a) $f[A]$ (b) $f[B]$ (c) $f^{-1}[C]$ (d) $f^{-1}[D]$.

Exercise 2.11
Suppose that $\alpha : S \longrightarrow T$ is a given mapping and $A \subseteq S$. We know that $\alpha(A)$ is empty only when A is empty. If $B \subseteq T$ then we define

$$\alpha^{-1}(B) = \{x \in S : \alpha(x) \in B\}.$$

Give an example of a mapping α such that $B \neq \emptyset$ but $\alpha^{-1}(B) = \emptyset$.(Hint: Use the mapping in Exercise 2.10)

Exercise 2.12
Let $f : A \to B$ and let $\{F_\alpha\}_{\alpha\in\Lambda}$ be a collection of subsets of B. Prove that

1. $f^{-1}[\cup_\alpha F_\alpha] = \cup_\alpha f^{-1}[F_\alpha]$,
2. $f^{-1}[\cap_\alpha F_\alpha] = \cap_\alpha f^{-1}[F_\alpha]$.

Exercise 2.13
Let $S = \{-2, 1, 2\}$ and $T = \{1, 4, 9\}$. Consider the mapping $\alpha : S \to T$ defined by

$$\alpha(-2) = 4, \alpha(1) = 1, \alpha(2) = 4.$$

(a) Show that α is neither one-to-one nor onto.
(b) Show that $\alpha^{-1}(\alpha(A)) \neq A$, where $A = \{-2, 1\}$.
(c) Show that $\alpha(\alpha^{-1}(B)) \neq B$, where $B = \{4, 9\}$.

Exercise 2.14
(a) Let $\alpha : S \to T$, where S and T are nonempty. Prove that α has the property $\alpha^{-1}(\alpha(A)) = A$ for every subset of S if and only if α is one-to-one.
(b) Prove that α has the property that $\alpha(\alpha^{-1}(B)) = B$ for every subset B of T if and only if α in onto.

Exercise 2.15
Let $\alpha : S \to T$ and $\beta : T \to U$. Show that if $\beta \circ \alpha$ is invertible then β is onto and α is one-to-one.

3 Binary Operations

We are used to addition and multiplication of real numbers. These operations combine two real numbers to generate a unique single real number. So we can look at these operations as functions on the set

$$\mathbb{R} \times \mathbb{R} = \{(a, b) : a \in \mathbb{R} \; and \; b \in \mathbb{R}\}$$

defined by

$$\begin{array}{rccc} + & : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & (a, b) & \longrightarrow & a + b \end{array}$$

and

$$\begin{array}{rccc} \cdot & : & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & (a, b) & \longrightarrow & a \cdot b \end{array}$$

These operations are examples of a binary operation. The general definition of a binary operation is as follows.

Definition 3.1
A **binary operation** on a set S is a mapping $*$ that assigns to each ordered pair of elements of S a uniquely determined element of S. That is, $* : S \times S \longrightarrow S$ is a mapping. The set S is said to be **closed** under the operation $*$.

The image $*(a, b)$ will be denoted by $a * b$.

Example 3.1
Addition and multiplication are binary operations on the set $\mathbb{Z}$ of integers so that this set is closed under these operations. However, $\mathbb{Z}$ is not closed under the operation of division since $1 \div 2$ is not an integer.■

Example 3.2
The "ordered pair" statement in Definition 3.1 is critical. For example, consider the binary operation $*$ defined on the set $\mathbb{N}$ by $a * b = a^b$. Then $2 * 3 = 2^3 = 8$ and $3 * 2 = 3^2 = 9$. That is, $2 * 3 \neq 3 * 2$.■

Example 3.3 *(Cayley's Tables)*
The idea of a binary operation is just a way to produce an element of a set from a given pair of ordered elements of the same set. In the case of a finite set we could list the rule in a table which we'll call a *multiplication table* or Cayley's table. For example, the following is the multiplication table of a binary operation $* : \{a, b\} \longrightarrow \{a, b\}$.

*	a	b
a	a	b
b	b	a ■

In studying binary operations on sets, we tend to be interested in those operations that have certain properties which we discuss next.

Definition 3.2
A binary operation $*$ on a set S is said to be **associative** if it satisfies the associative law:

$$a * (b * c) = (a * b) * c$$

for all $a, b, c \in S$.

The associative property allows us to speak of $a * b * c$ without having to worry about whether we should find the answer to $a * b$ first and then that answer "multiplied" by c rather than evaluate $b * c$ first and then "multiply" a with that answer. Which ever way we process the expression we end up with the same element of the set. Note though that it does not say we can do the product in any order (i.e. $a*b$ and $b*a$ may not have the same value).

Example 3.4
1. The operations " $+$ " and $\cdot$ on $\mathbb{R}$ are associative.
2. The operation " $-$ " on $\mathbb{R}$ is not associative since $2-(3-4) \neq (2-3)-4$. (Notice that if the associative law fails for just one triple (a, b, c) then the operation is not associative).
3. The operation $*$ defined by $a * b = a^b$ on the set $\mathbb{N}$ is not associative since $2 * (3 * 2) = 512$ and $(2 * 3) * 2 = 64$.■

Definition 3.3
A binary operation $*$ on a set S is said to be **commutative** if it satisfies the condition:

$$a * b = b * a$$

for all $a, b, \in S$. In this case, the order in which elements are combined does not matter.

Remark 3.1
When a set with a binary operation is given by a Cayley's table then the

operation is commutative if and only if equal elements appear in all positions that are symmetrically placed relative to the diagonal from upper left to lower right. That is, to check whether an operation defined by a Cayley's table is commutative, simply draw a diagonal line from upper left to lower right, and see if the table is symmetric about this line. For example, the operation $*$ defined by the table below is commutative.

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Example 3.5
The binary operations of addition and multiplication on $\mathbb{R}$ are both commutative. However, the binary operation of subtraction on $\mathbb{R}$ does not satisfy the commutative law since $5 - 7 \neq 7 - 5$.■

Example 3.6
The binary operation on $\mathbb{R}$ defined by $a * b = a + b - 1$ is commutative since

$$a * b = a + b - 1 = b + a - 1 = b * a.$$■

Example 3.7
Show that the binary operation on $\mathbb{R}$ defined by $a * b = 1 + ab$ is commutative but not associative.

Solution.
For any real numbers a and b we have $a * b = 1 + ab = 1 + ba = b * a$ where we used the fact that multiplication in $\mathbb{R}$ is commutative. Now, by letting $a = 0, b = 1$, and $c = -1$ then $a * (b * c) = a * 0 = 1$ and $(a * b) * c = 1 * c = 0$. Thus, $*$ is not associative.■

Definition 3.4
Let S be a set on which there is a binary operation $*$. An element e of this set is called a **left identity** if for all $a \in S$, we have $e * a = a$. Similarly, an element e is a **right identity** if $a * e = a$ for each $a \in S$.

Example 3.8
Given a binary operation on a set.

1. There might be left identities which are not right identities and vice-versa. For example, the operation $a * b = a$ on the set $\mathbb{R}$ has 2 as a right identity which is not a left identity. The set $\mathbb{R}$ with the operation $a * b = b$ has 2 as a left identity which is not a right identity.

2. There might be many left or right identity elements. The set $\mathbb{R}$ with the operation $a * b = a$, every number is a right identity. With the operation $a * b = b$, every number is a left identity.

3. There might be no left or right identity elements. For example, the set $\{2, 3, 4, \cdots\}$ has no left or right identity elements under the operation $a * b = a \cdot b$■

We tend to be familiar with the situation in which there is a unique identity. As soon as an operation has both a left and a right identity, they are necessarily unique and equal as shown in the next theorem.

Theorem 3.1
If S is a set with a binary operation $*$ that has a left identity element e_1 and a right identity element e_2 then $e_1 = e_2 = e$.

Proof.
Let $e_1 \in S$ be a left identity element and $e_2 \in S$ be a right identity element. Then

$$\begin{aligned} e_1 &= e_1 * e_2 (since\ e_2\ is\ a\ right\ identity) \\ &= e_2 (since\ e_1\ is\ a\ left\ identity) \end{aligned}$$ ■

Definition 3.5
An element which is both a right and left identity is called the **identity element**(Some authors use the term two sided identity.) Thus, an element is an identity if it leaves every element unchanged.

Remark 3.2
Note that an identity (left or right or both) for one operation does not have to be an identity for another operation. Think of addition and multiplication on the reals where the identities are 0 and 1 respectively.

Example 3.9
The operation $a * b = a + b - 1$ on the set of integers has 1 as an identity element since $1 * a = 1 + a - 1 = a$ and $a * 1 = a + 1 - 1 = a$ for all integer a.■

Example 3.10
Show that the operation $a * b = 1 + ab$ on the set of integers $\mathbb{Z}$ has no identity element.

—noindent **Solution.**
If e is an identity element then we must have $a * e = a$ for all $a \in \mathbb{Z}$. In particular, $1 * e = e$. But this imply that $1 + e = 1$ or $e = 0$. Since $2 * 0 \neq 0$ then e does not exist.■

Whenever a set has an identity element with respect to a binary operation on the set, it is then in order to raise the question of inverses.

Definition 3.6
Suppose that an operation $*$ on a set S has an identity element e. Let $a \in S$. If there is an element $b \in S$ such that $a * b = e$ then b is called a **right inverse** of a. Similarly, if $b * a = e$ then b is called a **left inverse.**

Example 3.11
1. An element can have no left or right inverses. For example, the number 2 has no left or right inverse with respect to multiplication on the set of integers.

2. There might be a left inverse which is not a right inverse and vice versa. For example, consider the set $M(\mathbb{Z})$ of all functions from the set of integers into itself. Then the operation of composition is a binary operation on $M(\mathbb{Z})$. Consider the two functions $f(n) = 2n$ and

$$g(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ 4 & \text{if } n \text{ is odd} \end{cases}$$

Then $(g \circ f)(n) = n$ for all $n \in \mathbb{Z}$. That is, g is a left inverse of f. However, since

$$(f \circ g)(n) = \begin{cases} n & \text{if } n \text{ is even} \\ 8 & \text{if } n \text{ is odd} \end{cases}$$

then g is not a right inverse since $f \circ g \neq \iota_{\mathbb{Z}}$ ■

Suppose that an element $a \in S$ has both a left inverse and a right inverse with respect to a binary operation $*$ on S. Under what condition are the two inverses equal?

Theorem 3.2
Let S be a set with an associative binary operation $*$ and identity element e. Let $a, b, c \in S$ be such that $a * b = e$ and $c * a = e$. Then $b = c$.

Proof.
Indeed,

$$\begin{aligned} b &= e * b \\ &= (c * a) * b \\ &= c * (a * b) \\ &= c * e \\ &= c \end{aligned}$$ ■

Definition 3.7
If a has both a left and right inverse then we say that a has **two-sided inverse** or simply an **inverse** element.

Example 3.12
Consider the operation $*$ on the set of integers defined by $a * b = a + b - 1$. We will show that each integer has an inverse under this operation. Indeed, let x be an integer. Let y be a right inverse of x. Then $x * y = 1$. That is, $x + y - 1 = 1$. Solving for y we find $y = -x + 2$. This is also a left inverse of x since $(-x + 2) * x = -x + 2 + x - 1 = 1$.■

Review Problems

Exercise 3.1
Which of the following equations define operations on the set of integers? Of those that do, which are associative?Which are commutative? Which have identity elements?

1. $a * b = ab + 1$.
2. $a * b = a$.
3. $a * b = a^2 + b^2$.
4. $a * b = 3$.

Exercise 3.2
Does $(a, b) \to a^b$ define an operation on the set of all integers?

Exercise 3.3
If $*$ is an operation on S and T is a subset of S that is closed with respect to $*$ then two of the following three statements are necessarily true, but one may be false. Which two are true?
(a) If $*$ is associative on S, then $*$ is associative on T.
(b) If there is an identity element for $*$ on S, then there is an identity element for $*$ on T.
(c) If $*$ is commutative on S, then $*$ is commutative on T.

Exercise 3.4
Complete the following table in such a way that makes $*$ commutative.

*	a	b	c	d
a	a	b		d
b		c		
c	c	d	a	b
d		a		c

Exercise 3.5
Determine the smallest subset A of $\mathbb{Z}$ such that $2 \in A$ and A is closed with respect to addition.

Exercise 3.6
Determine the smallest subset A of $\mathbb{Q}$ such that $2 \in A$ and A is closed with respect to addition and division.

Exercise 3.7
How many different operations are there on a 1-element set? 2-element set? 3- element set? n-element set?

Exercise 3.8
Assume that $*$ is an associative operation on S and that $a \in S$. Let

$$C(a) = \{x \in S : a * x = x * a\}.$$

Prove that $C(a)$ is closed with respect to $*$.

Exercise 3.9
Assume that $*$ is an operation on S with identity element e and that

$$x * (y * z) = (x * z) * y$$

for all $x, y, z \in S$. Prove that $*$ is commutative and associative.

Exercise 3.10
List all the binary operations defined on set with two elements. (See Exercise 3.7)

Exercise 3.11
Given the Cayley's table for a binary operation $*$ defined on the set $S = \{a, b, c, d\}$

*	a	b	c	d
a	b	c	a	b
b	c	d	b	a
c	a	b	c	d
d	a	b	d	d

(a) Is $*$ commutative? Why?
(b) Determine whether there is an identity element in S for $*$.
(c) If there is an identity element, which elements have inverses?

Exercise 3.12
(a) Prove that the set of all injective mappings from S to S is closed under mapping composition.
(b) Prove that the set of all surjective mappings from S to S is closed under mapping composition.

Exercise 3.13
Let $\mathcal{M}$ be the set of all rectangular arrays of two rows and two columns

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Such an array is called a **2-by-2 matrix**. Let addition be defined for elements of $\mathcal{M}$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}$$

(a) Prove that $+$ is commutative.
(b) Prove that $+$ is associative.
(c) Find the identity element for addition.
(d) What is the additive inverse of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

in $\mathcal{M}$?

Exercise 3.14
Let $\mathcal{M}$ be the collection defined in the previous exercise. Define the operation of multiplication by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix}$$

(a) Prove that multiplication is associative.
(b) Prove that multiplication is not commutative.
(c) Find the identity element of $\mathcal{M}$ with respect to multiplication.
(d) Show that if $ad - bc \neq 0$ then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

Exercise 3.15
Suppose that there are two binary operations $*$ and $\#$ defined on a set S. We say that $*$ is **distributive** with respect to $\#$ if for all $a, b, c \in S$, we have

$$a * (b \# c) = (a * b) \# (a * c).$$

Prove that: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, for any sets A, B, C.

4 Composition of Mappings as a Binary Operation

For a nonempty set S, let $\mathcal{M}(S)$ be the set of all mappings from S to S. We have seen that composition of mappings defines a binary operation in $\mathcal{M}(S)$. In this section, we want to study the properties of this operation.
First, we discuss the question of commutativity and inverse elements. In general, composition is not commutative in $\mathcal{M}(S)$. Also, not every element of $\mathcal{M}(S)$ is invertible.

Example 4.1
Let S be a nonempty set.

(a) Show that composition in $\mathcal{M}(S)$ is not , in general, commutative.
(b) Show that not every element of $\mathcal{M}(S)$ is invertible.

Solution.
(a) Consider the set $\mathcal{M}(\mathbb{Z})$ of all functions from the set of integers into itself. Then the operation of composition is a binary operation on $\mathcal{M}(\mathbb{Z})$. Consider the two functions $\alpha(n) = 2n$ and

$$\beta(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ 4 & \text{if } n \text{ is odd} \end{cases}$$

Then $(\beta \circ \alpha)(n) = n$ for all $n \in \mathbb{Z}$. That is, $\beta \circ \alpha = \iota_{\mathbb{Z}}$. However, since

$$(\alpha \circ \beta)(n) = \begin{cases} n & \text{if } n \text{ is even} \\ 8 & \text{if } n \text{ is odd} \end{cases}$$

then $\beta \circ \alpha \neq \alpha \circ \beta$. Hence, composition is not commutative.

(b) From part (a), we see that $\beta \circ \alpha = \iota_{\mathbb{Z}}$. Thus, β is a left inverse of α. However, $\alpha \circ \beta \neq \iota_{\mathbb{Z}}$ so that β is not a right inverse of α. Hence, α is not invertible.■

Under what conditions on S, composition in $\mathcal{M}(S)$ is commutative?

Theorem 4.1
Let S be a nonempty set such that $|S| < 2$. Then composition of mappings in $\mathcal{M}(S)$ is commutative.

Proof.
We will show that if $|S| \geq 2$ then composition of mappings is not commutative. Indeed, if $|S| \geq 2$ then there exist two distinct elements a and b of S. Define $\alpha, \beta : S \longrightarrow S$ as follows:

$$\begin{array}{rclrcl} \alpha(a) & = & a & \alpha(b) & = & a \\ \beta(a) & = & b & \beta(b) & = & b. \end{array}$$

Then $(\alpha \circ \beta)(a) = \alpha(\beta(b)) = \alpha(b) = a$ and $(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = b$. Since $a \neq b$ then $\alpha \circ \beta \neq \beta \circ \alpha$. That is, composition in $\mathcal{M}(S)$ is not commutative.■

The following theorem summarizes the two properties of composition in $\Updownarrow(S)$.

Theorem 4.2
Let S be a nonempty set.

(a) Composition in $\mathcal{M}(S)$ is associative.
(b) ι_S is the identity element in $\mathcal{M}(S)$.

Proof.
(a) Let $x \in S$. Then for any $\alpha, \beta, \gamma \in \mathcal{M}(S)$, we have

$$\begin{array}{rcl} [\alpha \circ (\beta \circ \gamma)](x) & = & \alpha(\beta \circ \gamma(x)) \\ & = & \alpha(\beta(\gamma(x))) \\ & = & (\alpha \circ \beta)(\gamma(x)) \\ & = & [(\alpha \circ \beta) \circ \gamma](x) \end{array}$$

Thus, $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
(b)If $x \in S$ and $\alpha \in \mathcal{M}(\mathcal{S})$ then

$$(\alpha \circ \iota_S)(x) = \alpha(\iota_S(x)) = \alpha(x)$$

so that $\alpha \circ \iota_S = \alpha$. Similarly, $\iota_S \circ \alpha = \alpha$. Hence, ι_S is the identity element of $\mathcal{M}(\mathcal{S})$ under the operation of composition.■

Example 4.2
Is is true that if a nonempty set S is closed under a binary operation $*$ then every subset A of S is also closed under $*$?

Solution.
If a set is closed under an operation then this does not mean that every subset is also closed under this operation. For example, $\mathbb{R}$ is closed under the operation of subtraction whereas $\mathbb{N}$ is not. Thus, composition is a binary operation on a subset of $\mathcal{M}(\mathcal{S})$ if and only if the subset is closed under composition.■

Now, let's look at the set $\mathcal{I}(\mathcal{S})$ of all invertible mappings from S to S. Clearly, $\mathcal{I}(\mathcal{S})$ is a subset of $\mathcal{M}(\mathcal{S})$.

Theorem 4.3
(a) $\mathcal{I}(\mathcal{S})$ is closed under composition.
(b) Composition is associative on $\mathcal{I}(\mathcal{S})$.
(c) ι_S is the identity element of $\mathcal{I}(\mathcal{S})$.
(d) Every element of $\mathcal{I}(\mathcal{S})$ is invertible.

Proof.
(a) Let α and β be two invertible mappings from S to S. Then by Theorem 2.5(b), $\alpha \circ \beta$ is also invertible. That is, $\alpha \circ \beta \in \mathcal{I}(\mathcal{S})$. Hence, $\mathcal{I}(\mathcal{S})$ is closed under composition.
(b) Since $\mathcal{I}(\mathcal{S})$ is closed with respect to composition and composition on $\mathcal{M}(\mathcal{S})$ is associative there then it is certainly associative when restricted on $\mathcal{I}(\mathcal{S})$.
(c) Since $\iota_S^{-1} = \iota_S$ then $\iota_S \in \mathcal{I}(\mathcal{S})$. Since ι_S is the identity element of $\mathcal{M}(\mathcal{S})$ then ι_S is the identity element of $\mathcal{I}(\mathcal{S})$.
(d) Follows from the definition of $\mathcal{I}(S)$. ■

The following theorem can be used to test whether a mapping is one-to-one.

Theorem 4.4
Let S be a nonempty set and $\alpha \in \mathcal{M}(\mathcal{S})$. Then α is one-to-one if and only if there exists a $\beta \in \mathcal{M}(\mathcal{S})$ such that $\beta \circ \alpha = \iota_S$.

Proof.
Suppose first that α is one-to-one. Pick an element $x_0 \in S$ and define $\beta : S \to S$ as follows

$$\beta(x) = \begin{cases} y & \text{if } \alpha(y) = x \\ x_0 & \text{if } \alpha(y) \neq x, \forall y \in S \end{cases}$$

We show that $\beta \in \mathcal{M}(\mathcal{S})$. Indeed, if $\beta(x) = y$ and $y' \in S$ is such that $\beta(x) = y'$ then $\alpha(y) = \alpha(y'$ and since α is one-to-one then $y = y'$. That is, y is the unique element such that $\beta(x) = y$. If $\beta(x) = x_0$ then x_0 is the unique element such that $\beta(x) = x_0$ since x_0 is fixed. It remains to show that $\beta \circ \alpha = \iota_S$. To see this, let $x \in S$ and $\alpha(x) = y$. Then $(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \beta(y) = x = \iota_S(x)$. Thus, $\beta \circ \alpha = \iota_S$.
Conversely, suppose that $\beta \in \mathcal{M}(\mathcal{S})$ such that $\beta \circ \alpha = \iota_S$. Since ι_S is one-to-one then $\beta \circ \alpha$ is one-to-one and therefore by Theorem 2.2(b) , α is one-to-one. ■

For testing onto mappings we have

Theorem 4.5
Let S be a nonempty set and $\alpha \in \mathcal{M}(\mathcal{S})$. Then α is onto if and only if there exists a $\beta \in \mathcal{M}(\mathcal{S})$ such that $\alpha \circ \beta = \iota_S$.

Proof.
Suppose first that α is onto. Then for each $y \in S$ there is an $x \in S$ such that $\alpha(x) = y$. Define $\beta : S \to S$ by $\beta(y) = x$. Then $(\alpha \circ \beta)(y) = \alpha(\beta(y)) = \alpha(x) = y$ so that $\alpha \circ \beta = \iota_S$.
Conversely, suppose that $\beta \in \mathcal{M}(\mathcal{S})$ is such that $\alpha \circ \beta = \iota_S$. Since ι_S is onto then $\alpha \circ \beta$ is onto. By Theorem 2.1 (b), α is also onto.■

Many important operations involve composition on special sets of invertible mappings. We close this section by giving two examples. The first example exhibits an example of a set of mappings where composition is commutative.

Example 4.3
Let P denote the Cartesian plane. Let G_p be the set of all rotations about a fixed point p. If two rotations differ by a multiple of 360° then we say that they are equal. If α and β are two elements of G_p then $\alpha \circ \beta$ is the rotation obtained by first applying β and then applying α. Thus, G_p is closed under composition. By Theorem 4.2, composition is associative. An identity element of G_p is the rotation of 0°. Each rotation has an inverse: rotation of the same magnitude in the opposite direction. Finally, as an operation on G_p, composition is commutative.■

Example 4.4
Let $\mathcal{L}$ be the set of all linear mappings $\alpha_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $\alpha_{a,b}(x) =$

$ax + b$ where a and b are two real numbers with $a \neq 0$.

(i) $\mathcal{L}$ is a set of invertible mappings from $\mathbb{R}$ into $\mathbb{R}$.
Indeed, if $\alpha_{a,b} = ax + b$ with $a \neq 0$ then $\alpha_{a,b}^{-1}(x) = \alpha_{\frac{1}{a},-\frac{b}{a}}(x) = \frac{1}{a}x - \frac{b}{a}$.

(ii) $\mathcal{L}$ is closed under composition
To see this, pick two members $\mathcal{L}$, say $\alpha_{a,b} = ax + b$ and $\alpha_{c,d}(x) = cx + d$, where $a \neq 0$ and $c \neq 0$. Note that $ac \neq 0$. Moreover,

$$\begin{aligned}(\alpha_{a,b} \circ \alpha_{c,d})(x) &= \alpha_{a,b}(\alpha_{c,d}(x)) \\ &= \alpha_{a,b}(cx + d) = a(cx + d) + b \\ &= (ac)x + ad + b = \alpha_{ac,ad+b}(x)\end{aligned}$$

Thus, $\alpha_{a,b} \circ \alpha_{c,d} \in \mathcal{L}$.

(iii) Composition is associative on $\mathcal{L}$
Since $\mathcal{L}$ is a subset $\mathcal{M}(\mathbb{R})$ and composition is associative on $\mathcal{M}(\mathbb{R})$ then composition is also associative on $\mathcal{L}$.

(iv) $\alpha_{1,0}$ is the identity element of $\mathcal{L}$
To see this, let $\alpha_{a,b} \in \mathcal{L}$. Then by (ii)

$$\alpha_{a,b} \circ \alpha_{1,0} = \alpha_{a,b}$$

and

$$\alpha_{1,0} \circ \alpha_{a,b} = \alpha_{a,b}.\blacksquare$$

Remark 4.1
The identity element can be found as follows: If $\alpha_{e,f}$ is the identity element of $\mathcal{L}$ then for any $\alpha_{a,b} \in \mathcal{L}$ we must have

$$\alpha_{e,f} \circ \alpha_{a,b} = \alpha_{a,b} \circ \alpha_{e,f} = \alpha_{a,b}.$$

This and (ii) imply that $ea = a$ and $eb + f = b$. Thus, $e = 1$ and $f = 0$.

Remark 4.2
Note that, $\alpha_{a,0}(x) = ax, a > 1$ is magnification since it magnifies the distance of each point from the origin by a factor of a. Also, $\alpha_{1,b}(x) = x + b, b > 0$ is a translation of x, b units to the right. Finally, note that $\alpha_{a,b} = \alpha_{1,b} \circ \alpha_{a,0}$ so that for $a > 1$ and $b > 0$, $\alpha_{a,b}$ corresponds to a magnification followed by a translation.

Review Problems

Exercise 4.1
Consider the set $S = \{a, b\}$.

(a) Find the four elements of $\mathcal{M}(\mathcal{S}) = \{\pi, \rho, \sigma, \theta\}$.
(b) Construct the Cayley table for composition.
(c) What is the identity element?
(d) Is $\circ$ *commutative as an operation on* $\mathcal{M}(\mathcal{S})$?
(e) Which elements of $\mathcal{M}(\mathcal{S})$ *are invertible?*

Exercise 4.2
Consider the set $G_p = \{\rho_1, \rho_2, \rho_3, \rho_4\}$, *where* $\rho_1, \rho_2, \rho_3,$ *and* ρ_4 *denote clockwise rotation through* $0°, 90°, 180°, 270°$.

(a) Construct the Cayley table for composition as an operation on G_p.
(b) Is there an identity element?
(c) Does each element have ab inverse?

Exercise 4.3
Let $\mathcal{B}$ *and* $\mathcal{C}$ *be subsets of* $\mathcal{L}$.

$$\begin{aligned} B &= \{\alpha_{a,0} : a \in \mathbb{R} \text{ and } a \neq 0\} \\ C &= \{\alpha_{1,b} : b \in \mathbb{R}\} \end{aligned}$$

(a) Verify that $\mathcal{B}$ *is closed under the operation of composition. Is* $\circ$ *associative? Commutative? Is there an identity element?*
(b) Verify that $\mathcal{C}$ *is closed under the operation of composition. Is* $\circ$ *associative? Commutative? Is there an identity element?*
(c) Verify that each mapping in $\mathcal{L}$ *is the composition of a mapping in* $\mathcal{B}$ *and a mapping in* $\mathcal{C}$.

Exercise 4.4
Let $S = \mathbb{R} - \{0, 1\}$. *Consdier the mappings from* S *to* S *defined by*

$$\begin{array}{lllllllll} \alpha_1(x) &=& x & , & \alpha_2(x) &=& \frac{1}{x} & , & \alpha_3(x) = 1 - x, \\ \alpha_4(x) &=& 1 - \frac{1}{x} & , & \alpha_5(x) &=& \frac{1}{1-x} & , & \alpha_6(x) = \frac{x}{x-1} \end{array}$$

(a) Verify that $\circ$ is a binary composition on $\{\alpha_1, \cdots, \alpha_6\}$ by constructing a Cayley table.
(b) Is there an identity element?
(c) Show that each of the six elements has an inverse.
(d) Is $\circ$ commutative?
(e) Is $\circ$ associative?

Exercise 4.5
Is composition a binary operation on the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$?

Exercise 4.6
Is composition a binary operation on the set of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$?

Exercise 4.7
Prove by induction that the composition of any finite number of invertible mappings is invertible.

Exercise 4.8
Let $f : S \to T$ and $g : T \to U$ be two mappings such that $g \circ f$ is invertible. Show that f is one-to-one and g is onto.

Exercise 4.9
Let S and T be nonempty sets. Prove the following: There exists a one-to-one mapping $f : S \to T$ if and only if there exists an onto mapping $g : T \to S$.

Exercise 4.10
Prove the following: (i) $f : A \to B$ is one-to-one if and only if $f \circ g = f \circ h$ implies $g = h$ for all maps $g, h : B \to A$.
(ii) If A has at least two elements, then $f : A \to B$ is onto if and only if $g \circ f = h \circ f$ implies $g = h$ for all maps $g, h : B \to A$.

Exercise 4.11
Prove that if $f : \mathbb{R} \to \mathbb{R}$ is either strictly increasing or strictly decreasing then f is invertible.

Exercise 4.12
Suppose that f and g are the functions

$$\begin{aligned} f &= \{(-3,6),(2,12),(4,0),(0,-14)\} \\ g &= \{(0,0),(2,0),(-3,-3),(12,4),(1,2),(15,4)\}. \end{aligned}$$

Find the elements of $f \circ g$ as points in the form (x, y).

Exercise 4.13
Make up an example in which $f \circ g = g \circ f$.

Exercise 4.14
Let S and T be two nonempty sets.

(a) Let $\alpha : S \to T$ be a bijection. Show that $\phi : \mathcal{M}(\mathcal{S}) \to \mathcal{M}(\mathcal{T})$ defined by $\phi(f) = \alpha \circ f \circ \alpha^{-1}$ is a bijection between $\mathcal{M}(\mathcal{S})$ and $\mathcal{M}(\mathcal{T})$.
(b) Show that $\beta : \mathcal{M}(\mathcal{T}) \to \mathcal{M}(\mathcal{S})$ defined by $\beta(g) = \alpha^{-1} \circ g \circ \alpha$ is a bijection.
(c) Prove that $\beta \circ \phi = \iota_{\mathcal{M}(\mathcal{S})}$.

5 Definition and Examples of Groups

In Section 3, properties of binary operations were emphasized-closure, identity, inverses, associativity. Now these properties will be studied from a slightly different viewpoint by considering systems $(S, *)$ that satisfy all four of the properties. Such mathematical systems are called *groups.*
A group may be defined as follows.

Definition 5.1
A set G is a **group** with respect to a binary operation $*$ if the following properties are satisfied:

(i) $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the Associative Law);
(ii) there exists an element e of G (the identity element of G) such that $e * x = x = x * e$, for all elements x of G;
(iii) for each element x of G there exists an element x' of G (the inverse of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

A group G is **Abelian** (or **commutative**) if $x * y = y * x$ for all elements x and y of G.

Remark 5.1
The phrase "with respect" should be noted. For example, the set $\mathbb{Z}$ is a group with respect to addition but not with respect to multiplication (it has no inverses for elements other than ± 1.)

Example 5.1
We can obtain some simple examples of groups by considering appropriate subsets of the familiar number systems.

(a) The set of even integers is an Abelian group with respect to addition.
(b) The set $\mathbb{N}$ of positive integers is not a group with respect to addition since it has no identity element.
(c) The set $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ is not a group with respect to addition since no element other than zero has an inverse.
(d) The set of all nonzero rational numbers is an abelian group under multiplication. ■

Example 5.2
For any nonempty set S the collection of all invertible mappings from S to S is a group with respect to composition. This is a consequence of Theorem 4.3. ■

The following examples give some indication of the great variety there is in groups.

Example 5.3
(a) Let p be a fixed point in the plane P and G_p denote the set of all rotations of the plane about the point p. By Example 4.3, G_p is an Abelian group with respect to composition.
(b) The set of 2-by-2 matrices with respect to addition is an Abelian group. (Show this) ■

Example 5.4
By Theorem 4.3, the set $\mathcal{L}$ of all linear mappings $\alpha_{a,b}$, with $a \neq 0$, from $\mathbb{R}$ into $\mathbb{R}$ is a group with respect to composition.■

Next, we look at a group given by a Cayley table. In this case, it is easy to locate the identity and inverses of elements.

Example 5.5
Let $G = \{e, a, b, c\}$ with multiplication as defined by the table below.

·	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

From the table, we observe that

(i) G is closed under this multiplication.
(ii) e is the identity element.
(iii) $e^{-1} = e, b^{-1} = b, c^{-1} = a$, and $a^{-1} = c$.
(iv) the multiplication is commutative.
It can be checked that the multiplication is associative. Thus, $(G, .)$ is an abelian group. ■

Next, we record some simple consequences of the definition of a group in the following theorem.

Theorem 5.1
Let G be a group with respect to a binary operation $*$.

(i) The identity element is unique. That is, if $e, f \in G$ are such that $e * a = f * a = a$ and $a * e = a * f = a$ for all $a \in G$ then $e = f$.
(ii) Every element in G has a unique inverse. That is, if a, b, c are elements in G such that $a * b = a * c = e$ and $b * a = c * a = e$, where e is the identity element of G then $b = c$.

Proof.
(i) Since $a * e = a$ for all $a \in G$ then in particular $f * e = f$. Similarly, since $f * a = a$ for all $a \in G$ then in particular $f * e = e$. Thus, $e = f$.
(ii) With a, b, and c as stated, we have

$$\begin{aligned} b &= b * e \text{ (e is the identity)} \\ &= b * (a * c) \text{ (since a} * \text{c = e)} \\ &= (b * a) * c \ (* \text{ is associative)} \\ &= e * c \text{ (since b} * \text{a = e)} \\ &= c \text{ (e is the identity)} \blacksquare \end{aligned}$$

Remark 5.2
By the theorem, it makes sense to speak of *the* identity element of a group, and *the* inverse element. It is customary to use a^{-1} for the inverse of an element a.

Definition 5.2
The **order** of a group is the number of elements in the group. It is denoted by $|G|$. If $|G|$ is finite then the group is called a **finite group.** Otherwise, the group is called **infinite group**.

Review Problems

In Problems 5.1 - 5.6 decide if each of the given sets is a group with respect to the indicated operation. If it is not a group, state all of the conditions in Definition 5.1 which fail to hold.

Exercise 5.1
The set of all rational numbers with respect to addition.

Exercise 5.2
The set $\{-1, 1\}$ *with respect to multiplication.*

Exercise 5.3
The set $\{-1, 0, 1\}$ *with respect to addition.*

Exercise 5.4
The set $\{10n : n \in \mathbb{Z}\}$ *with respect to addition.*

Exercise 5.5
The set $\{2^n : n \in \mathbb{Z}\}$ *with respect to multiplication.*

Exercise 5.6
The set $\{2^m 3^n : m, n \in \mathbb{Z}\}$ *with respect to multiplication.*

Exercise 5.7
For $f, g \in \mathcal{M}(\mathbb{R})$*, define addition by* $(f + g)(x) = f(x) + g(x)$ *for all* $x \in \mathbb{R}$*. Show that* $\mathcal{M}(\mathbb{R})$ *is a group with respect to addition.*

Exercise 5.8
Let H *be the set of all functions* f *from* $\mathbb{R}$ *to* $\mathbb{R}$ *that satisfy* $f(x) \neq 0$ *for all* $x \in \mathbb{R}$*. Define, on* H*, the operation of multiplication by* $(fg)(x) = f(x)g(x)$ *for all* $x \in \mathbb{R}$*. Show that* H *is a group with respect to multiplication.*

Exercise 5.9
Let G *be a set of complex numbers given by* $G = \{1, -1, i, -i\}$*, where* $i^2 = -1$*, and consider the operation of multiplication of complex numbers in* G*.*

(a) Construct the Cayley table of G*.*
(b) Use (a) to show that G *is an Abelian group with respect to multiplication.*

Exercise 5.10
Consider the Cayley table of a set G *with a binary operation* $*$*.*

$*$	a	b	c	d
a	b	c	a	b
b	c	d	b	a
c	a	b	c	d
d	a	b	d	d

Is $(G, *)$ a group?

Exercise 5.11
For an arbitrary set A, the power set of A is the set $\mathcal{P}(\mathcal{A}) = \{\mathcal{X} : \mathcal{X} \subseteq \mathcal{A}\}$. Let $A = \{a, b, c\}$. Show that the power set $\mathcal{P}(\mathcal{A})$ is not a group with respect to the operation of union.

Exercise 5.12
Let $A = \{a, b, c\}$. Show that the power set $\mathcal{P}(\mathcal{A})$ is not a group with respect to the operation of intersection.

Exercise 5.13
Let A be a nonempty set. Define addition on $\mathcal{P}(\mathcal{A})$ by

$$X + Y = (X \cup Y) - (X \cap Y).$$

Prove that $\mathcal{P}(\mathcal{A})$ is a group with respect to this operation.

Exercise 5.14
Let G be a nonempty set that is closed under an associative binary operation $*$. Prove that G is a group with respect to $*$ is and only if the equations $a * x = b$ and $y * a = b$ have solutions x and y for all choices of a and b in G.

Exercise 5.15
Prove that if a, x, and y are elements of a group G such that $xa = ya$ then $x = y$.

Exercise 5.16
An element x in a group G is called **idempotent** *if $x^2 = x$. Prove that the identity element e is the only idempotent element in a group G.*

Exercise 5.17
Prove that if $x = x^{-1}$ in a group G then G is Abelian.

Exercise 5.18
Prove that if G is a group, $a \in G$, and $a * b = b$ for some $b \in G$, then a must be the identity element of G.

Exercise 5.19
Prove that if $|S| > 1$ then $\mathcal{M}(\mathcal{S})$ is not a group with respect to composition.

6 Permutation Groups

Let S be a nonempty set and $\mathcal{M}(\mathcal{S})$ be the collection of all mappings from S into S. In this section, we will emphasize on the collection of all invertible mappings from S into S. The elements of this set will be called permutations because of Theorem 2.4 and the next definition.

Definition 6.1
Let S be a nonempty set. A one-to-one mapping from S onto S is called a **permutation.**

Consider the collection of all permutations on S. Then this set is a group with respect to composition.

Theorem 6.1
The set of all permutations of a nonempty set S is a group with respect to composition. This group is called the **symmetric group on** S and will be denoted by $Sym(S)$.

Proof.
By Theorem 2.4, the set of all permutations on S is just the set $\mathcal{I}(\mathcal{S})$ of all invertible mappings from S to S. According to Theorem 4.3, this set is a group with respect to composition. ■

Definition 6.2
A group of permutations , with composition as the operation, is called a **permutation group on** S.

Example 6.1
1. $Sym(S)$ is a permutation group.
2. The collection $\mathcal{L}$ of all invertible linear functions from $\mathbb{R}$ to $\mathbb{R}$ is a permutation group with respect to composition.(See Example 4.4.) Note that $\mathcal{L}$ is a proper subset of $Sym(\mathbb{R})$ since we can find a function in $Sym(\mathbb{R})$ which is not in $\mathcal{L}$, namely, the function $f(x) = x^3$. This example shows that, in general, a permutation group on S needs not contain all the permutations on S.■

Example 6.2
Let $S = \{1, 2, 3\}$. There are six permutations on S. We will represent these permutations using the *two-row form* as follows:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad , \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad , \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad , \quad \rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad , \quad \rho_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \blacksquare$$

In composing permutations we always follow the same convention we use in composing any other mappings: read from right to left. Thus,

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

That is, $1 \to 3 \to 2, 2 \to 2 \to 1, 3 \to 1 \to 3$.

Example 6.3
Let $S = \{1, 2, 3\}$. Then $Sym(S) = \{\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6\}$, where the $\rho' s$ are defined in Example 6.2. Let's construct the Cayley table for this group.

$\circ$	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_2	ρ_2	ρ_3	ρ_1	ρ_5	ρ_6	ρ_4
ρ_3	ρ_3	ρ_1	ρ_2	ρ_6	ρ_4	ρ_5
ρ_4	ρ_4	ρ_6	ρ_5	ρ_1	ρ_3	ρ_2
ρ_5	ρ_5	ρ_4	ρ_6	ρ_2	ρ_1	ρ_3
ρ_6	ρ_6	ρ_5	ρ_4	ρ_3	ρ_2	ρ_1

Notice that the permutation

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

is the identity mapping of $Sym(S)$. Moreover,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Thus, the inverse of an element is obtained by reading from the bottom entry to the top entry rather than from top to bottom:if 1 appears beneath 3 in ρ_2

then 3 appears beneath 1 in ρ_2^{-1}.
We will denote the above group by S_3. In general, if $S = \{1, 2, \cdots, n\}$ then the symmetric group on S will be denoted by S_n.

The number of elements of S_n is found in the following theorem.

Theorem 6.2
The order of S_n is $n!$, where $0! = 1! = 1$ and $n! = n(n-1)(n-2)\cdots 2 \cdot 1$.

Proof.
The proof involves the following counting principle: If a decision consists of two steps, if the first step can be done in r different ways and the second step can be done in s different ways then the decision can be made in rs different ways.
The problem of computing the number of elements of S_n is the same as the problem of computing the number of different ways the integers $1, 2, \cdots, n$ can be placed in the n blanks indicated(with each number used only once)

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ - & - & - & \cdots & - \end{pmatrix}$$

Filling the blanks from the left, we see that the first blank can be filled with n different ways. Once this is completed, the second blank can be filled in $n-1$ ways, the third in $n-2$ ways and so on. Thus, by the principle of counting, there are $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ ways of filling the blanks. In conclusion, $|S_n| = n!$ ■

Now, since $S_1 = \{(1)\}$ then S_1 with respect to composition is commutative. Similarly, since $(1)(12) = (12)(1)$ then $S_2 = \{(1), (12)\}$ is also Abelian. Unfortunately, this is not true anymore for $|S| > 2$.

Theorem 6.3
S_n is non-Abelian for $n \geq 3$.

Proof.
All that we need to do here is to find two permutations α and β in S_n with $n \geq 3$ such that $\alpha \circ \beta \neq \beta \circ \alpha$. Indeed, consider the permutations

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 1 & 3 & 2 & 4 & 5 & \cdots & n \end{pmatrix} \quad \textit{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 2 & 1 & 4 & 5 & \cdots & n \end{pmatrix}$$

Then

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 3 & 1 & 4 & 5 & \cdots & n \end{pmatrix} \text{ and } \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 1 & 2 & 4 & 5 & \cdots & n \end{pmatrix}$$

so that $\alpha \circ \beta \neq \beta \circ \alpha$ ■

Cycle Notation for Permutations

The cycle notation for permutations can be thought as a condensed way to write permutations. Here is how it works.
Let $\alpha \in S_n$ be the permutation

$$\alpha(a_1) = a_2, \alpha(a_2) = a_3, \cdots, \alpha(a_k) = a_1$$

and $\alpha(a_i) = a_i$ for $i = k+1, \cdots, n$, where $a_1, a_2, \cdots, a_n \in \{1, 2, 3, \cdots, n\}$. That is, α follows the circle pattern shown in Figure 6.1

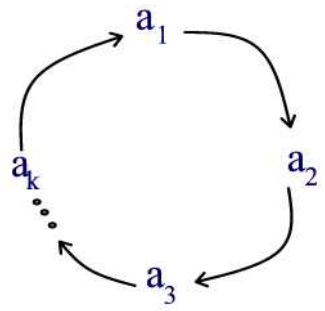


Figure 6.1

Such a permutation is called a *cycle of length k* or simply a *k-cycle.* We will write

$$\alpha = (a_1 a_2 a_3 \cdots a_k) \tag{1}$$

Let us elaborate a little further on the notation employed in (1). The cycle notation is read from left to right, it says α takes a_1 into a_2, a_2 into a_3, etc., and finally a_k, the last symbol, into a_1, the first symbol. Moreover, α leaves all the other elements not appearing in the representation (1) fixed.

Example 6.4
The permutation

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

can be represented as a 4-cycle

$$\alpha = (2647).$$

Note that one can write the same cycle in many ways using this type of notation.

$$\begin{aligned} \alpha &= (2647) \\ &= (6472) \\ &= (4726) \\ &= (7264)\blacksquare \end{aligned}$$

Remark 6.1
A k-cycle can be written in k different ways, since

$$(a_1 a_2 \dots a_k) = (a_2 a_3 \dots a_k a_1) = \cdots = (a_k a_1 \dots a_{k-1}).$$

Example 6.5
It is easy to write the inverse of a cycle. Since $\alpha(a_k) = a_{k+1}$ implies $\alpha^{-1}(a_{k+1}) = a_k$, we only need to reverse the order of the cyclic pattern. For example,

$$(2647)^{-1} = (7462).\blacksquare$$

Example 6.6
Multiplication of cycles is performed by applying the right permutation first. Consider the product in S_5

$$(12)(245)(13)(125)$$

Reading from right to left

$$1 \longmapsto 2 \longmapsto 2 \longmapsto 4 \longmapsto 4$$

so $1 \longmapsto 4$.
Now

$$4 \longmapsto 4 \longmapsto 4 \longmapsto 5 \longmapsto 5$$

so $4 \longmapsto 5$.
Next

$$5 \longmapsto 1 \longmapsto 3 \longmapsto 3 \longmapsto 3$$

so $5 \longmapsto 3$.
Then

$$3 \longmapsto 3 \longmapsto 1 \longmapsto 1 \longmapsto 2$$

so $3 \longmapsto 2$.
Finally

$$2 \longmapsto 5 \longmapsto 5 \longmapsto 2 \longmapsto 1$$

so $2 \longmapsto 1$. Since all the elements of $A = \{1, 2, 3, 4, 5\}$ have been accounted for, we have

$$(12)(245)(13)(125) = (14532).\blacksquare$$

Remark 6.2
A 1-cycle of S_n is the identity of S_n and is denoted by (1). Of course, $(1) = (2) = (3) = \cdots = (n)$.

Now not all permutations are cycles; for example, the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}$$

is not a cycle. However, one can check easily that

$$\alpha = (123)(4567)$$

This suggests how we may extend the idea of cycles to cover all permutations.

Definition 6.3
If α and β are two cycles, they are called **disjoint** if the elements moved by one are left fixed by the other, i.e., their cycle representations contain different elements of the set $S = \{1, 2, 3 \cdots, n\}$.

Example 6.7
The cycles (124) and (356) are disjoint whereas the cycles (124) and (346) are not since they habe the number 4 in common.

Theorem 6.4
If α and β are disjoint cycles then $\alpha\beta = \beta\alpha$.

Proof.
Indeed, since the cycles α and β are disjoint, each element moved by α is fixed by β and vice versa. Let $\alpha = (a_1 a_2 \cdots a_s)$ and $\beta = (b_1 b_2 \cdots b_t)$ where $\{a_1, a_2, \cdots, a_s\} \cap \{b_1, b_2, \cdots, b_t\} = \emptyset$.

(i) Let $1 \leq k \leq s$. Then

$$(\alpha\beta)(a_k) = \alpha(\beta(a_k)) = \alpha(a_k) = a_{k+1}$$

and

$$(\beta\alpha)(a_k) = \beta(\alpha(a_k)) = \beta(a_{k+1}) = a_{k+1}.$$

(ii) Let $1 \leq k \leq t$. Then

$$(\alpha\beta)(b_k) = \alpha(\beta(b_k)) = \alpha(b_{k+1}) = b_{k+1}$$

and

$$(\beta\alpha)(b_k) = \beta(\alpha(b_k)) = \beta(b_k) = b_{k+1}.$$

(iii) Let $1 \leq m \leq n$ and $m \notin \{a_1, a_2, \cdots, a_s, b_1, b_2, \cdots, b_t\}$. Then

$$(\alpha\beta)(m) = \alpha(\beta(m)) = \alpha(m) = m$$

and

$$(\beta\alpha)(m) = \beta(\alpha(m)) = \beta(m) = m.$$

It follows from (i), (ii), and (iii) that $\alpha\beta = \beta\alpha$.■

Theorem 6.5
Every permutation of S_n is either a cycle or can be written uniquely, except for order of cycles or the different ways a cycle is written, as a product of disjoint cycles.

Proof.
The proof is by induction on n. If $n = 1$ then there is only one permutation, and it is the cycle (1).
Assume that the result is valid for all sets with fewer than n elements. We will prove that the result is valid for a set with n elements.
Let $\sigma \in S_n$. If $\sigma = (1)$ then we are done. Otherwise there exists a positive integer m such that $\sigma^{m-1}(1) \neq 1$ and $\sigma^m(1) = 1$. For example, if $\sigma =$

$(145) \in S_5$ then $m = 3$ since $\sigma(1) = 4, \sigma^2(1) = \sigma(\sigma(1)) = \sigma(4) = 5$, and $\sigma^3(1) = \sigma(\sigma^2(1)) = \sigma(5) = 1$.
Let

$$Q = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{m-1}(1)\}.$$

If $Q = \{1, 2, \ldots, n\}$ then σ is the cycle $\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))$. If $Q \neq S$ then

$$\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))\tau$$

where τ is a permutation on the set $S - Q = \{t \in S : t \notin Q\}$. Since this set has order smaller than n, then by the induction hypothesis τ can be written as a product of disjoint cycles, say, $\tau = \tau_1\tau_2\ldots\tau_k$. Thus,

$$\sigma = (1\sigma(1)\sigma^2(1)\ldots\sigma^{m-1}(1))\tau_1\tau_2\ldots\tau_k$$

But this says that σ is expressed as a product of disjoint cycles. This completes the induction step, and establishes the result for all n■

Example 6.8
Let $S = \{1, 2, ..., 8\}$ and let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 1 & 7 & 3 & 8 \end{pmatrix}$$

Start the first cycle with 1 and continue until we get back to 1, and then close the first cycle. Then start the second cycle with the smallest number not in the first cycle, continue until we get back to that number, and then close the second cycle, and so on to obtain

$$\alpha = (1245)(367)(8)$$

It is customary to omit such cycles as (8), i.e., elements left fixed by α, and write α simply as

$$\alpha = (1245)(367)$$■

Review Problems

Exercise 6.1
Asuume $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ *and* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Compute each of the following.

$$\begin{array}{cccccccc} (a) & \beta \circ \alpha & (b) & \alpha \circ \beta & (c) & \alpha^{-1} & (d) & \beta^{-1} \\ (e) & \beta^{-1} \circ \alpha^{-1} & (f) & \alpha^{-1} \circ \beta^{-1} & (g) & (\beta \circ \alpha)^{-1} & (h) & (\alpha \circ \beta)^{-1} \end{array}$$

Exercise 6.2
Write each of the following as a single cycle or a product of disjoint cycles.

$$\begin{array}{cccc} (a) & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} & (b) & (12)(13)(14) \\ (c) & (13)^{-1}(24)(235)^{-1} & (d) & (145)(1235)(13) \end{array}$$

Exercise 6.3
(a) Write all of the elements of S_4 both in two-row form and using cycle notation.
(b) Which elements of S_4 are their own inverses?

Exercise 6.4
For which values of k will every k-cycle be its own inverse?

Exercise 6.5
Show that every non identity element of S_n is either a 2-cycle or can be written as the product of 2-cycles.

Exercise 6.6
Prove that if S contains at least three elements then $Sym(S)$ is non-Abelian.

Exercise 6.7
For m a positive integer, we define $\alpha^m = \alpha \circ \alpha^{m-1}$. If α is a cycle then α^m maps each integer in the cycle onto the integer located m places farther along in the cycle. For instance, if $\alpha = (123456789)$ then $\alpha^2 = (13572468)$. Find α^3 and α^4.

Exercise 6.8
For $\sigma \in S_n$, define the **order** *of σ to be the smallest positive integer such that $\sigma^m = (1)$. Prove that if $\sigma \in S_n$ has order m then $\tau\sigma\tau^{-1}$ has order m for all $\tau \in S_n$.*

Exercise 6.9
Compute the order of $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$. Let $\sigma = (387) \in S_{11}$. Find the order of $\sigma\tau\sigma^{-1}$.

Exercise 6.10
Let S be a nonempty set and X a subset of S. Let $G = \{\sigma \in Sym(S) : \sigma(X) = X\}$. Prove that G is a permutation group.

Exercise 6.11
Let S be a nonempty set and X a subset of S. Let $G = \{\sigma \in Sym(S) : \sigma(t) = t \forall t \in X\}$. Prove that G is a permutation group.

Exercise 6.12
Let S be a nonempty set and $G \subseteq Sym(S)$. Let τ be a fixed element of $Sym(S)$. Prove that

$$\tau G \tau^{-1} = \{\sigma \in Sym(S) : \sigma = \tau \mu \tau^{-1} \ for \ some \ \mu \in G\}.$$

Exercise 6.13
Let α be a fixed element of S_n. Show that the function $\phi : S_n \to S_n$ defined by $\phi(\tau) = \alpha \tau \alpha^{-1}$ is one-to-one and onto.

7 Subgroups

In this section we discuss the concept of a subgroup and look at an important subgroup of S_n, the so-called alternating group.

7.1 Definition and Examples of Subgroups

You may have noticed that we sometimes had groups contained within larger groups. For example, the group $(\mathbb{Z}, +)$ is contained within the group $(\mathbb{R}, +)$. In this situation, we will say that $(\mathbb{Z}, +)$ is a **subgroup** of $(\mathbb{R}, +)$.

Definition 7.1
If a subset H of a group G is closed under the binary operation of G and if H is itself a group with respect to the induced binary operation, then H is a *subgroup of G.* We write $H < G$.

Definition 7.2
A group G is considered to be a subgroup of itself. We say that G is the **improper subgroup of G.** All other subgroups are **proper subgroups.** The subgroup $\{e\}$ consisiting of the identity element of G is called the **trivial subgroup of G.** All other subgroups are **nontrivial.**

Example 7.1
1. The set I of even integers is a nontrivial subgroup of $\mathbb{Z}$ with respect to addition. The identity element of $(I, +)$ is 0.
2. $\{-1, 1\}$ is a nontrivial subgroup of $(\mathbb{R} - \{0\}, \cdot)$ with identity element 1. ■

You might have noticed that in the above examples the identity of the subgroup always appeared to be the identity of the group. The following theorem shows that this is always the case.

Theorem 7.1
Let $(G, *)$ be a group with identity element e and $H < G$. Then $e \in H$ and e is the identity element of H.

Proof.
Since H is a group itself then it has an identity element which we denote by

e_H. We will show that $e_H = e$. Since $e_H \in G$ then e_H is invertible. That is, $e_H * e_H^{-1} = e_H^{-1} * e_H = e$. Thus,

$$\begin{aligned} e_H &= e_H * e \ (e \textit{ is the identity element of } G) \\ &= e_H * (e_H * e_H^{-1}) \ (\textit{since } e_H * e_H^{-1} = e) \\ &= (e_H * e_H) * e_H^{-1} \ (* \textit{ is associative}) \\ &= e_H * e_H^{-1} \ (\textit{since } e_H \textit{ is the identity of } H) \\ &= e \ (\textit{since } e_H * e_H^{-1} = e) \blacksquare \end{aligned}$$

The following result shows that the inverse of an element in H is the same as the inverse of that element in G.

Theorem 7.2
Let $(G, *)$ be a group with identity element e and $H < G$. If $a \in H$ then $a^{-1} \in G$. If c is the inverse of a in H then $c = a^{-1}$.

Proof.
Let $a \in H$. Then $a \in G$ and so $a^{-1} \in G$. Let $c \in H$ such that $c * a = a * c = e_H$.(That is, c is the inverse of a in H) We will show that $c = a^{-1}$. Indeed, since $c * a = a * c = e_H = e$ then c is an inverse of a in G. By Theorem 3.2, $c = a^{-1}$. This completes the proof of the theorem.■

It is convenient to have a routine step-by-step procedure for determining whether a subset of a group is a subgroup of G. The following theorem gives such a procedure.

Theorem 7.3
A nonempty subset H of a group G is a subgroup of G if and only if

(i) H is closed under the binary operation of G, i.e., if $a, b \in H$ then $a*b \in H$;
(ii) if $a \in H$ then $a^{-1} \in H$.

Proof.
Suppose that H is a subgroup of G. The property (i) follows directly from the definition of a subgroup. Condition (ii) is just Theorem 7.2.
Assume now that H is a nonempty subset of G satisfying conditions (i) and (ii). By (i), $*$ is a binary operation on H. Since $*$ is associative in G then it is still associative when restricted to H. Now, if $a \in H$, then by condition (ii), $a^{-1} \in H$ so that by (i) $a * a^{-1} = a^{-1} * a = e \in H$. Hence, e is the identity of H. By condition (ii), every element of H has an inverse in H. Thus, H satisfies the conditions of a group and so is a subgroup of G. ■

Example 7.2
In $\mathcal{M}(\mathbb{R})$ under addition, consider the subset $C(\mathbb{R})$ of all continuous functions. Clearly, $C(\mathbb{R})$ is closed under addition (for the sum of continuous functions is continuous). For a continuous function f, the function $-f$ (which plays the role of its inverse) is continuous. Thus, $C(\mathbb{R})$ is a subgroup of $\mathcal{M}(\mathbb{R})$ under addition. ■

If the set H in Theorem 7.3 is finite then condition (ii) can be omitted altogether.

Theorem 7.4
A finite subset of a group that is closed under the group operation is a subgroup of that group.

Proof.
Consider the Cayley table of H. By closure, each element in the table belongs to H. Each element of H appears exactly once in each row or column of the table. That is, each row/column is a rearrangement of the elements of H. To illustarte, suppose that $b \in H$ and in the row of b we can find two elements x and y in H such that $b*x = a$ and $b*y = a$, where $a \in H$. Then $b*x = b*y$. But this implies that $x = e*x = (b^{-1}*b)*x = b^{-1}*(b*x) = b^{-1}*(b*y) = (b^{-1}*b)*y = e*y = y$. Thus, for a given element, $a \in H$, the row and column corresponding to a must each contain a. Thus some member of H multiplies a to give the result a. The only element that could do this is the identity element e. Thus, $e \in H$. Similarly, if e is in H then it must appear once in the row and once in the column corresponding to a. Therefore there is some element of H which multiplies a to give e. That can only be $a^{-1.}$ Thus e must be in H and for every $a \in H$, $a^{-1} \in H$. Therefore, H is a subgroup of G.■

A variation of Theorem 7.3, where the conditions (i) and (ii) can be combined, is given by the next result.

Theorem 7.5
Let H be a nonempty subset of $(G, *)$. Then H is a subgroup of G if and only if for all $a, b \in H$, we have $a * b^{-1} \in H$.

Proof.
Assume first that H is a subgroup of G. Let $a, b \in H$. Then by Theorem 7.3 (ii), $b^{-1} \in H$. By Theorem 7.3(i), $a * b^{-1} \in H$.

Conversely, assume that for all $a, b \in H$ we have $a * b^{-1} \in H$. Since H is nonempty then it contains an element a. But then $a * a^{-1} = e \in H$. Now, if $a \in H$ then $e * a^{-1} = a^{-1} \in H$. Finally, if $a, b \in H$ then $a * b = a * (b^{-1})^{-1} \in H$. Hence, by Theorem 14, H is a subgroup of G.■

Example 7.3
Let G be a nonempty group and $a \in G$. Define the set

$$H = \{x \in G : ax = xa\}.$$

Then H is a subgroup of G. To see this, note first that $e \in H$ since $ae = ea$. Thus, H is nonempty. Now, let $x, y \in H$. Then

$$\begin{aligned} a(xy) &= (ax)y \\ &= (xa)y \\ &= x(ay) \\ &= x(ya) = (xy)a \end{aligned}$$

It follows that H is closed under multiplication. Now, if $x \in H$ then

$$\begin{aligned} ax^{-1} &= e(ax^{-1}) \\ &= (x^{-1}x)(ax^{-1}) \\ &= x^{-1}[(xa)x^{-1}] \\ &= x^{-1}[(ax)x^{-1}] \\ &= x^{-1}[a(xx^{-1})] \\ &= x^{-1}(ae) \\ &= x^{-1}a \end{aligned}$$

Thus, $x^{-1} \in H$. It follows from Theorem 7.5 that H is a subgroup of G.■

Next, we discuss two other types of subgroups of permutation groups. Let $S \neq \emptyset$ and G a permutation group on S. Note that $G \subseteq Sym(S)$. Let T be a subset of S. We define

$$G_T = \{\alpha \in G : \alpha(t) = t \ \ \forall t \in T\}$$

and

$$G_{(T)} = \{\alpha \in G : \alpha(T) = T\}.$$

Example 7.4
Let $S = \{1, 2, 3, 4\}, G = S_4$, and $T = \{1, 2\}$. Then

$$G_T = \{(1), (34)\}$$

and

$$G_{(T)} = \{(1), (12), (34), (12)(34)\}\blacksquare$$

Theorem 7.6
Let S, G, G_T and $G_{(T)}$ be defined as above. Then

(a) G_T and $G_{(T)}$ are subgroups of G.
(b) G_T is a subgroup of $G_{(T)}$.

Proof.
(a)Since $\iota_S(t) = t$ for all $t \in T$ then $\iota_S \in G_T$ so that G_T is nonempty. Let $\alpha, \beta \in G_T$. Then for any $t \in T$ we have

$$\begin{array}{rcl} \alpha\beta^{-1}(t) & = & \alpha(\beta^{-1}(t)) \\ & = & \alpha(t) \quad (Since\ \beta(t) = t\ implies\ \beta^{-1}(t) = t) \\ & = & t \quad (Since\ \alpha(t) = t) \end{array}$$

By Theorem 7.5, G_T is a subgroup of G.
The proof that $G_{(T)}$ is a subgroup of G is similar; simply replace t by T.

(b) We just need to show that $G_T \subset G_{(T)}$. Indeed, if $\alpha \in G_T$ then $\alpha(t) = t$ for all $t \in T$. But this implies that $\alpha(T) = T$. Hence $\alpha \in G_{(T)}$. ■

7.2 The Alternating Group

In this section we consider a class of subgroups known as the alternating groups. We start with the following definition.

Definition 7.3
Any 2-cycle (ab) in S_n is called a *transposition.*

That is, a transposition is a permutation (a b) of a set S that interchanges two elements a and b of S and fixes the remaining elements.

Theorem 7.7
Every element of $S_n, n \geq 2$, can be expressed as a finite composition of transpositions.

Proof.
Let $\sigma \in S_n$ with $\sigma \neq (1)$. By Theorem 6.5, σ can be written as a finite product of disjoint cycles. But any $k - cycle$ can be written as a finite product of transpositions. That is,

$$(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$$

Thus, σ can be written as a finite product of transpositions. If $\sigma = (1)$ then since $n \geq 2$ then $(1) = (ab)(ab)$ where $a, b \in \{1, 2, \dots, n\}$. ■

Example 7.5
One can verify easily that

$$(123) = (13)(12)$$

and

$$(123) = (23)(12)(13)(23).$$■

Note that the previous example shows that a permutation can be written in two different ways as a product of transpositions. However, the number of transpositions in both forms is even. Indeed, we have

Theorem 7.8
If a permutation is expressed as a product of p transpositions and as a product of q transpositions then either p and q are both even, or p and q are both odd.

Proof.
Consider the product

$$P = P(x_1, x_2, \dots, x_n) = \Pi_{1 \leq i < j \leq n}(x_i - x_j).$$

For any $\sigma \in S_n$ define

$$\sigma(P) = P(\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n)) = \Pi_{1 \leq i < j \leq n}(x_{\sigma(i)} - x_{\sigma(j)}).$$

Note that if $\gamma = (kl)$ with $k < l$ (if $k > l$ then use the fact that $(lk) = (kl)$) then

$$\gamma(P) = -P$$

To see this, note that the only factors that change sign when swapping x_k and x_l are $(x_k - x_l), (x_k - x_i)$, and $(x_i - x_l)$, where $k < i < l$, and there is an odd number of them.
Now assume that $\sigma \in S_n$ can be written as a product of an even number of transpositions $\sigma = \gamma_1\gamma_2 \dots \gamma_{2q}$ and as an odd number of transpositions $\sigma = \delta_1\delta_2 \dots \delta_{2r+1}$. Then

$$\sigma(P) = \gamma_1(\gamma_2(\dots(\gamma_{2q}(P)))) = (-1)^{2q}P = P$$

and

$$\sigma(P) = \delta_1(\delta_1(\dots(\delta_{2r+1}(P)))) = (-1)^{2r+1}P = -P.$$

Thus, $P = -P$ which is a contradiction.■

Definition 7.4
A permutation that can be written as a product of an even number of transpositions is called an **even permutation,** and the one that can be written as a product of an odd number of transpositions is called an **odd permutation.**

We close this section we the following result.

Theorem 7.9
For $n \geq 2$, the set A_n of all even permutations in S_n is a subgroup of S_n of order $\frac{n!}{2}$.

Proof.
Since $(1) = (12)(12) \in A_n$ then $A_n \neq \emptyset$. Let $\sigma = \gamma_1\gamma_2 \dots \gamma_{2k}$ and $\tau = \delta_1\delta_2 \dots \delta_{2l}$. Then

$$\sigma\tau^{-1} = \gamma_1\gamma_2 \dots \gamma_{2k}\delta_{2l}^{-1}\delta_{2l-1}^{-1} \dots \delta_1^{-1} = \gamma_1\gamma_2 \dots \gamma_{2k}\delta_{2l}\delta_{2l-1} \dots \delta_1 \in A_n.$$

Thus, by Theorem 7.5, A_n is a subgroup of S_n.
To prove that $|A_n| = \frac{n!}{2}$ we just need to prove that S_n has the same number of even permutations as odd permutations. Let O_n be the set of all odd permutations of S_n. Define the mapping $f : A_n \to O_n$ by $f(\sigma) = \sigma(12)$.

f is one-to-one
Suppose that $f(\sigma_1) = f(\sigma_2)$. Then $\sigma_1(12) = \sigma_2(12)$. Thus, $\sigma_1(12)(12)^{-1} = \sigma_2(12)(12)^{-1}$. That is, $\sigma_1 = \sigma_2$.

f is onto
Let $\sigma \in O_n$. Then $\alpha = \sigma(12) \in A_n$. Moreover,

$$f(\alpha) = \sigma(12)(12) = \sigma.$$

By Theorem 7.8, $S_n = A_n \cup O_n$ and $A_n \cap O_n = \emptyset$. Thus, $|A_n| = |O_n|$ and $|S_n| = |A_n| + |O_n| = 2|A_n|$. By Theorem 6.2, $|S_n| = n!$ and hence $|A_n| = \frac{n!}{2}$.■

Definition 7.5
A_n is called the *alternating group* on $\{1, 2, \ldots, n\}$.

Example 7.6
If $S = \{1, 2, 3, 4\}$ then

$A_4 = \{(1), (124), (142), (132), (123), (143), (134), (234), (243), (12)(34), (13)(24), (14)(23)\}$.

Review Problems

Exercise 7.1
Decide in each case whether the given subset is a subgroup of S_5. Justify your answers.

$$\begin{array}{llll} (a) & \{(1),(134),(143)\} & (b) & \{(1),(123),(234)\} \\ (c) & \{(1),(12)34)\} & (d) & \{(1),(1234),(1432)\} \end{array}$$

Exercise 7.2
Decide in each case whether the given subset is a subgroup of $\{1,-1,i,-i\}$ under multiplication. Justify your answers.

$$\begin{array}{llll} (a) & \{1,-1\} & (b) & \{1,i\} \\ (c) & \{i,-i\} & (d) & \{1,-i\} \end{array}$$

Exercise 7.3
Find a subset of $(\mathbb{Z},+)$ that is closed under addition but is not a subgroup of $(\mathbb{Z},+)$.

Exercise 7.4
Let $S=\{1,2,3\}$ and $G=S_3$. Write all the elements of G_T and $G_{(T)}$ if $T=\{2,3\}$.

Exercise 7.5
Prove that if H and K are subgroups of a group G then $H\cap K$ is also a subgroup of G.

Exercise 7.6
Let $H=\{(1),(12)\}$ and $K=\{(1),(123),(132)\}$ be subgroups of S_3. Show that $H\cup K$ is not a subgroup of S_3.

Exercise 7.7
Prove that if G is a group with identity e, and $x\in G$ such that $x*x=x$ then $x=e$.

Exercise 7.8
Assume that G is a group with operation $*$ and that $a\in G$. Let

$$C(a)=\{x\in G : xa=xa\}$$

Prove that $C(a)$ is a subgroup of G. We call $C(a)$ the **centralizer** *of a in G.*

Exercise 7.9
Assume that G is a group with operation $*$ and let

$$Z(G) = \{a \in G : a * x = x * a \forall x \in G\}.$$

Prove that $Z(G)$ is a subgroup of G. We call $Z(G)$ the **center** *of G.*

Exercise 7.10
Let H be a subgroup of a group G, and a a fixed element of G. Let

$$K = \{aha^{-1} : for\ some\ h \in H\}.$$

Prove that K is a subgroup of G.

Exercise 7.11
Prove that $H = \{h \in G : h^{-1} = h\}$ is a subgroup of G if G is Abelian.

Exercise 7.12
Let H and K be subgroups of an Abelian group G and let

$$HK = \{hk : h \in H \text{ and } k \in K\}.$$

Prove that HK is a subgroup of G.

Exercise 7.13
Find two subgroups H and K of S_3 such that HK is not a subgroup of S_3.

Exercise 7.14
Let H be a nonempty subset of a group G. Prove that H is a subgroup of G if and only if $a^{-1} * b \in H$ for all $a, b \in H$.

Exercise 7.15
Let $n \in \mathbb{Z}$. Prove that the set $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

Exercise 7.16
Prove that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $(\mathbb{Z}, +)$.

Exercise 7.17
Prove that if H is a subgroup of K and K is a subgroup of G then H is a subgroup of G.

Exercise 7.18
Let $G = \mathbb{R} \times \mathbb{R}$ with binary operation $(a, b) + (c, d) = (a + c, b + d)$.

(a) Show that $(G, +)$ is a group.
(b) Let $A = \{(a, 0) : a \in \mathbb{R}\}$ and $B = \{(0, b) : b \in \mathbb{R}\}$ be two subsets of G. Prove that A and B are subgroups of G.
(c) Show that $A \cup B$ is not a subgroup of G.

Exercise 7.19
Solve for x in $S_4 : 142)^2 \cdot x = (234)^{-1}$

Exercise 7.20
Prove that O_n is not a subgroup of S_n.

Exercise 7.21
Show that a k-cycle is even if and only if k is odd.

8 Symmetry Groups

In this section, we are interested in the symmetries of planar figures. We can identify a symmetry as a transformation of the plane that moves the figure so that it falls back on itself. The only transformations that we'll consider are those that preserve distance, called *isometries.* There are four kinds of planar isometries: *translations, rotations, reflections, and glide reflections.* In this section we will just consider rotations and reflections.

Rotations: A rotation fixes one point in the plane and turns the rest of it some angle around that point.
Translations: A translation is a mapping that sends all points the same distance in the same direction.
Reflections: A reflection fixes one line in the plane, called the *axis of reflection,* and exchanges points on one side of the axis with points on the other side of the axis at the same distance from the axis.
Glide-reflection: Any product of a translation and a reflection.

Next, we will associate to each figure a group which characterizes the symmetry of the figure. Let P denote the set of all points in the plane then $Sym(P)$ is the set of all permutations from P to P. Let M be the set of all isometries.

Theorem 8.1
M is a subgroup of $Sym(P)$.

Proof.
We will show that M satisfies the conditions of Theorem 7.5. Indeed, since $dist(\iota_P(p), \iota_P(q)) = dist(p, q)$ for any points $p, q \in P$ then ι_P is an isometry and therefore belongs to M. Thus, $M \neq \emptyset$.
Next, let $\alpha, \beta \in M$. We will show that $\alpha \circ \beta^{-1} \in M$. Since α and β are permutations on P then $\alpha \circ \beta^{-1}$ is also a permutation on P. Moreover, if $p, q \in P$ then

$$\begin{aligned}
dist((\alpha \circ \beta^{-1})(p), (\alpha \circ \beta^{-1})(q)) &= dist(\alpha(\beta^{-1}(p)), \alpha(\beta^{-1}(q))) \\
&= dist(\beta^{-1}(p), \beta^{-1}(q)) \ \ (since\ \alpha \in M) \\
&= dist(\beta(\beta^{-1}(p)), \beta(\beta^{-1}(q))) \ \ (since\ \beta \in M) \\
&= dist(\iota_P(p), \iota_P(q)) \\
&= dist(p, q)
\end{aligned}$$

Thus, $\alpha \circ \beta^{-1} \in M$. By Theorem 7.5, M is a subgroup of $Sym(P)$. ■

Now, let T be a subset of P. Define the set

$$M_{(T)} = \{\alpha \in M : \alpha(T) = T\}.$$

By Theorem 7.6(a), $M_{(T)}$ is a subgroup of M.

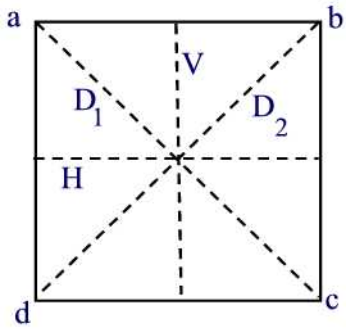
Definition 8.1
$M_{(T)}$ is the group of all symmetries leaving T invariant. We call this group the **symmetry group of T**.

Example 8.1
In this example we describe the symmetry group of a square with vertices $\{a, b, c, d\}$ consisting of rotations and reflections. The eight symmetries of the square are

$$\begin{array}{rcccl}
\mu_1 & = & \text{identity permutation} & = & \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} \\
\mu_2 & = & \text{Rotation clockwise } 90^\circ \text{ around p} & = & \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \\
\mu_3 & = & \text{Rotation clockwise } 180^\circ \text{ around p} & = & \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix} \\
\mu_4 & = & \text{Rotation clockwise } 270^\circ \text{ around p} & = & \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix} \\
\mu_5 & = & \text{Reflection through H} & = & \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \\
\mu_6 & = & \text{Reflection through V} & = & \begin{pmatrix} a & b & c & d \\ b & a & d & a \end{pmatrix} \\
\mu_7 & = & \text{Reflection through } D_1 & = & \begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix} \\
\mu_8 & = & \text{Reflection through } D_2 & = & \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}
\end{array}$$

Thus,

$$M_{(T)} = \{\mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6, \mu_7, \mu_8\}.$$■



Example 8.2
Below is the Cayley table for $M_{(T)}$m where T is the square in the previous example.

$\circ$	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_1	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_2	μ_2	μ_3	μ_4	μ_1	μ_7	μ_8	μ_6	μ_5
μ_3	μ_3	μ_4	μ_1	μ_2	μ_6	μ_5	μ_8	μ_7
μ_4	μ_4	μ_1	μ_2	μ_3	μ_8	μ_7	μ_5	μ_6
μ_5	μ_5	μ_8	μ_6	μ_7	μ_1	μ_3	μ_4	μ_2
μ_6	μ_6	μ_7	μ_5	μ_8	μ_3	μ_1	μ_2	μ_4
μ_7	μ_7	μ_5	μ_8	μ_6	μ_2	μ_4	μ_1	μ_3
μ_8	μ_8	μ_6	μ_7	μ_5	μ_4	μ_2	μ_3	μ_1

Review Problems

Exercise 8.1
Determine the symmetry group of an equilateral triangle.

Exercise 8.2
Determine the symmetry group of an isosceles triangle.

Exercise 8.3
Determine the symmetry group of a rectangle.

Exercise 8.4
Determine the symmetry group of a parallelogram.

Exercise 8.5
Determine the symmetry group of a regular pentagon.

Exercise 8.6
Determine the symmetry group of a regular hexagon.

Exercise 8.7
Construct the Cayley table for the symmetry group of a rectangle.

Exercise 8.8
Construct the Cayley table for the symmetry group of an equilateral triangle.

Exercise 8.9
Consider the symmetry group of the square. Let $\iota = \mu_1, \alpha = \mu_2$, *and* $\beta = \mu_6$ *as described in Example 8.1.*

(a) Compute α^4 *and* β^2.
(b) Show that $\{\mu_1, \cdots, \mu_8\} = \{\iota, \alpha, \alpha^2, \alpha^3, \beta, \beta \circ \alpha, \beta \circ \alpha^2, \beta \circ \alpha^3\}$.

Exercise 8.10
Let G *be the symmetry group of an equilateral triangle. Let* ι *be the identity element,* α *be the rotation by* $120°$, *and* β *be the reflection in the vertical axis of symmetry. Show that*

$$G = \{\iota, \alpha, \alpha^2, \beta, \beta \circ \alpha, \beta \circ \alpha^2\}.$$

9 Equivalence Relations

In the study of mathematics, we deal with many examples of relations between elements of various sets. For example, in working with the integers, we encounter relations such as "x is less than y". Notice the importance of the ordering of the elements of the set in this relation. That is, "x less than y" is not the same as "y less than x." A relation such as the one just mentioned can be described by the following definition

Definition 9.1
A relation $\sim$ on a nonempty set S is a subset of the Cartesian product $S \times S$. Thus, if $(a, b) \in \sim$ then we write $a \sim b$.

Example 9.1
1. On the set $\mathbb{Z}$ of integers, $\sim = \{(x, 2x) : x \in \mathbb{Z}\}$ is a relation on $\mathbb{Z}$. Note that $a \sim b$ if and only if $b = 2a$.
2. A mapping between two nonempty sets is a relation.■

We now consider some properties which a given relation $\sim$ on a set S may or may not have.

Definition 9.2
Let $\sim$ be a relation on a nonempty set S. We say that $\sim$ is:

• **reflexive** *if and only if for all $a \in S$, we have $a \sim a$;*
• **symmetric** *if and only if for $a, b \in S$ if $a \sim b$ then $b \sim a$;*
• **transitive** *if and only if whenever $a, b, c \in S$ such that $a \sim b$ and $b \sim c$ then $a \sim c$.*

Example 9.2
Let S be a nonempty set and $\mathcal{P}(\mathcal{S})$ be the collection of all subsets of S. Let $\sim$ be the relation defined by

$$A \sim B \Longleftrightarrow A \subseteq B, \quad \textit{where } A, B \in \mathcal{P}(\mathcal{S}).$$

Then $\sim$ is reflexive and transitive but not symmetric since it is not always true that if $A \subseteq B$ then $B \subseteq A$.(For example, $\{2\} \subseteq \{1, 2\}$ but $\{1, 2\} \not\subseteq \{2\}$.)■

Just as there were different classes of functions (one-t-one, onto, and one-to-one correspondence), there are also special classes of relations. One of the most useful kind of relations (besides functions, which of course are also relations) are those called equivalence relations which we define next.

Definition 9.3
A relation $\sim$ on a set S which is reflexive, symmetric, and transitive is called an **equivalence relation.**

Example 9.3
1. The equality "=" relation between real numbers or sets.
2. The relation "is similar to" on the set of all triangles.
3. The relation " $\geq$ " between real numbers is not an equivalence relation, because although it is reflexive and transitive, it is not symmetric. e.g. $7 \geq 5$ does not imply that $5 \geq 7$.■

The following example is important in applications to combinatorics.

Example 9.4
Let S be a nonempty set and G be a subgroup of $Sym(S)$. Define the relation $\sim$ on S by

$$a \sim b \Longleftrightarrow \alpha(a) = b \ for \ some \ \alpha \ \in \ G.$$

Then $\sim$ is an equivalence relation on S. Indeed,

$\sim$ **is reflexive**: If $a \in S$ then $\iota_S(a) = a$. Since G is a subgroup and $\iota_S \in G$ then $a \sim a$.
$\sim$ **is symmetric**: Let $a, b \in S$ such that $a \sim b$. Then there is an $\alpha \in G$ such that $\alpha(a) = b$. Since G is a group then $\alpha^{-1} \in G$. Moreover, $a = \iota_S(a) = (\alpha^{-1} \circ \alpha)(a) = \alpha^{-1}(\alpha(a)) = \alpha^{-1}(b)$. Thus, $b \sim a$.
$\sim$ **is transitive**: Let $a, b, c \in S$ such that $a \sim b$ and $b \sim c$. Then there exist permutations α and β in G such that $\alpha(a) = b$ and $\beta(b) = c$. Since G is a group then G is closed under composition and therefore $\beta \circ \alpha \in G$. Moreover, $(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = c$. Hence, $a \sim c$. ■

An important fact about an equivalence relation on a set A is that it induces a partition of A into disjoint sets as indicated in the next theorem.

Theorem 9.1
Let A be a nonempty set. Let $\{A_i\}_{i\in\mathbb{N}}$ be a partition of A. That is, $\{A_i\}_{i\in\mathbb{N}}$ is a family of subsets of A that satisfies the two conditions:

(i) $A = \cup_{i\in\mathbb{N}} A_i$;
(ii) For $i \neq j$, $A_i \cap A_j = \emptyset$.

The relation

$$x \sim y \iff x, y \in A_i, \ \textit{for some } i$$

is an equivalence relation on A.

Proof.
We need to show that $\sim$ is reflexive, symmetric and transitive.

$\sim$ **is reflexive**: If $a \in A$ then by (i), $a \in A_i$ for some $i \in \mathbb{N}$. From the definition of $\sim$ with $b = a$ we have $a \sim a$.
$\sim$ **is symmetric**: Let $a, b \in A$ such that $a \sim b$. Then $a, b \in A_i$ for some $i \in \mathbb{N}$. But then $b, a \in A_i$ so that $b \sim a$.
$\sim$ **is transitive**: Let $a, b, c \in A$ such that $a \sim b$ and $b \sim c$. Then $a, b \in A_i$ for some $i \in \mathbb{N}$ and $b, c \in A_j$ for some $j \in \mathbb{N}$. By (ii), we must have $i = j$. Thus, $a, c \in A_i$ for some $i \in \mathbb{N}$. Hence, $a \sim c$. ■

The converse of the above theorem is also true. Before proving this claim we introduce the following concept.

Definition 9.4
If $\sim$ is an equivalence relation on a nonempty set A and $a \sim b$ for some $a, b \in A$ then we say that a and b are **equivalent.** *For a fixed $a \in A$ the set of all elements in S equivalent to a is called an* **equivalence class with representative a**. *We will write $[a]$. In set-builder notation*

$$[a] = \{x \in A : x \sim a\}.$$

The subset of A containing exactly one element from each equivalent class is called a **complete set of equivalence class representatives.**

Exercise 9.1
In the rectangular coordinate system we define the relation

$$(x_1, y_1) \sim (x_2, y_2) \iff y_1 = y_2.$$

(i) Show that $\sim$ is an equivalence relation on the set of points in the plane.
(ii) Describe the equivalence classes geometrically.
(iii) Give a complete set of equivalence class representatives.

Solution.
(i) For any $(x, y) \in \mathbb{R}^2$, $(x, y) \sim (x, y)$ so that $\sim$ is reflexive. Now, if $(x_1, y_1) \sim (x_2, y_2)$ then $y_1 = y_2$. But equality in $\mathbb{R}$ is symmetric so that $y_2 = y_1$. Thus, $(x_2, y_2) \sim (x_1, y_1)$ and hence *sim* is symmetric. To show that $\sim$ is transitive, suppose that $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$. Then $y_1 = y_2$ and $y_2 = y_3$. Since '=' is transitive in $\mathbb{R}$ then $y_1 = y_3$. Hence $(x_1, y_1) \sim (x_3, y_3)$.
(ii) For a fixed $(a, b) \in \mathbb{R}^2$, the equivalence class of (a, b) is the horizontal line going through the point (a, b).
(iii) The set of points on a line not parrallel to the x-axis.■

Theorem 9.2
If $\sim$ is an equivalence relation on a nonempty set A and $a, b \in A$ are such that $a \sim b$ then $[a] = [b]$.

Proof.
The proof is by double inclusions. Let $x \in [a]$. Then $x \sim a$. Since $a \sim b$ and $\sim$ is transitive then $x \sim b$ which means that $x \in [b]$. Thus, $[a] \subseteq [b]$. Now interchange the letters a and b to show that $[b] \subseteq [a]$. Hence, $[a] = [b]$ ■

Theorem 9.3
Let A be a nonempty set and $\sim$ be an equivalence relation on A. Then the equivalence classes of A define a partition of A. That is,

(i) $A = \cup_{a \in A}[a]$;
(ii) If $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.

Proof.
By the definition of $[a]$ we have that $[a] \subseteq A$. Hence, $\cup_{a \in A}[a] \subseteq A$. We next show that $A \subseteq \cup_{a \in A}[a]$. Indeed, let $b \in A$. Since $\sim$ is reflexive then $b \in [b]$ and consequently $b \in \cup_{a \in A}[a]$. Hence, $A \subseteq \cup_{b \in A}[b]$. It follows that $A = \cup_{a \in A}[a]$. This establishes (i).
It remains to show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$ for $a, b \in A$. Equivalently. we must show that if $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$. Since $[a] \cap [b] \neq \emptyset$ then there is an element $c \in [a] \cap [b]$. This means that $c \in [a]$ and $c \in [b]$. Hence, $a \sim c$ and $b \sim c$. Since $\sim$ is symmetric and transitive then $a \sim b$. Now, by Theorem 9.2, $[a] = [b]$.■

Review Problems

Exercise 9.2
Assume that $S = \{w, x, y, z\}$ and that $w \sim y$ and $z \sim y$. Which of the following must also be true if $\sim$ is to be an equivalence relation on S?

(a) $y \sim y$ *(b)* $y \sim z$ *(c)* $w \sim z$ *(d)* $y \sim x$.

Exercise 9.3
Let $A = \{1, 2, 3, 4, 5\}$.

(a) Show that $\mathcal{P} = \{\{\infty, \ni\}, \{\in\}, \{\triangle, \bigtriangledown\}\}$ *is a partition of* A.
(b) For the corresponding equivalence relation $\sim$*, which of the following are true?*

(i) $4 \sim 5$ *(ii)* $3 \sim 3$ *(iii)* $1 \sim 2$ *(iv)* $5 \sim 1$.

Exercise 9.4
For points (x_1, y_1) *and* (x_2, y_2) *in a plane with rectangular coordinate system, let* $(x_1, y_1) \sim (x_2, y_2)$ *means* $x_1 = x_2$ *or* $y_1 = y_2$*. Show that* $\sim$ *is not an equivalence relation on the set of points in the plane.*

Exercise 9.5
Define a relation $\sim$ *on* $\mathbb{R}$ *by*

$$a \sim b \quad iff \quad |a| = |b|.$$

(a) Prove that $\sim$ *is an equivalence relation on* $\mathbb{R}$.
(b) Give a complete set of equivalence class representatives.

Exercise 9.6
For $x, y \in \mathbb{R}$ *let* $x \sim y$ *mean that* $xy > 0$*. Is* $\sim$ *reflexive? symmetric? transitive?*

Exercise 9.7
For sets S *and* T*, let* $S \sim T$ *mean that there is an invertible mapping of* S *onto* T*. Prove that* $\sim$ *is an equivalence relation.*

Exercise 9.8
Let L be the set of all lines in the Cartesian plane. For $l_1, l_2 \in L$, define the relation $l_1 \sim l_2$ if and only if either the slopes of both lines are equal or undefined. Geometrically, $l_1 \sim l_2$ if and only if l_1 is parallel to l_2.

(a) Show that $\sim$ is an equivalence relation on L.
(b) For a fixed $l \in L$, what is the equivalence class of l?

Exercise 9.9
On the set of all 2×2 matrices over $\mathbb{R}$, define $A \sim B$ if there exists an invertible matrix P such that $PAP^{-1} = B$. Prove that $\sim$ defines an equivalence relation.

Exercise 9.10
Let $\mathbb{Z}$ be the set of integers and $n \in \mathbb{Z}$. Let $\sim$ be the relation on $\mathbb{Z}$ defined by $a \sim b$ if $a - b$ is a multiple of 4. We denote this relation by $a \equiv b \pmod 4$ read "a congruent to b modulo 4."

(a) Show that R is an equivalence relation on $\mathbb{Z}$.
(b) Find the equivalence classes of $\sim$.

Exercise 9.11
Let G be a group and H a subgroup of G. Define on G the relation $\sim$ given by $a \sim b$ if and only if $ab^{-1} \in H$. Prove that $\sim$ is an equivalence relation on G.

Exercise 9.12
Let $M = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}$. Define on M the relation $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that $\sim$ is an equivalence relation on M.

Exercise 9.13
Let $\sim$ be an equivalence relation on a nonempty set A. Define $A/\sim = \{[a] : a \in A\}$. Show that $\eta : A \to A/sim$ given by $\eta(a) = [a]$ is onto.

Exercise 9.14
Let $f : A \to B$ be a given function. Define the relation $a \sim b$ if and only if $f(a) = f(b)$. Show that $\sim$ is an equivalence relation.

Exercise 9.15
For the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$, for all $x \in \mathbb{R}$, describe the equivalence relation determined by f.

Exercise 9.16
Let $f : A \to B$ be a function and $\sim$ be the equivalence relation defined in the previous exercise. Prove that the mapping $\rho : A/\sim \to B$ defined by $\rho([a]) = f(a)$ is one-to-one.

Exercise 9.17
Prove that every mapping $\alpha : A \to B$ can be written in the form $\alpha = \rho \circ \eta$ where ρ is one-to-one and η is onto.

Exercise 9.18
True or false: The number of equivalence relations on a set A is the number of different partitions of A.

Exercise 9.19
(a) Find all of the partitions of $\{x, y, z\}$.
(b) How many different equivalence relations are there on a 3-element set?

10 The Division Algorithm. Congruence Modulo n

In this section, we want to introduce an important equivalence relation on the set of integers $\mathbb{Z}$. This relation depends on the concept of divisibility of integers which we discuss next.

10.1 Divisibility. The Division Algorithm

In this section we study the divisibility of integers. Our main goal is to obtain the *Division Algorithm*. This is achieved by applying the well-ordering principle which we prove next.

Theorem 10.1 *(The Well-Ordering Principle)*
If S is a nonempty subset of $\mathbb{N}$ then there is an $m \in S$ such that $m \leq x$ for all $x \in S$. That is, S has a smallest element.

Proof.
We will use contradiction to prove the theorem. That is, by assuming that S has no smallest element we will prove that $S = \emptyset$.
We will prove that $n \notin S$ for all $n \in \mathbb{N}$. We do this by induction on n. Since S has no smallest element then $1 \notin S$. Asuume that we have proved that $1, 2, \cdots, n \notin S$. We will show that $n + 1 \notin S$. If $n + 1 \in S$ then since $1, 2, 3, c \ldots \notin S$ then $n + 1$ would be the smallest element of S and this contradicts the assumption that S has no smallest element. Thus, we must have $n+1 \notin S$. Hence, by the principle of mathematical induction, $n \notin S$ for all $n \in \mathbb{N}$. But this leads to $S = \emptyset$. This conclusion contradicts the hypothesis of the theorem where S is given to be nonempty. This establishes a proof of the theorem.■

Remark 10.1
The above theorem is false if $\mathbb{N}$ is replaced by $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$.(See Exercise 10.6

Before establishing the Division Algorithm, we introduce the concept of divisibility and derive some of its properties.

Definition 10.1
An integer m is **divisible** *by a nonzero integer n if and only if $m = nq$ for*

some integer q. We also say that n **divides** *m, n is a* **divisor** *of m, m is a* **multiple** *of n, or n is a* **factor** *of m. We write $n|m$. If n does not divide m we write $n \nmid m$. A positive integer n with only divisors 1 and n is called* **prime.**

Example 10.1
Since $8 = 2 \cdot 4$ then $2|\ 8$ and $4|\ 8$. However, $4 \nmid 6$.■

The following theorem discusses some of the properties of divisibility.

Theorem 10.2
(a) If $n|m$ then $n|(-m)$.
(b) If $n|a$ and $n|b$ then $n|(a \pm b)$
(c) If $n|m$ and $m|p$ then $n|p$.
(d) If $n|m$ and $m|n$ then either $n = m$ or $n = -m$.

Proof.
(a) Suppose that $n|m$. Then $m = nq$ for some $q \in \mathbb{Z}$. Thus, $-m = (n)(-q)$ and hence $n|(-m)$.
(b) Suppose that $n|a$ and $n|b$. Then $a = nq$ and $b = nq'$ for some $q, q' \in \mathbb{Z}$. Thus, $a \pm b = n(q \pm q')$. Hence, $n|(a \pm b)$.
(c) Suppose that $n|m$ and $m|p$. Then $m = nq$ and $p = mq'$ for some $q, q' \in \mathbb{Z}$. Thus, $p = n(qq')$. Since $qq' \in \mathbb{Z}$ then $n|p$.
(d) If $n|m$ and $m|n$ then $m = nq$ and $n = mq'$ for some $q, q' \in \mathbb{Z}$. Thus, $m = mqq'$ or $(1 - qq')m = 0$. Since $m \neq 0$ then $qq' = 1$. This only true if either $q = q' = 1$ or $q = q' = -1$. That is, $n = m$ or $n = -m$.■

With the Well-Ordering Principle we can establish the following theorem.

Theorem 10.3 *(Division Algorithm)*
If a and b are integers with $b \geq 1$ then there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

Proof.
Existence
Consider the sets

$$S = \{a - bt : t \in \mathbb{Z}\}, \qquad S' = \{x \in S : x \geq 0\}.$$

The set S' is nonempty. To see this, if $a \geq 0$ then $a - 0t \in S$ and $a - 0t \geq 0$. That is, $a \in S'$. If $a < 0$ then since $a - ba \in S$ and $a - ba = a(1 - b) \geq 0$ so that $a - ba \in S'$.
Now, if $0 \in S'$ then $a - qb = 0$ for some $q \in \mathbb{Z}$ and so $r = 0$ and in this case the theorem holds. So, assume that $0 \notin S'$. By Theorem10.1, there exist a smallest element $r \in S'$. That is,

$$a - qb = r, \quad for\ some\ q \in \mathbb{Z}.$$

Since $r \in S'$ then $r \geq 0$. It remains to show that $r < b$. If we assume the contrary, i.e. $r \geq b$, then

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

and this implies that $a - b(q + 1) \in S'$. But $b > 0$ so that

$$a - b(q + 1) = a - bq - b < a - bq = r$$

and this contradicts the definition of r as being the smallest element of S'. Thus, we have

$$a = bq + r, \quad 0 \leq r < b.$$

Uniqueness
Suppose that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We must show that $r_1 = r_2$ and $q_1 = q_2$. Indeed, since $bq_1 + r_1 = bq_2 + r_2$ then $b(q_1 - q_2) = r_2 - r_1$. This says that $b|(r_2 - r_1)$. But $0 \leq r_1 < b$ and $0 \leq r_2 < b$ so that $-b < -r_1 < r_2 - r_1 < r_2 < b$. That is, $-b < r_2 - r_1 < b$. The only multiple of b strictly between $-b$ and b is zero. Hence, $r_1 = r_2$. But then $b(q_1 - q_2) = 0$ and since $b \neq 0$ then $q_1 = q_2$. ■

Example 10.2
If $a = 11$ and $b = 4$ then $q = 2$ and $r = 3$.

Remark 10.2
The above theorem is still valid for $b < 0$. Thus, given two integers a and b with $b \neq 0$, there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

(See Exercise 10.7).

10.2 Congruence Modulo n.

Divisibility leads to the concept of congruence.

Definition 10.2
Let n be a positive integer. Integers a and b are said to be **congruent modulo** *n if $a - b$ is divisible by n. This is denoted by writing $a \equiv b(mod\ n)$. We call n the* **modulus.** *If a is not congruent b modulo n we write $a \not\equiv b\ (mod\ n)$.*

Example 10.3
17 and 65 are congruent modulo 6, because $65 - 17 = 48$ is divisible by 6. ■

Theorem 10.4
The following statements are all equivalent:

(i) $a \equiv b(mod\ n)$
(ii) $n|(a - b)$
(iii) $a - b = nt$ for some $t \in \mathbb{Z}$
(iv) $a = b + nt$ for some $t \in \mathbb{Z}$.

Proof.
(i) $\Longrightarrow$ (ii): Suppose that $a \equiv b(mod\ n)$. Then from Definition def32, $n|(a-b)$.
(ii) $\Longrightarrow$ (iii): Suppose that $n|(a - b)$. Then by Definition 10.1, there exists a $t \in \mathbb{Z}$ such that $a - b = nt$.
(iii) $\Longrightarrow$ (iv): Suppose that $a - b = nt$ for some $t \in \mathbb{Z}$. Then by adding b to both sides we get $a = b + nt$ which is the statement of (iv).
(iv) $\Longrightarrow$ (i): Suppose that $a = b + nt$ for some $t \in \mathbb{Z}$. Then $a - b = nt$. By Definition 10.1, $a - b$ is divisible by n and so $a \equiv b(mod\ n)$. ■

Congruence modulo n is an equivalence relation on $\mathbb{Z}$ as shown in the next theorem.

Theorem 10.5
For each positive integer n, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof.
We shall show that $\equiv$ is reflexive, symmetric, and transitive.
Reflexive: Since $a - a = 0t$ for any $t \in \mathbb{Z}$ then $a \equiv a(mod\ n)$.

Symmetric: Let $a, b \in \mathbb{Z}$ be such that $a \equiv b(mod\ n)$. Then $a - b = nt$ for some $t \in \mathbb{Z}$. Multiplying both sides by -1 to obtain $b - a = n(-t)$. Since $(\mathbb{Z}, +)$ is a group then $-t \in \mathbb{Z}$ and so $b \equiv a(mod\ n)$.
Transitive: Suppose that $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$. Then $a - b = nt$ and $b - c = nt'$ for some $t, t' \in \mathbb{Z}$. Adding these equations together to obtain $a - c = n(t + t')$. But $\mathbb{Z}$ is closed under addition so that $t + t' \in \mathbb{Z}$. Hence, $a \equiv c(mod\ n)$. ■

Definition 10.3
The equivalence classes for the equivalence relation $\equiv$ are called congruence classes. They form a partition of $\mathbb{Z}$. The set of all congruence classes is denoted by $\mathbb{Z}_n$.

The following theorem shows that for each positive integer n, there are n congruence classes and each integer is congruent to either $0, 1, 2, \cdots, n-1$. Thus, the set $\{0, 1, 2, \cdots, n-1\}$ is a complete set of representatives of the relation $\equiv$.

Theorem 10.6
Let n be a positive integer. Then each integer is congruent modulo n to precisely one of the integers $0, 1, 2, \cdots, n-1$. That is, there are n distinct congruence classes, $[0], [1], \cdots, [n-1]$.

Proof.
Let a be any integer. Then by the Division Algorithm there exist unique integers q and r such that

$$a = nq + r, \quad 0 \leq r < n.$$

This impplies that $a - r = nq$ and so by Theorem 10.4, $a \equiv r(mod\ n)$. Since $0 \leq r < n$ then a is congruent to at least one of the integers,$0, 1, 2, \cdots, n-1$.We will show that a is congruent to exactly one of the integers listed. To see this, assume that $a \equiv s(mod\ n)$ where $0 \leq s < n$. Then by Theorem 10.4, $a = nt + s$ for some $t \in \mathbb{Z}$. By uniqueness, we have $r = s$. This completes a proof of the theorem.■

Remark 10.3
It follows from the previous theorem that

$$\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\}.$$

Example 10.4
For $n = 4$ the congruence classes are

$$\begin{aligned} [0] &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} \\ [1] &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} \\ [2] &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} \\ [3] &= \{\cdots, -5, -1, 3, 7, 11, \cdots\} \end{aligned}$$

Thus, $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$■

Review Problems

Exercise 10.1
List all the positive divisors of -101.

Exercise 10.2
List all the prime numbers less than 100.

Exercise 10.3
Find q *and* r *such that* $a = bq + r$.

(a) $a = -7, b = 5$.
(b) $a = 50, b = 6$.
(c) $a = 11, b = 17$.

Exercise 10.4
How many positive integers divide (a) 3? (b) 9? (c) 27? (d) 3^k, *where* k *is a positive integer.*

Exercise 10.5
Assume that p *is a prime and that* k *is a positive integer. How many positive integers divide (a)* p*? (b)* p^2*? (c)* p^3*? (d)* p^k*?*

Exercise 10.6
Verify that each of the following statements is false.

(a) Every nonempty subset of $\mathbb{Z}$ *contains a smallest element.*
(b) Every nonempty subset of $\mathbb{Q}$ *contains a smallest element.*

Exercise 10.7
Show that the Division algorithm is valid for $b < 0$. *Thus, given two integers* a *and* b *with* $b \neq 0$, *there exist unique integers* q *and* r *such that*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Exercise 10.8
List the distinct congruence classes modulo 5, exhibiting at least three elements in each class.

Exercise 10.9
Find all x such that $2x \equiv x (mod\ 5)$.

Exercise 10.10
Find all the integers x such that $-25 < x < 25$ and $x \equiv 3 (mod\ 5)$.

Exercise 10.11
Find all x such that $0 \leq x < 6$ and $2x \equiv 4 (mod\ 6)$.

Exercise 10.12
For which n is $25 \equiv 4 (mod\ n)$?

Exercise 10.13
Assume that $a \equiv b (mod\ n)$ and $c \equiv d (mod\ n)$. Prove eac of the following:

(a) $a \pm c \equiv b \pm d (mod\ n)$.
(b) $ac \equiv bd (mod\ n)$.
(c) $a^m \equiv b^m (mod\ n)$, where m is a positive integer.

Exercise 10.14
Prove that if $a \equiv b (mod\ n)$ and $n|a$, then $n|b$.

Exercise 10.15
Prove that if $a + x \equiv a + y (mod\ n)$ then $x \equiv y (mod\ n)$.

11 Arithmetic Modulo n

For a positive integer n, the congruence modulo n relation induces a partition on the set of integers by means of the elements of $\mathbb{Z}_n$ given by

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}.$$

Also, recall from Theorem 9.2, that if $a \equiv b(mod\ n)$ then $[a] = [b]$. Thus, for example, if $n = 6$ then all of the following congruence classes are equal:

$$[3] = [9] = [-3] = \{\cdots, -9, -3, 3, 9, \cdots\}$$

A word of caution must me made regarding the notation $[a]$. In later sections we will consider mappings from $\mathbb{Z}_m$ to $\mathbb{Z}_n$. So in order to distinguish between the elements of these sets we will adopt the notation $[a]_m$ to be an element of $\mathbb{Z}_m$ and that of $[a]_n$ to be an element of $\mathbb{Z}_n$. In a context where only the elements of $\mathbb{Z}_n$ are involved then we will keep the using the notation $[a]$.

Next, we consider two operations on $\mathbb{Z}_n$: Addition and multiplication.

Definition 11.1
For $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$ we define addition by the rule

$$[a] \oplus [b] = [a + b]$$

Example 11.1
For $n = 6$, we have $[-2]\oplus[7] = [-2+7] = [5]$ and $[3]\oplus[9] = [3+9] = [12] = [0]$.
■

The operation of addition turns $\mathbb{Z}_n$ into a finite Abelian group as shown next.

Theorem 11.1
(a) $\oplus$ defines a binary operation on $\mathbb{Z}_n$. That is, $\mathbb{Z}_n$ is closed under $\oplus$.
(b) $\oplus$ is commutative.
(c) $\oplus$ is associative.
(d) $[0]$ is the additive identity.
(e) Each $[a] \in \mathbb{Z}_n$ has an additive inverse $[-a] \in \mathbb{Z}_n$.
(f) $|\mathbb{Z}_n| = n$.

Proof.
(a) We need to show that if $([a],[b]) \in \mathbb{Z}_n \times \mathbb{Z}_n$ and $([c],[d]) \in \mathbb{Z}_n \times \mathbb{Z}_n$ are such that $([a],[b]) = ([c],[d])$ then $[a] \oplus [b] = [c] \oplus [d]$. That is, $[a+b] = [c+d]$. Equivalently, according to Theorem 9.2, we need to show that $a + b \equiv c + d(mod\ n)$. Since $[a] = [c]$ then $a \equiv c(mod\ n)$. Similarly, since $[b] = [d]$ then $b \equiv d(mod\ n)$. But Theorem 10.4, $a - c = nq$ and $b - d = nq'$ for some integers q, q'. Thus, $(a + b) - (c + d) = n(q + q')$ and by Theorem 10.4, $a + b \equiv c + d(mod\ n)$. Applying Theorem 9.2, we have $[a + b] = [c + d]$.
(b) The commutative property follows from the fact that addition in $\mathbb{Z}$ is commutative

$$\begin{aligned} [a] \oplus [b] &= [a + b] \\ &= [b + a] \\ &= [b] \oplus [a] \end{aligned}$$

(c) The associative property follows from the fact that addition in $\mathbb{Z}$ is associative

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

(d) Since 0 is the identity of the group $(\mathbb{Z}, +)$ then $[a] \oplus [0] = [a + 0] = [a]$ and $[0] \oplus [a] = [0 + a] = [a]$.
(e) Since for each $a \in \mathbb{Z}$ we have $a + (-a) = (-a) + a = 0$ then

$$\begin{aligned} [a] \oplus [-a] &= [a + (-a)] \\ &= [0] \end{aligned}$$

and

$$\begin{aligned} [-a] \oplus [a] &= [(-a) + a] \\ &= [0] \end{aligned}$$

(f) This follows from the definition of $\mathbb{Z}_n$.■

Remark 11.1
With the above theorem, we have a tool now to construct finite abelian groups of any order.

Example 11.2
Let us construct the Cayley table for $(\mathbb{Z}_4, \oplus)$.

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2] ■

Definition 11.2
The group $(\mathbb{Z}_n, \oplus)$ *is called the* **group of integers modulo** n.

Multiplication in $\mathbb{Z}_n$ is defined as follows:

$$[a] \odot [b] = [ab]$$

Example 11.3
For $n = 6]$, we have $[3] \odot [5] = [15] = [3]$.■

We next state the basic properties for this operation.

Theorem 11.2
(a) $\mathbb{Z}_n$ *is closed under* $\odot$.
(b) $\odot$ *is commutative.*
(c) $\odot$ *is associative.*
(d) $[1]$ *is the identity element.*

Proof.
The proofs of (a) - (d) are quite similar to those for the corresponding parts of Theorem th33, and are left as exercises.(See Exercise 11.10) ■

When we compare the properties listed in Theorems 11.1 and 11.2, we see that the existence of multiplicative inverses is missing. So, in contrast to $\mathbb{Z}_n$ with $\oplus$, $\mathbb{Z}_n$ with $\odot$ needs not be a group. The following example illustrates this situation.

Example 11.4
Writing Cayley table for $\mathbb{Z}_4$ we find

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Note that no element in $\mathbb{Z}_4$ satisfy the equation $[x] \odot [0] = [1]$. That is, $[0]$ has no multiplicative inverse.■

You might suspect that by removing the zero elements, the set $\mathbb{Z}_n^* = \{[1], [2], \cdots, [n-1]\}$ with $\oplus$ might be a group. Unfortunately, this is true for some values of n but not for all n as shown in the following two examples.

Example 11.5
$\mathbb{Z}_6^*$ is not a group with respect to $\odot$ since $\mathbb{Z}_6^*$ is not closed under $\odot$. Indeed, $[2] \odot [3] = [0] \notin \mathbb{Z}_6^*$. ■

Example 11.6
Constructing the Cayley table of $\mathbb{Z}_5^*$ with respect to $\odot$ we find

$\odot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Thus, $[1]^{-1} = [1], [2]^{-1} = [3], [3]^{-1} = [2]$, and $[4]^{-1} = [4]$.■

In the next section, we will characterize those elements in $\mathbb{Z}_n^*$ that have multiplicative inverses in $\mathbb{Z}_n^*$ and establish a condition on n for which $\mathbb{Z}_n^* = \{[1], [2], \cdots, [n-1]\}$ is a group under the operation $\odot$.

Review Problems

Exercise 11.1
(a) Give five elements in $[3]$ *as an element of* $\mathbb{Z}_5$.
(b) Give five elements in $[3]$ *as an element of* $\mathbb{Z}_7$.

Exercise 11.2
Simplify each of the following expressions in $\mathbb{Z}_5$ *and write the answer in terms of the elements of* $\mathbb{Z}_5$.

$$\begin{array}{llllll} (a) & [2] \oplus [-7] & (b) & [17] \oplus [76] & (c) & [2] \odot [-7] \\ (d) & [17] \odot [76] & (e) & [3] \odot ([2] \oplus [4]) & (f) & ([3] \odot [2]) \oplus ([3] \odot [4]) \end{array}$$

Exercise 11.3
Verify that $[1] \odot [2] \odot [3] \odot [4] = [4]$ *in* $\mathbb{Z}_4$.

Exercise 11.4
Find the elements $[a]$ *of* $\mathbb{Z}_6$ *for which the equation* $[a] \odot [x] = [0]$ *has a nonzero solution in* $\mathbb{Z}_6$.

Exercise 11.5
Whenever possible, find a solution for each of the following equations in the given $\mathbb{Z}_n$.

$$\begin{array}{ll} (a) \quad [3] \odot [x] = [2] \text{ in } \mathbb{Z}_6 & (b) [6] \odot [x] = [4] \text{ in } \mathbb{Z}_8 \\ (c) \quad [4] \odot [x] = [6] \text{ in } \mathbb{Z}_8 & (d) [8] \odot [x] = [6] \text{ in } \mathbb{Z}_{12} \end{array}$$

Exercise 11.6
Contruct the Cayley table for $(\mathbb{Z}_4, \oplus)$.

Exercise 11.7
Construct the Cayley table for $(\mathbb{Z}_6^*, \odot)$. *Show that* $\mathbb{Z}_6^*$ *is not a group under* $\odot$.

Exercise 11.8
Prove that $\odot$ *is distributive with respect to* $\oplus$ *in* $\mathbb{Z}_n$.

Exercise 11.9
Prove that $(\mathbb{Z}_3^*, \odot)$ *is a group.*

Exercise 11.10
Give a proof of Theorem 11.2.

Exercise 11.11
Solve the equation: $[x]^2 + [x] - [6] = [0]$ *in* $\mathbb{Z}_{11}$.

Exercise 11.12
Solve the system of congruences: $2x \equiv 9 (mod\ 15)$ *and* $x \equiv 8 (mod\ 11)$.

12 Greatest Common Divisors. The Euclidean Algorithm

As mentioned at the end of the previous section, we would like to establish a condition on n so that $(\mathbb{Z}_n^*, \odot)$ is a group. This section provides the tool needed for that.
We start this section with the following definition.

Definition 12.1
Let a and b be two integers, not both zero. A positive integer d is called a **greatest common divisor** *of a and b if the following two conditions hold:*

(1) $d|a$ and $d|b$.
(2) If $c|a$ and $c|b$ then $c|d$.
We write $d = (a, b)$ or $d = gcd(a, b)$.

Example 12.1
The greatest common divisor of -42 and 56 is 14. The greatest common divisor is useful for writing fractions in lowest term. For example, $-\frac{42}{56} = -\frac{3}{4}$ where we cancelled $14 = (42, 56)$.■

We next discuss a systematic procedure for finding the greatest commom divisor of two integers, known as the **Euclid's Algorithm.** For that purpose, we need the following result.

Theorem 12.1
If $a, b, q,$ and r are integers such that $a = bq + r$ then $(a, b) = (b, r)$.

Proof.
Let $d_1 = (a, b)$ and $d_2 = (b, r)$. We will show that $d_1 = d_2$. Since $d_2|bq$ and $d_2|r$ then by Theorem 10.2, $d_2|(bq+r)$. That is $d_2|a$. Thus, by Definition 12.1, $d_2|d_1$. Since $d_1|b$ then $d_1|bq$. Since $d_1|a$ then $d_1|(a - bq)$. That is, $d_1|r$. Hence, from the definition of d_2, we have $d_1|d_2$. Since d_1 and d_2 are positive then by Theorem 10.2(d), we have $d_1 = d_2$. ■

The following theorem, establishes the existence and uniqueness of the greatest common divisor and provide an algorithm of how to find it.

Theorem 12.2 *(The Euclidean Algorithm)*
If a and b are two integers, not both zero, then there exists a unique positive integer d such that the two conditions (1) and (2) of Definition 12.1 are satisfied.

Proof.
Uniqueness: Let d_1 and d_2 be two positive integers that satisfy conditions (1) and (2). Then by (2) we can write $d_1|d_2$ and $d_2|d_1$. Since d_1 and d_2 are both positive then Theorem 10.2 (d) implies that $d_1 = d_2$.

Existence: Without loss of generality, we may assume that $b \neq 0$. Note that if $a = 0$ then $d = |b|$. Indeed, $|b|$ $|0$ and $|b|$ $|b$. Moreover, if c is a common divisor of a and b then $b = cq$ so that $|b| = cq'$. That is, $c|$ $|b|$.
So assume that $a \neq 0$. By the Division algorithm there exist unique integers q_1 and r_1 such that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|.$$

If $r_1 = 0$ then as above, one can easily check that $d = |b|$. So assume that $r_1 \neq 0$. Using the Division algorithm for a second time to find unique integers q_2 and r_2 such that

$$b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1.$$

We keep this process going and eventually we will find integers r_n and r_{n+1} such that

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

and

$$r_{n-1} = r_nq_{n+1}.$$

That is, r_n is the last nonzero remainder in the process. By Theorem 12.1, we see that $r_n = (a, b)$.■

Example 12.2
Performing the arithmetic for the Euclidean algorithm we have

$$\begin{aligned} 1776 &= (1)(1492) + 284 \\ 1492 &= (5)(284) + 72 \\ 284 &= (3)(72) + 68 \\ 72 &= (1)(68) + 4 \\ 68 &= 4(17) \end{aligned}$$

So $(1776, 1492) = 4$.■

An alternative proof for the existence of the greatest common divisor which does not provide a systematic way for finding (a, b) is given next.

Theorem 12.3
If a and b are two integers, not both zero, then there exist integers m and n such that

$$(a, b) = ma + nb.$$

That is, (a, b) can be expressed as a linear combination of a and b.

Proof.
Without loss of generality, we assume that $b \neq 0$. Let $S = \{xa+yb : x, y \in \mathbb{Z}\}$ and $S' = \{xa + yb \in S : xa + yb > 0\}$. Since $b = 0a + (1)b$ then $b \in S$. Thus, $S \neq \emptyset$. Also, $S' \neq \emptyset$. To see this, note that if $b > 0$ then $b = 0a + (1)b \in S'$. If $b < 0$ then $-b = 0a + (-1)b \in S'$. By Theorem 10.1, S' has a smallest element d. Thus, $d = ma + nb > 0$ for some integers m and n. We will show next that $d = (a, b)$. Applying the Division algorithm we can find integers q and r such that $a = dq + r$ with $0 \leq r < d$. From this equation we see that

$$\begin{aligned} r &= a - dq \\ &= a - (ma + nb)q \\ &= (1 - mq)a + (-nq)b \end{aligned}$$

If $r > 0$ then $r \in S'$ and $r < d$. This contradicts the definition of d. Therefore, $r = 0$ and this gives $a = dq$ and hence $d|a$. A similar argument holds for $d|b$. Finally, if c is an integer such that $c|a$ and $c|b$ then $a = cq$ and $b = cq'$. Thus,

$$d = ma + nb = mcq + ncq' = c(mq + nq')$$

This means that $c|d$. Thus, $d = (a, b)$. This ends a proof of the Theorem. ■

Remark 12.1
The integers m and n in Theorem 12.3 are not unique. Indeed,

$$\begin{aligned} (a, b) &= ma + nb \\ &= ma + ab + nb - ab \\ &= (m + b)a + (n - a)b \quad = \quad m'a + n'b \end{aligned}$$

Example 12.3
From Example 12.2, we found that $(1776, 1492) = 4$. Let's write this as a

linear combination of 1776 and 1492. We use the equations in Example 12.2, beginning with $72 = (1)(68) + 4$ and working backward one step at a time.

$$4 = 72 - (1)(68).$$

Solve the equation $284 = (3)(72) + 68$ for 68 and substitute in the previous equation and simplify to obtain

$$\begin{aligned} 4 &= 72 - (1)(284 - 3 \cdot 72) \\ &= 72 \cdot (4) - 284 \end{aligned}$$

Solve the equation $1492 = (5)(284) + 72$ for 72 and substitute in the previous equation and simplify to obtain

$$\begin{aligned} 4 &= (1492 - 5 \cdot 284) \cdot 4 - 284 \\ &= 1492 \cdot 4 - 21 \cdot 284 \end{aligned}$$

Finally, solve the equation $1776 = 1492 + 284$ for 284 and substitute to obtain

$$\begin{aligned} 4 &= 1492 \cdot 4 - 21(1776 - 1492) \\ &= -21 \cdot 1776 + 25 \cdot 1492 \ \blacksquare \end{aligned}$$

Theorem 12.4
If a and b are integers, not both zero, then $(a, b) = 1$ if and only if $ma + nb = 1$ for some integers m and n.

Proof.
Suppose first that $(a, b) = 1$. By Theorem **??**, there exist integers m and n such that $ma + nb = 1$.
Conversely, suppose that $ma + nb = 1$ for some integers m and n. If $d = (a, b)$ then $d|a$ and $d|b$ so $d|(ma + nb)$. That is, $d|1$. Since $d > 0$ then by Theorem 10.2(d) we must have $d = 1$. ■

Definition 12.2
If a and b are integers such that $(a, b) = 1$ then we say that a and b are **relatively prime.**

The next result, characterizes those elements of $\mathbb{Z}_n$ that have multiplicative inverses.

Theorem 12.5
$[a] \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $(a, n) = 1$.

Proof.
Suppose first that $[a]$ has a multiplicative inverse $[b]$ in $\mathbb{Z}_n$. Then $[a] \odot [b] = [ab] = [1]$. This implies that $ab \equiv 1(modn)$. Therefore, $ab = nq + 1$ for some integer q. This last equality can be written in the form $ba + (-q)n = 1$. By Theorem 12.4, $(a, n) = 1$.
Conversely, suppose that $(a, n) = 1$. Then by Theorem 12.4, there exist integers m and q such that $ma + qn = 1$. Thus, $ma - 1 = (-q)n$ and hence $ma \equiv 1(mod\ n)$. In terms of $\odot$, we have $[m] \odot [a] = [1]$. Thus, $[a]$ has a multiplicative inverse in $\mathbb{Z}_n$.■

As a consequence of the above theorem we have

Theorem 12.6
Every nonzero element of $\mathbb{Z}_n$ has a multiplicative inverse if and only if n is a prime number. Thus, $(\mathbb{Z}_n^*, \odot)$ is a group if and only if n is prime.

Proof.
If n is prime then $(a, n) = 1$ for every $1 \leq a < n$. By Theorem 12.6, $[a]$ has a multiplicative inverse for all $1 \leq a < n$. Conversely, suppose that $[a]$ has a multiplicative inverse for all $1 \leq a < n$. Again, by Theorem 12.6, $(a, n) = 1$ for $1 \leq a < n$. This is true only if n is prime.■

Review Problems

Exercise 12.1
In each part, find the greatest common divisor (a, b) and integers m and n such that $(a, b) = ma + nb$.

(a) $a = 65, b = 91$.
(b) $a = 5088, b = 156$.
(c) $a = -75, b = 105$.

Exercise 12.2
List all the prime numbers less than 100.

Exercise 12.3
Find the smallest integer in the set

$$\{x \in \mathbb{Z} : x > 0 \text{ and } x = 6m + 15n,\ m, n \in \mathbb{Z}\}$$

Exercise 12.4
List all of the positive integers that are less than 12 and relatively prime to 12.

Exercise 12.5
Prove that if c is a divisor of a and b then c is a divisor of $ma + nb$ for all $m, n \in \mathbb{Z}$.

Exercise 12.6
Prove that if a and b are distinct prime then there exist integers m and n such that $ma + nb = 1$.

Exercise 12.7
Prove that $(ab, c) = 1$ if and only if $(a, c) = (b, c) = 1$.

Exercise 12.8
Prove that if c is a positive integer then $(ac, bc) = (a, b)c$.

Exercise 12.9
Prove that if a is an integer and p is a prime such that $p \not| a$ then $(a, p) = 1$.

Exercise 12.10
Prove that if $(a, b) = 1$ *and* $c|a$ *then* $(c, a) = 1$.

Exercise 12.11
Prove that if $(a, n) = 1$ *then there is a solution to the congruence equation* $ax \equiv 1(mod\ n)$.

Exercise 12.12
For each positive integer n*, let* $\phi(n)$ *denote the number of positive integers less than and rlatively prime to* n*. For example,* $\phi(3) = 2$ *and* $\phi(4) = 2$*. We define* $\phi(1) = 1$*. We call* ϕ *the Euler's function.*

(i) Find $\phi(n)$ *for* $1 \leq n \leq 10$.
(ii) Find a formula for $\phi(p)$ *if* p *is a prime number.*

Exercise 12.13
For each positive integer n *let*

$$\mathbb{Z}_{(n)} = \{[k] : 1 \leq k < n \text{ and } (k, n) = 1\}.$$

(a) List the elements of $\mathbb{Z}_{(12)}$.
(b) Prove that $(\mathbb{Z}_{(n)}, \odot)$ *is a group.*
(c) Show that the number of elements of $\mathbb{Z}_{(n)}$ *is* $\phi(n)$.

13 Least Common Multiple. The Fundamental Theorem of Arithmetic

In the previous section, we learned how to find the largest positive divisor of two integers that are not both zero. In this section, we want to find the smallest common factor of two nonzero integers.

Theorem 13.1
If a and b are nonzero integers then there is a unique positive integer m such that

(1) $a|m$ and $b|m$;
(2) if c is an integer such that $a|c$ and $b|c$ then $m|c$.

Proof.
Let $S = \{x \in \mathbb{N} : a|x \text{ and } b|x\}$. Since $a|\ |ab|$ and $b|\ |ab|$ then $|ab| \in S$ and therefore $S \neq \emptyset$. By Theorem 10.1, S has a smallest element m. Thus, $a|m$ and $b|m$. This proves (1).
To prove (2), we assume that c is an integer such that $a|c$ and $b|c$. By the Division Algorithm there exist unique integers q and r such that

$$c = mq + r, \quad 0 \leq r < m.$$

Since $a|c$ then $c = aq_1$ for some $q_1 \in \mathbb{Z}$. Since $a|m$ then $m = aq_2$ for some $q_2 \in \mathbb{Z}$. Thus,

$$aq_1 = aqq_2 + r$$

This implies that $a|r$. A similar argument with b replacing a we find that $b|r$. If $r > 0$ then $r \in S$ and this contradicts the definition of m. So we must have $r = 0$. Therefore, $c = mq$ and $m|c$. This completes a proof of the theorem.■

Definition 13.1
The positive integer m is called the **least common multiple** *of a and b and is denoted by $[a, b]$.*

Example 13.1
If $a = 25$ and $b = 33$ then $[25, 33] = 825$. Similarly, $[4, -6] = 12$.■

Our next goal is to find a method for finding the least common multiple of two nonzero integers. The method is a result of the Fundamental Theorem of Arithmetic.
For that purpose we need the following lemmas.

Lemma 13.1
If a, b, and c are integers such that $a|bc$ and $(a, b) = 1$ then $a|c$.

Proof.
Since $(a, b) = 1$ then by Theorem 12.4, there are integers m and n such that $ma + nb = 1$. Multiply this equation by c to obtain $mac + nbc = c$. Since $a|\ bc$ then $a|\ (mac + nbc)$. That is, $a|c$. ■

Remark 13.1
The condition $(a, b) = 1$ is critical. For example, if $a = 6, b = 3$, and $c = 4$. Then $a|bc$ but neither a divides b or a divides c. Note that $(a, b) = 3 \neq 1$.

Lemma 13.2
If a is an integer and p is a prime number such that $p \not| a$ then $(a, p) = 1$.

Proof.
Let $d = (a, p)$. Then $d|a$ and $d|p$. Since p is prime then either $d = 1$ or $d = p$. If $d = p$ then $p|a$ which contradicts the fact that $p \not| a$. Thus, $d = 1$. ■

Lemma 13.3
If $a_1, a_2, \cdots, a_n$ are integers and p is a prime such that $p|\ a_1a_2 \cdots a_n$ then $p|\ a_i$ for some $1 \leq i \leq n$.

Proof.
The proof is by induction on n. The case $n = 1$ is trivial. So assume that the lemma holds for all positive integers up to and including n-1. We will show that the result still holds for n. Since $p|\ a_1a_2 \cdots a_n$ then either $p|a_1a_2 \cdots a_{n-1}$ or $p\ \not|a_1a_2 \cdots a_{n-1}$. If $p|\ a_1a_2 \cdots a_{n-1}$ then by the induction hypothesis, $p|\ a_i$ for some $1 \leq i \leq n - 1$. If $p\ \not|a_1a_2 \cdots a_{n-1}$ then by Lemma 13.2, $(p, a_1a_2 \cdots a_{n-1}) = 1$. By Lemma13.1 (with $a = a_1a_2 \cdots a_{n-1}$ and $b = a_n$) we have $p|a_n$. ■

Theorem 13.2 *(The Fundamental Theorem of Arithmetic)*
Every positive integer $n > 1$ is either a prime or can be written as a product of prime integers, and this product is unique except for the order of the factors.

Proof.
The proof is by induction on n. The theorem is trivially true for $n = 2$ since 2 is prime. Assume, then that it is true for the integers $2, 3, \cdots, n-1$. We shall prove that it is also true for n. If n is prime there is nothing to prove. Assume, then, that n is composite and that n has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \tag{2}$$

Since p_1 divides the product $q_1, q_2, \cdots, q_t$, then by Lemma 13.3, it must divide at least one factor. Relabel $q_1, q_2, \cdots, q_t$ so that $p_1 | \ q_1$. Then $p_1 = q_1$ since both p_1 and q_1 are primes. In (2), we may cancel p_1 on both sides to obtain

$$\frac{n}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t < n.$$

By the induction hypothesis, the two factorizations of $\frac{n}{p_1}$ must be identical except for the order of the factors. Therefore, $s = t$ and the factorizations in (2) are also identical, except for the order of factors. This ends a proof of the theorem.■

Remark 13.2
In the factorization of an integer $n > 1$, a particular prime p may occur more than once. If the distinct prime factors of n are $p_1 < p_2 < \cdots < p_s$ and if p_i occurs as a factor k_i times, we can write

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

We shall call this the **standard form** for n.

Lemma 13.4
Let m and n be two integers with the following prime factorization

$$m = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad \textit{and} \quad n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

Then $m|n$ if and only if $k_i \leq t_i$ for $1 \leq i \leq s$.

Proof.
If p is a prime and a and b are integers such that α is the highest power of p dividing a and β is the highest power of p dividing b then $a = p^\alpha q$ and $b = p^\beta q'$ for some $q, q' \in \mathbb{Z}$. Thus, $ab = p^{\alpha+\beta} q''$, where $q'' \in \mathbb{Z}$. Hence, $\alpha + \beta$ is the highest power of p dividing ab. So if $m|n$ then $m = nu$ for some integer

u. Thus, for each $1 \leq i \leq s$, the highest power of p_i dividing n is the sum of the highest powers of p_i dividing m and u. Thus, $k_i \leq t_i$ for $1 \leq i \leq s$.
Conversely, suppose that $k_i \leq t_i$ for all $1 \leq i \leq s$. Let $u_i = t_i - k_i$ for $1 \leq i \leq s$. Let $w = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$. Then $n = mw$ and so $m|n$.■

We have the following result which expresses $[a, b]$ in terms of the factorizations of a and b.

Theorem 13.3
If two nonzero integers a and b have the factorizations

$$a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad \textit{and} \quad b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

then

$$[a, b] = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$$

where u_i is the maximum of k_i and t_i for each $1 \leq i \leq s$.

Proof.
Let $m = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$ where u_i is the maximum of k_i and t_i. We will show that $m = [a, b]$. Since $k_i \leq u_i$ and $t_i \leq u_i$ for all $1 \leq i \leq s$ then by Lemma 13.4, $a|m$ and $b|m$. Now, if c is an integer such that $a|c$ and $b|c$. Write $c = p_1^{w_1} p_2^{w_2} \cdots p_s^{w_s}$. Then by Lemma 13.4, $k_i \leq w_i$ and $t_i \leq w_i$ for all $1 \leq i \leq s$. Thus, $u_i \leq w_i$ for all $1 \leq i \leq s$. By Lemma 4, $m|c$. It follows that $m = [a, b]$. ■

Finding the least common multiple Similarly, Theorem 13.2 can be used to find the greatest common divisor of two integers.

Theorem 13.4
If two nonzero integers a and b have the factorizations

$$a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad \textit{and} \quad b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

then

$$(a, b) = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$$

where u_i is the minimum of k_i and t_i for each $1 \leq i \leq s$.

Proof.
Left as an exercise for the reader. See Exercise 13.3.■

Remark 13.3
The above theorem gives a way to find (a, b) if we know the factorizations of a and b. But factorizing a number is a very hard problem and so, the above method is ineffective. Instead, the Euclidean Algorithm is more practical.

Example 13.2
Consider the prime factorizations of the integers 31752 and 126000 :

$$31752 = 2^3 \cdot 3^4 \cdot 7^2 \quad and \quad 126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7.$$

Then from Theorems 13.3 and 13.4 we have

$$[31752, 126000] = 2^4 \cdot 3^4 \cdot 5^3 \cdot 7^2 = 7938000$$

and

$$(31752, 126000) = 2^3 \cdot 3^2 \cdot 7 = 504.\blacksquare$$

Review Problems

Exercise 13.1
Determine the standard form for each of the following integers.

(a) 684 (b) 1375

Exercise 13.2
Compute the greatest common divisor and the least common multiple using the standard forms.

(a) 10,105 (b) -2860,-2310 (c) -39, 54.

Exercise 13.3
Prove Theorem 13.4.

Exercise 13.4
Prove that if a and b are positive integers then

$$(a, b)[a, b] = ab.$$

Exercise 13.5
Prove that if $(a, b) = 1, a|m,$ and $b|m$ then $ab|m$.

Exercise 13.6
Determine $\phi(p^k)$ if p is a prime number and k is a positive integer, where ϕ is the Euler function.

Exercise 13.7
Prove that if $a|bc$ then $a|(a, b)c$.

Exercise 13.8
Prove that $[a, b, c] = [[a, b], c] = [a, [b, c]]$.

Exercise 13.9
(a) Prove that $(a, b, c) = ((a, b), c) = (a, (b, c))$.
(b) Prove that $(a, b, c) = ma + nb + pc$ for some integers m, n, p.

Exercise 13.10
Let $p > 1$ be an integer with the property that if $p|ab$ then $p|a$ or $p|b$. Prove that p must be a prime number.

Exercise 13.11
Let n be an integer. Prove that $\sqrt{n} \in \mathbb{Q}$ if and only if $n = k^2$ for some $k \in \mathbb{Z}$.

Exercise 13.12
Prove that $\sqrt[3]{2}$ is irrational.

14 Elementary Properties of Groups

In this section, we prove more theorems about groups. In what follows the group binary operation will be referred to as multiplication and thus we will write ab.
Several simple consequences of the definition of a group are recorded in the following two theorems.

Theorem 14.1
For any group G, the following properties hold:

(i) If $a, b, c, \in G$ and $ab = ac$ then $b = c$. (left cancellation law)
(ii) If $a, b, c, \in G$ and $ba = ca$ then $b = c$. (right cancellation law)
(iii) If $a \in G$ then $(a^{-1})^{-1} = a$. The inverse of the inverse of an element is the element itself.
(iv) If $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$. That is the inverse of a product is the product of the inverses in reverse order.

Proof.
(i) Suppose that $ab = ac$. Then

$$\begin{aligned} b &= eb = (a^{-1}a)b \\ &= a^{-1}(ab) = a^{-1}(ac) \\ &= (a^{-1}a)c = ec = c \end{aligned}$$

(ii) Suppose that $ba = ca$. Then

$$\begin{aligned} b &= be = b(aa^{-1}) \\ &= (ba)a^{-1} = (ca)a^{-1} \\ &= c(aa^{-1}) = ce = c \end{aligned}$$

(iii) If $a \in G$ then since $aa^{-1} = a^{-1}a = e$ then a is an inverse of a^{-1}. Since inverses are unique then $(a^{-1})^{-1} = a$.
(iv) Let x be the inverse of ab. Then $(ab)x = e$ By associativity, we have $a(bx) = aa^{-1}$. By (i), we have $bx = a^{-1}$. But $bx = ea^{-1} = b(b^{-1}a^{-1})$ so that by applying (i) again we obtain $x = b^{-1}a^{-1}$. Therefore, $(ab)^{-1} = b^{-1}a^{-1}$.■

Theorem 14.2
If G is a group and $a, b \in G$ then each of the equations $ax = b$ and $xa = b$ has a unique solution. In the first, the solution is $x = a^{-1}b$ whereas in the second $x = ba^{-1}$.

Proof.
Consider first the equation $ax = b$. We want to isolate the x on the left side. Indeed, this can be done as follows.

$$\begin{aligned} x &= ex = (a^{-1}a)x \\ &= a^{-1}(ax) = a^{-1}b \end{aligned}$$

To prove uniqueness, suppose that y is another solution to the equation $ax = b$. Then, $ay = b = ax$. By the left cancellation property we have $x = y$. Finally, the proof is similar for the equation $xa = b$.■

Remark 14.1
Suppose G is a finite group and $a, b \in G$. The product ax is in the row labelled by a of the Cayley table. By Theorem 14.2, the equation $ax = b$ has a unique solution means that b appears only once in the row of a of the table. Thus, each element of a finite group appears exactly once in each row of the table. Similarly, because there is a unique solution of $xa = b$, each element appears exactly once in each column of the Cayley table. It follows that each row is a rearrangement of the elements of the group.

Next, we discuss the extension of the associative property to products with any number of factors. More specifically, we will prove the so-called *generalized associative law* which states that in a set with associative operation, a product of factors is unchanged regardless of how parentheses are inserted as long as the factors and their order of appearance in the product are unchanged.

Definition 14.1
For elements $a_1, a_2, \cdots, a_n$ $(n \geq 2)$ of a group G define

$$a_1a_2 \cdots a_{n-1}a_n = (a_1a_2 \cdots a_{n-1})a_n.$$

Theorem 14.3 *(Generalized Associative Law)*
For any integer $1 \leq m < n$ we have

$$(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_n) = a_1a_2 \cdots a_n.$$

Proof.
For $n \geq 2$, let $\mathcal{S}(n)$ be the statement

$$(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_n) = a_1a_2 \cdots a_n : \textit{ where } a_1, a_2, \cdots, a_n \in G \textit{ and } 1 \leq m < n.$$

We prove that $\mathcal{S}(n)$ is true for all $n \geq 2$ by induction on n. For $n = 2$ the statement is true since $(a_1)(a_2) = a_1a_2$ (the only possible value for m is $m = 1$.) So assume that the statement is valid for $2, 3, \cdots, n-1$. We will show that $\mathcal{S}(n)$ is also true. Suppose that $1 \leq m < n$. Then either $m = n-1$ or $1 \leq m < n-1$. If $m = n-1$ then

$$(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_n) = (a_1a_2 \cdots a_{n-1})a_n = a_1a_2 \cdots a_n.$$

So suppose that $1 \leq m < n-1$. Then

$$\begin{aligned}(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_n) &= (a_1a_2 \cdots a_m)[(a_{m+1} \cdots a_{n-1})a_n] \\ &= [(a_1a_2 \cdots a_m)(a_{m+1} \cdots a_{n-1})]a_n \\ &= (a_1a_2 \cdots a_{n-1})a_n \\ &= a_1a_2 \cdots a_n\end{aligned}$$

Thus, $\mathcal{S}(n)$ is true for all $n \geq 2$ and this completes a proof of the theorem. ■

Next, we introduce the concept of integral exponents of elements in a group. The concept plays an important role in the theory of cyclic groups.

Definition 14.2
For any $a \in G$ we define

$$\begin{aligned}a^0 &= e \\ a^n &= a^{n-1}a, \quad for\ n \geq 1 \\ a^{-n} &= (a^{-1})^n \quad for\ n \geq 1.\end{aligned}$$

Remark 14.2
By Theorem 14.3, $a^n = a \cdot a \cdot a \cdots a$ where the product contains n copies of a. Also, note that $aa^{n-1} = a^{n-1}a = a^n$.

The familiar laws of exponents hold in a group.

Theorem 14.4
Let a be an element of a group G and m and n denote integers. Then

(i) $a^na^{-n} = e$.
(ii) $a^ma^n = a^{m+n}$
(iii) $(a^m)^n = a^{mn}$.

Proof.
(i) The identity is trivial for $n = 0$. So suppose that $n > 0$. We use induction on n. Since $aa^{-1} = e$ then the result is true for $n = 1$. Suppose the identity holds for $1, 2, \cdots, n-1$. We must show that it is valid for n. Indeed,

$$\begin{aligned} a^n a^{-n} &= (a^{n-1}a)[(a^{-1})^{-(n-1)}a^{-1}] \\ &= (aa^{n-1})[(a^{-1})^{-(n-1)}a^{-1}] \\ &= [(aa^{n-1})(a^{-1})^{-(n-1)}]a^{-1} \\ &= [a(a^{n-1}a^{-(n-1)})]a^{-1} \\ &= (ae)a^{-1} = aa^{-1} = e \end{aligned}$$

Thus, the identity is true for all positive integers n.
Now, suppose that $n < 0$ then

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

(ii) We have to show that for a fixed integer m the identity holds for all integers n. That is, the identity holds for $n = 0, n > 0$, and $n < 0$. If $m = 0$ then $a^m a^n = a^0 a^n = ea^n = a^n = a^{0+n}$ for all integers n. So, suppose first that $m > 0$.

$\underline{n = 0}$

$$\begin{aligned} a^{m+n} &= a^{m+0} = a^m \\ a^m a^n &= a^m a^0 = a^m e = a^m \end{aligned}$$

$\underline{n > 0}$
By induction on $n > 0$. The case $n = 1$ follows from Definition 14.2. Suppose that the identity has been established for the numbers $1, 2, \cdots, n-1$. We will show that it is still true for n. Indeed,

$$\begin{aligned} a^m a^n &= a^m(a^{n-1}a) \\ &= (a^m a^{n-1})a \\ &= a^{m+n-1}a \\ &= a^{m+n} \quad (by\ Definition\ 14.2) \end{aligned}$$

By induction, it follows that the identity is true for all $n > 0$.

$\underline{n < 0, n = -m}$
Since $n = -m$ then $n + m = 0$ and in this case we have $a^{m+n} = a^0 = e$. By

(i), we have $a^m a^n = a^m a^{-m} = e$. It follows that $a^m a^n = a^{m+n}$.

$\underline{n < 0, n > -m}$
Then $m = (m+n) + (-n)$ where both $m+n$ and $(-n)$ are positive.

$$\begin{aligned} a^m a^n &= a^{(m+n)+(-n)} a^n \\ &= (a^{m+n} a^{-n}) a^n \\ &= a^{m+n} (a^{-n} a^n) \\ &= a^{m+n} e = a^{m+n} \end{aligned}$$

$\underline{n < 0, n < -m}$
In this case, $-n = m + [-(m+n)]$ where both m and $-(n+m)$ are positive.

$$\begin{aligned} a^m a^n &= a^m (a^{-1})^{-n} \\ &= a^m (a^{-1})^{m-(m+n)} \\ &= a^m [(a^{-1})^m (a^{-1})^{-(m+n)}] \\ &= a^m [a^{-m} (a^{-1})^{-(m+n)}] \\ &= (a^m a^{-m})(a^{-1})^{-(m+n)} \\ &= (a^{-1})^{-(m+n)} = a^{m+n} \end{aligned}$$

Similar arugument holds for a fixed $m < 0$ and all integers n. This completes a proof of (ii).

(iii) Similar to (ii) and is left as an exercise. See Exercise 14.21.■

Remark 14.3
In the case of an group G written with the binary operation $+$, for $n \in \mathbb{Z}^+$ and $a \in G$, one writes na instead of a^n, where $na = a + ... + a$ (n times), and $(-n)a = -(na) = n(-a)$. The laws corresponding to (ii) and (iii) of Theorem 14.4 become

$$ma + na = (m+n)a$$

and

$$n(ma) = (mn)a.$$

where $m, n \in \mathbb{Z}$.

The set of all integral exponents of an element a in a group G forms a subgroup of G as shown in the next theorem.

Theorem 14.5
Let G be a group and $a \in G$. Then the set

$$< a >= \{a^n : n \in \mathbb{Z}\}$$

is a subgroup of G.

Proof.
The set $< a >$ is nonempty since $a^0 = e \in < a >$. Now, let $x, y \in < a >$. Then $x = a^n$ and $y = a^m$ for some integers n and m. Thus,

$$\begin{aligned} xy^{-1} &= a^n(a^m)^{-1} \\ &= a^n a^{-m} \ (by\ Theorem\ 14.1(iv)) \\ &= a^{n-m} \ (by\ Theorem\ 14.4(ii)) \end{aligned}$$

Since $n - m \in \mathbb{Z}$ then $xy^{-1} \in < a >$. Thus, by Theorem 7.5, $< a >$ is a subgroup of G, as required. ■

Definition 14.3
The subgroup $< a >$ is called the **subgroup generated by a**. *Any subgroup H of G that can be written as $K =< a >$ is called a* **cyclic subgroup.** *The element a is called a* **generator**. *In particular, G is a* **cyclic group** *if there is an element $a \in G$ such that $G =< a >$.*

Example 14.1
1. The group $\mathbb{Z}$ of integers under addition is a cyclic group, generated by 1 (or -1). Thus, $(\mathbb{Z}, +)$ is a cyclic group of infinite order.
2. Let n be a positive integer. The set Z_n of congruence classes of integers modulo n is a cyclic group of order n with respect to the operation of addition with generator [1].

The following theorem shows that when powers of a are equal then the cyclic group $< a >$ is of finite order.

Theorem 14.6
Let G be a group and $a \in G$ be such that $a^r = a^s$ for some integers r and s with $r \neq s$.

(i) There is a smallest positive integer n such that $a^n = e$.
(ii) $a^t = e$ if and only if $n|t$.
(iii) The elements $e, a, a^2, \cdots, a^{n-1}$ are distinct and

$$< a >= \{e, a, a^2, \cdots, a^{n-1}\}.$$

Proof.
(i) Let $S = \{p \in \mathbb{Z}^+ : a^p = e\}$. Assume that $r > s$. (If $s > r$ then interchange the letters r and s in the following sentences) Since $a^r = a^s$ then $a^r a^{-s} = a^s a^{-s} = e$. Thus, $r - s \in S$. By Theorem 10.1, there is a smallest positive integer n such that $a^n = e$.
(ii) Suppose first that $a^t = e$ for some integer t. By the Division Algorithm there exist integers q and r such that $t = nq + r$ where $0 \leq r < n$. Thus, $e = a^t = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$. By the definition of n we must have $r = 0$. That is, $t = nq$ and consequently $n|t$. Conversely, suppose that $n|t$. Then $t = nq$ for some integer q. Thus, $a^t = (a^n)^q = e$.
(iii) First we prove that $e, a, a^2, \cdots, a^{n-1}$ are all distinct. To see this, suppose that $a^u = a^v$ with $0 \leq u < n$ and $0 \leq v < n$. Without loss of generality we may assume that $u \geq v$. Since $a^u = a^v$ then $a^{u-v} = e$. By (ii), $n|(u - v)$. But $0 \leq u - v \leq u < n$. Thus, we must have $u - v = 0$ or $u = v$.
We prove $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$ by double-inclusions. It is trivially true that $\{e, a, a^2, \cdots, a^{n-1}\} \subseteq < a >$. Now, let $a^t \in < a >$. By the division algorithm, there exist integers q and r such that $t = nq + r$ with $0 \leq r < n$. Thus, $a^t = (a^n)^q a^r = a^r$ with $0 \leq r < n$. That is, $a^t \in \{e, a, a^2, \cdots, a^{n-1}\}$. This completes a proof of the theorem ■

Definition 14.4
Let a be an element of a group G. The **order** *of a is the smallest positive integer n, if it exists, for which $a^n = e$. If such an integer does not exist then we say that a has an* **infinite order.** *We denote the order of a by $o(a)$.*

Example 14.2
1. In $\mathbb{Z}_4$, $o([2]) = 2$.
2. In $(\mathbb{Q}^*, \cdot)$ the number 2 has infinite order since $2^n \neq 1$ for all positive integer n.

We end this section with a theorem that gives the relationship between the order of a group and the order of an element.

Theorem 14.7
If G is a group and $a \in G$ then $o(a) = | < a > |$.

Proof.
If $o(a) = n$ then by Theorem 14.6 (iii) we have $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$. Thus, $| < a > | = n = o(a)$. If $o(a)$ is infinite then by Theorem 14.6(i) the integral powers of a are all distinct. Thus, $< a >$ is infinite and $o(a) = | < a > |$ ■

Review Problems

Exercise 14.1
Solve the equation $(12)x = (123)$ *in* S_3.

Exercise 14.2
Solve the equation $x(132) = (13)$ *in* S_3.

Exercise 14.3
Find the order of the element $(12)(34)$ *in* S_4.

Exercise 14.4
Consider the group $\mathbb{Z}_{16}$ *under addition. List all the elements of the subgroup* $< [6] >$.

Exercise 14.5
Consider the group $\mathbb{Z}_{13}^*$ *under multiplication. List all the elements of the subgroup* $< [4] >$.

Exercise 14.6
(a) Determine the elements in the subgroup $< (1234) >$ *of* S_4.
(b) Determine the elements in the subgroup $< (12345) >$ *of* S_5.
(c) What is the order of the subgroup $< (12 \cdots n) >$ *of* S_n?

Exercise 14.7
Determine the elements of the subgroup $< \mu_3 >$ *of the group of symmetries of the square.*

Exercise 14.8
Let α *denote the clockwise rotation of the plane through* 90° *about a fixed point* p.*(*$\alpha \in G$ *in Example 5.3(a)) What is the order of* $< \alpha >$?

Exercise 14.9
Prove that $axb = c$ *has a unique solution in a group.*

Exercise 14.10
(a) Prove that if a *and* b *are elements in an Abelian group* G, *with* $o(a) = m$ *and* $o(b) = n$ *then* $(ab)^{mn} = e$.
(b) Give an example in which the above statement is false if the group is not Abelian.

Exercise 14.11
Let a and b be elements of a group G. Prove that $ab = ba$ if and only if $a^{-1}b^{-1} = b^{-1}a^{-1}$.

Exercise 14.12
Assume $m, n \in \mathbb{Z}$. Find a necessary and sufficient condition for $< m > \subseteq < n >$.

Exercise 14.13
Prove that a nonidentity element of a group has order 2 if and only if it is its own inverse.

Exercise 14.14
Prove that every group of even order has an element of order 2.

Exercise 14.15
Prove that a group G is Abelian if anf only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Exercise 14.16
Prove that if a group G has no subgroup other than G and $\{e\}$, then G is cyclic.

Exercise 14.17
Prove that if G is a group and $a, b \in G$ then $o(a^{-1}ba) = o(b)$.

Exercise 14.18
Prove that if $a, b \in G$ then $o(ab) = o(ba)$.

Exercise 14.19
Let a be an element of a group G. Prove that $o(a^{-1}) = o(a)$.

Exercise 14.20
Prove that a group G is Abelian if each of its nonidentity elements has order 2.

Exercise 14.21
Prove Theorem 14.4(iii).

Exercise 14.22
In S_3, list all the elements of $< (123) >$. Find $o((123))$.

Exercise 14.23
Prove that if G is a group then the mapping $\lambda : G \to G$ defined by $\lambda(x) = ax$ is one-to-one and onto.

Exercise 14.24
There is only one way to complete the following Cayley table so as to get a group. Find it. Why is it unique?

$*$	a	b	c
a		b	
b			
c			

Exercise 14.25
Let G be a cyclic group, $G =< a >$. Prove that G is Abelian.

Exercise 14.26
Let G be a cyclic group of order $n, G =< a >$. Prove that $a^s = a^t$ if and only if $s \equiv t(mod\ n)$.

Exercise 14.27
Let $G =< a >$ be a cyclic group and H be a subgroup of G. Prove that $H =< a^k >$ where k is the smallest positive integer such that $a^k \in H$. Thus, every subgroup of a cyclic group is cyclic.

Exercise 14.28
(a) Let $G =< a >$ be a finite cyclic group of order n. Prove that $< a^d >=< a^m >$ where $d = (m, n)$. Thus, the distinct subgroups of G are those subgroups $< a^d >$ where d is a divisor of n.
(b) Find the distinct subgroups of a cyclic group of order 12.

Exercise 14.29
(a) Let $G =< a >$ be a cyclic group of order n. Prove that $G =< a^m >$ if and only if $(m, n) = 1$.
(b) Suppose that $G =< a >$ is a cyclic group of order 10. Find all possible generators of G.

15 Generated Groups. Direct Product

In this section, we discuss two procedures of building (sub)groups, namely, the (sub)groups generated by a subset of a given group and the direct product of two or more groups.

15.1 Finitely and Infinitely Generated Groups

The concept of generators can be extended from cyclic groups $< a >$ to more complicated situations where a subgroup is generated by more than one element. It is easy to see that a cyclic group with generator a is the smallest subgroup containing the set $S = \{a\}$. Can we extend groups generated by sets with more than one element? The answer is affirmative as suggested by the following theorem.

Theorem 15.1
Let G be a group and $\mathcal{C}$ be the collection all subgroups of G. Then $\cap_{H\in\mathcal{C}}H$ is a subgroup of G.

Proof.
Let $K = \cap_{H\in\mathcal{C}}H$. Since e belongs to all the subgroups of G then $e \in K$ so that $K \neq \emptyset$. Now, let $a, b \in K$. Then $a \in H$ and $b \in H$ for all subgroups H of G. But then $a \in H$ and $b^{-1} \in H, \forall H \in \mathcal{C}$. Since every H in $\mathcal{C}$ is closed under multiplication then $ab^{-1} \in H, \forall H \in \mathcal{C}$. That is, $ab^{-1} \in K$. By Theorem 7.5, K is a subgroup of G. ■

Theorem 15.2
Let G be a group and $S \subseteq G$. Let $\mathcal{C}$ be the collection of all subgroups of G containing S. Then the set $< S >= \cap_{H\in\mathcal{C}}H$ satisfies the following:

(i) $< S >$ is a subgroup of G containing S.
(ii) For every $H \in \mathcal{C}$, $< S > \subseteq H$.
Thus, $< S >$ is the smallest subgroup of G containing S.

Proof.
(i) Note that since $S \subseteq G$ then $G \in \mathcal{C}$. Thus, $\mathcal{C} \neq \emptyset$. The fact that $< S >$ is a subgroup of G follows from Theorem 15.1. Since $S \subseteq H$ for all $H \in \mathcal{C}$ then $S \subseteq \cap_{H\in\mathcal{C}}H$. That is, $S \subseteq < S >$.
(ii) Let $H \in \mathcal{C}$. If $x \in < S >$ then $x \in \cap_{H\in\mathcal{C}}H$ and in particular, $x \in H$. Hence, $< S > \subseteq H$. ■

Theorem 15.3
$< S >$ is the only subgroup of G that satisfies conditions (i) and (ii) of Theorem 15.2

Proof.
Suppose that K is a subgroup of G satisfying conditions (i) and (ii) of the previous theorem. We will show that $K =< S >$. Since $< S >$ is a subgroup containing S then by (ii), we have $< S > \subseteq K$. Also, since K is a subgroup of G containing S then by condition (ii) again, we have $K \subseteq < S >$. Thus, $< S >= K$. ■

Definition 15.1
If G is a group and $S \subseteq G$ then the subgroup $< S >$ is called the **subgroup of G generated by** *S. If $G =< S >$, then we say S generates G; and the elements in S are called* **generators.** *For $S = \{a_1, a_2, \cdots, a_n\}$ we write $< S >=< a_1, a_2, \cdots, a_n >$.*

Example 15.1
Consider the subgroup of S_4 generated by $S = \{(1432), (24)\}$. Then

$$< S >= \{(1), (1432), (24), (14)(23), (1234), (12)(34), (13)(24), (13)\}.\blacksquare$$

The following theorem characterizes the elements of $< S >$.

Theorem 15.4
Let G be a group and $S \subseteq G$. Then $< S >$ consists of finite products of elements of S and inverses of elements of S.. That is, if $K = \{a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}, a_i \in S, s_i = \pm\}$ then $< S >= K$.

Proof.
The proof is by double inclusions. By closure, $K \subseteq < S >$. It remains to show that $< S > \subseteq K$. Since each element of S is in K then $S \subseteq K$. We will show that K is a subgroup of G. Indeed, if $x = a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}$ and $y = b_1^{t_1} b_2^{t_2} \cdots b_m^{t_m}$ are two elements in K then

$$\begin{aligned} xy^{-1} &= (a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k})(b_1^{t_1} b_2^{t_2} \cdots b_m^{t_m})^{-1} \\ &= (a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k})(b_m^{-t_m} \cdots b_2^{-t_2} b_1^{-t_1}) \\ &= a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k} b_m^{-t_m} \cdots b_2^{-t_2} b_1^{-t_1} \end{aligned}$$

Thus, xy^{-1} is a product of elements of S and/or inverses of elements of S. Hence, $xy^{-1} \in K$. By Theorem 7.5, K is a subgroup of G. By Theorem 15.2(ii), $< S > \subseteq K$. Hence, $< S >= K$. ■

The next theorem provides a condition under which two groups generated by different sets are equal.

Theorem 15.5
Let T_1 and T_2 be subsets of a group G. Then

$$< T_1 >=< T_2 > \ if \ and \ only \ if \ T_1 \subseteq < T_2 > \ and \ T_2 \subseteq < T_1 >$$

Proof.
Suppose first that $< T_1 >=< T_2 >$. Since $T_1 \subseteq < T_1 >$ and $< T_1 >=< T_2 >$ then $T_1 \subseteq < T_2 >$. Similarly, $T_2 \subseteq < T_1 >$.
Conversely, suppose that $T_1 \subseteq < T_2 >$ and $T_2 \subseteq < T_1 >$. By Theorem 15.2(ii), we have $< T_1 > \subseteq < T_2 >$ and $< T_2> \subseteq < T_1 >$. Hence, $< T_1 >=< T_2 >$. ■

Example 15.2
rm Since $\{3\} \subseteq < 9, 12 >$ *(*$3 = 12 + (-9)$*) and* $\{9, 12\} \subseteq < 3 >$ *then by the previous theorem we have* $< 9, 12 >=< 3 >$. ■

Example 15.3
rm In S_4 we have that

$$\begin{array}{rcc} (124) & = & (123)(12)(34)(123) \\ (234) & = & (132)(12)(34) = (123)^{-1}(12)(34) \\ (123) & = & (124)(234) \\ (12)(34) & = & (234)(124)^{-1} \end{array}$$

Thus, we conclude that $\{(124), (134)\} \subseteq < (123), (12)(34) >$ *and* $\{(123), (12)(34)\} \subseteq < (124), (134) >$. *Hence, by Theorem 15.5, we have* $< (124), (234) >=< (123), (12)(34) >$. ■

15.2 Direct Product of Groups.

In this section we keep building examples of groups. By defining a binary operation on the Cartesian product of two groups we obtain the group known as the direct product of the two groups.

Let H and K be two arbitrary groups and let $H \times K$ be the Cartesian product of H and K. In set-builder notation

$$H \times K = \{(h, k) : h \in H \text{ and } k \in K\}.$$

Equality in $H \times K$ is defined by $(h, k) = (h', k')$ if and only if $h = h'$ and $k = k'$.
Define multiplication on $H \times K$ as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

The set $H \times B$ is a group under the above multiplication as shown in the next theorem.

Theorem 15.6
Multiplication on $H \times K$ satisfies the following properties:

(i) $H \times K$ is closed under multiplication.
(ii) Multiplication is associative.
(iii) (e_H, e_K) is the identity element.
(iv) For each $(h, k) \in H \times K$ we have $(h, k)^{-1} = (h^{-1}, k^{-1})$.

Proof.
(i) We must show that the rule on $(H \times K) \times (H \times K) \longrightarrow H \times K$ defined by $((h, k), (h', k')) \longrightarrow (hh', kk')$ is a mapping. Indeed, if $((h_1, k_1), (h_1', k_1')) = ((h_2, k_2), (h_2', k_2'))$ then $(h_1, k_1) = (h_2, k_2)$ and $(h_1', k_1') = (h_2', k_2')$. Thus, $h_1 = h_2, k_1 = k_2, h_1' = h_2'$, and $k_1' = k_2'$. Thus, $h_1 h_1' = h_2 h_2'$ and $k_1 k_1' = k_2 k_2'$. Hence, $(h_1 h_1', k_1 k_1') = (h_2 h_2', k_2 k_2')$. So multiplication is a binary operation.
(ii) Multiplication on $H \times K$ is associative since multiplication is associative as operation on H and K.

$$\begin{aligned}
(h_1, k_1)[(h_2, k_2)(h_3, k_3)] &= (h_1, k_1)(h_2 h_3, k_2 k_3) \\
&= (h_1(h_2 h_3), k_1(k_2 k_3)) \\
&= ((h_1 h_2)h_3, (k_1 k_2)k_3) \\
&= (h_1 h_2, k_1 k_2)(h_3, k_3) \\
&= [(h_1, k_1)(h_2, k_2)](h_3, k_3)
\end{aligned}$$

(iii) Let $(h, k) \in H \times K$. Since $he_H = e_H h = h$ and $ke_K = e_K k = k$ then $(he_H, ke_K) = (e_H h, e_K k) = (h, k)$. Hence, $(h, k)(e_H, e_K) = (e_H, e_K)(h, k) =$

(h,k). That is, (e_H, e_K) is the identity element of $H \times K$.
(iv) Let $(h,k) \in H \times K$. Since $hh^{-1} = h^{-1}h = e_H$ and $kk^{-1} = k^{-1}k = e_K$ then $(hh^{-1}, kk^{-1}) = (e_H, e_K)$. That is, $(h,k)(h^{-1},k^{-1}) = (e_H, e_K)$. Similarly, $(h^{-1},k^{-1})(h,k) = (e_H, e_K)$ so that (h,k) is invertible with inverse (h^{-1},k^{-1})■

Definition 15.2 *By the above theorem, $H \times K$ is a group, called the* **direct product** *of the groups H and K.*

Example 15.4
If $\mathbb{Z}_3 = \{[0],[1],[2]\}$ and $S_2 = \{(1),(12)\}$ then

$$\mathbb{Z}_3 \times S_2 = \{([0],(1)),([1],(1)),([2],(1)),([0],(12)),([1],(12)),([2],(12))\}$$

For example,

$$([1],(12))([2],(1)) = ([1] \oplus [2],(12)(1)) = ([0],(12)).$$■

Some of the subgroups of $H \times K$ can be constructed as follows.

Theorem 15.7
The sets

$$H \times \{e_K\} = \{(h, e_K) : h \in H\}$$

and

$$\{e_H\} \times K = \{(e_H, k)) : k \in K\}$$

are subgroups of $H \times K$.

Proof.
We prove that $H \times \{e_K\}$ is a subgroup of $H \times K$ and we leave the second part of the theorem as an exercise for the reader. See Exercise **??**
Since $(e_H, e_K) \in H \times \{e_K\}$ then $H \times \{e_K\} \neq \emptyset$. Let (h_1, e_K) and (h_2, e_K) be two elements of $H \times \{e_K\}$. Then

$$(h_1, e_K)(h_2, e_K)^{-1} = (h_1, e_K)(h_2^{-1}, e_K) = (h_1 h_2^{-1}, e_K) \in H \times \{e_K\}$$

since $h_1 h_2^{-1} \in H$. Hence, by Theorem 7.5, $H \times \{e_K\}$ is a subgroup of $H \times K$
■

Remark 15.1
By the Principle of Counting, $|H \times K| = |H| \cdot |K|$.

Review Problems

Exercise 15.1
Show that $< 24, -36, 54 > + < 6 >$.

Exercise 15.2
Show that $< (123), (456) > = < (123)(456), (465) >$ *in* S_6.

Exercise 15.3
Determine the elements of $< \mu_2, \mu_5 >$ *as a subgroup of the group of symmetries of the square (Example 8.1).*

Exercise 15.4
The subgroup $< (1432), (24) >$ *of* S_4 *has order 8. List its elements.*

Exercise 15.5
What is $< \emptyset >$?

Exercise 15.6
Find a necessary and sufficient condition on a susbet S *of a group* G *for* $S = < S >$.

Exercise 15.7
Prove that if $a, b \in \mathbb{Z}$ *then* $< a, b > = < d >$, *where* $d = (a, b)$.

Exercise 15.8
Prove that $< [a] > = \mathbb{Z}_n$ *if and only if* a *and* n *are relatively prime.*

Exercise 15.9
Prove that if $(a, n) = d$ *then* $< [a] > = < [d] >$ *in* $\mathbb{Z}_n$.

Exercise 15.10
Prove that $< [a] > = < [b] >$ *in* $\mathbb{Z}_n$ *if and only if* $(a, n) = (b, n)$.

Exercise 15.11
Prove that $H \times K$ *is Abelian if and only if* H *and* K *are Abelian.*

Exercise 15.12
Prove that if H *is a group, then the set* $D = \{(h, h) : h \in H\}$ *is a subgroup of* $H \times H$. *This is called the diagonal subgroup of* $H \times H$. *What is it, geometrically, for* $H = \mathbb{R}$, *with addition as the binary operation?*

Exercise 15.13
Prove that if A is a subgroup of H and B is a subgroup of K then $A \times B$ is a subgroup of $H \times K$.

Exercise 15.14
Simplify the following expression in $\mathbb{Z}_4 \times S_4$.

$$([2], (123))^{-1}([1], (24))([2], (123)).$$

Exercise 15.15 ??
Let H and K be groups. Prove that $\{e_H\} \times K$ is a subgroup of $H \times K$.

Exercise 15.16
What is the order of $S_3 \times \mathbb{Z}_2$.

Exercise 15.17
Construct a Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_7$. Show that the group is cyclic.

Exercise 15.18
Find two cyclic groups H and K such that $H \times K$ is not cyclic.

Exercise 15.19
(a) List the elements of $S_3 \times \mathbb{Z}_2$.
(b) List the elements of the cyclic subgroup $< ((12), [1]) >$ of $S_3 \times \mathbb{Z}_2$.

Exercise 15.20
Let H and K be two groups. Show that the projection maps $\pi_1 : H \times K \to H$ defined by $\pi_1(h, k) = h$ and $\pi_2 : H \times K \to K$, defined by $\pi_2(h, k) = k$ satisfy the relation $\pi_i((h_1, k_1)(h_2, k_2)) = \pi_i(h_1, k_1)\pi_i(h_2, k_2)$ where $i = 1, 2$ and $(h_1, k_1), (h_2, k_2) \in H \times K$.

16 Cosets

We recall from Section 11, the equivalence relation congruence modulo n on the set of integers. So if $a \equiv b(mod\ n)$ then $n|(a-b)$ which means that $a-b=nq$ for some $q \in \mathbb{Z}$. Since $< n >= \{nt : t \in \mathbb{Z}\}$ then it follows that $a-b \in < n >$, where $< n >$ is a subgroup of $\mathbb{Z}$. Thus, we have

$$a \equiv b(mod\ n) \Longleftrightarrow a-b \in < n > .$$

Now $-b$ is the inverse of b in the additive group $\mathbb{Z}$; so by replacing $\mathbb{Z}$ by a group G and $< n >$ by a subgroup H of G the above relation suggests considering the relation defined by

$$a \sim b \Longleftrightarrow ab^{-1} \in H$$

Theorem 16.1
If H is a subgroup of a group G, the relation $\sim$ defined above is an equivalence relation on G. The equivalence class with representative a is the set

$$[a] = \{ha : h \in H\}.$$

Proof.
Given $a \in G$ we have $aa^{-1} = e \in H$, so that $a \sim a$; hence $\sim$ is reflexive. If $a, b \in G$ with $a \sim b$, then $ab^{-1} \in H$; but $ba^{-1} = (ab^{-1})^{-1} \in H$; thus $b \sim a$ and $\sim$ is symmetric. Finally, if $a, b, c \in G$ with $a \sim b$ and $b \sim c$, then $ab^{-1}, bc^{-1} \in H$; thus $ab^{-1}bc^{-1} \in H$, i.e., $ac^{-1} \in H$, and so $a \sim c$; thus, $\sim$ is transitive. This shows that $\sim$ is an equivalence relation on G.
Now, let $a \in G$. If $b \in [a]$ then $b \sim a$ so that $ba^{-1} \in H$. If we let $h = ba^{-1}$ then $b = ha$ and therefore $b \in \{ha : h \in H\}$. This proves that $[a] \subseteq \{ha : h \in H\}$. On the other hand, if $b \in \{ha : h \in H\}$ then $b = ha$ for some $h \in H$ or $h = ba^{-1}$ so that $b \sim a$. Thus, $b \in [a]$ and $\{ha : h \in H\} \subseteq [a]$. This ends a proof of the theorem.■

Definition 16.1
The set $\{ha : h \in H\}$ is called the **right coset** *of H to which a belongs and will be denoted by Ha.*

Remark 16.1
It follows from Theorem 16.1 and Definition 16.1 that the family $\{Ha\}_{a \in G}$ form a partition of G.

Example 16.1
Consider the set A_4 of all even permutations of S_4. The set $H = \{(1), (123), (132)\}$ is a subgroup of A_4. The right cosets of H in A_4 are:

$$\begin{array}{rcl} H & = & \{(1), (123), (132)\} \\ H(12)(34) & = & \{(12)(34), (134), (234)\} \\ H(13)(24) & = & \{(13)(24), (243), (124)\} \\ H(14)(23) & = & \{(14)(23), (142), (143)\}\blacksquare \end{array}$$

Lemma 16.1
Let H be a subgroup of a group G and $a, b \in G$. Then the following statements are all equivalent.

(i) $ab^{-1} \in H$.
(ii) $a = hb$ *for some* $h \in H$.
(iii) $a \in Hb$.
(iv) $Ha = Hb$.

Proof.
(i) $\Longrightarrow$ (ii): If $ab^{-1} \in H$ then $h = ab^{-1}$ for some $h \in H$ and therefore $a = hb$.
(ii) $\Longrightarrow$ (iii): If $a = hb$ for some $h \in H$ then by the definition of Hb we have $a \in Hb$.
(iii) $\Longrightarrow$ (iv): If $a \in Hb$ then $a \sim b$ so that the equivalence class of a is equal to the equivalence class of b.(See Theorem 9.2). That is, $Ha = Hb$.
(iv) $\Longrightarrow$ (i): If $Ha = Hb$ then since $a = ea \in Ha$ then $a \in Hb$. That is, $a = hb$ for some $h \in H$ and therefore $ab^{-1} = h \in H$. This completes a proof of the lemma.$\blacksquare$

Remark 16.2
The above lemma provides a way in computing all the right cosets when G is finite. To compute all the right cosets of a subgroup H in a finite group G, first write H, and then choose any element $a \in G$ such that $a \notin H$, and compute Ha. Next, choose any element $b \in G$ such that $b \notin H \cup Ha$, and compute Hb. Continue in this way until all the elements of G have been exhausted.

Looking back at Example 16.1, you notice that H and all the right cosets of H in G have the same number of elements. This is not accidental.

Lemma 16.2
If H is a finite subgroup of a group G then for any $a \in G$, $|H| = |Ha|$.

Proof.
To show that two finite sets have the same number of elements is equivalent to establishing a bijection mapping between the two sets. So define $\alpha : H \longrightarrow Ha$ by $\alpha(h) = ha$. This is a well-defined mapping. For if $h_1 = h_2$ then $h_1a = h_2a$ or $\alpha(h_1) = \alpha(h_2)$. To see that α is one-to-one, suppose that $\alpha(h_1) = \alpha(h_2)$. Then $h_1a = h_2a$. By the right cancellation law, we have $h_1 = h_2$. Thus, α is one-to-one. Now to show that α is onto, let $b \in Ha$. Then by Lemma 16.1, $Hb = Ha$ so that $a \in Hb$ and thus $a = hb$ for some $h \in H$. Hence, $h^{-1} = ba^{-1} \in H$ and $\alpha(ba^{-1}) = b$. This ends a proof of the lemma.■

Remark 16.3
Left cosets result from considering the equivalence relation

$$a \sim b \Longleftrightarrow a^{-1}b \in H.$$

A left coset has the form

$$aH = \{ah : h \in H\}.$$

One can easily proof versions of Theorem 16.1 and Lemma 16.1 for left cosets.

Example 16.2
The left cosets in Example 16.1 are:

$$\begin{array}{rcl} H & = & \{(1), (123), (132)\} \\ (12)(34)H & = & \{(12)(34), (243), (143)\} \\ (13)(24)H & = & \{(13)(24), (142), (234)\} \\ (14)(23)H & = & \{(14)(23), (134), (124)\}\blacksquare \end{array}$$

Remark 16.4
Note that, other than the subgroup H, no left coset is a right coset.

Review Problems

Exercise 16.1
Determine the right cosets of $< [4] >$ *in* $\mathbb{Z}_8$.

Exercise 16.2
Determine the left cosets of $< [3] >$ *in* $\mathbb{Z}_{12}$.

Exercise 16.3
In the group of symmetries of the square, determine the right cosets of $< \mu_7 >$.

Exercise 16.4
Determine the left cosets of $< (123) >$ *in* S_3.

Exercise 16.5
Prove that if H *is a subgroup of an Abelian group* G *then left cosets are equal to right cosets.*

Exercise 16.6
Let $G = S_3$ *and* $H =< (13) >$.

(a) Determine the right cosets of H *in* G.
(b) Determine the left cosets of H *in* G.
(c) Verify that the collection of right cosets is different from the collection of left cosets.

Exercise 16.7
Prove that each right coset of $A \times \{e\}$ *in* $A \times B$ *contains precisely one element from* $\{e\} \times B$.

Exercise 16.8
Compute the right cosets of $< (12), [1] >$ *in* $S_3 \times \mathbb{Z}_2$.

Exercise 16.9
Compute the left cosets of $< (12), [1] >$ *in* $S_3 \times \mathbb{Z}_2$.

Exercise 16.10
Let H *and* K *be two subgroups of a group* G. *For* $a, b \in G$ *define the relation*

$$a \sim b \Longleftrightarrow hak = b \quad for\ some\ h \in H\ and\ k \in K.$$

Prove that $\sim$ *is an equivalence relation on* G.

Exercise 16.11
Consider the equivalence relation of the previous exercise. Let $a \in G$. Prove that

$$[a] = HaK = \{hak : h \in H \text{ and } k \in K\}.$$

We call HaK a **double coset** *of H and K in G.*

Exercise 16.12
Prove that if Hak and Hbk are double cosets of H and K in G then they are either equal or disjoint.

Exercise 16.13
Let H and K be subgroups of a group G and $a \in G$. Let $\phi : HaK \to a^{-1}HaK$ be defined by $\phi(hak) = a^{-1}hak$. Show that ϕ is one-to-one and onto.

Exercise 16.14
Let H be a subgroup of a group G. Prove that $Hh = H = hH$ for all $h \in H$.

Exercise 16.15
If H is a subgroup of a group G, prove that gHg^{-1} is a subgroup of G for any $g \in G$.

Exercise 16.16
For an arbitrary subgroup H of a group G, define the mapping ϕ from the set of all left cosets of H in H to the set of all right cosets of H in G by $\phi(aH) = Ha^{-1}$. Prove that ϕ is one-to-one and onto.

Exercise 16.17
Let H be a subgroup of a group H with the property that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. Prove that $Ha = aH$ for any $a \in G$.

Exercise 16.18
Suppose that H is a subgroup of a group G such that $gH = Hg$ for all $g \in G$. Prove that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Exercise 16.19
The **center** *of a group G is defined by*

$$Z(G) = \{a \in G : ax = xa, \forall x \in G\}.$$

Prove that $aZ(G) = Z(G)a$ for all $a \in G$.

Exercise 16.20
For an arbitrary subgroup H of a group G, the **normalizer** *of H in G is the set*

$$\mathcal{N}(\mathcal{H}) = \{x \in G : xHx^{-1} = H\}$$

(a) Prove that $\mathcal{N}(\mathcal{H})$ is a subgroup of G.
(b) Prove that $g\mathcal{N}(\mathcal{H}) = \mathcal{N}(\mathcal{H})g$ for all $g \in G$.

17 Lagrange's Theorem

A very important corollary to the fact that the left cosets of a subgroup partition a group is Lagrange's Theorem. This theorem gives a relationship between the order of a finite group and the order of any subgroup (in particular, if $|G| < \infty$ and $H \subseteq G$ is a subgroup, then $|H| \mid |G|$).

Theorem 17.1 *(Lagrange's Theorem)*
Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.

Proof.
By Theorem 16.1, the right cosets of H form a partition of G. Thus, each element of G belongs to at least one right coset of H in G, and no element can belong to two distinct right cosets of H in G. Therefore every element of G belongs to exactly one right coset of H. Moreover, each right coset of H contains $|H|$ elements (Lemma 16.2). Therefore, $|G| = n|H|$, where n is the number of right cosets of H in G. Hence, $|H| \mid |G|$. This ends a proof of the theorem.■

Example 17.1
If $|G| = 14$ then the only possible orders for a subgroup are 1, 2, 7, and 14.■

Definition 17.1
The number of different right cosets of H in G is called the **index** *of H in G and is denoted by $[G : H]$.*

It follows from the above definition and the proof of the above theorem that

$$|G| = [G : H]|H|.$$

Example 17.2
Since $|S_3| = 3! = 6$ and $|(12)| = | < (12) > | = 2$ then $[S_3, < (12) >] = \frac{6}{2} = 3$.■

The rest of this section is devoted to consequences of Lagrange's theorem; we begin with the order of an element.

Corollary 17.1
If G is a finite group and $a \in G$ then $o(a) \mid |G|$.

Proof.
Since $< a >$ is a subgroup of G then $| < a > | \mid |G|$. By Theorem 15.7, $o(a) = | < a > |$. Hence, $o(a) \mid |G|$. ■

The next two results classify all groups of order n for infinitely many values of n.

Corollary 17.2
If $|G| = p$, where p is prime then the only subgroups of G are $\{e\}$ and G.

Proof.
Suppose the contrary, that is G has a subgroup H such that $H \neq \{e\}$ and $H \neq G$. By Theorem 17.1, $|H||G|$ with $1 < |H| < p$. This contradicts the fact that p is prime.■

Corollary 17.3
If G is a goup of prime order then it is cyclic. That is, $G =< a >$ where a is any nonidentity element of G.

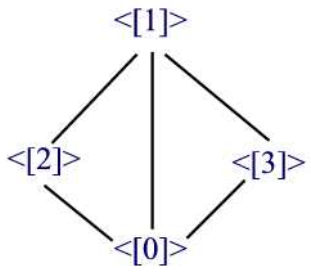
Proof.
Let $a \in G$ with $a \neq e$. Then $< a > \neq \{e\}$. By the previous corollary, $G =< a >$.■

Example 17.3
The previous corollary tells that groups of prime order are always cyclic. What about groups of prime-squared order? The group

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{([0],[0]),([0],[1]),([1],[0]),([1],[1])\}$$

has order $4 = 2^2$. Since each element has order 2 then by Theorem 15.7, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.■

Example 17.4
Lagrange's Theorem greatly simplifies the problem of determining all the subgroups of a finite group. For example, consider the group $(\mathbb{Z}_6, \oplus)$. Aside from $\{[0]\}$ and $\mathbb{Z}_6$ any subgroup of $\mathbb{Z}_6$ must have order 2 or 3. There is only one subgroup of order 2, $< [3] >$. Also, there is only one subgroup of order 3, $< [2] >$. A subgroup lattice shows the subgroups of $\mathbb{Z}_6$ and the inclusion relation between them.



Another important corollary to Lagrange's Theorem is Fermat's little theorem.

Theorem 17.2 *(Fermat's Little Theorem)*
If p is a prime number and $p \not| n$ then

$$n^{p-1} \equiv 1(mod\ p).$$

Proof.
Since p is prime then $(\mathbb{Z}_p^*, \odot)$ is a group of order $p-1$.(See Theorem 12.6). Hence, the order of each element of $\mathbb{Z}_p^*$ is a divisor of $p-1$. If $p \not| n$ then $[n] \in \mathbb{Z}_p^*$. Since $o([n]) = | < [n] > | \mid (p-1)$ then $[n]^{p-1} = [1]$. That is, $[n^{p-1}] = [1]$. Hence $n^{p-1} \equiv 1(mod\ p)$.■

The above theorem suggests a test of primality for p. Take a number n such that $p \not| n$ and raise it to the $(p-1)$st power and find its remainder when divided by p. If the remainder is not 1 then we can conclude that p is not a prime number.

The Converse of Lagrange's Theorem
The converse of Lagrange's theorem is not true in general. That is, if n is a divisor of G then it does not necessarily follow that G has a subgroup of order n.

Example 17.5
The set of all even permutations

$$\begin{aligned} A_4 \ = \ \{&(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), \\ &(142), (134), (143), (234), (243)\} \end{aligned}$$

is a subgroup of S_4 (and therefore a group itself) of order 12 (See Theorem 7.9). Note that A_4 has three elements of order 2 (namely, $(12)(34), (13)(24), (14)(23)$) and 8 elements of order 3. $((123), (132), (124), (142), (134), (143), (234), (243))$
We will show that A_4 has no subgroup of order 6.
Let H be a subgroup of A_4 of order 6. Then $(1) \in H$. Since A_4 contains only 3 elements of order 2 then H must contain at least one element of order 3 of the form (abc). Then by closure, $(acb) = (abc)(abc) \in H$. If H also contains an element of the form $(ab)(cd)$(or of the form (abd)) then by closure $(abc)(ab)(cd) = (ac)(bd) \in H$ and $(acb)(ab)(cd) = (bcd)$. Thus, $(bdc) = (bcd)^{-1} \in H$. In either case, H has more than six elements. Thus, A_4 has no subgroup of order 6.■

The converse of Lagrange's theorem is valid for cyclic groups. To prove this result we need the following two theorems.

Theorem 17.3
Let G be a finite cyclic group of order n and generator a. That is,

$$G = \{e, a, a^2, \cdots, a^{n-1}\}$$

Every subgroup of G is cyclic. That is, a subgroup of a cyclic group is also cyclic.

Proof.
Let H be a subgroup of G. Then elements of H are of the form a^k with $1 \leq k < n$. Let t be the smallest positive integer such that $a^t \in H$. We shall prove that $H =< a^t >$. Indeed, let $a^m \in H$. By the Division Algorithm there exist unique integers q and r such that $m = tq + r$ where $0 \leq r < t$. It follows that $a^m = (a^t)^q a^r$ or $a^r = a^m (a^t)^{-q}$. But $a^m \in H$ and $a^t \in H$ then by closure $a^r \in H$. Since t is the smallest positive integer such that $a^t \in H$ then we must have $r = 0$. Hence, $a^m = (a^t)^q$ or $a^m \in < a^t >$. Clearly, $< a^t > \subseteq H$ since $a^t \in H$ and H is a group.■

Theorem 17.4
Let G be as in the statement of Theorem 17.3. If $1 \leq k < n$ then a^k generates a subgroup of order $\frac{n}{(k,n)}$.

Proof.
Let $d = (k, n)$. By Theorem 14.6(i), $| < a^k > |$ is the smallest positive integer

such that $a^{k|<a^k>|} = e$. By Theorem 14.6 (ii), $n|\ (k|\ <a^k>\ |)$. That is, $k|\ <a^k>\ | = nq$ for some integer q. Hence, $\frac{k|<a^k>|}{d} = \frac{nq}{d}$ so that $\frac{n}{d} \mid \frac{k|<a^k>|}{d}$. Since $(\frac{n}{d}, \frac{k}{d}) = 1$ then by Lemma 13.1, we have $\frac{n}{d} \mid |<a^k>|$. On the other hand, $(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e$ so that $|<a^k>| \mid \frac{n}{d}$. Hence, by Theorem 10.2 (d), $|<a^k>| = \frac{n}{d}$.■

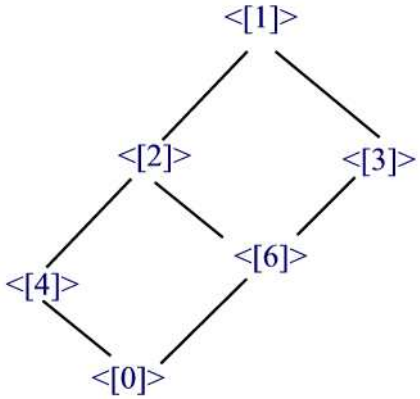
Theorem 17.5
Let G be a cyclic group of order n and generator a. For each positive divisor d of n, G has exactly one subgroup of order d.

Proof.
Existence: Let d be a positive divisor of n. Then there exists a positive integer $q < n$ such that $n = dq$. Thus, $q|n$ and $(n, q) = q$. By Theorem 17.4, a^q generates a subgroup of G of order $\frac{n}{(n,q)} = \frac{n}{q} = d$. Thus, G has at least one subgroup of order d.

Uniqueness: Suppose that G has two subgroups of order d, say H and K. We will show that $H = K$. Let $1 \leq m < n$ be the smallest positive integer such that $a^m \in H$ and $1 \leq k < n$ be the smallest positive integer such that $a^k \in K$. As in the proof of Theorem 17.3, we establish that $H =< a^m >$ and $K =< a^k >$. By Theorem **??** $|<a^m>| = \frac{n}{(n,m)}$ and $|<a^k>| = \frac{n}{(n,k)}$. Thus, $\frac{n}{(n,m)} = \frac{n}{(n,k)} = d$ or $(n, m) = (n, k)$. Now, by the Division Algorithm, $n = mq + r$ with $0 \leq r < m$. Since $a^n = e \in H$ then $a^r = (a^m)^{-q} \in H$. From the definition of m we see that $r = 0$. Hence, $n = mq$ and $m|n$. It follows that $(n, m) = m$. A similar argument shows that $(n, k) = k$ and therefore $m = k$. Hence, $< a^m >=< a^k >$, i.e. $H = K$. This ends a proof of the theorem.■

Remark 17.1
The converse of Lagrange's theorem holds also for finite Abelian groups. This topic will not be covered in this book.

Example 17.6
Consider the group $(\mathbb{Z}_{12}, \oplus)$. Since $|\mathbb{Z}_{12}| = 12$ then the positive divisors of 12 are 1, 2, 3, 4, 6, and 12. The subgroup lattice below shows the different subgroups of $\mathbb{Z}_{12} =< [1] >$.■


<[1]>
<[2]>
<[3]>
<[6]>
<[4]>
<[0]>

Review Problems

Exercise 17.1
Find $[S_3 :< (12) >]$.

Exercise 17.2
Find $[\mathbb{Z}_{10} :< [2] >]$.

Exercise 17.3
Let G denote the group of symmetries of the square.(Example 8.1) Find $[G :< \mu_8 >]$.

Exercise 17.4
A group G has subgroups of orders 4 and 10, and $|G| < 50$. *What can you conclude about* $|G|$?

Exercise 17.5
Assume that G is a group with a subgroup H such that $|H| = 6, [G : H] > 4$, *and* $|G| < 50$. *What are the possibilities about* $|G|$?

Exercise 17.6
Assume that G is a group with a subgroup H such that $|G| < 45, |H| > 10$, *and* $[G : H] > 3$. *Find* $|G|, |H|$, *and* $[G : H]$.

Exercise 17.7
Find all of the subgroups of $\mathbb{Z}_6$. *Also construct the subgroup lattice.*

Exercise 17.8
Assume that G is a cyclic group of order n, that $G =< a >$, *that* $k|n$, *and* $H =< a^k >$. *Find* $[G : H]$.

Exercise 17.9
Assume that A is a subgroup of a finite group G and B is a subgroup of a finite group H. We have seen that $A \times B$ *is a subgroup of* $G \times H$. *Express* $[G \times H : A \times B]$ *in terms of* $[G : A]$ *and* $[H : B]$.

Exercise 17.10
Assume that G is a finite group and D denotes the diagonal subgroup of $G \times G$.. *Find* $[G \times G : D]$.

Exercise 17.11
Let G be a group of order p^2. Prove that if G is not cyclic then $a^p = e$ for every nonidentity element of G.

Exercise 17.12
Prove that if H is a subgroup of a group $G, a, b \in G$ and $a, b \notin H$ then $ab \in H$.

Exercise 17.13
Prove that if A and B are finite subgroups of a group G such that $(|A|, |B|) = 1$ then $A \cap B = \{e\}$.

Exercise 17.14
If H is a subgroup of G and $[G : H] = 2$ then G is Abelian.

Exercise 17.15
Prove that if H is a subgroup of a finite group G then the number of right cosets of H in G is equal to the number of left cosets of H in G.

Exercise 17.16
Prove that the number of generators of a finite cyclic group of order n is $\phi(n)$, where ϕ is Euler's function.

Exercise 17.17
Let G be a group. Define the relation

$$a \sim b \iff a = gbg^{-1}, for\ some\ g \in G.$$

(a) Prove that $\sim$ is an equivalence relation.
(b) Prove that $[a] = \{b \in G : a = gbg^{-1}\ for\ some\ g \in G\}$.
(c) Prove that $|[a]| = 1$ if and only if $a \in Z(G)$, where $Z(G)$ is the center of G, i.e. $Z(G) = \{a \in G : ax = xa \forall x \in G\}$.
(d) Prove that $G = Z(G) \cup [a]$ where the union is taken over all $a \in G$ such that $|[a]| \geq 2$.

Exercise 17.18
Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. If the orders of a and b are relatively prime, then $o(ab) = o(a)o(b)$.

Exercise 17.19
Let G be a group, and let $a, b \in G$ be elements such that $ab = ba$. Prove if $(o(a), o(b)) = 1$ then $o(ab)$ is the least common multiple of $o(a)$ and $o(b)$.

Exercise 17.20
Prove that in a finite group G or order n, we have $a^n = e$ for all $a \in G$.

Exercise 17.21
Show that S_4 has no element of order 6.

Exercise 17.22
Let G be a finite group, let H and K be subgroups of G such that K is also a subgroup of H. Find $[G : K]$ in terms of $[G : H]$ and $[H : K]$.

18 Group Isomorphisms

We start this section by constructing the Cayley tables of the groups $(\mathbb{Z}_3, \oplus)$ and $(< (123) >, \circ)$.

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\circ$	(1)	(123)	(132)
(1)	(1)	(123)	(132)
(123)	(123)	(132)	(1)
(132)	(132)	(1)	(123)

By setting the correspondence $[0] \leftrightarrow (1), [1] \leftrightarrow (123), [2] \leftrightarrow (132)$ we see that the two tables differ only in the names of the symbols, and not in their positions. If we name the mentioned correspondence by the letter f, i.e. by writing $f([0]) = (1), f([1]) = (123)$ and $f([2]) = (132)$, and then constructing a Venn diagram of this mapping we see that f is a bijection mapping with the property $f([a] \oplus [b]) = f([a]) \circ f([b])$. This example, leads to the following definition.

Definition 18.1
Let $(G, *)$ and $(H, \#)$ be two groups. We say that G and H are isomorphic if there is a bijective map $\theta : G \longrightarrow H$ which respects the group structure. That is to say, for every g and h in G,

$$\theta(g * h) = \theta(g) \# \theta(h) \tag{3}$$

The map θ is called an **isomorphism.** *We write $G \approx H$. If $G = H$ then we call θ an* **automorphism** *on G.*

In words, you can first multiply in G and take the image in H, or you can take the images in H first and multiply there, and you will get the same answer either way. This is referred to as "operation preserving".
Notice that the operation on the left is occurring in G while the operation on the right is occurring in H.

Definition 18.2
A function θ satisfying (3) is called a **homomorphism.** *If $G = H$ then we say that θ is an* **endomorphism** *on G. A one-to-one homomorphism is called a* **monomorphism.** *An onto homomorphism is called an* **epimorphism**.

Example 18.1
Consider the mapping $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ defined by $f(x) = \log_{10} x$. We know from calculus that this mapping is a bijective map with the property

$$\log_{10}(xy) = \log_{10} x + \log_{10} y.$$

Thus, f is an isomorphism.■

Remark 18.1
The use of $*$ and $\#$ in Definition 18.1 is intended to emphasize the fact that the group operations may be different. Now that this point has been made, we revert to our convention of using multiplicative notation. Thus, we will write

$$\theta(ab) = \theta(a)\theta(b).$$

Isomorphism is a very important idea in abstract mathematics. It allows us to establish properties of one basic structure, and then immediately deduce them for a whole range of isomorphic 'look-alikes'.

Theorem 18.1
If $G \approx H$ and G is Abelian then H is also Abelian.

Proof.
Let $\theta : G \longrightarrow H$ be an isomorphism. Let $a, b \in H$. Since θ is onto then $\theta(x) = a$ and $\theta(y) = b$ for some unique $x, y \in G$. Thus,

$$ab = \theta(x)\theta(y) = \theta(xy) = \theta(yx) = \theta(y)\theta(x) = ba.$$

Hence, H is Abelian.■

More properties shared by isomorphic groups will be discussed in Section 19.

The next theorem list some technical facts about homomorphisms.

Theorem 18.2 *(Basic properties of homomorphisms)*
Let $\theta : G \longrightarrow H$ be a homomorphism between two groups G and H. Then

(i) $\theta(e_G) = e_H$.
(ii) $\theta(a^{-1}) = [\theta(a)]^{-1}$.

(iii) $\theta(a^k) = [\theta(a)]^k$, *where* $k \in \mathbb{Z}$.
(iv) The set $\theta(G) = \{\theta(a) : a \in G\}$ *is a subgroup of* H.
(v) If θ *is one-to-one then* $G \approx \theta(G)$.
(vi) If $a \in G$ *then* $o(\theta(a)) \mid o(a)$.

Proof.
(i)Since $\theta(e_G)\theta(e_G) = \theta(e_G)e_H$ then by the left cancellation rule we have $\theta(e_G) = e_H$.
(ii) Let $a \in G$. The equation $\theta(a)x = e_H$ has a unique solution $x = [\theta(a)]^{-1}$. But $\theta(a)\theta(a^{-1}) = \theta(aa^{-1}) = \theta(e_G) = e_H$. Thus, $[\theta(a)]^{-1} = \theta(a^{-1})$.
(iii) We consider the cases, $k = 0, k > 0$, and $k < 0$. The case $k = 0$ is just (i). For the case $k > 0$, we use induction on $k \geq 1$. The result is true for $k = 1$. Assume it is true up to $k - 1$. Then

$$\theta(a^k) = \theta(a^{k-1}a) = \theta(a^{k-1})\theta(a) = (\theta(a))^{k-1}\theta(a) = [\theta(a)]^k.$$

Hence, the result is true for all $k > 0$. If $k < 0$ then

$$\theta(a^k) = \theta((a^{-1})^{-k}) = [\theta(a^{-1})]^{-k} = [(\theta(a))^{-1}]^{-k} = [\theta(a)]^k.$$

(iv) Since $\theta(e_G) = e_H$ then $e_H \in \theta(G)$ so that $\theta(G) \neq \emptyset$. Now, if $\theta(a), \theta(b) \in \theta(G)$ then

$$\theta(a)[\theta(b)]^{-1} = \theta(a)\theta(b^{-1}) = \theta(ab^{-1}) \in \theta(G)$$

since by closure, $ab^{-1} \in G$. Hence, by Theorem 7.5, $\theta(G)$ is a subgroup of H.
(v) By the definition of $\theta(G)$, $\theta : G \to \theta(G)$ is onto. Hence, if θ is one-to-one then θ is a bijective homomorphism, i.e. $G \approx \theta(G)$.
(vi) Since $a^{o(a)} = e_G$ then $\theta(a^{o(a)}) = \theta(e_G)$ or $[\theta(a)]^{o(a)} = e_H$. By Theorem 14.6(ii), $o(\theta(a)) \mid o(a)$. ■

Remark 18.2
If you want to show that a function is not a homomorphism, do a quick check: Does it send the identity to the identity? If not, then the above theorem shows that it's not a homomorphism. For example, if $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ is defined by $f(x) = x + 1$ f is not an homomorphism since $f(0) = 1 \neq 0$.

Remark 18.3
The properties in the above theorem are not part of the definition of a homomorphism. To show that f is a homomorphism, all you need to show is that $f(ab) = f(a)f(b)$. The properties in the theorem are automatically true of any homomorphism. For example, the mapping $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ defined by $f(x) = x^2$ satisfies $f(0) = 0$ but still f is not a homomorphism.

Review Problems

Exercise 18.1
Let $A = \{2^m : m \in \mathbb{Z}\}$. Prove that $\mathbb{Z} \approx A$.

Exercise 18.2
Let $B = \{2^m 3^n : m, n \in \mathbb{Z}\}$. Prove that $\mathbb{Z} \times \mathbb{Z} \approx B$.

Exercise 18.3
Assume that $H = \{u, v, w, x, y, z\}$ is a group with respect to multiplication and that $\theta : \mathbb{Z}_6 \longrightarrow H$ is an isomorphism with

$$\begin{array}{lll} \theta([0]) = u & , \quad \theta([1]) = v & , \quad \theta([2]) = w \\ \theta([3]) = x & , \quad \theta([4]) = y & , \quad \theta([5]) = z \end{array}$$

Replace each of the following by the appropraite letter, either $u, v, x, y,$ or z.

(a) xw (b) w^{-1} (c) v^5 (d) $zv^{-1}x$.

Exercise 18.4
Given two groups $(G, *)$ and $(H, \#)$. Prove that $G \times H \approx H \times G$.

Exercise 18.5
Prove that $(\mathbb{Z}_4, \oplus) \approx (\mathbb{Z}_5^*, \odot)$.

Exercise 18.6
Let $\theta : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ be defined by $\theta([a]_6) = ([a]_2, [a]_3)$.

(a) Show that θ is well-defined.
(b) Prove that $\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$.

Exercise 18.7
Prove that if $(m, n) = 1$ then $\mathbb{Z}_{mn} \approx \mathbb{Z}_m \times \mathbb{Z}_n$.

Exercise 18.8
Consider $G = \{1, i, -1, -i\}$ under multiplication. Prove that $G \approx \mathbb{Z}_4$, with $(\mathbb{Z}_4, \oplus)$.

Exercise 18.9
Let G be a nonempty group. For each $a \in G$, define $f_a : G \to G$ by $f_a(x) = ax$.

(a) Prove that f_a is well-defined.
(b) Prove that f_a is a permutation on G.
(c) Prove that the set $G' = \{f_a : a \in G\}$ is a group of permutations.

Exercise 18.10
Let G and G' be as in the previous exercise. Define $\phi : G \to G'$ by $\phi(a) = f_a$.

(a) Prove that ϕ is well-defined.
(b) Prove that ϕ is one-to-one and onto.
(c) Prove that $G \approx G'$.

Exercise 18.11
Let G be an arbitrary group. Prove or disprove that the mapping $\phi(a) = a^{-1}$ is an isomorphism from G to G.

Exercise 18.12
For each a in a goup G, define a mapping $\tau_a : G \to G$ by $\tau_a(x) = axa^{-1}$. Prove that τ_a is an isomorphism from G to G.

Exercise 18.13
For an arbitrary positive integer n, prove that any two cyclic groups of order n are isomorphic.

Exercise 18.14
Let G_1, G_2, H_1, H_2 be nonempty groups, and suppose that $\theta_1 : G_1 \to H_1$ and $\theta_2 : G_2 \to H_2$ are group isomorphisms. Define $\phi : G_1 \times G_2 \to H_1 \times H_2$ by $\phi(x_1, x_1) = (\theta_1(x_1), \theta_2(x_2))$.

(a) Prove that ϕ is well-defined.
(b) Prove that ϕ is an isomorphism.

Exercise 18.15
Let G be a group, and let S be any set for which there exists a one-to-one and onto function $\phi : G \to S$. Define an operation on S by setting $x_1 \cdot x_2 = \phi(phi^{-1}(x_1)\phi^{-1}(x_2))$. Prove that S is a group under this operation, and that ϕ is actually a group somorphism.

Exercise 18.16
Prove that $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_6$.

Exercise 18.17
Prove that S_3 is not isomorphic to $\mathbb{Z}_6$.

Exercise 18.18
Let $\phi : G \to H$ be an isomorphism and N a subgroup of G with the property $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Prove that $hyh^{-1} \in \phi(N)$ for $y \in \phi(N)$ and $h \in H$.

Exercise 18.19
Suppose that $G =< a >$. Let H be a group and suppose that $\theta, \phi : G \to H$ are group isomorphisms. Prove that if $\theta(a) = \phi(a)$ then $\theta(x) = \phi(x)$ for all $x \in G$.

Exercise 18.20
Let H be a subgroup of a group G. For $a \in G$, define

$$a^{-1}Ha = \{a^{-1}ha : h \in H\}.$$

(a) Show that $a^{-1}Ha$ is a subgroup of G.
(b) Prove that $H \approx a^{-1}Ha$.

19 More Properties of Isomorphims

In this section we discuss more properties of group isomorphisms. We start with the following lemma.

Lemma 19.1
Let $\theta : G \longrightarrow H$ and $\gamma : H \longrightarrow K$ be two group isomorphisms. Then

(a) $\theta^{-1} : H \longrightarrow G$ is an isomorphism.
(b) $\gamma \circ \theta : G \longrightarrow K$ is also an isomorphism.

Proof.
(a) First we show that θ^{-1} is one-to-one. If $\theta^{-1}(h_1) = \theta^{-1}(h_2)$ then $\theta(\theta^{-1}(h_1)) = \theta(\theta^{-1}(h_2))$ or $\iota_H(h_1) = \iota_H(h_2)$. Hence, $h_1 = h_2$. To see that θ^{-1} is onto, let $g \in G$. Then $\theta(g) \in H$ and $\theta^{-1}(\theta(g)) = g$. Finally, we show that θ^{-1} is a homomorphism. If $a, b \in H$ then $a = \theta(u)$ and $b = \theta(v)$ for some $u, v \in G$, since θ is onto. Hence, if $w = \theta^{-1}(ab)$ then $\theta(w) = ab = \theta(u)\theta(v) = \theta(uv)$. Thus, $\theta^{-1}(ab) = uv = \theta^{-1}(a)\theta^{-1}(b)$. Hence, θ^{-1} is an isomorphism.
(b) To see that $\gamma \circ \theta$ is one-to-one, suppose that $\gamma \circ \theta(g_1) = \gamma \circ \theta(g_2)$. Then $\gamma(\theta(g_1)) = \gamma(\theta(g_2))$. Since γ is one-to-one then $\theta(g_1) = \theta(g_2)$. Since θ is one-to-one then $g_1 = g_2$. To see that $\gamma \circ \theta$ is onto, let $k \in K$. Since γ is onto then we can find $h \in H$ such that $\gamma(h) = k$. Since θ is onto then we can find a $g \in G$ such that $\theta(g) = h$. Hence, $\gamma(\theta(g)) = \gamma(h) = k$. To see that $\gamma \circ \theta$ is a homomorphism, let $a, b \in G$. Since both θ and γ are homomorphisms then

$$(\gamma \circ \theta)(ab) = \gamma(\theta(ab)) = \gamma(\theta(a)\theta(b)) = \gamma(\theta(a))\gamma(\theta(b)) = (\gamma \circ \theta)(a)(\gamma \circ \theta)(b).\blacksquare$$

Theorem 19.1
Isomorphism is an equivalence relation on the collection of all groups.

Proof.
Reflexive: Let G be a group. Then the identity map $\iota_G(a) = a$ for all $a \in G$ is an isomorphism. Hence, $G \approx G$.
Symmetric: Suppose that $G \approx H$ for some groups G and H. Then there is an isomorphism $\theta : G \longrightarrow H$. By Lemma 19.1(a), $\theta^{-1} : H \longrightarrow G$ is also an isomorphism. Hence, $H \approx G$.
Transitive: Suppose that $G \approx H$ and $H \approx K$, where G, H, and K are groups. Then there are isomorphisms $\theta : G \longrightarrow H$ and $\gamma : H \longrightarrow K$. By Lemma 19.1(b), $\gamma \circ \theta : G \longrightarrow K$ is also an isomorphism. Hence, $G \approx K$.$\blacksquare$

The following theorem lists more properties shared by isomorphic groups. Thus, the simplest way to show that two groups are not isomorphic is to find a property not shared by the two groups.

Theorem 19.2
Let G and H be groups such that $\theta : G \longrightarrow H$ is an isomorphism.

(a) $|G| = |H|$.
(b) If $G =< a >$ then $H =< \theta(a) >$. That is, if G is cyclic, then H is also cyclic.
(c) If K is a subgroup of G of order n then $\theta(K)$ is a subgroup of H of order n.
(d) If $a \in G$ and $o(a) = n$ then $o(\theta(a)) = n$.

Proof.
(a) There's a one-to-one onto map between the two sets. So counting the elements of one set simultaneously counts the elements of the other.
(b) Suppose that G is cyclic with generator a. We will show that $H =< \theta(a) >$. Clearly, since $\theta(a) \in H$ and H is a group then $< \theta(a) > \subseteq H$. Now suppose that $h \in H$ then there is an $g \in G$ such that $\theta(g) = h$(since θ is onto). But then $g = a^n$ for some $n \in \mathbb{Z}$. Hence, by Theorem 18.2(iii), $\theta(g) = \theta(a^n) = (\theta(a))^n$. That is, $h \in < \theta(a) >$ and so $H \subseteq < \theta(a) >$.
(c) If K is a subgroup of G then by Theorem 18.2(iv), $\theta(K)$ is a subgroup of H. The mapping θ restricted to K is a one-to-one mapping from K onto $\theta(K)$. Thus, $|K| = |\theta(K)|$.
(d) If $o(a) = n$ then $a^n = e_G$. By Theorem 18.2 (iii), we have $(\theta(a))^n = \theta(a^n) = \theta(e_G) = e_H$. By Theorem 14.6(ii), $o(\theta(a))|n$. On the other hand, since $(\theta(a))^{o(\theta(a))} = e_H$ then $\theta(a^{o(\theta(a))}) = e_H = \theta(e_G)$. Thus, $a^{o(\theta(a))} = e_G$ (since θ is one-to-one) and by Theorem 14.6(ii), $n|o(\theta(a))$. Hence, by Theorem 10.2(d), $o(\theta(a)) = n$.■

Example 19.1
1. $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic. Both groups have 4 elements, however, every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 1 or 2, while $\mathbb{Z}_4$ has two elements of order 4(namely, [1] and [3].)■

The following theorem shows that any two finite groups of the same order are isomorphic.

Theorem 19.3
If G is a cyclic group of order n then $G \approx \mathbb{Z}_n$.

Proof.
Suppose that $G =< a >$. Define $\theta : G \longrightarrow \mathbb{Z}_n$ by $\theta(a^k) = [k]$ where $1 \leq k < n$. We show that θ is well-defined. Indeed, if $a^k = a^m$ then $a^{k-m} = e_G$ so that by Theorem 14..6 (ii), $n|(k-m)$. Thus, $a \equiv m(mod\ n)$ and by Theorem 9.2, $[k] = [m]$. Next, we show that θ is one-to-one. Indeed, if $\theta(a^k) = \theta(a^m)$ then $[k] = [m]$ and this implies that $n|(k-m)$. Thus, $k - m = nq$ for some $q \in \mathbb{Z}$. Therefore, $a^{k-m} = a^{nq} = (a^n)^q = e_G$. Hence, $a^k = a^m$. Next, we show that θ is onto. Let $b \in \mathbb{Z}$. Then by the Division Algorithm, $b = nq + r, 0 \leq r < n$. Hence, $a^b = (a^n)^q a^r = a^r \in G$ and $\theta(a^b) = \theta(a^r) = [r]$. Since $b - r = nq$ then $n|(b - r$ so that $b \equiv r(mod\ n)$. By Theorem 9.2, $[b] = [r]$. Finally, it remains to show that θ is a group homomorphism. Indeed,

$$\theta(a^k a^m) = \theta(a^{k+m}) = [k+m] = [k] \oplus [m] = \theta(a^k)\theta(a^m).\blacksquare$$

The following result classifies all groups of prime order.

Example 19.2
If p is prime then $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic. For if it is, then by the previous theorem, $\mathbb{Z}_p \times \mathbb{Z}_p \approx \mathbb{Z}_{p^2}$. But every nonidentity element of $\mathbb{Z}_p \times \mathbb{Z}_p$ has order p whereas $\mathbb{Z}_{p^2}$ has an element of order p^2, namely, $[p^2 - 1]$.

Corollary 19.1
If $|G| = p$, where p is a prime number, then $G \approx \mathbb{Z}_p$.

Proof.
Since G has a prime order then by Corollary 17.3, G is cyclic. By the previous theorem, $G \approx \mathbb{Z}_p$.$\blacksquare$

Theorem 19.4
If G is an infinite cyclic group then $G \approx \mathbb{Z}$.

Proof.
Suppose that $G =< a >$ with $o(a) = \infty$. Define $\theta : \mathbb{Z} \longrightarrow < a >$ by $\theta(n) = a^n$. Then θ is a well-defined mapping. Indeed, if $n = m$ then $a^n = a^m$. We will

show next that θ is one-to-one. Suppose that $\theta(n) = \theta(m)$. Without loss of generality we can assume that $n < m$. Then

$$e = a^0 = a^{n-n} = a^n a^{-n} = a^m a^{-n} = a^{m-n}.$$

This contradicts the fact that $o(a) = \infty$ Since $m - n \in \mathbb{N}$. Thus, we must have $n = m$. To show that θ is onto, pick an $x \in G$. Then $x = a^n$ for some $n \in \mathbb{Z}$ and $\theta(n) = a^n = x$. It remains to show that θ is a homomorphism: $\theta(n + m) = a^{n+m} = a^n a^m = \theta(n)\theta(m)$. Thus, $\mathbb{Z} \approx < a >$ or $< a > \approx \mathbb{Z}$ since $\approx$ is symmetric. This ends a proof of the theorem.■

A principal problem in finite group theory is the problem of classifying groups of finite orders. For example, the problem of determining all isomorphism classes is settled by the following theorem whose proof is omitted.

Theorem 19.5 *(Fundamental Theorem of Finite Abelian Groups)*
Every finite abelian group is isomorphic to a direct product of cyclic groups in the form

$$C_{{p_1}^{r_1}} \times C_{{p_2}^{r_2}} \times \cdots \times C_{{p_t}^{r_t}},$$

where the p_i are (not necessarily distinct) primes; the product is unique up to reordering of the factors.

Example 19.3
There are six isomorphism classes of Abelian groups of order 360. If G is Abelian with $|G| = 360 = 2^3.3^2.5$, then the possible sets of prime powers are as follows:

$$\{2^3, 3^2, 5\},$$
$$\{2^3, 3, 3, 5\},$$
$$\{2, 2^2, 3^2, 5\},$$
$$\{2, 2^2, 3, 3, 5\},$$
$$\{2, 2, 2, 3^2, 5\},$$
$$\{2, 2, 2, 3, 3, 5\}.$$

Hence there are six mutually non-isomorphic abelian groups of order 360:

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5,$$
$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \blacksquare$$

Review Problems

Exercise 19.1
Give a reason why each of the following two groups are not isomorphic.

(a) $\mathbb{Z}_5, \mathbb{Z}_6$.
(b) $\mathbb{Z}_4 \times \mathbb{Z}_2$, symmetry group of the square.
(c) $\mathbb{Z}, \mathbb{Q}$ *(with both* $+$*.*
(d) $\mathbb{Z}_8 \times \mathbb{Z}_4, \mathbb{Z}_1 6 \times \mathbb{Z}_2$.

Exercise 19.2
Is there a noncyclic group of order 59?Why?

Exercise 19.3
Is there a noncyclic group of order 39?Why?

Exercise 19.4
Give an example of a noncyclic group of order 49.

Exercise 19.5
Find two groups of order 9 that are not isomorphic.

Exercise 19.6
If p *is a prime, then there are five isomorphism classes of Abelian group of order* p^4*. Give one group from each class.*

Exercise 19.7
An isomorphism of a group G *onto itself is called an* **automorphism**. *Prove that the set of all automorphisms on* $G, Aut(G)$*, is a group with respect to composition.*

Exercise 19.8
Prove that if G *is Abelian then the mapping* $\theta : G \to G$ *given by* $\theta(a) = a^{-1}$ *is an automorphism on* G*.*

Exercise 19.9
Prove that if $[a]$ *is a generator of* $\mathbb{Z}_n$*, and* $\theta : \mathbb{Z}_n \to \mathbb{Z}_n$ *is defined by* $\theta([k]) = [ka]$*, then* $\theta \in Aut(\mathbb{Z}_n)$.

Exercise 19.10
Prove that $Aut(\mathbb{Z}) \approx \mathbb{Z}_2$.

Exercise 19.11
Prove that for p prime, $Aut(\mathbb{Z}_p) \approx \mathbb{Z}_{p-1}$.

Exercise 19.12
Consider $\mathbb{R}^2$ *under addition. Show that the mapping* $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ *defined by* $\theta(a, b) = (b, a)$ *is an automorphism.*

Exercise 19.13
Prove that any two groups of order 3 are isomorphic.

Exercise 19.14
Prove that $Aut(Z_n) \approx \mathbb{Z}_n^*$.

Exercise 19.15
Let G *be agroup and for* $a \in G$ *define* $\theta_a : G \to G$ *by* $\theta_a(x) = axa^{-1}$. *Prove that* $\theta_a \in Aut(G)$.

Exercise 19.16
Let G *be a group and define* $Inn(G) = \{theta_a : a \in G\}$, *where* θ_a *is the mapping defined in the previous exercise. Prove that* $Inn(G)$ *is a subgroup of* $Aut(G)$.

Exercise 19.17
Let $\theta : G \to H$ *be an isomorphism. Let* $a \in G$ *and* k *be a positive integer. Show that the equation* $x^k = a$ *has the same number of solutions in* G *as does the equation* $x^k = \theta(a)$ *in* H.

Exercise 19.18
(a) Solve the equation $x^4 = 1$ *in* $\mathbb{R}^*$.
(b) Solve the equation $x^4 = 1$ *in* C^*, *where* C^* *denote the group of all nonzero complex numbers.*
(c) Is $\mathbb{R}^*$ *isomorphic to* C^*?

Exercise 19.19
Let G *be a finite group and* $\theta \in Aut(G)$ *such that* $\theta^2 = \iota_G$ *and* $\theta(x) \neq e_G$ *for all* $x \neq e_G$. *Prove that* G *is Abelian.*

Exercise 19.20
Suppose that G *and* H *are isomorphic groups. Prove that if every element of* G *is its own inverse then every element of* H *is its own inverse.*

20 Cayley's Theorem

We have already met (i.e. Section 6) the symmetric group $Sym(S)$, the group of all permutations on a set S. It was one of our first examples of a group. In fact it is a very important group, partly because of Cayley's theorem which we discuss in this section.
Cayley's theorem represents a group as a subgroup of a permutation group(up to an isomorphism). This is often advantageous, because permutation groups are fairly concrete objects. For example, it's straightfroward to write programs to do arithmetic in finite permutation groups.

Theorem 20.1 *(Cayley's Theorem)*
Any group G is isomorphic to a subgroup of $Sym(G)$.

Proof.
Given $g \in G$, we define a map $\lambda_g : G \to G$ by $\lambda_g(x) = gx$ for all $x \in G$. This is a well-defined mapping. Indeed, if $x = y$ then $gx = gy$ so that $\lambda_g(x) = \lambda_g(y)$. Next, we show that λ_g is one-to-one. To see this, suppose that $\lambda_g(x) = \lambda_g(y)$. Then $gx = gy$ and by the left-cancellation property $x = y$. To see that λ_g is onto, let $y \in G$. Then $g^{-1}y \in G$ and $\lambda_g(g^{-1}y) = y$. Hence, $\lambda_g \in Sym(G)$.
Next, We define $\Lambda : G \to Sym(G)$ by $\Lambda(g) = \lambda_g$. This is a well-defined mapping. For if $g_1 = g_2$ then $g_1x = g_2x$ for all $x \in G$, that is, $\lambda_{g_1}(x) = \lambda_{g_2}(x)$ for all $x \in G$ and hence $\lambda_{g_1} = \lambda_{g_2}$, i.e. $\Lambda(g_1) = \Lambda(g_2)$.
Now, given $g_1, g_2 \in G$ we have

$$\lambda_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \lambda_{g_1}(g_2x) = \lambda_{g_1}\lambda_{g_2}(x) \qquad \text{for all } x \in G.$$

Thus, $\Lambda(g_1g_2) = \lambda_{g_1g_2} = \lambda_{g_1}\lambda_{g_2} = \Lambda(g_1)\Lambda(g_2)$, and so Λ is a homomorphism. Finally, we show that Λ is one-to-one. Indeed, if $\Lambda(g_1) = \Lambda(g_2)$ then $\lambda_{g_1}(x) = \lambda_{g_2}(x)$ for all $x \in G$. In particular, $\lambda_{g_1}(e) = \lambda_{g_2}(e)$. That is, $g_1e = g_2e$ or $g_1 = g_2$. By Theorem 18.2(v), $G \approx \Lambda(G)$.■

Corollary 20.1
Every finite group G of order n is isomorphic to a subgroup of S_n.

Proof.
Write G in set-builder notation as $G = \{a_1, a_2, \cdots, a_n\}$. The proof of Theorem 20.1 assigns to the element a_i the map $\lambda_{a_i} = \begin{pmatrix} a_1 & \cdots & a_n \\ a_ia_1 & \cdots & a_ia_n \end{pmatrix}$.

Now, $a_i a_1, \cdots, a_i a_n$ is just the ith row of the Cayley table for G, and thus is simply a rearrangement of $a_1, \cdots, a_n$, say $a_{\theta_i(1)}, \cdots, a_{\theta_i(n)}$ where $\theta_i \in S_n$; so $\lambda_{a_i} = \begin{pmatrix} a_1 & \cdots & a_n \\ a_{\theta_i(1)} & \cdots & a_{\theta_i(n)} \end{pmatrix}$. If we now replace a_i by i, we map λ_{a_i} to $\begin{pmatrix} 1 & \cdots & n \\ \theta_i(1) & \cdots & \theta_i(n) \end{pmatrix} = \theta_i$. By Theorem 20.1, $\{\theta_1, \theta_2, \cdots, \theta_n\} \approx \Lambda(G) \approx G$. That is, G is isomorphic to a subgroup of S_n.■

Example 20.1
Consider the following Cayley table of a group $G = \{e, a, b, c\}$.

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We then have

$$\lambda_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, \quad \theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)$$
$$\lambda_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$
$$\lambda_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, \quad \theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$
$$\lambda_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}, \quad \theta_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

Hence G is isomorphic to the subgroup

$$\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$$

of S_4.■

Review Problems

Exercise 20.1
Write the permutation associated with each element of $\mathbb{Z}_5$ *by the isomorphism* Λ *in the proof of Cayley's Theorem.*

Exercise 20.2
Write the permutation associated with each element of the symmetry group of the square by the isomorphism Λ *in the proof of Cayley's Theorem.*

Exercise 20.3
Write the permutation associated with each element of group $G = \{1, i, -1, -i\}$ *(under multiplication) of the by the isomorphism* Λ *in the proof of Cayley's Theorem.*

Exercise 20.4
Write the permutation associated with each element of a cyclic group $G =< a >$ *of order 4 by the isomorphism* Λ *in the proof of Cayley's Theorem.*

Exercise 20.5
For each a *in a group* g*, define* $\delta_a : G \to G$ *by* $\delta_a(x) = xa$*.*

(a) Prove that δ_a *is a permutation on* G*.*
(b) Prove that $H = \{\delta_a : a \in G\}$ *is a group with respect to composition.*
(c) Define $\phi : G \to H$ *by* $\phi(a) = \delta_a$*. Determine whether or not* ϕ *is always an ismorphism.*

Exercise 20.6
For each a *in a group* g*, define* $\rho_a : G \to G$ *by* $\rho_a(x) = xa^{-1}$*.*

(a) Prove that ρ_a *is a permutation on* G*.*
(b) Prove that $H = \{\rho_a : a \in G\}$ *is a group with respect to composition.*
(c) Define $\phi : G \to H$ *by* $\phi(a) = \rho_a$*. Determine whether or not* ϕ *is always an ismorphism.*

Exercise 20.7
Assume that G *is a group, and that* $\lambda_a : G \to G$ *and* $\rho_a : G \to G$ *are defined by* $\lambda_a(x) = ax$ *and* $\rho_a(x) = xa^{-1}$ *for each* $x \in G$*. For each* $a \in G$*, define* $\gamma_a : G \to G$ *by* $\gamma_a = \rho_a \circ \lambda_a$*. Prove that* $\gamma_a \in Aut(G)$*.*

Exercise 20.8
Let γ_a be defined as in Exercise 20.7, and define $\phi : G \to Sym(G)$ by $\phi(a) = \gamma_a$ for each $a \in G$. Prove that $\phi(a) = \iota_G$ if and only if $ax = xa$ for all $x \in G$.

Exercise 20.9
Let $\theta : G \to G$ is a one-to-one and onto mapping such that $\lambda_g\theta = \theta\lambda_g$ for all $g \in G$. Prove that there is an $a \in G$ such that $\theta = \rho_a$.

Exercise 20.10
Prove that for each positive integer n, there are finitely many isomorphism classes of groups of order n.

21 Homomorphisms and Normal Subgroups

Recall that an isomorphism is a function $\theta : G \longrightarrow H$ such that θ is one-to-one, onto and such that $\theta(ab) = \theta(a)\theta(b)$ for all $a, b \in G$. We shall see that an isomorphism is simply a special type of function called a *group homomorphism.* We will also see a relationship between group homomorphisms and normal subgroups.

Definition 21.1
A function θ from a group G to a group H is said to be a **homomorphism** *provided that for all $a, b \in G$ we have that*

$$\theta(ab) = \theta(a)\theta(b).$$

If $\theta : G \longrightarrow H$ is a one-to-one homomorphism, we call θ a **monomorphism** *and if $\theta : G \longrightarrow H$ is an onto homomorphism, then we call θ an* **epimorphism.** *Of course, a bijective homomorphism is an* **isomorphism.**

Example 21.1
Define $\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $\theta(a) = [a]$. Then

$$\theta(a + b) = [a + b] = [a] \oplus [b] = \theta(a) \oplus \theta(b),$$

so that θ is a homomorphism. Note that $\theta(n) = \theta(2n)$ with $n \neq 2n$ so that θ is not one-to-one. However, θ is onto.■

Example 21.2
Define $\theta : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\theta(a) = 2a$. Then

$$\theta(a + b) = 2(a + b) = 2a + 2b = \theta(a) + \theta(b),$$

so that θ is a homomorphism. Note that θ is not onto since there is no integer n that satisfies $\theta(n) = 3$. However, θ is one-to-one since $\theta(n) = \theta(m)$ implies $2n = 2m$ and this in turn implies that $n = m$.■

We have seen that the range of a homomorphism is a subgroup of the codomain. (Theorem 18.2(iv)). The following subset determines a subgroup of the domain of a homomorphism.

Definition 21.2
Let $\theta : G \longrightarrow H$ be a group homomorphism. Then the **kernel** *of θ is the set*

$$Ker\ \theta = \{g \in G : \theta(g) = e_H\}.$$

Example 21.3
In Example 21.1, $a \in Ker\ \theta$ iff $[a] = \theta(a) = [0]$, i.e iff $a = nq$ for some $q \in \mathbb{Z} >$ Thus,$Ker\ \theta = \{nq : q \in \mathbb{Z}\}$. In Example 21.2, $a \in Ker\ \theta$ iff $2a = \theta(a) = 0$, i.e. iff $a = 0$. Hence, $Ker\ \theta = \{0\}$.■

As point it out earlier the kernel is a subgroup of the domain.

Theorem 21.1
Let $\theta : G \longrightarrow H$ be a homomorphism. Then

(i) $Ker\ \theta$ is a subgroup of G.
(ii) For any $x \in Ker\ \theta$ and $g \in G$ we have $gxg^{-1} \in Ker\ \theta$.

Proof.
(i) By Theorem 18.2(i), $\theta(e_G) = e_H$ so that $e_G \in Ker\ \theta$. Hence, $Ker\ \theta \neq \emptyset$. Now, let $x, y \in Ker\ \theta$. Then

$$\theta(xy^{-1}) = \theta(x)\theta(y^{-1}) = \theta(x)(\theta(y))^{-1} = e_H e_H^{-1} = e_H.$$

Thus, $xy^{-1} \in Ker\ \theta$. By Theorem 7.5, $Ker\ \theta$ is a subgroup of G.

(ii) Let $x \in Ker\ \theta$ and $g \in G$. Then

$$\theta(gxg{-}1) = \theta(g)\theta(x)\theta(g^{-1}) = \theta(g)e_H(\theta(g))^{-1} = \theta(g)(\theta(g))^{-1} = e_H.$$

Thus, $gxg^{-1} \in Ker\ \theta$. ■

Theorem 21.1(ii) is one of the common properties that kernels share: They are all normals in the sense of the following definition.

Definition 21.3
Let H be a subgroup of a group G. Then H is **normal** *iff $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. We write $H \triangleleft G$.*

Example 21.4
Let H be any subgroup of an Abelian group G. Since $hg = gh$ for all $g \in G$ and all $h \in H$ then $ghg^{-1} = h \in H$ for all $g \in G$ and $h \in H$. That is, $H \triangleleft G$.■

Example 21.5
Let $G = S_3$ and $H =< (12) >= \{(1), (12)\}$. Since $(123)(12)(123)^{-1} = (23) \notin H$ then H is not a normal subgroup of G.■

Lemma 21.1
The following statements are equivalent:

(i) $gng^{-1} \in N$ *for all* $n \in N$ *and* $g \in G$;
(ii) $g^{-1}ng \in N$ *for all* $n \in N$ *and* $g \in G$;

Proof.
(i) $\rightarrow$ (ii): Suppose that $gng^{-1} \in N$ for all $n \in N$ and $g \in G$. In particular, $g^{-1}n(g^{-1})^{-1} \in N$ since $g^{-1} \in G$. But $(g^{-1})^{-1} = g$ so that $g^{-1}ng \in N$.
(ii) $\rightarrow$ (i): Suppose that $g^{-1}ng \in N$ for all $n \in N$ and $g \in G$. Since $(g^{-1})^{-1} = g$ then $gng^{-1} = (g^{-1})^{-1}ng^{-1} \in N$.■

The following lemma shows that the homomorphic image of a normal subgroup is normal for onto maps.

Lemma 21.2
Let $\theta : G \rightarrow H$ *be an epimorphism and* $N \triangleleft G$. *Then* $\theta(N) \triangleleft H$.

Proof.
From Theorem 18.2 (iv), we know that $\theta(N)$ is a subgroup of H. Let $y \in \theta(N)$ and $h \in H$. Then $y = \theta(x) \in \theta(N)$ for some $x \in N$ and $h = \theta(g)$ for some $g \in G$ (since θ is onto). But $N \triangleleft G$ so that $gxg^{-1} \in N$. Thus, $\theta(gxg^{-1}) \in \theta(N)$. But $\theta(gxg^{-1}) = \theta(g)\theta(x)\theta(g^{-1}) = hyh^{-1} \in \theta(N)$. Hence, $\theta(N) \triangleleft H$.■

The following theorem describes a commonly used way for testing whether a homomorphism is one-to-one or not.

Theorem 21.2
Let $\theta : G \longrightarrow H$ *be a homomorphism. Then* θ *is one-to-one if and only if* $Ker\ \theta = \{e_G\}$.

Proof.
Suppose first that θ is one-to-one. Let $x \in Ker\ \theta$. Then $\theta(x) = e_H = \theta(e_G)$. Hence, $x = e_G$. Thus, $Ker\ \theta \subseteq \{e_G\}$. Since $\theta(e_G) = e_H$ then $\{e_G\} \subseteq Ker\ \theta$. It follows that $Ker\ \theta = \{e_G\}$. Conversely, suppose that $Ker\ \theta = \{e_G\}$. Suppose that $\theta(x) = \theta(y)$. Then $e_H = \theta(x)(\theta(y))^{-1} = \theta(x)\theta(y^{-1}) = \theta(xy^{-1})$. Thus, $xy^{-1} \in Ker\ \theta$. But then $xy^{-1} = e_G$ so that $x = y$.■

Review Problems

Exercise 21.1
Define $\theta : \mathbb{Z}_6 \to \mathbb{Z}_3$ *by* $\theta([a]_6) = [a]_3$.

(a) Prove that θ *is well-defined.*
(b) Prove that θ *is a homomorphism.*
(c) Find $Ker\ \theta$.

Exercise 21.2
(a) Prove that $\theta : \mathbb{Z}_3 \to \mathbb{Z}_3$ *defined by* $\theta([a]_3) = [a]_6$ *is not well-defined.*
(b) For which pairs m, n *is* $\beta : \mathbb{Z}_n \to \mathbb{Z}_m$, *given by* $\beta([a]_n) = [a]_m$, *well-defined?*

Exercise 21.3
(a) Prove that every homomorphic image of an Abelian group is Abelian.
(b) Prove that every homomorphic image of a cyclic group is cyclic.

Exercise 21.4
Let G *denote the subgroup* $\{1, -1, i, -i\}$ *of complex numbers (operation multiplication). Define* $\theta : \mathbb{Z} \to G$ *by* $\theta(n) = i^n$. *Show that* θ *is a homomorphism and determine* $Ker\ \theta$.

Exercise 21.5
There is a unique homomorphism $\theta : \mathbb{Z}_6 \to S_3$ *such that* $\theta([1]) = (123)$. *Determine* $\theta([k])$ *for each* $[k] \in \mathbb{Z}_6$. *Which elements are in* $Ker\ \theta$?

Exercise 21.6
Prove that $N \triangleleft G$ *if and only if* $gN = Ng$ *for all* $g \in G$.

Exercise 21.7
Prove that if N *is a subgroup of* G *such that* $[G : N] = 2$ *then* $N \triangleleft G$.

Exercise 21.8
Prove that $A_n \triangleleft S_n$ *for all* $n \geq 2$.

Exercise 21.9
Consider the subgroup $H = A_3 = \{(1), (123), (132)\}$ *of* S_3. *Let* $x = (12)$ *and* $h = (123)$. *Show that* $xh \neq hx$ *and* $xH = Hx$. *This shows that the equality* $xH = Hx$ *does not mean that* $xh = hx$ *for all* $x \in G$ *and* $h \in H$.

Exercise 21.10
Prove that if $\mathcal{C}$ denote the collection of all normal subgroups of a group G. prove that $N = \cap_{H \in \mathcal{C}} H$ is also a normal subgroup of G.

Exercise 21.11
Prove that if $N \triangleleft G$ then for any subgroup H of G, we have $H \cap N \triangleleft H$.

Exercise 21.12
Find all normal subgroups of S_3.

Exercise 21.13
Let H be a subgroup of G and $K \triangleleft G$.

(a) Prove that HK is a subgroup of G, where $HK = \{hk : h \in H \text{ and } k \in K\}$.
(b) Prove that $HK = KH$.
(c) Prove that $K \triangleleft HK$.

Exercise 21.14
Prove that if H and K are normal subgroups of G then HK is a normal subgroup of G.

Exercise 21.15
Prove that if H and K are normal subgroups of G such that $H \cap K = \{e_G\}$ then $hk = kh$ for all $h \in H$ and $k \in K$.

Exercise 21.16
The **center** *of the group G is defined by*

$$Z(G) = \{g \in G : xg = gx \forall x \in G\}.$$

Prove that $Z(G) \triangleleft G$.

Exercise 21.17
Let G and H be groups. Prove that $G \times \{e_H\}$ is a normal subgroup of $G \times H$.

Exercise 21.18
Let N be a normal subgroup of G, and let $a, b, c, d \in G$. prove that if $aN = cN$ and $bN = dN$ then $abN = cdN$.

Exercise 21.19
Let G be a non-abelian group of order 8. Prove that G has at least one element of order 4. Hence prove that G has a normal cyclic subgroup of order 4.

Exercise 21.20
Suppose that $\theta : G \to H$ is a homomorphism. Let $K = Ker\ \theta$ and $a \in G$. Prove that $aK = \{x \in G : \theta(x) = \theta(a)\}$.

Exercise 21.21
Let S be any set, and let B be any proper subset of S. Let $H = \{\theta \in Sym(S) : \theta(B) = B\}$. Prove that H is a subgroup of $Sym(S)$ that is not normal.

Exercise 21.22
A group G is called **simple** *if $\{e_G\}$ and G are the only normal subgroups of G. Prove that a cyclic group of prime order is simple.*

Exercise 21.23
Let U and V be nonabelian simple groups. Show that $G = U \times V$ has precisely four different normal subgroups.

22 Quotient Groups

Let's look closely on the construction of the group $(\mathbb{Z}_n, \oplus)$. We know that the elements in $\mathbb{Z}_n$ are equivalence classes of the equivalence relation defined on $\mathbb{Z}$ by

$$a \sim b \ \ if \ and \ only \ if \ \ n|(a-b).$$

Also, an element of $\mathbb{Z}_n$ is a right coset. Indeed, if $0 \leq k < n$ then

$$< n > +k = [k] = \{nq + k : q \in \mathbb{Z}\}.$$

The operation $\oplus$ is defined by

$$[a] \oplus [b] = [a + b]$$

or using right cosets

$$(< n > +a) \oplus (< n > +b) =< n > +(a + b).$$

Note that the cyclic group $< n >$ is a normal subgroup of $\mathbb{Z}$ since $\mathbb{Z}$ is Abelian (See Example 21.4). We are going to use the above ideas to construct new groups where G is a group replacing $\mathbb{Z}$ and N is a normal subgroup of G playing the role of $< n >$. More precisely, we have the following theorem.

Theorem 22.1
Let N be a normal subgroup of a group G and let G/N be the set of all right cosets of N in G. Define the operation on $G/N \times G/N$ by

$$(Na)(Nb) = N(ab).$$

Then $(G/N, \cdot)$ is a group, called the **quotient group** *of G by N.*

Proof.
$\cdot$ is a well-defined operation
We must show that if $(Na_1, Nb_1) = (Na_2, Nb_2)$ then $N(a_1b_1) = N(a_2b_2)$. To see this, since $(Na_1, Nb_1) = (Na_2, Nb_2)$ then $Na_1 = Na_2$ and $Nb_1 = Nb_2$. Since $a_1 = ea_1 \in Na_1$ then $a_1 \in Na_2$ so that $a_1 = na_2$ for some $n \in N$. Similarly, $b_1 = n'b_2$ for some $n' \in N$. Therefore, $a_1b_1 = na_2n'b_2$. Since $N \triangleleft G$ then $a_2n'a_2^{-1} \in N$, say $a_2n'a_2^{-1} = n'' \in N$. Hence, $a_2n' = n''a_2$ so that $a_1b_1 = nn''a_2b_2$. But $nn'' \in N$ so that $a_1b_1 \in N(a_2b_2)$. Since $N(a_2b_2)$ is an equivalence class and $a_1b_1 \in N(a_2b_2)$ then $N(a_1b_1) = N(a_2b_2)$ (Theorem 9.2).

$\cdot$ is associative
Let $a, b, c \in G$. Then

$$Na(NbNc) = Na(Nbc) = N(a(bc)) = N((ab)c) = N(ab)Nc = (NaNb)(Nc)$$

where we used the fact that multiplication in G is associative.

$Ne = N$ is the identity element
If $a \in G$ then $(Na)(Ne) = N(ae) = Na$ and $(Ne)(Na) = N(ea) = Na$.

Every element of G/N is invertible
If $a \in G$ then $(Na)(Na^{-1}) = N(aa^{-1}) = Ne$ and $(Na^{-1})(Na) = N(a^{-1}a) = Ne$ so that $(Na)^{-1} = Na^{-1}$. ■

Remark 22.1
Note that for a finite group G, the number of elements of G/N is just the index of N in G, i.e. $[G : N]$. That is, $|G/N| = [G : N]$. By Lagrange's theorem, $|G| = [G : N]|N|$ so that $[G : N] = \frac{|G|}{|N|}$. Hence, $|G/N| = \frac{|G|}{|N|}$.

Remark 22.2
If N is not a normal subgroup of G, then the operation defined in the previous theorem will not be well-defined. To see this, consider the subgroup $N =< (12) >= \{(1), (12)\}$ of S_3. Since $(123)(12)(123)^{-1} = (23) \notin N$ then N is not a normal subgroup of S_3. However, $N(123) = N(23) = \{(123), (23)\}$ and $N(132) = N(13) = \{(13), (132)\}$. But $N(123)(132) \neq N(23)(13)$ since $N(123)(132) = N$ and $N(23)(13) = N(123)$.■

Example 22.1
Let $G = S_3$ and $N =< (123) >= \{(1), (123), (132)\}$. One can verify easily that $N \triangleleft G$, $G/N = \{N, N(12)\}$.■

Example 22.2
Quotient groups can be used to show that A_4 has no subgroup of order 6 and thus showing that the converse of Lagrange's Theorem is false in general. To see this, assume that N is a subgroup of A_4 of order 6. Then $[G : N] = 2$ and therefore $N \triangleleft A_4$ (See Exercise 21.7). Hence, A_4/N makes sense. Moreover, for each $a \in N$, $(Na)^{-1} = Na$ so that $Na^2 = N$ and hence $a^2 in N$. One can show that $(123)^2 = (132), (132)^2 = (123), (124)^2 = (142), (142)^2 = (124), (134)^2 =$

$(143), (143)^2 = (134), (234)^2 = (243)$, and $(243)^2 = (234)$. This yields more than six different elements of A_4 in N. That is, $|N| > 6$, a contradiction. Thus, A_4 has no subgroup of order 6.■

By Theorem 21.1(ii), the kernel of a homomorphism is a normal subgroup. Conversely, quotient groups enable us to show that every normal subgroup is the kernel of some homomorphism.

Theorem 22.2
Let G be a group and let $N \triangleleft G$. The mapping $\eta : G \longrightarrow G/N$ defined by $\eta(a) = Na$ for all $a \in G$ is a homomorphism such that $Ker\ \eta = N$. We call η the **natural homomorphism** *from G onto G/N.*

Proof.
First we show that η is well-defined. Indeed, if $a = b$ then $Na = Nb$, i.e. $\eta(a) = \eta(b)$. Since $\eta(ab) = N(ab) = NaNb = \eta(a)\eta(b)$ then η is a homomorphism. η is onto since any member of G/N is of the form Na for some $a \in G$. That is, $\eta(a) = Na$. It remains to show that $Ker\ \eta = N$. The proof is by double inclusions. If $a \in Ker\ \eta$ then $\eta(a) = Ne$. Thus, $Na = Ne$ so that $a = ne = n$ for some $n \in N$. Hence, $a \in N$ and $Ker\ \eta \subseteq N$. Conversely, for all $n \in N$ we have $\eta(n) = Nn = N = Ne$ so that $N \subseteq Ker\ \eta$. ■

The operation of multiplication on the quotient group was defined in terms of right cosets. The following theorem shows that when working with cosets of a normal subgroup N, it is immaterial whether we use Na or aN.

Example 22.3
If $G = \mathbb{Z}$ and $N =< n >$ then $G/N = \mathbb{Z}_n$ and $\eta : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ is given by $\eta(a) =< n > +a = [a]$ and $Ker\ \eta =< n >$.■

Theorem 22.3
Let N be a normal subgroup of a group G. Then $aN = Na$ for all $a \in G$.

Proof.
Let $x \in aN$. Then $x = an$ for some $n \in N$. Since N is normal then $ana^{-1} \in N$. Thus, $ana^{-1} = n' \in N$ and therefore $an = n'a$. That is, $x \in Na$. Hence, $aN \subseteq Na$. A similar argument shows that $Na \subseteq aN$.■

We close this section with some properties of quotient groups. More properties of quotient groups are discussed in the exercises.

Lemma 22.1
If G is Abelian and $N \triangleleft G$ then G/N is also Abelian.

Proof.
We have to show that for any $Na, Nb \in G/N$ we have $(Na)(Nb) = (Nb)(Na)$. Now, since G is Abelian then $ab = ba$. Thus,

$$(Na)(Nb) = Nab = Nba = (Nb)(Na).$$

That is, G/N is Abelian.■

Lemma 22.2
If G is a group such that $G/Z(G)$ is cyclic then G is Abelian, where

$$Z(G) = \{g \in G : xg = gx \ \forall x \in G\}.$$

Proof.
First we show that $Z(G) \triangleleft G$. Indeed, if $g \in G$ and $x \in Z(G)$ then $gxg^{-1} = gg^{-1}x = x \in Z(G)$. Since $G/Z(G)$ is a cyclic group then $G/Z(G) =< Z(G)g >$ for some $g \in G$. If $a, b \in G$ then $Z(G)a$ and $Z(G)b$ belong to $G/Z(G)$. Thus, $Z(G)a = Z(G)g^n$ and $Z(G)b = Z(G)g^m$ for some integers n and m. Hence, $a = xg^n$ and $b = yg^m$ for some $x, y \in Z(G)$. This implies that $ab = (xg^n)(yg^m) = xyg^{n+m} = yxg^m g^n = yg^m xg^n = ba$. Hence, G is Abelian.■

Lemma 22.3
Let G be a group of order p^2 where p is a prime number. Assuming that the center of G is nontrivial, then G is Abelian.

Proof.
Let G be a group such that $|G| = p^2$. Since $e \in C(G)$ then $C(G) \neq \emptyset$. By Lagrange's theorem either $|C(G)| = p^2$ or $|C(G)| = p$. If $|C(G)| = p^2$ then $C(G) = G$ and so G is Abelian. If $|C(G)| = p$ then $|G/C(G)| = p$ and so $G/C(G)$ is cyclic (See Corollary 3). By the previous lemma, G is Abelian.■

Review Problems

Exercise 22.1
Find the order of each of the following quotient groups.

(i) $\mathbb{Z}_8/ < [4] >$.
(ii) $< 2 > / < 8 >$.

Exercise 22.2
Let $G = A_4$ *and* $H = \{(1), (12)(34), (13)(24), (14)(23)\} \triangleleft G$. *Write out the distinct elements of* G/H *and make a Cayley table for* G/H.

Exercise 22.3
Construct the Cayley table for $\mathbb{Z}_{12}/ < [4] >$.

Exercise 22.4
Let G *be a cyclic group. Prove that for every subgroup* H *of* G, G/H *is cyclic.*

Exercise 22.5
Assume $N \triangleleft G$.

(a) Prove that if $[G : N]$ *is prime, then* G/N *is cyclic.*
(b) Prove or disprove the converse of the statement in part (a).

Exercise 22.6
Determine the order of $\mathbb{Z}_{12} \times \mathbb{Z}_4/ < [3], [2] >$.

Exercise 22.7
Prove that if $N \triangleleft G$ *and* $a \in G$ *then* $o(Na)|o(a)$.

Exercise 22.8
Prove that G/N *is Abelian if and only if* $aba^{-1}b^{-1} \in N$ *for all* $a, b \in G$.

Exercise 22.9
Let N *be a normal subgroup of* G *and* $a \in G$. *Prove that the order of* Na *in* G/N *is the smallest positive integer* n *such that* $a^n \in N$.

Exercise 22.10
Let $\theta : G \to H$ be a homomorphism and $K = Ker\ \theta$. Show that $\phi : G/K \to \theta(G)$ defined by $\phi(Ka) = \theta(a)$ is an isomorphism. Also, show that $\phi \circ \eta = \theta$, where η is the canonical homomorphism.

Exercise 22.11
Let H and K be subgroups of a group G such that $K \triangleleft G$. Prove that $H/H \cap K$ and HK/K make sense, where $HK = \{hk : h \in H \text{ and } k \in K\}$.

Exercise 22.12
Let H and K be as in the previous exercise. Show that $\phi : H \to HK/K$ defined by $\phi(h) = Kh$ an epimorphism with $Ker\ \phi = H \cap K$.

Exercise 22.13
Assume that $H, K \triangle G$ and $K \triangle H$. Prove that $H/K \triangleleft G/K$.

Exercise 22.14
Let H, K, and G as in the previous exercise. Show that $\phi : G/K \to G/H$, defined by $\phi(Kg) = Hg$ is an epimorphism with $Ker\ \phi = H/K$.

Exercise 22.15
If N is a subgroup of G such that the product of two right cosets of N in G is again a right coset of N in G, prove that $N \triangleleft G$.

23 Isomorphism Theorems

Theorem 22.2 shows that each quotient group of a group G is the homomorphic image of G. The theorem below shows that the converse is also true. That is, each homomorphic image is isomorphic to a quotient group.

Theorem 23.1 *(The Fundamental Homomorphism Theorem)*
Let $\theta : G \longrightarrow H$ be a homomorphism. Then

$$G/K \approx \theta(G)$$

where $K = Ker\ \theta$. Moreover, $\phi \circ \eta = \theta$ where η is the natural homomorphism introduced in Theorem 22.2

Proof.
By Theorem 21.1, $K = Ker\ \theta \triangleleft G$ so that by Theorem 22.1, G/K is a group. Define $\phi : G/K \longrightarrow \theta(G)$ by $\phi(Ka) = \theta(a)$. This is a well-defined mapping. To see this, suppose that $Ka = Kb$. Since $a = ea \in Ka$ then $a \in Kb$ so that $a = kb$ for some $k \in K$. Hence, $\theta(a) = \theta(kb) = \theta(k)\theta(b) = e_H\theta(b) = \theta(b)$. Thus, $\phi(Ka) = \phi(Kb)$.
Next, we show that ϕ is a homomorphism. Let $Ka, Kb \in G/K$. Then

$$\phi(KaKb) = \phi(Kab) = \theta(ab) = \theta(a)\theta(b) = \phi(Ka)\phi(Kb).$$

To show that ϕ is one-to-one we use Theorem 21.2. That is we show that $Ker\ \phi = \{K\}$. If $Ka \in Ker\ \phi$ then $\phi(Ka) = e_H$. Thus, $\theta(a) = e_H$ so that $a \in K$. This implies that $Ka = K$.
Now, if $y \in \theta(G)$ then $y = \theta(a) = \phi(Ka)$ for some $a \in G$. This shows that ϕ is onto. Hence, ϕ is an ismomorphism and thus $G/K \approx \theta(G)$.
Finally, note that $\phi \circ \eta$ and θ have the same domain, codomain and for all $g \in G$, $(\phi \circ \eta)(g) = \phi(\eta(g)) = \phi(Ng) = \theta(g)$. Thus, $\phi \circ \eta = \theta$. This completes a proof of the theorem.■

Example 23.1
Looking at Example 22.3, we see that the mapping $\theta : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ defined by $\theta(a) = [a]$ satisfies the assumptions of Theorem 23.1. Hence, $\mathbb{Z}/ < n > \approx \mathbb{Z}_n$■

As a consequence of Theorem 23.1, we have the following two theorems.

Theorem 23.2 *(First Isomorphism Theorem)*
Let H and K be subgroups of a group G such that $K \triangleleft G$. Then the set

$$HK = \{hk : h \in H \text{ and } k \in K\}$$

is a subgroup of G such that $K \triangleleft HK$ and

$$H/H \cap K \approx HK/K.$$

Proof.
First we show that HK is a subgroup of G. Since $e_G = e_G e_G$ and $e_G \in H \cap K$ then $e_G \in HK$ so that $HK \neq \emptyset$. Now, if $a, b \in HK$ then $a = h_1 k_1$ and $b = h_2 k_2$. Thus, $ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 k h_2^{-1}$, where $k = k_1 k_2^{-1} \in K$. Since $K \triangleleft G$ then $h_2 k h_2^{-1} \in K$ so that $h_2 k h_2^{-1} = k'$ for some $k' \in K$. Thus, $k h_2^{-1} = h_2^{-1} k'$. This shows that $ab^{-1} = h_1 h_2^{-1} k' \in HK$. Hence, by Theorem 7.5, HK is a subgroup of G.
Next, we show that $K \triangleleft HK$. Since $k = e_H k \in HK$ then $K \subseteq HK$. Consider the product $(hk)k'(hk)^{-1} = hkk'k^{-1}h^{-1} = hk''h^{-1} \in K$ since $K \triangleleft G$. Hence, $K \triangleleft HK$.
Now, consider the mapping $\theta : H \longrightarrow HK/K$ defined by $\theta(h) = Kh$. This is a well-defined mapping: if $h_1 = h_2$ then $Kh_1 = Kh_2$. This mapping is onto from its definition. To see that θ is a homomorphism, we take $h_1, h_2 \in H$ and find

$$\theta(h_1 h_2) = Kh_1 h_2 = (Kh_1)(Kh_2) = \theta(h_1)\theta(h_2).$$

Finally, we show that $Ker\ \theta = H \cap K$. Indeed, if $x \in H \cap K$ then $x \in K$ and $x \in H$. Thus, $Kx = K$. That is, $\theta(x) = K$ and so $x \in Ker\ \theta$. Conversely, if $x \in Ker\ \theta$ then $Kx = K$ and this implies that $x \in K$. Since the kernel is a subset of H then $x \in H$. Thus, $x \in H \cap K$ and so $Ker\ \theta = H \cap K$. Applying Theorem 23.1, we obtain $H/(H \cap K) \approx HK/K$.■

Theorem 23.3 *(Second Isomorphism Theorem)*
Assume that $H, K \triangleleft G$ with $K \triangleleft H$. Then $H/K \triangleleft G/K$ and $(G/K)/(H/K) \approx G/H$.

Proof.
First we prove that H/K is a subgroup of G/K. Since $K \in H/K$ then $H/K \neq \emptyset$. Since $(Kh_1)(Kh_2)^{-1} = (Kh_1)(Kh_2^{-1}) = Kh_1 h_2^{-1} \in H/K$ then by

Theorem 7.5, H/K is a subgroup of G/K. To see that $H/K \triangleleft G/K$ we pick elements $Kh \in H/K$ and $Kg \in G/K$ and find that

$$(Kg)(Kh)(Kg)^{-1} = KghKg^{-1} = Kghg^{-1} \in H/K$$

since $ghg^{-1} \in H$ $(H \triangleleft G.)$
Next, we define $\theta : G/K \longrightarrow G/H$ by $\theta(Kg) = Hg$. This is well-defined map for if $Kg = Kg'$ then $g = kg'$ for some $k \in K \subseteq H$. Hence, $g \in Hg'$ and $Hg = Hg'$. From the definition of θ, we have that θ is onto.
θ is a homomorphism: If $Kg_1, Kg_2 \in G/K$ then $\theta(Kg_1Kg_2) = \theta(Kg_1g_2) = Hg_1g_2 = (Hg_1)(Hg_2) = \theta(Kg_1)\theta(Kg_2)$.
$Ker\ \theta = H/K$: If $Kg \in Ker\ \theta$ then $\theta(Kg) = H$, i.e. $Hg = H$ so that $g \in H$. Thus, $Kg \in H/K$ and this shows that $Ker\ \theta \subseteq H/K$. Now, if $Kh \in H/K$ then $\theta(Kh) = Hh = H$ so that $Kh \in Ker\ \theta$. Hence, $H/K \subseteq Ker\ \theta$ and this shows that $Ker\ \theta = H/K$. By Theorem 23.1, we have

$$(G/K)/(H/K) \approx G/H.\blacksquare$$

Review Problems

Exercise 23.1
Find all the homomorphic images of S_3.

Exercise 23.2
Prove that if G is any group with identity e then $G/\{e\} \approx G$.

Exercise 23.3
For any groups A and B, prove the following.

(a) $A \approx A \times \{e\} \triangleleft A \times B$.
(b) $\frac{A \times B}{A \times \{e\}} \approx B$.

Exercise 23.4
Prove that if G is a simple Abelian group then $G \approx \mathbb{Z}_p$ for some prime number p.

Exercise 23.5
Prove that $\frac{\mathbb{Z}_{18}}{<[3]>} \approx \mathbb{Z}_3$.

Exercise 23.6
Prove that if θ is a homomorphism of G onto H, $B \triangleleft H$, and $A = \{g \in G : \theta(g) \in B\}$, then $A \triangleleft G$.

Exercise 23.7
Give an example to show that if A and B are subgroups of a group G then AB need not be a subgroup of G.

Exercise 23.8
Suppose that $N \triangleleft G$. Let $\mathcal{C}$ be the collection of all subgroups of G containing H. Prove that the map ϕ defined by $\phi(S) = S/H$, where $S \in \mathcal{C}$ is one-to-one and onto.

Exercise 23.9
Let G be a group with normal subgroups H and K such that $G = HK$ and $H \cap K = \{e\}$. Prove that $G \approx H \times K$.

Exercise 23.10
Let G be a group.

(a) Prove that $f_a : G \to G$, given by $f_a(x) = axa^{-1}$ is an isomorphism.
(b) Prove that the set $Inn(G) = \{f_a : a \in G\}$ is a group under composition.
(c) Prove that $Inn(G) \approx G\mathbb{Z}(G)$, where $Z(G)$ is the center of G.

Exercise 23.11
Prove that $\frac{6\mathbb{Z}}{12\mathbb{Z}} \approx \frac{2\mathbb{Z}}{4\mathbb{Z}}$. Hint:Use First Isomorphism Theorem.

Exercise 23.12
Prove that if H is a normal subgroup of G of prime index p then for all subgroups K of G either (i) K is a subgroup of H or (ii) $G = HK$ and $[K : K \cap H] = p$.

Exercise 23.13
Let G be a finite group, H and N are subgroups of G such that $N \triangleleft G$. Prove that if $|H|$ and $[G : N]$ are relatively prime then H is a subgroup of N.

Exercise 23.14
Let G be a finite group and let H and K be subgroups of G with $K \triangleleft G$. Prove that

$$|HK| = \frac{|H|\ |K|}{|H \cap K}.$$

Exercise 23.15
Let G be a group and let H and K be normal subgroups of G with $K \subseteq H$. Suppose that G/K is cyclic. Prove that G/H and H/K are cyclic.

Exercise 23.16
Suppose that $K \triangleleft G$ and H is a subgroup of G such that $H \cap K = \{e_G\}$. Prove that H is isomorphic to a subgroup of G/K. Prove that if $G = HK$ then $G/K \approx H$.

Exercise 23.17
Suppose that $\phi : G \to H$ is an epimorphism and $N \triangleleft G$. Prove that there exists a homomorphism from G/N onto $H/\phi(N)$.

Exercise 23.18
Let G and H be groups and let $K \triangleleft G$ and $K' \triangleleft H$.

(a) Prove that $K \times K' \triangleleft G \times H$.
(b) Prove that $\frac{G \times H}{K \times K'} \approx G/K \times H/K'$.

Exercise 23.19
Let M and n be relatively prime. Show that $\phi : \mathbb{Z} \times \mathbb{Z}_m \times \mathbb{Z}_n$, given by $\phi(a) = ([a]_m, [a]_n)$ is a homomorphism, onto, and $Ker\ \phi =< mn >$.

Exercise 23.20
Prove that if m and n are relatively prime then $\mathbb{Z}_{mn} \approx \mathbb{Z}_m \times \mathbb{Z}_n$.

24 Rings: Definition and Basic Results

In this section, we introduce another type of algebraic structure, called *ring.* A group is an algebraic structure that requires one binary operation. A ring is an algebraic structure that requires two binary operations that satisfy some conditions listed in the following definition.

Definition 24.1
A **ring** *is a nonempty set R with two binary operations (usually written as addition and multiplication) such that for all $a, b, c \in R$,*

(1) R is closed under addition: $a + b \in R$. (2) Addition is associative: $(a + b) + c = a + (b + c)$.
(3) Addition is commutative: $a + b = b + a$.
(4) R contains an additive identity element, called **zero** *and usually denoted by 0 or 0_R: $a + 0 = 0 + a = a$.*
(5) Every element of R has an additive inverse: $a + (-a) = (-a) + a = 0$.
(6) R is closed under multiplication: $ab \in R$.
(7) Multiplication is associative: $(ab)c = a(bc)$.
(8) Multiplication distributes over addition: $a(b+c) = ab+ac$ and $(a+b)c = ac + bc$.
If $ab = ba$ for all $a, b \in R$ then we call R a **commutative ring.**

In other words, a ring is a commutative group with the operation + and an additional operation, multiplication, which is associative and is distributive with respect to +.

Remark 24.1
Note that we don't require a ring to be commutative with respect to multiplication, or to have multiplicative identity, or to have multiplicative inverses. A ring may have these properties, but is not required to. These additional properties will be discussed in the next section.

Example 24.1
The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, with the usual operations of multiplication and addition form commutative rings.

Example 24.2
The set $\mathbb{Z}_n$ with the operations of multiplication and addition modulo n forms

a commutative ring for any $n \in \mathbb{N}$. The only properties left to establish are the distributive laws. We will show that $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$. The proof of $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$ is similar.

$$\begin{aligned} [a] \odot ([b] \oplus [c]) &= [a] \odot [b + c] \\ &= [a(b + c)] \\ &= [ab + ac] \\ &= [ab] \oplus [ac] \\ &= [a] \odot [b] \oplus [a] \odot [c] \end{aligned}$$

Example 24.3
The set of even integers together with the usual addition and multiplication in $\mathbb{Z}$ is a commutative ring.

We next turn to discussing some basic properties of rings.

Theorem 24.1
The following hold in any ring R.

(i) $a + b = a + c$ implies $b = c$ for all $a, b, c \in R$.
(ii) $a0 = 0a = 0$ for all $a \in R$;
(iii) $a(-b) = (-a)a = -(ab)$ for all $a, b \in R$;
(iv) $-(-a) = a$.
(v) $-(a + b) = (-a) + (-b)$.
(vi) $(-a)(-b) = ab$ for all $a, b \in R$;
(vii) $a(b - c) = ab - ac$ and $(a - b)c = ac - bc$ for all $a, b, c \in R$, where we $a - b$ stands for $a + (-b)$.
(viii) $(-1)a = -a$ if R has a multiplicative identity,i.e. $1_R a = a1_R = a$ for all $a \in R$.

Proof.
(i) $b = 0+b = ((-a)+a)+b = (-a)+(a+b) = (-a)+(a+c) = ((-a)+a)+c = 0 + c = c$.
(ii) $a0 = a(0 + 0) = a0 + a0$. Thus, $0 + a0 = a0 = a0 + a0$ so that by the right cancellation property of the additive group we have $a0 = 0$. A similar argument holds for $0a = 0$.
(iii) Since $ab+(-a)b = (a+(-a))b = 0b = 0$ then $(-a)b$ is the additive inverse of ab. That is, $-(xab) = (-a)b$. Similarly, since $ab + a(-b) = a(b + (-b)) = a0 = 0$ then $-(ab) = a(-b)$.

(iv) Follows from the definition of additive inverse.
(v) Since $(a+b)+((-a)+(-b)) = [(a+b)+(-a)]+(-b) = [(-a)+(a+b)]+(-b) = [((-a)+a)+b]+(-b) = (0+b)+(-b) = 0+(b+(-b)) = 0+0 = 0$ then $(-a)+(-b)$ is the additive inverse of $a+b$. That is, $-(a+b) = (-a)+(-b)$.
(vi) Using (iii), we have $(-a)(-b) = -[a(-b)] = -[-(ab)] = ab$.
(vii) We prove that $a(b-c) = ab-ac$. The prove that $(a-b)c = ac-bc$ is similar.

$$\begin{aligned} a(b-c) &= a(b+(-c)) \\ &= ab + a(-c) \text{ by } Definition\ 24.1(8) \\ &= ab - ac \text{ by } (ii) \end{aligned}$$

(viii) Follows from (iii). ■

As we pointed out earlier in the section, the multiplicative operation in a ring does not necessarily have to satisfy either the commutative law or have an identity element. The following definition introduces the terminology used when multiplication is either commutative or has an identity element.

Definition 24.2
Let R be a ring such that $ab = ba$ for all $a, b \in R$. Then we call R a **commutative ring.** *If $e \in R$ is such that $ae = ea = a$ for all $a \in R$ then e is called a* **unity** *for the ring and the ring is called* **unitary ring.**

Example 24.4
1. $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are commutative rings with unity 1.
2. The ring of even integers is a commutative ring with no unity.
3. The ring of integers modulo n is a commutative ring with unity [1].
4. The ring $\mathcal{M}$ of 2×2 matrices is noncommutative with unity the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

When a unity in a ring exists then it must be unique.

Theorem 24.2
If R is a ring and e_1 and e_2 are unity elements then we must have $e_1 = e_2$.

Proof.
Since e_1 is a unity then $e_1 a = a$ for all $a \in R$. In particular, letting $a = e_2$ to obtain $e_1 e_2 = e_2$. Similarly, since e_2 is a unity then $ae_2 = a$ for all $a \in R$.

Letting $a = e_1$ to obtain $e_1e_2 = e_1$. Thus, $e_1 = e_2$.■

As in the case of a group, the existence of the unity element leads to the discussion of multiplicative inverses.

Definition 24.3
Let R be a ring with unity e. We say that x is a **multiplicative inverse** *of an element $a \in R$ if $ax = xa = e$.*

Multiplicative inverses are unique according to the following theorem.

Theorem 24.3
Let R be a ring with unity e. Let $a \in R$ and suppose that x and y are multiplicative inverses of a. Then $x = y$.

Proof.
Since x and y are multiplicative inverses of a then we have $ax = xa = e$ and $ay = ya = e$. Thus, $x = ex = (ya)x = y(ax) = ye = y$.■

Notation Let R be a ring with unity. If $a \in R$ has a multiplicative inverse then we will denote the inverse by a^{-1}.

Example 24.5
In a ring R, it is possible that some of the elements have multiplicative inverses whereas others don't. For example, in the ring $\mathbb{Z}_{10}$, [1] and [9] are their own multiplicative inverses, [3] and [7] are inverses of each other. The remaining elements of $\mathbb{Z}_{10}$ have no multiplicative inverses.

Review Problems

Exercise 24.1
Compute $[3] \odot ([4] \oplus [5])$ *in* $\mathbb{Z}_6$.

Exercise 24.2
Let $\mathcal{M}$ *be the collection of all 2 by 2 matrices with entry in* $\mathbb{R}$. *Show that* $(\mathcal{M}, +, \cdot)$ *is a non commutative ring, where addition and multiplication as defined in Exercises 3.15 and 3.16.*

Exercise 24.3
Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. *Show that* $\mathbb{Z}[\sqrt{2}]$ *with the usual addition and multiplication in* $\mathbb{Z}$ *is a commutative ring.*

Exercise 24.4
Let $\mathcal{M}(\mathbb{R})$ *be the collection of all mappings from* $\mathbb{R}$ *to* $\mathbb{R}$. *Define addition by* $(f + g)(x) = f(x) + g(x)$ *and multiplication by* $(fg)(x) = f(x)g(x)$. *Show that* $(\mathcal{M}(\mathbb{R}), +, \cdot)$ *is a commutative ring.*

Exercise 24.5
Let E *be the set of even integers. Prove that with the usual addition, and with the multiplication* $mn = \frac{1}{2}mn$, E *is a ring. Is there a unity?*

Exercise 24.6
Find the elements of $\mathbb{Z}_8$ *that have multiplicative inverses.*

Exercise 24.7
Let R *and* S *be two rings. Show that the Cartesian product* $R \times S$ *together with the operations*

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b)(c, d) &= (ac, bd) \end{aligned}$$

is a ring.

Exercise 24.8
The addition table and part of the multiplication table for the ring $R = \{a, b, c\}$ *are given below. Use the distributive laws to complete the multiplication table.*

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	c	
c	a		

Exercise 24.9
Let $(R, +)$ be an Abelian group. Define multiplication by $ab = 0$ for all $a, b \in R$. Show that $(R, +, \cdot)$ is a commutative ring.

Exercise 24.10
In the ring of integers, if $ab = ac$, with $a \neq 0$, then $b = c$. Is this true for all rings?

Exercise 24.11
Prove that in a ring R we have

$$(x + y)(z + t) = xz + xt + yz + yt$$

for all $x, y, z, t, \in R$.

Exercise 24.12
Let R be a ring in which $a^2 = a$ for all $a \in R$. Prove that R is commutative and that $a + a = 0$ for all $a \in R$. (Hint: Consider $(a + a)^2$ and $(a + b)^2$.)

Exercise 24.13
Prove that $(a + b)^2 = a^2 + 2ab + b^2$ for all a, b in a ring R if and only if R is commutative.

Exercise 24.14
Prove that if R is a commutative ring, $a, b \in R$, and $n \in \mathbb{N}$ then

$$(a+b)^n = a^n + \left(\begin{array}{c} n \\ 1 \end{array} \right) a^{n-1}b + \left(\begin{array}{c} n \\ 2 \end{array} \right) a^{n-2}b^2 + \cdots + \left(\begin{array}{c} n \\ n-1 \end{array} \right) ab^{n-1} + b^n$$

where

$$\left(\begin{array}{c} n \\ p \end{array} \right) = \frac{n!}{p!(n-p)!}$$

Exercise 24.15
An element a of a ring R is said to be **nilpotent** *if $a^n = 0$ for some positive integer n. Prove that if R is commutative and if a and b are nilpotent, then so is $a + b$.*

Exercise 24.16
Show that the set

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

with the usual matrix addition and multiplication is a ring.

Exercise 24.17
A (real) polynomial is a formal expression of the form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a)0,$$

where $a_0, \cdots, a_n \in \mathbb{R}$ and x is a variable. Polynomials can be added and multiplied as usual. With these operations, show that the set $\mathbb{R}[x]$ of all polynomials is a ring.

Exercise 24.18
Suppose that R is a ring in which all elements a satisfy $a^2 = a$.(Such a ring is called a **Boolean ring***.)*

(i) Prove that $a = -a$ for all $a \in R$.
(ii) Prove that R is commutative.

25 Integral Domains. Subrings

In Section 24 we defined the terms **unitary rings** and **commutative rings.** These terms together with the concept of **zero divisors** discussed below are used to define a special type of ring known as an **integral domain.**
Let R be a ring. Then, by Theorem 24.1(ii), we have $a0 = 0a = 0$ for all $a \in R$. This shows that if a product is zero then one of the factors is 0. The converse is not always true. For example, in $\mathbb{Z}_{10}$, [2] and [5] are nonzero elements with $[2] \odot [5] = [0]$. The following definition singles out those rings where a product of two (additive) nonidentity elements is the zero element.

Definition 25.1
Let R be a commutative ring. An element $a \in R, a \neq 0$ is called a **zero divisor** *in R if there exists an element $b \in R, b \neq 0$ such that $ab = 0$.*

Example 25.1
1. The ring of integers $\mathbb{Z}$ has no zero divisors.
2. The elements [2] and [5] are zero divisors in $\mathbb{Z}_{10}$.■

Remark 25.1
Definition 25.1 is restricted to elements in a commutative ring. It is possible to have noncommutative rings where $ab = 0$ but $ba \neq 0$. Indeed, the ring of all 2×2 matrices is noncommutative. Moreover, we have

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

The following definition shows that zero divisors can not exist in an integral domain.

Definition 25.2
A commutative ring with unity $e \neq 0$ and no zero divisors is called an **integral domain.**

Remark 25.2
The requirement $e \neq 0$ means that the ring has at least two elements, the zero element and the unity element.

Example 25.2
1. $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all integral domains.
2. The set E of evens integers is not an integral domain since it has no unity element.
3. $\mathbb{Z}_{10}$ is not an integral domain since [2] and [5] are zero divisors.
4. The ring $\mathcal{M}$ of all 2×2 matrices is not an integral domain for two reasons: first, the ring is noncommutative, and second, it has zero divisors. (See Remark 25.1■

Example 25.2(4), shows that $\mathbb{Z}_{10}$ is a commutative ring with unity but is not an integral domain since [2] and [5] are zero divisors. Note that $10 = 2 \times 5$. We can generalize this fact to any composite number n. So if $n = rs$ where $r, s > 1$, then $[r] \odot [s] = [rs] = [n] = [0]$ so that $[r]$ and $[s]$ are zero divisors of $\mathbb{Z}_n$. That is, $\mathbb{Z}_n$ is not an integral domain.
The next result provides a condition on n so that $\mathbb{Z}_n$ is an integral domain.

Theorem 25.1
For $n > 1$, $\mathbb{Z}_n$ has no zero divisors if and only if n is prime.

Proof.
Suppose first that n is prime. Let $[a] \odot [b] = [0]$ in $\mathbb{Z}_n$ with $[a] \neq [0]$. We will show that $[b] = [0]$ in $\mathbb{Z}_n$. Since $[a] \odot [b] = [0]$ then $[ab] = [0]$ and this implies that $n|ab$. Since $[a] \neq [0]$ then $n \not| a$. Since n is prime then by Lemma 13.3, we must have $n|b$. That is, $[b] = [0]$. Therefore, $\mathbb{Z}_n$ has no zero divisors, and is an integral domain.
Conversely, suppose that $\mathbb{Z}_n$ is an integral domain. Assume that n is not prime. As pointed out in the discussion preceding the theorem, $\mathbb{Z}_n$ is not an integral domain, a contradiction. Hence, n must be prime.■

An important consequence of the absence of zeros in an integral domain is that the cancellation law for multiplication must hold.

Theorem 25.2
If a, b, and c are elements in integral domain D such that $a \neq 0$ and $ab = ac$, then $b = c$.

Proof.
Since $ab = ac$ then $a(b-c) = 0$ with $a \neq 0$ in D. But D is an integral domain so we must have $b - c = 0$ or $b = c$.■

The converse of the previous theorem is also true.

Theorem 25.3
If D is a commutative ring with unity $e \neq 0$ such that the cancellation property holds then D is an integral domain.

Proof.
Suppose that for all $a, b, c \in D, ab = ac$ and $a \neq 0$ implies $b = c$. We will show that D has no zero divisors. Let $a, b \in D$ be such that $ab = 0$ with $a \neq 0$. Since $a0 = 0$ then $ab = a0$. By the cancellation law, $b = 0$. This shows that D has no zero divisors, so D is an integral domain.■

The notion of subring is the abvious analogue of the notion of subgroup.

Definition 25.3
A subring of a ring R is any subset $S \subseteq R$ which forms a ring with respect to the operation of R.

Example 25.3
The set E of even integers is a subring of all integers. The set of integers is a subring of the ring of rational numbers. The set of rational numbers is a subring of the ring of all real numbers. The set of all real numbers is a subring of the ring of complex numbers.■

As in groups, we can reduce the number of axioms one has to check when proving that something is a subring.

Theorem 25.4
Let R be a ring and S a subset of R. Then S is a subring of R if and only if

(i) $S \neq \emptyset$;
(ii) For all $a, b \in S$ we have $a - b \in S$ and $ab \in S$.

Proof.
Suppose first that S is a subring of R. Then S being a ring itself, it must contain the zero element of R. Thus, $S \neq \emptyset$. Now, let $a, b \in S$. Since S is a ring then $(S, +)$ is a group so that $a - b \in S$. Also, S is closed with respect to multiplication so that $ab \in S$.

Conversely, suppose that S is a subset of R satisfying conditions (i) and (ii). Since S is nonempty and $a - b \in S$ for all $a, b \in S$ then by Theorem 7.5, $(S, +)$ is a group. By (ii), S is closed with respect to multiplication. Since multiplication is associative in R and S is closed then multiplication is associative when restricted to S. Thus, S is a ring and hence a subring of R.■

Example 25.4
Consdier the subset of the ring $\mathcal{M}$ of all 2×2 matrices:

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

We will show that S is a subring of $\mathcal{M}$. Since the zero matrix is in S then $S \neq \emptyset$. Since

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix} \in S$$

and

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in S$$

then by Theorem 25.4, S is a subring of $\mathcal{M}$.■

Review Problems

Exercise 25.1
Find the zero divisors of $\mathbb{Z}_6$.

Exercise 25.2
Verify that $([2],[0])$ *is a zero divisor in* $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Exercise 25.3
Which elements of $\mathbb{Z} \times \mathbb{Z}$ *are zero divisors?*

Exercise 25.4
Prove that if an element a *in a ring* R *has a multiplicative inverse in* R*, then* a *is not a zero divisor in* R.

Exercise 25.5
Show that a zero divisor can not have a multiplicative inverse.

Exercise 25.6
Let R *be a commutative ring with unity* e*. Let* $a \in R$ *be such that* $a^n = 0$ *for some* $n \in \mathbb{N}$*. Prove that* a *is either 0 or a zero divisor.*

Exercise 25.7
Let D *be an integral domain. Show that if* $a \in D$ *such that* $a^2 = a$ *and* $a \neq e$ *then* a *is a zero divisor.*

Exercise 25.8
Let R *be a commutative ring. For each* $a \in R$ *let* $H_a = \{x \in R : ax = 0\}$*. Show that for all* $x, y \in H_a$*, we have* $xy \in H_a$.

Exercise 25.9
Show that $\mathbb{Z}[\sqrt{2}]$ *(Exercise 24.3) is an integral domain.*

Exercise 25.10
Show that the ring $\mathcal{M}(\mathbb{R})$ *of all mappings from* $\mathbb{R}$ *to* $\mathbb{R}$ *is not an integral domain.(See Exercise 24.4.)*

Exercise 25.11
State and prove a theorem giving a necessary and sufficient condition for a subset of an integral domain to be an integral domain.

Exercise 25.12
Prove that if D is an integral domain and $a^2 = e$ then $a = \pm e$.

Exercise 25.13
Let R and S be integral domains. Prove that $R \times S$ is also an integral domain.

Exercise 25.14
Let R be a ring with unity e. Let S be the collection of all elements in R with multiplicative inverse. Prove that $(S, \cdot)$ is a group.

Exercise 25.15
Let R be a commutative ring with unity e such that every nonzero element of R has a multiplicative inverse. Show that R is an integral domain.

Exercise 25.16
Let $C(\mathbb{R})$ denote the collection of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that $C(\mathbb{R})$ is a subring of $\mathcal{M}(\mathbb{R})$.

Exercise 25.17
Prove that $\{(a, a) : a \in R\}$ is a subring of $R \times R$.

Exercise 25.18
Let R be a ring with identity e and S a subring of R such that $e \in S$. Prove that if u is a unit in S then u is a unit in R. Show by an example that the converse is false.

Exercise 25.19
The **center** *of a ring R is defined to be $\{c \in R : cr = rc \; \forall r \in R\}$. Prove that the center of a ring is a subring. What is the center ofa commutative ring?*

Exercise 25.20
Let $\mathcal{C}$ be the collection of all subrings of a ring R. Prove that $\cap_{H \in \mathcal{C}} H$ is a subring of R.

Exercise 25.21
Show that the set

$$S = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \right\}$$

is not a subring of the ring $\mathcal{M}$ of all 2×2 matrices.

26 Ideals and Quotient Rings

In this section we develop some theory of rings that parallels the theory of groups discussed in ealrier sections of the book. We shall see that the concept of an **ideal** in a ring is analogous to that of a normal subgroup in a group. Using ideals we will construct quotient rings.

Definition 26.1
A subring I of a ring R is an **ideal** *if whenever $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$.*

Example 26.1
1. The subrings $I = \{0\}$ and $I = R$ are always ideals of a ring R.
2. The set E of even integers is an ideal of $\mathbb{Z}$.
3. The set $I = \{[0], [2], [4]\}$ is an ideal of $\mathbb{Z}_6$.■

Remark 26.1
Note that if R is a ring with unity element e and I is an ideal of R then from the above definition, for any $r \in R$ we have $re = er = r \in I$. That is, $R = I$.

Example 26.1(1) can be generalized to the set of all multiples of any fixed integer n as shown in the next lemma.

Lemma 26.1
Let R be a commutative ring with unity element e. The set

$$(a) = \{ar : r \in R\}$$

is an ideal of R.

Proof.
First, we will show that (a) is a subring of R. Since $a = ae$ then $a \in (a)$ and so $(a) \neq \emptyset$. Let $ax \in (a)$ and $ay \in (a)$. Then $ax - ay = a(x - y) \in (a)$ since $x - y \in R$. Thus, $ax - ay \in (a)$. Also, $(ax)(ay) = a(xy) \in (a)$ since $xy \in R$. Thus, by Theorem 25.4, (a) is a subring of R. Finally, for any $ar \in (a)$ and all $t \in R$ we have $t(ar) = t(ra) = (tr)a \in (a)$ and $(ar)t = a(rt) = (rt)a \in (a)$. Thus, (a) is an ideal of R.

Definition 26.2
Let R be a commutative ring with unity and $a \in R$. Then the ideal (a) is called the **principal ideal** *generated by a in R.*

Theorem 26.1
Every ideal in the ring $\mathbb{Z}$ is a principal ideal.

Proof.
Let I be an ideal in R. If $I = \{0\}$ then there is nothing to prove since $\{-\} = (0)$. So assume that $I \neq \{0\}$. Since $I \neq \{0\}$ then there exists an $m \in I$ such that $m \neq 0$. Since I is an ideal and $-1 \in \mathbb{Z}$ then $-m \in I$. Thus, both m and $-m$ belong to I so that I contains positive integers. Let $M = \{m \in I : m > 0\}$. By Theorem 10.1, M contains a smallest element, call it n.
Now, for any $k \in I$, by the Division algorithm there exist integers q and r such that

$$k = nq + r \quad 0 \leq r < n.$$

Thus, $r = k - nq$. Since I is a subring of R then by closure $r \in I$. By the definition of n we must have $r = 0$. This implies that $k = nq$ and so $I \subseteq (n)$. Since $(n) \subseteq I$ then we conclcude that $I = (n)$. This establsihes a proof of the theorem.■

In analogy to congruence in $\mathbb{Z}$ and $\mathbb{Z}_n = \mathbb{Z}/ < n >$ we now will build a ring R/I for any ideal I in any ring R. For $a, b \in R$, we say a is *congruent to b modulo I* [and write $a \equiv b(mod\ I)$] if and only if $a - b \in I$. Note that when $I = (n) \subseteq \mathbb{Z}$ is the principal ideal generated by n, then $a-b \in I \iff n|(a-b)$, so this is our old notion of congruence.

Theorem 26.2
Let I be an ideal of a ring R. Then congruence modulo I is an equivalence relation on R. For any $a \in R$ we have

$$[a] = \{r \in R : a \equiv r(mod\ I)\} = \{a + i : i \in I\}.$$

Proof.
Reflexive: $a - a = 0 \in I$ since I is a subring.
Symmetric: Assume that $a \equiv b(mod\ I)$. Then $a - b \in I$. Since I is a subring, its additive inverse, $b - a$ is also in I, so $b \equiv a(mod\ I)$.
Transitive: Assume $a \equiv b(mod\ I)$ and $b \equiv c(mod\ I)$. Then $a - b \in I$ and $b-c \in I$. Hence, by closure, $a-c = (a-b)+(b-c) \in I$. That is, $a \equiv c(mod\ I)$.
Now, for any $a \in R$, the equivalence class of a is the set

$$[a] = \{r \in R : a \equiv r(mod\ I)\}.$$

But $a \equiv r(mod\ I)$ if and only if $a - r \in I$ and this is equivalent to saying that $a - r = i \in I$. That is,

$$[a] = \{a + i : i \in I\}.\blacksquare$$

We denote the equivalence class of $a \in R$ by $a + I$.

Remark 26.2
Note that by Theorem 9.2, $a \equiv b(mod\ I) \iff a - b \in I \iff a + I = b + I$.

Next, consider the set R/I of all cosets $a + I$ where $a \in R$. On this set, we define addition as follows:

$$(a + I) + (b + I) = (a + b) + I.$$

Theorem 26.3
The set R/I is an Abelian group with respect to addition.

Proof.
First, we show that addition is well-defined. Suppose that $(a + I, b + I) = (c+I, d+I)$. Then $a+I = c+I$ and $b+I = d+I$. Thus, $a-c \in I$ and $b-d \in I$. By the closure of addition in I we have $(a-c)+(b-d) = (a+b)-(c+d) \in I$. Hence, $(a + b) + I = (c + d) + I$.
Addition is commutative since $(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+I)+(a+I)$ since addition is R is commutative. Similarly, since addition in R is associative then addition is R/I is associative. The coset I is the zero element and the additive inverse of $a + I$ is $(-a) + I$. Hence, $(R/I, +)$ is an Abelian group.$\blacksquare$

In order to turn R/I into a ring we need to introduce a multiplication on R/I. For $a + I \in R/I$ and $b + I \in R/I$ we define

$$(a + I)(b + I) = ab + I.$$

Theorem 26.4
(a) R/I is closed with respect to multiplication.
(b) Multiplication is associative.
(c) Multiplication is distributive with respect to addition.

Proof.
(a) Suppose that $(a+I, b+I) = (c+I, d+I)$. Then $a+I = c+I$ and $b+I = d+I$. Thus, $a-c \in I$ and $b-d \in I$. It follows that $a = c+x$ and $b = d+y$ for some $x, y \in I$. Thus, $ab = (c+x)(d+y) = cd+cy+dx+xy$. Since I is an ideal then $cy, dx, xy \in I$. By the closure of addition in I we have $w = cy+dx+xy \in I$. Hence, $ab = cd+w$ with $w \in I$ and this means that $ab-cd \in I$ so that $ab \equiv cd(mod\ I)$ and consequently $ab+I = cd+I$.
(b)Multiplication is associative.

$$\begin{aligned}
(a+I)[(b+I)(c+I)] &= (a+I)(bc+I) \\
&= a(bc)+I \\
&= (ab)c+I \qquad (\textit{since multiplication is associative in } R) \\
&= (ab+I)(c+I) \\
&= [(a+I)(b+I)](c+I)
\end{aligned}$$

(c) We will verify the left distributive law. The proof of the right distributive law is similar.

$$\begin{aligned}
(a+I)[(b+I)+(c+I)] &= (a+I)(b+c+I) \\
&= a(b+c)+I \\
&= ab+ac+I \qquad (\textit{by the distributive law in } R) \\
&= (ab+I)(ac+I) \\
&= (a+I)(b+I)+(a+I)(c+I)\blacksquare
\end{aligned}$$

It follows from Theorem 26.4 and Theorem 26.3 that R/I is a ring.

Definition 26.3
If I is an ideal of a ring R then with the operations of addition and multiplication defined above, R/I is a ring called the **quotient ring** *of R by I.*

Review Problems

Exercise 26.1
Consider the ring

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

Show that the set

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

is an ideal of R.

Exercise 26.2
Prove that $x\mathbb{R}[x]$ is an ideal of $\mathbb{R}[x]$.

Exercise 26.3
Show that the set $I_r = \{f \in \mathcal{M}(\mathbb{R}) : f(r) = 0\}$, where $r \in \mathbb{R}$ is fixed, is an ideal of $\mathcal{M}(\mathbb{R})$. Can we replace the 0 by any number and still get an ideal?

Exercise 26.4
Show that the set

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

is not an ideal of the ring of all 2×2 matrices.

Exercise 26.5
Let R be a commutative ring with unity element e. Let $c_1, c_2, \cdots, c_n \in R$. Show that the set $I = \{r_1c_1 + r_2c_2 + \cdots + r_nc_n : r_1, r_2, \cdots, r_n \in R\}$ is an ideal of R.

Exercise 26.6
Let I be an ideal of a ring R. Prove that if $a \equiv b (mod\ I)$ and $c \equiv d (mod\ I)$ then $a + c \equiv b + d (mod\ I)$ and $ac \equiv bd (mod\ I)$.

Exercise 26.7
Prove that every subring of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 26.8
Prove that if R is a commutative ring with unity, and $a \in R$, then (a) is the smallest ideal of R containing a.

Exercise 26.9
Let m and n be nonzero integers. Prove that $(m) \subseteq (n)$ if and only if $n|m$.

Exercise 26.10
An element a in a commutative ring is said to be **nilpotent** *if $a^n = 0$ for some positive integer n. Prove that the set of all nilpotent elements in a commutative ring R is an ideal of R.*

Exercise 26.11
Prove that a nonempty susbet I ofa ring R is an ideal of R if and only if I satisfies:

(i) if $a, b \in I$ then $a - b \in I$;
(ii) if $r \in R$ and $a \in I$ then $ar \in I$ and $ra \in I$.

Exercise 26.12
Let R be a commutatvie ring with unity and I an ideal of R. Prove that the set of all $a \in I$ such that $a^n \in I$ for some $n \in \mathbb{N}$ is an ideal of R.

Exercise 26.13
Prove that an arbitrary intersection of ideals of a ring R is an ideal of R.

Exercise 26.14
Find two ideals I_1 and I_2 of the ring $\mathbb{Z}$ such that $I_1 \cup I_2$ is not an ideal.

Exercise 26.15
An ideal P of a commutative ring R is called **prime** *ideal if $P \neq R$ and if $a, b \in R$ then either $a \in P$ or $b \in P$. Prove that if n is a positive integer then (n) is a prime ideal of $\mathbb{Z}$ if and only if n is prime.*

Exercise 26.16
Prove that if I is an ideal of a ring R then R/I is commutative if and only if $ab - ba \in I$ for all $a, b \in R$.

Exercise 26.17
Prove that if R is commutative and I is an ideal of R then R/I is commutative.

Exercise 26.18
Prove that if R has unity e, then $I + e$ is a unity for R/I.

Exercise 26.19
Assume that R is a commutative ring with unity and $P \neq R$ is an ideal of R. Prove that R is a prime ideal if and only if R/I is an integral domain.

Exercise 26.20
Prove that if I is a subring of a ring R, and the operations of addition and multiplication on the collection of all right cosets R/I are well-defined then I is an ideal of R.