Bana Al Subaiei
Muneerah Al Nuwairan

A Gentle Introduction to Group Theory

Springer

A Gentle Introduction to Group Theory

Bana Al Subaiei · Muneerah Al Nuwairan

A Gentle Introduction to Group Theory

Springer

Bana Al Subaiei
Department of Mathematics and Statistics
College of Science
King Faisal University
Al-Ahsa, Saudi Arabia

Muneerah Al Nuwairan
Department of Mathematics and Statistics
College of Science
King Faisal University
Al-Ahsa, Saudi Arabia

ISBN 978-981-99-0146-3 ISBN 978-981-99-0147-0 (eBook)
https://doi.org/10.1007/978-981-99-0147-0

Mathematics Subject Classification: 20-xx, 20-01, 20A05, 20B99, 20D99, 20K01, 20M10

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Young man, in mathematics you don't
understand things, you just get used to them.[1]
John von Neumann

[1] Gary Zukav: "The Dancing Wu Li Masters. An Overview of the New Physics".

To our husbands and children

Preface

Group theory has been studied since the late eighteenth century and continues to gain importance due to its widespread applications in the fields of physics, chemistry, geometry, and mathematics. This book aims to serve as an introductory course in group theory, directed toward second-year university students. The main goal of the book is to provide students with adequate knowledge to continue studying advanced courses in algebra. This book reflects the authors' many years of experience in teaching mathematics, making it a rich source of purposive examples and exercises for other lecturers to utilize.

The text can be broadly divided into three parts. The first part includes the initial three chapters, establishes the prerequisites needed to study group theory, covering topics in set theory, geometry, and number theory. Each of the three chapters ends with solved and unsolved exercises relating to the topic. In this part, the authors hope to rectify any gap in the reader's background.

The course on group theory consist of Chaps. 4–9. First, binary operations and semigroups are described in Chap. 4, along with some relevant notions. Chapter 5 contains the core of our study, "the groups". This chapter provides many examples and studies of the main characteristics of groups. Chapter 6 presents an important example of a finite group, which contains copies of all finite groups. Chapter 7 describes the notion of subgroups. As the longest and richest chapter of the book, this chapter covers two important theorems: Lagrange and Cauchy theorems. In Chap. 8, the authors considered the concepts of group homomorphisms, and their bijective versions, group isomorphisms. The notion of isomorphic groups and the three fundamental theorems of homomorphisms are described in Chap. 8. The course on group theory ends with Chap. 9, which describes the classification of finite abelian groups. Chapter 9 begins by studying cyclic groups, then primary groups, which are not necessarily abelian but play an important role in proving the fundamental theorem of finite abelian groups. As in the first three chapters, each chapter in this part of the book is supplemented by many solved and unsolved exercises.

The last part of the book introduces Sage, a mathematical software that is used to solve group theory problems. In Chap. 10, the authors explain some of the important commands in Sage and provide many examples and exercises. The authors hope that the book will be a beneficial contribution to the field.

The authors acknowledge the Deanship of Scientific Research at King Faisal University in Al-Ahsa for the financial support for the authorship of the book (Grant No. 184006/GRANT75).

Al-Ahsa, Saudi Arabia

Bana Al Subaiei
Muneerah Al Nuwairan

Contents

About the Authors

Bana Al Subaiei is Associate Professor at the Department of Mathematics and Statistics, King Faisal University, Saudi Arabia. She earned her Master and Ph.D. degrees from the University of Southampton, United Kingdom. Al Subaiei has more than 10 years of experience in higher education during which she served in many committees at department, college and university levels. Her research interest includes group theory, semigroup theory, ring theory and graph theory. She has published research appears in several academic journals.

Muneerah Al Nuwairan is an Associate Professor at the Department of Mathematics and Statistics, King Faisal University, Saudi Arabia. She obtained her Master's degree from King Faisal University, and then a Ph.D. degree in mathematics from the University of Ottawa, Canada. Al Nuwairan is an active researcher in applied mathematics, where one of her main research interests is group theory.

Symbols and Acronyms

$\mathbb{N}$	The set of natural numbers (positive integers)
$\mathbb{Z}$	The set of integers
$\mathbb{Q}$	The set rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$\mathcal{P}(A)$	The set power of A
$\emptyset$	The empty set
$\lvert A\rvert$	The cardinally of the set A
A^c	The compliment of A
$A\backslash B$	The difference of A and B
$A \vartriangle B$	The symmetric difference of A and B
$A \times B$	The Cartesian Product of A and B
$D(\mathcal{R})$	The domain of a relation $\mathcal{R}$
$Rang(\mathcal{R})$	The rang of a relation $\mathcal{R}$
$[a]_{\mathcal{R}}$, $[a]$	The equivalence classes of a
f^{-1}	The inverse of the function f
$f \circ g$	The composition of two function f and g
$\mathcal{R}_{s,t}$	The transposition map that exchanging s and t
I_A	The identity map on A
$\mathcal{M}_{mn}(K)$	The set of all $m \times n$ matrices with entries in K
$\mathcal{M}_n(K)$	The set of all of square matrices of dimension n over K
$\cong_n$	The equivalence relation modulo n
$U(K)$	The set of all upper triangle matrices over K
$L(K)$	The set of all lower triangle matrices over K
$\otimes_n$	The multiplication modulo n on $\mathbb{Z}_n$
A^A	The set of all functions on A
$\bar{a}$	The complex conjugate of a, $a \in \mathbb{C}$
A^T	The transpose of a matrix A
A^*	The Hermitian conjugate of a matrix A
$trace(A)$	The trace of a matrix A
I_n	The identity matrix of $\mathcal{M}_n(K)$

$\det(A)$	The determinant of a matrix A
$O(n)$	The orthogonal group of order n
$\mathcal{U}(n)$	The subset of all unitary matrices of $\mathcal{M}_n(K)$
$GL_n(K)$	General linear group
$SL_n(K)$	Special linear group
$Adj(A)$	The adjugate matrix of A
A^{-1}	The inverse matrix of A
R_θ	The rotation around the origin with angle θ
l_θ	The reflection around a line passes the origin and makes angle θ with x-axis
$\vert a \vert$	The absolute value of a
$\text{Div}(a)$	The set of divisors of a
$\text{Mult}(a)$	The set of multiples of a
$D(a, b)$	The set of all common divisors of a and b
$\gcd(a, b)$	The greatest common divisor of a and b
$M(a, b)$	The set of all common multiples of a and b
$\text{lcm}(a, b)$	The least common multiple of a and b
$\mathcal{O}r_\phi(i)$	The orbit of i under ϕ
$\mathbb{Z}_n$	The integers modulo n
$\oplus_n$	The addition modulo n on $\mathbb{Z}_n$
$\mathcal{B}_n$	The set of odd permutations in $\mathfrak{S}_n$
$\text{sgn}(\phi)$	The sign of permutation ϕ
e_l	The left identity
e_r	The right identity
e	The identity
a^{-1}	The inverse of a
$\text{Inv}(G)$	The set of all invertible elements G
K^*	The subset $K\backslash\{0\}$
$E(G)$	The set of idempotent elements of G
D_{2n}	*Dihedral group*, The set of all symmetries of the regular n-polygon
$\mathfrak{S}_A$	The symmetric group of A
$\mathfrak{S}_n$	The nth symmetric group
$\text{Inv}(\mathbb{Z}_n)$	The invertible elements in $(\mathbb{Z}_n, \otimes_n)$
$\varphi(n)$	The Euler number
$C(G)$	The center of a group G
$ord(a)$	The order of a
mG	The set of elements a^m where $a \in G$
$G[m]$	The set of elements which contains a satisfies $a^m = e$
$\text{Exp}(G)$	The exponent of G
$Move(\phi)$	The subset of all elements that are moved by a permutation ϕ
$\phi_{\vert A}$	The restriction of ϕ on A
$\mathcal{A}_n$	The set of even permutations in $\mathfrak{S}_n$, the Alternating group of degree n
$H < G$	H is a subgroup of G
$H(n)$	The group of the nth roots of unity

T	The torsion subgroup of G, The set of elements which have finite order in G
$Lm(G)$	The set of all left multiplication on a group G
$\langle S\rangle$	The subgroup of G generated by S
$\langle a\rangle$	The subgroup of G generated by a
aH	The left coset of H
Ha	The right coset of H
G/H	The quotient of a group G by H
$[G:H]$	The index of H
$H \trianglelefteq G$	H is a normal subgroup of G
$Hom(G_1,\ G_2)$	The set of all group homomorphisms from G_1 to G_2
$Aut(G)$	The set of all group automorphisms on G
$Im(f)$	The image of f
$ker(f)$	The kernel of f
ϕ_a	The inner automorphism
$Inn(G)$	The set of all inner automorphism on G

List of Figures

List of Tables

Chapter 1
Background Results in Set Theory

This chapter summarizes the basic mathematical information required for studying this book, including definitions and results regarding operations on sets, functions, and matrices. The first section discusses operations on sets such as unions, intersections and differences. Moreover, the properties and fundamental results of these operations are presented. Section 1.2 describes the principle of mathematical induction. Section 1.3 is devoted to binary relations on sets and their properties while Sect. 1.4 classifies binary relations into different types. Equivalence and ordered relations are also discussed. The concept of a function, which is a special and important type of binary relations, is defined and examined in Sect. 1.5. Section 1.6 describes matrices and their operations. The last section contains results regarding the symmetries of the regular n-polygon.

1.1 Operations on Sets

Set theory is considered the foundation of most branches of mathematics. Abstract algebra, for example, focused on sets that are closed under one or more operations. This section discusses the basic operations on sets such as unions, intersections, and symmetric differences. The essential results related to these operations are presented. The reader may refer to (Printer, 2014) and (Halmos, 2013) for proofs of these results.

Definition 1.1.1 A set is any collection of distinct objects, which are called elements of the set.

Sets are denoted by uppercase letters such as A, B, C, ..., while lowercase letters such as x, y, a, b, c, ... are usually used to denote the elements. The notation $a \in A$ (read a belongs to A, or a in A) is used to express that a is an element of A. If a is not an element of A, the notation $a \notin A$ is used. The symbol $\emptyset$ denotes the empty set $\{\}$, which has no elements. The universal set that contains all the elements under consideration is denoted by U. A set can be described by two methods: One

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_1

method is to list (if possible) all the elements of the set between two curly braces {}, this method is known as the roster method. To describe an infinite set in roster notation, some dots are placed at the end of the list, or at both ends, to indicate that the list continues forever. The other method, the descriptive method, involves stating a common characteristic of all elements of the set. The type of elements of a given set determines the method that is more appropriate. A set is called finite if it has a finite number of elements; otherwise, the set is called infinite. Figure 1.1 lists the most important infinite sets.

Example 1.1.2

1. The rainbow color set is a finite set that can be expressed by listing all its elements as {red, orange, yellow, green, blue, indigo, violet}.
2. The set of positive integers, denoted by $\mathbb{N}$, is an infinite set described using the roster method as $\{1, 2, 3, 4, 5, \ldots, \ldots\}$.
3. The finite set {2, 4, 6, 8} can be expressed using the descriptive method as

$$\{x \in \mathbb{N} : x \text{ is even } \wedge 1 \leq x \leq 8\}$$

4. The set {7, 8, 9, 10} can be expressed sing the descriptive method as

$$\{x \in \mathbb{N} : 7 \leq x \leq 10\}$$

5. The infinite set of all integers $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is denoted by $\mathbb{Z}$, which can be described as

$$\{x : x \in \mathbb{N} \vee x = 0 \vee x = -y, y \in \mathbb{N}\}$$

6. The set of rational numbers, denoted by $\mathbb{Q}$, is expressed as

$$\{m/n : m, n \in \mathbb{Z} \wedge n \neq 0\}.$$

7. The set of all real numbers, denoted by $\mathbb{R}$, consisting of rational and irrational numbers, cannot be easily described using the abovementioned methods.
8. The set of complex numbers, denoted by $\mathbb{C}$, is formed using real numbers and described as

$$\left\{a + ib : a, b \in \mathbb{R}, i^2 = -1\right\}$$

9. Several sets are difficult or impossible to list using the roster method. These sets can be expressed using only the descriptive method. For example,

   a. The set of second-year students at King Faisal University (KFU) can be expressed as

$$\{x \in S\text{KFU} : x \text{ is a student in the second year}\}$$

Fig. 1.1 Sets of numbers

$\mathbb{N}$ = The positive integers.

$\mathbb{Z}$= The integers.

$\mathbb{Q}$= The rational numbers.

$\mathbb{Q}^c$= The irrational numbers.

$\mathbb{R}$= The reals.

$\mathbb{C}$= The complex numbers.

where SKFU denotes all the students in King Faisal university.

b. The set of integers that are greater than 100 can be described as

$$\{x \in \mathbb{Z} : x > 100\}$$

c. The set of real numbers that lie between 0 and 1 can be described as

$$\{x \in \mathbb{R} : 0 < x < 1\}$$

In Fig 1.1, the main sets of numbers are listed.

Definition 1.1.3 Let A be any set. The cardinality of A, denoted by $|A|$, is defined as the number of its elements if A is finite. If A is an infinite set, the cardinality of A is said to be infinite.

Definition 1.1.4 Let A and B be two sets. The set A is a subset of B, denoted by $A \subseteq B$, if each element in A belongs to B, i.e., $A \subseteq B \Leftrightarrow (x \in A \Leftrightarrow x \in B)$. The sets A and B are said to be equal, denoted by $A = B$, if $A \subseteq B$ and $B \subseteq A$. The set of all subsets of a given set A is called the power set of A and is denoted by $\mathcal{P}(A)$.

Example 1.1.5

1. The empty set $\emptyset$ is a subset of any set, and any set is a subset of itself.
2. The sets $\{1, 2\}$, $\{1, 3\}$ and $\{3\}$ are subsets of $\{1, 2, 3\}$.
3. The set of positive integers $\mathbb{N}$, is a subset of $\mathbb{Z}$. As $\mathbb{Z} = \{m/1 : m \in \mathbb{Z}\}$, the set $\mathbb{Z}$ can be considered as a subset of the rational numbers $\mathbb{Q}$. Generally,

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

4. The set of all negative integers $-\mathbb{N}$ is a subset of $\mathbb{Z}$.
5. The set $\{-2, 0, 2\}$ is a subset of $\mathbb{Z}$ but not a subset of $\mathbb{N}$.
6. For any set A, the power set of A is never empty as $\emptyset \subseteq A$ and $A \subseteq A$ for any A.

7. $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}, \mathcal{P}(\emptyset) = \{\emptyset\}$.
8. $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
9. $\mathcal{P}(\mathbb{Z})$ is an infinite set.
10. The sets $A = \{x \in \mathbb{Z} : |x| = 1\}$ and $B = \left\{x \in \mathbb{R} : x^2 - 1 = 0\right\}$ are equal. The integer solutions of $|x| = 1$ and the real solution of $x^2 - 1 = 0$ are the same, both sets are equal to $\{1, -1\}$.
11. The sets $A = \left\{x \in \mathbb{Q} : x^3 = x\right\}$ and $B = \left\{x \in \mathbb{R} : x^2 = x\right\}$ are not equal. The set A is the rational solutions of the equation $x^3 = x$, specifically, $A = \{-1, 0, 1\}$, while B is the real solutions of the equation $x^2 = x$, which are 0 and 1.
12. The sets $A = \left\{x \in \mathbb{R} : x^2 + 1 = 0\right\}$ and $B = \left\{x \in \mathbb{C} : x^2 + 1 = 0\right\}$ are not equal. The set A is the empty set $\emptyset$, while B equals to $\{i, -i\}$.

In the above examples, we saw that

- The power set of $\emptyset$ has only one element, i.e., $|\mathcal{P}(\emptyset)| = 1 = 2^0$.
- The power set of $\{1, 2, 3\}$ has eight elements, i.e., $|\mathcal{P}(\{1, 2, 3\})| = 8 = 2^3$.
- If A has six elements, $|\mathcal{P}(A)| = 64 = 2^6$.

In general, the following proposition holds, the proof of which is presented in Exercise 1.5.

Proposition 1.1.6 *Let A be a finite set. The power set of A is a finite set whose cardinality equals* $2^{|A|}$.

Definition 1.1.7 Let be any set. The compliment of A, denoted by A^c, is defined as the set of all elements in the universal set U that are not in A, i.e., $A^c = \{x \in U : x \notin A\}$.

Definition 1.1.8 Let A and B be any two sets.

1. The union of A and B, denoted by $A \cup B$, is the set of elements that are either in A, in B, or both, i.e., $A \cup B = \{x : x \in A \vee x \in B\}$.
2. The intersection of A and B, denoted by $A \cap B$, is the set of elements that are in both A and B, i.e., $A \cap B = \{x : x \in A \wedge x \in B\}$.

   – If $A \cap B = \emptyset$, we say that A and B are disjoint sets. The sets $A_1, A_2, \ldots, A_n$ are called mutually disjoint if $A_i \cap A_j = \emptyset$ for each $i \neq j$.

3. The difference of A and B, denoted by $A \backslash B$ or $A - B$, is the set of elements that are in A but not in B, i.e., $A \backslash B = \{x : x \in A \wedge x \notin B\}$.
4. The symmetric difference (disjunctive union) of A and B, denoted by $A \Delta B$, is the set of elements in either A or B but not in their intersection, i.e., $A \Delta B = (A \backslash B) \cup (B \backslash A)$.

Example 1.1.9

1. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{5, 6, 7, 8\}$.

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\}, \;\; A \cap B = \{5, 6\}$$
$$A \backslash B = \{1, 2, 3, 4\}, \;\; B \backslash A = \{7, 8\},$$
$$\mathrm{A \Delta B} = \{1, 2, 3, 4, 7, 8\}.$$

Clearly, the sets A and B are not disjoint. Note that $A\backslash B$ and $B\backslash A$ are different sets.

2. The set of positive integers $\mathbb{N}$, and the set of negative integers $-\mathbb{N}$ are examples of disjoint sets.

Proposition 1.1.10 *Let* A, B, and C *be any sets.*

1. $A \subseteq A \cup B$, $B \subseteq A \cup B$, $A \cap B \subseteq A$, and $A \cap B \subseteq B$.
2. $A \cup (B\backslash A) = A \cup B$, and $A \cap (B\backslash A) = \emptyset$.
3. If $A \subseteq B$, then $A \cup B = B$ and $A \cap B = A$.
4. If $A \subseteq B$ and $C \subseteq D$, then $A \cup C \subseteq B \cup D$, and $A \cap C \subseteq B \cap D$.
5. $A\backslash B = A \cap B^c$.
6. $A \subseteq B$ if and only if $B^c \subseteq A^c$.

Proposition 1.1.11 *Let* A, B, *and* C *be sets, and* U *be the universal set. The following identities hold.*

1. Complementation Law:$(A^c)^c = A$.
2. Idempotent Laws: $A \cup A = A$, and $A \cap A = A$.
3. Identity Laws: $A \cup \emptyset = A$, and $A \cap U = A$.
4. Domination Laws: $A \cup U = U$, and $A \cap \emptyset = \emptyset$.
5. $A\backslash\emptyset = A$, and $A\backslash A = \emptyset$.
6. $A \triangle A = \emptyset$, $A \cap A^c = \emptyset$, and $A \cup A^c = U$.
7. Commutative Laws: $A \cup B = B \cup A$, $A \cap B = B \cap A$ and $A \Delta B = B \Delta A$
8. Associative Laws:

$$A \cup (B \cup C) = (A \cup B) \cup C,$$
$$A \cap (B \cap C) = (A \cap B) \cap C,$$
$$(A \Delta B) \Delta C = A \Delta (B \Delta C).$$

9. Distributive Laws:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

10. De Morgan's Laws:

$$(A \cup B)^c = A^c \cap B^c, \;\; (A \cap B)^c = A^c \cup B^c$$

11. Difference Laws:

$$A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$$
$$A\backslash(B \cap C) = (A\backslash B) \cup (A\backslash C)$$

Definition 1.1.12 Let I be an index set. For each $i \in I$, let A_i be a set indexed by i. The union and intersection of A_i for all values of i are defined as.

$$\bigcup_{i=I} A_i = \{x : \exists\, i \in I \ni \mathrm{x} \in \mathrm{A_i}\}, \bigcap_{i \in I} A_i = \{x : x \in A_i \quad \forall\, i \in I\}$$

If $I = \{k, k+1, \ldots, m\}$ is a finite set,

$$\bigcup_{i \in I} A_i = A_k \cup A_{k+1} \cup \cdots \cup A_m = \bigcup_{i=k}^{m} A_i$$

and

$$\bigcap_{i \in I} A_i = A_k \cap A_{k+1} \cap \cdots \cap A_m = \bigcap_{i=k}^{m} A_i$$

If $\mathcal{F}$ is a collection of sets,

$$\bigcup_{A \in \mathcal{F}} A = \{x : \exists\, A \in \mathcal{F} \ni x \in A\}$$

and

$$\bigcap_{A \in \mathcal{F}} A = \{x : x \in A \quad \forall A \in \mathcal{F}\}$$

Proposition 1.1.13 *Let I be an index set. For each $i \in I$, let A_i be the set indexed by i.*

1. For each $j \in I$, $\bigcap_{i \in I} A_i \subseteq A_j$ and $A_j \subseteq \bigcup_{i \in I} A_i$.
2. If B is a set such that for all $i \in I$, $A_i \subseteq B$, then $\bigcup_{i \in I} A_i \subseteq B$.
3. If B is a set such that for all $i \in I$, $B \subseteq A_i$, then $B \subseteq \bigcap_{i \in I} A_i$.

If $I = \mathcal{F}$ is a collection of sets, the above statements can be restated as follows:

1. For all $B \in \mathcal{F}$, $\bigcap_{A \in \mathcal{F}} A \subseteq B$ and $B \subseteq \bigcup_{A \in \mathcal{F}} A$.

2. If $A \subseteq B$ for all $A \in \mathcal{F}$, then $\bigcup\limits_{A\in\mathcal{F}} A \subseteq B$.
3. If $B \subseteq A$ for all $A \in \mathcal{F}$, then $B \subseteq \bigcap\limits_{A\in\mathcal{F}} A$.

Example 1.1.14

1. Let $I = \{1, 2, 3\}$. If $A_1 = \{1, 2, 3, 5, 7\}$, $A_2 = \{3, 7, 8, 9\}$, and $A_3 = \{3, 4, 6, 7\}$, then

$$\bigcup_{i=1}^{3} A_i = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \text{ and } \bigcap_{i=1}^{3} A_i = \{3, 7\}.$$

2. For each $i \in \mathbb{N}$, let $A_i = \{m \in \mathbb{N} : m \geq i\}$. Since $A_i \subseteq \mathbb{N}$ for all $i \in I$,

$$\bigcup_{i=1} A_i \subseteq \mathbb{N} = A_1 \subseteq \bigcup_{i\in I} A_i.$$

Hence, $\bigcup\limits_{i=1}^{\infty} A_i = \mathbb{N}$

Moreover, $\bigcap\limits_{i=1}^{\infty} A_i = \emptyset$. For if not, then there exists $x \in \bigcap\limits_{i=1}^{\infty} A_i$, i.e.,

$$x \in A_i = \{m \in \mathbb{N} : m \geq i\} \text{ for each } i \in \mathbb{N}.$$

That is, $x \geq i \ \forall i \in \mathbb{N}$. If $i = x + 1$, then $x \geq x + 1$, which is a contradiction.

3. Let $I = \{x \in \mathbb{R} : x > 0\}$ and for all $x \in I$, let $A_x = (-x, x)$. We show that $\bigcup\limits_{x\in I} A_x = \mathbb{R}$ as follow: since $A_x \subseteq \mathbb{R}$ for each $x \in I$, then $\bigcup\limits_{x\in I} A_x \subseteq \mathbb{R}$. For the other inclusion, let $y \in \mathbb{R}$ and pick $x = |y| + 1$, then $|y| < x$, i.e., $-x < y < x$. Hence, $y \in A_x$. Since $y \in \mathbb{R}$ is an arbitrary element, then $\mathbb{R} \subseteq \bigcup_{x\in I} A_x$.

For the intersection, $\{0\} \subseteq (-x, x) = A_x$ for each $x \in I$, and thus, $\{0\} \subseteq \bigcap\limits_{x\in I} A_x$. However, if y $\neq 0$, then $|y| > 0$. Let $x = \frac{|y|}{2} < |y|$, then $y \notin (-x, x)$. Hence, $y \notin \bigcap\limits_{x\in I} A_x$ and $\bigcap\limits_{x\in I} A_x \subseteq \{0\}$. Therefore, $\bigcap\limits_{x\in I} A_x = \{0\}$.

Proposition 1.1.15 *Let I be an index set and A_i be a set for all $i \in I$. The following identities hold:*

1. $(\bigcup\limits_{i\in I} A_i)^c = \bigcap\limits_{i\in I} A_i^c$ *and* $(\bigcap\limits_{i\in I} A_i)^c = \bigcup\limits_{i\in I} A_i^c$.
2. $B \cup (\bigcap\limits_{i\in I} A_i) = \bigcap\limits_{i\in I} (B \cup A_i)$ *and* $B \cap (\bigcup\limits_{i\in I} A_i) = \bigcup\limits_{i\in I} (B \cap A_i)$.

The equations in item (1) in Proposition 1.1.15 are known by Generalized De Morgan's Laws.

Definition 1.1.16 (Partition of a set) Let A be a nonempty set and $\mathcal{C} \subseteq \mathcal{P}(A)$. The set $\mathcal{C}$ is called a partition of A if

1. $\emptyset \notin \mathcal{C}$ and $\bigcup\limits_{E \in C} E = A$
2. For all $E, F \in \mathcal{C}$, either $E = F$ (equal) or $E \cap F = \emptyset$ (disjoint).

A partition of a set can be considered a split of the set into smaller separate and nonempty parts.

Example 1.1.17 Let $A = \{1, 2, 3, 4\}$. Each of the sets

$$\mathcal{C}_1 = \{\{1\}, \{2, 4\}, \{3\}\}, \mathcal{C}_2 = \{\{1, 2\}, \{3, 4\}\}, \text{ and } C_3 = \{\{1\}, \{2, 3, 4\}\}.$$

is an example of a partition of A, as they all satisfy the above two conditions. However, none of the sets

$$\mathcal{D}_1 = \{\{1, 2\}, \{2, 3, 4\}\}, \mathcal{D}_2 = \{\emptyset, \{1\}, \{2, 3, 4\}\}, \text{ and } \mathcal{D}_3 = \{\{1, 3\}, \{4\}\}$$

forms a partition of A (Check!).

Example 1.1.18

1. Consider the set of integers $\mathbb{Z}$. Let E_1 and E_2 be the sets of positive and negative integers, respectively. The set $\mathcal{C} = \{E_1, E_2\}$ is not a partition of $\mathbb{Z}$ because $E_1 \cup E_2 \neq \mathbb{Z}$. The set $\mathcal{D} = \{E_1, E_2, \{0\}\}$ forms a partition of $\mathbb{Z}$.
2. Consider the set of positive integers $\mathbb{N}$. Let E_1, E_2 and E_3 be the sets of even positive integers, odd positive integers, and primes, respectively. The set $\mathcal{C} = \{E_1, E_2\}$ forms a partition of $\mathbb{N}$, and $\mathcal{D} = \{E_1, E_2, E_3\}$ does not, because $E_2 \cap E_3 \neq \emptyset$.
3. Consider the set of positive real numbers $\mathbb{R}^+$. For each $n \in \mathbb{N}$, let $E_n = (n - 1, n)$. The set $\mathcal{C} = \{E_n : n \in \mathbb{N}\}$ is not a partition of $\mathbb{R}^+$ since $\bigcup\limits_{n \in \mathbb{N}} E_n = \mathbb{R}^+ \backslash \mathbb{Z} \neq \mathbb{R}^+$. If E_n is replaced by $[n - 1, n]$, then $\mathcal{C}$ will not form a partition of $\mathbb{R}^+$ because $E_n \cap E_{n+1} \neq \emptyset$. If E_n is replaced by $(n - 1, n]$, then $\mathcal{C}$ forms a partition of $\mathbb{R}^+$.

Another operation that is defined on sets is the Cartesian product, in which two sets form a new one using the notion of ordered pairs. An ordered pair of a and b is defined as the set $\{\{a\}, \{a, b\}\}$ and expressed as (a, b), where a and b are called the first and second components of the pair. Two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$. In general, the n-tuple of $a_1, a_2, \ldots, a_n$ is the ordered list $(a_1, a_2, \ldots, a_n)$. The jth element in the n-tuple is called the jth component.

Definition 1.1.19 (Cartesian product of sets) Let A and B be two sets. The Cartesian product of A and B, denoted by $A \times B$, is defined as the set of all ordered pairs whose first and second components are elements of A and B, respectively. That is,

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

In general, if $A_1, A_2, \ldots, A_n$ are sets, then their Cartesian product, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is the set of n-tuples of which the i th component belongs to A_i. That is

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, 1 \leq i \leq n\}.$$

Proposition 1.1.20 *Let A and B be any sets, the following statements hold.*

1. $A \times \emptyset = \emptyset$.
2. $A \times B = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$.
3. If A and B are nonempty sets, then $A \times B = B \times A \Leftrightarrow A = B$.
4. $|A \times B| = |B \times A| = |A||B|$.
5. If $A \times B \neq \emptyset$, then $A \times B \subseteq C \times D$ if and only if $A \subseteq C$ and $B \subseteq D$.
6. If $A \times B \neq \emptyset$, then $A \times B = C \times D$ if and only if $A = C$ and $B = D$.
7. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Example 1.1.21

1. If $A = \{1, 2\}$ and $B = \{x, y, z\}$, then
$$A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}.$$
2. If $A = \{1, 2\}$ and $B = \{0\}$, then
$$A \times B = \{(1, 0), (2, 0)\}.$$
3. If $A = \mathbb{R}$, and $B = \{0\}$, then
$$A \times B = \{(x, y) : x \in \mathbb{R} \wedge y = 0\} = \{(x, 0) : x \in \mathbb{R}\}$$
is the set of points that represent the x-axis on the plane.
4. Consider the real numbers $\mathbb{R}$. Let $A = (0, 1)$ and $B = [0, 1)$, then
$$A \times B = \{(x, y) : 0 < x < 1 \wedge 0 \leq y < 1\}$$
is the set of points on the plane represented by a square bounded by the lines $x = 0, x = 1, y = 0$, and y $= 1$. The square's side on the x-axis ($y = 0$) is included (Fig. 1.2).
5. The set $\mathbb{Z} \times \mathbb{R} = \{(x, y) : x \in \mathbb{Z} \wedge y \in \mathbb{R}\}$ represents all vertical lines on the plane at which the x-coordinates are integers (Fig. 1.3)
6. The set $\mathbb{Z} \times \mathbb{Z} = \{(x, y) : x \in \mathbb{Z}, y \in \mathbb{Z}\}$ consists of points in the plane with both of coordinates integers. This set is represented on the plane as (Fig. 1.4):
7. The set $\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\} = \mathbb{R}^2$ represents the entire plane. Note that $\mathbb{R} \times \mathbb{R}^* = \{(x, y) : x, y \in \mathbb{R} \wedge y \neq 0\}$ represents the plane $\mathbb{R}^2$ except the line $y = 0$.

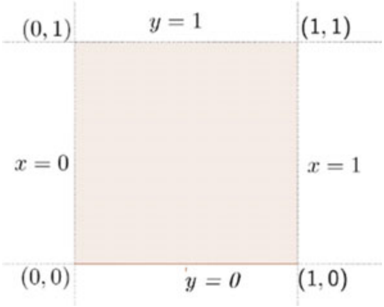


Fig. 1.2 Graph of (0,1) × [0,1) in the plane

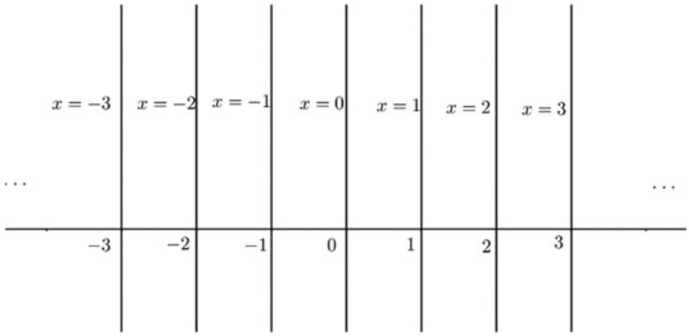


Fig. 1.3 Graph of $\mathbb{Z} \times \mathbb{R}$

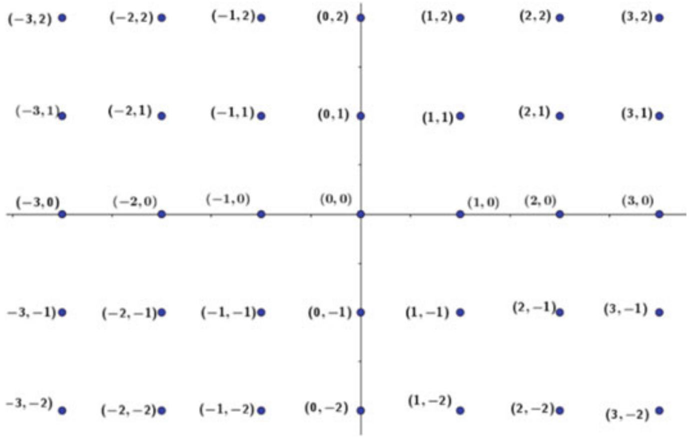


Fig. 1.4 Graph of $\mathbb{Z} \times \mathbb{Z}$

1.2 Principle of Mathematical Induction

The principle of mathematical induction, or simply, mathematical induction, is a mathematical technique used to prove a statement defined for the set of integers $\mathbb{Z}$, or any of its subsets. Among the many forms of mathematical induction, we present two forms and examples of each form. For the proofs of the theorem and proposition provided in this section, see (Hammack, 2013).

Theorem 1.2.1 (Principle of mathematical induction) *Let $n \in \mathbb{Z}$ and $P(n)$ be a mathematical statement that depends on n. If*

1. there exists $m \in \mathbb{Z}$ such that $P(m)$ is a true statement, and
2. for all $n \geq m$,

$$P(n) \text{ is true } \Rightarrow P(n+1) \text{ is true}$$

then $P(n)$ is a true statement for all $n \geq m$.

The statement in item (1), in above theorem, is called Base step, the statement in item (2) is called Inductive step. The process of the mathematical induction is intuitive, as the base step assumes that the statement is true for m; subsequently, the inductive step ensures that the statement is true for the next integer. Figure 1.5 provides an intuitive justification for the principle of mathematical induction.

$$P(m) \text{ true } \Rightarrow P(m+1) \text{ true } \Rightarrow P(m+2) \text{ true } \Rightarrow P(m+3) \text{ true } \cdots\cdots$$

Remark 1.2.2 The principle of mathematical induction can also be used to prove mathematical statements on a finite subset of $\mathbb{Z}$. If $A = \{m, m+1, m+2, \ldots, n\}$ is a subset of $\mathbb{Z}$ and $P(k)$ is a mathematical statement, then we can show that $P(k)$ is true for all $k \in A$ by demonstrating that $P(m)$ is true, and $P(k)$ is true $\Rightarrow P(k+1)$ is true for all $m \leq k < n$.

Example 1.2.3 Let $n \in \mathbb{N}$. Using the principle of mathematical induction, one can show that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for all } n \geq 1$$

as follows:

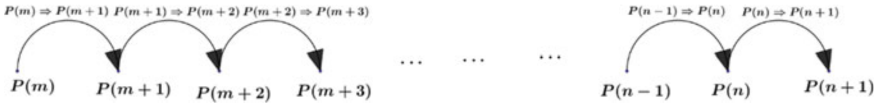

$P(m) \Rightarrow P(m+1)$
$P(m+1) \Rightarrow P(m+2)$
$P(m+2) \Rightarrow P(m+3)$
$P(n-1) \Rightarrow P(n)$
$P(n) \Rightarrow P(n+1)$
$P(m)$
$P(m+1)$
$P(m+2)$
$P(m+3)$
$\cdots$ $\cdots$ $\cdots$
$P(n-1)$
$P(n)$
$P(n+1)$

Fig. 1.5 Principle of mathematical induction

Base step: since $1 = 1(2)/2$, then the equality holds if $n = 1$.

Inductive step: Assume that the statement is true for n, i.e., $1 + 2 + \cdots + n = n(n + 1)/2$. We verify

$$1 + 2 + \cdots + n + (n + 1) = (n + 1)(n + 2)/2$$

as follows:

$$\begin{aligned} \text{L.H.S } &= 1 + 2 + \cdots + n + (n + 1) = n(n + 1)/2 + (n + 1) \\ &= (n(n + 1) + 2(n + 1))/2 = (n + 1)(n + 2)/2 = \text{ R.H.S.} \end{aligned}$$

As the two conditions are satisfied, according to the principle of mathematical induction, the statement is true for all $n \geq 1$.

In mathematical induction, the validity of the statement at $n + 1$ is derived from the validity of the statement at the previous value n. However, in several situations, the process might need information about several values to complete the proof. For example, if

$$a_1 = 1, a_2 = 4 \text{ and } a_n = 4a_{n-1} - 4a_{n-2} \text{ for all } n \geq 3,$$

then two values must be considered to show that $a_n = n2^{n-1}$ for all $n \geq 1$. Such a problem cannot be solved using the principle of mathematical induction in the abovementioned form. Other forms of the principle can be used to address such situations, one of which is called the principle of strong induction or simply strong induction.

Proposition 1.2.4 (The principle of strong induction) *Let $n \in \mathbb{Z}$ and $P(n)$ be a mathematical statement that depends on n. If*

1. There exists $m \in \mathbb{Z}$ such that $P(m)$ is a true statement, and "Base step"
2. If $P(k)$ is true for all k such that $m \leq k < n$ implies that $P(n)$ is true. "Inductive step"

then $P(n)$ is a true statement for all $n \geq m$.

Example 1.2.5 Let $a_1 = 1, a_2 = 4$, and $a_n = 4a_{n-1} - 4a_{n-2}$ for all $n \geq 3$. Using the principle of strong induction, we can show that

$$a_n = n2^{n-1} \text{ for all } n \geq 1$$

as follows:

Base step: The statement is true for $n = 1$ and $n = 2$.

Inductive step: Assume that $n > 2$ and the statement is true for all $1 \leq k < n$, as $1 \leq n - 2, n - 1 < n$, then

$$a_{n-1} = (n-1)2^{n-2}, \text{ and } a_{n-2} = (n-2)2^{n-3}.$$

Hence,

$$\begin{aligned} a_n &= 4(n-1)2^{n-2} - 4(n-2)2^{n-3} \\ &= 4(2(n-1)-(n-2))2^{n-3} = n2^{n-1}. \end{aligned}$$

i.e., the statement is true for n. According to the strong induction, the statement holds for all $n \geq 1$.

1.3 Binary Relations on Sets

As in any other field of study, objects in mathematics are related in various ways. For example, the relation of a point lying on a line, or the inclusion relation for sets. In mathematics, relations are usually represented by a set of ordered pairs in which the first and second components are related. For example, let P be a set of points and L be a set of lines on the plane. The set $\mathcal{J} = \{(p, l) \in P \times L : p \text{ lies on } l\}$ represents the relation that p lies on l. The inclusion relation among a family of sets is represented by $\mathcal{S} = \{(A, B) \in \mathfrak{F} \times \mathfrak{F} : A \subseteq B\}$, where $\mathfrak{F}$ is a collection of sets. In general, the following definition can be stated.

Definition 1.3.1 Let A and B be two sets. A binary relation (or simply, a relation) $\mathcal{R}$ from A to B is a subset of $A \times B$, i.e.,

$$\mathcal{R} \subseteq \{(a, b) : a \in A, b \in B\}$$

If $A = B$, we say $\mathcal{R}$ is a relation on A.

For an ordered pair, $(a, b) \in A \times B$, either $(a, b) \in \mathcal{R}$ or $a\mathcal{R}$b is used to denote that a is related to b through the relation $\mathcal{R}$. Both notations $(a, b) \notin \mathcal{R}$ and $a\not\mathcal{R}b$ are used to express that a and b are not related through the relation $\mathcal{R}$. The notion of a binary relation is generalized to more than two sets as follows:

Let $A_1, A_2, \ldots, A_n$ be any sets. A relation $\mathcal{R}$ of these sets is a subset of $A_1 \times A_2 \times \ldots \times A_n$, i.e., $\mathcal{R} \subseteq \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ \ldots, a_n \in A_n\}$. In this book, only the binary relation is considered unless otherwise stated.

For any two sets A and B, two relations always exist from A to B. Namely, $\mathcal{R} = \emptyset$ and $\mathcal{R} = A \times B$. More examples are presented below.

Example 1.3.2

1. The set $\mathcal{R} = \{(1, 7), (1, 8), (1, 9), (3, 7)\}$ is a relation from $\{1, 3\}$ to $\{7, 8, 9\}$.
2. The set $\mathcal{R} = \{(a, 7), (a, 8), (a, 9), (b, 7)\}$ is a relation from $\{a, b\}$ to $\{7, 8, 9\}$.
3. The set $\mathcal{R} = \{(1, 1), (2, 2), (1, 3)\}$ is a relation on $\{1, 2, 3\}$.
4. The set $\mathcal{S} = \{(A, B) \in \mathfrak{F} \times \mathfrak{F} : A \subseteq B\}$ is a relation on $\mathfrak{F}$, where $\mathfrak{F}$ is any family of sets.

5. The set $\mathcal{S} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n \text{ divides } m\}$ is a relation on $\mathbb{Z}$.
6. The set $\mathcal{R} = \left\{(x, y) \in \mathbb{N}^2 : y = x + 1\right\}$ is a relation on $\mathbb{N}$.
7. The set $\mathcal{R} = \left\{(x, y) \in \mathbb{R}^2 : y = x + 1\right\}$ is a relation on $\mathbb{R}$.
8. Let $\mathcal{R}_1 = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\right\}$ and $\mathcal{R}_2 = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 1\right\}$ be the unit circle and the unit disk in the plane, respectively. Both $\mathcal{R}_1$ and $\mathcal{R}_2$ are relations on $\mathbb{R}$. The sets $\mathcal{R}_1$ and $\mathcal{R}_2$ are not relations on $\mathbb{Z}$ since $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ belongs to $\mathcal{R}_1$ and $\mathcal{R}_2$ but it does not belong to $\mathbb{Z} \times \mathbb{Z}$.

Definition 1.3.3 Let A and B be any two sets and $\mathcal{R}$ be a relation from A to B.

1. The domain of $\mathcal{R}$, denoted by $D(\mathcal{R})$, is the set of elements of A that appear as the first components in the elements of $\mathcal{R}$. i.e., $D(\mathcal{R}) = \{a \in A : \exists\, b \in B \wedge (a, b) \in \mathcal{R}\}$.
2. The range of $\mathcal{R}$, denoted by $Rang(\mathcal{R})$, is the set of elements of B that appear as the second components in the elements of $\mathcal{R}$. i.e., $Rang(\mathcal{R}) = \{b \in B : \exists\, a \in A \wedge (a, b) \in \mathcal{R}\}$.
3. The set B is called the codomain of $\mathcal{R}$.
4. For each $(a, b) \in \mathcal{R}$, the element b is called the image of a under $\mathcal{R}$.

For any sets A and B, we have
$D(\emptyset) = Rang(\emptyset) = \emptyset$, $D(A \times B) = A$, and $Rang(A \times B) = B$.

Example 1.3.4 The domains and ranges of the relations in Example 1.3.2 are

1. $D(\mathcal{R}) = \{1, 3\}$, and $Rang(\mathcal{R}) = \{7, 8, 9\}$.
2. $D(\mathcal{R}) = \{a, b\}$, and $Rang(\mathcal{R}) = \{7, 8\}$.
3. $D(\mathcal{R}) = \{1, 2\}$, and $Rang(\mathcal{R}) = \{1, 2, 3\}$.
4. $D(\mathcal{R}) = \mathfrak{F}$, and $Rang(\mathcal{R}) = \mathfrak{F}$ (This is true because any set is a subset of itself).
5. $D(\mathcal{R}) = \mathbb{Z}$, and $Rang(\mathcal{R}) = \mathbb{Z}\backslash\{0\}$.
6. $D(\mathcal{R}) = \mathbb{N}$, and $Rang(\mathcal{R}) = \mathbb{N}\backslash\{1\}$.
7. $D(\mathcal{R}) = \mathbb{R}$, and $Rang(\mathcal{R}) = \mathbb{R}$.
8. $D(\mathcal{R}_1) = D(\mathcal{R}_2) = [-1, 1]$, and $Rang(\mathcal{R}_1) = Rang(\mathcal{R}_2) = [-1, 1]$.

In the following, we restrict our study to the relations in which $A = B$. We study the properties of these relations and discuss two types of relations that appear frequently in algebra. Recall that a relation from A to A is called a relation on A.

Definition 1.3.5 (*Properties of a relation on a set*) Let A be any set and $\mathcal{R}$ be a relation on A. The relation $\mathcal{R}$ is

1. Reflexive: if $(a, a) \in \mathcal{R}$ for all $a \in A$.
2. Symmetric: if for all $a, b \in A$, $(a, b) \in \mathcal{R} \Rightarrow (b, a) \in \mathcal{R}$.
3. Antisymmetric: if for all $a, b \in A$, $((a, b) \in \mathcal{R} \wedge (b, a) \in \mathcal{R}) \Rightarrow a = b$.
4. Transitive: if for all $a, b, c \in A$, $((a, b) \in \mathcal{R} \wedge (b, c) \in \mathcal{R}) \Rightarrow (a, c) \in \mathcal{R}$.

Definition 1.3.6 Let A be any set and $\mathcal{R}$ be a relation on A. The relation $\mathcal{R}$ is called a connex relation if either $(a, b) \in \mathcal{R}$ or $(b, a) \in \mathcal{R}$ for each $a, b \in A$.

It is clear that any connex relation is reflexive.

Example 1.3.7

1. Let $A = \emptyset$. As $A \times A$ is the empty set $\emptyset$, the only relation that can be defined on A is the empty relation $\emptyset$. Clearly, $\emptyset$ is reflexive (if not, then there exists $a \in A = \emptyset$ such that $(a, a) \notin \mathcal{R}$, which is impossible). As $\emptyset$ does not contain any elements, the conditional statement for the symmetry is true, which implies that $\emptyset$ is symmetric. The same justification implies that $\emptyset$ is antisymmetric and transitive. Clearly, since there are no elements in A, the relation $\emptyset$ is a connex relation.
2. Let $A \neq \emptyset$. The set $\emptyset$ represents a relation on A that is symmetric, antisymmetric, and transitive. It is not reflexive (pick $a \in A$, then $(a, a) \notin \emptyset$), therefore, it is not a connex relation.
3. Let $A = \{1, 2, 3\}$. The relation $\mathcal{R} = \{(1, 1), (2, 2), (1, 3)\}$ is not reflexive since $(3, 3) \notin \mathcal{R}$. It is not symmetric as $(1, 3) \in \mathcal{R}$ but $(3, 1) \notin \mathcal{R}$. The relation $\mathcal{R}$ is transitive since the only ordered pairs in the form $(a, b), (b, c)$ in $\mathcal{R}$ are $(1, 1), (1, 3)$ and $(a, c) = (1, 3) \in \mathcal{R}$. Moreover, $\mathcal{R}$ is antisymmetric, because no elements in $\mathcal{R}$ in the form $(a, b), (b, a)$ where $a \neq b$. As $\mathcal{R}$ is not reflexive, it is not a connex relation.
4. For any set A, define the relation $\Delta_A = \{(a, a) \in A \times A : a \in A\}$. It straightforward to check that Δ_A is reflexive, symmetric, antisymmetric, and transitive. Moreover, Δ_A is not a connex relation for any A such that $|A| \geq 2$ (if $a \neq b$ are two elements in A, then neither (a, b) nor (b, a) belongs to Δ_A). The relation Δ_A expresses the equality relation and is called the identity (or the diagonal) relation. The symbol Δ_A denotes the identity relation on A. If $A = \{1, 2, 3\}$, then $\Delta_A = \{(1, 1), (2, 2), (3, 3)\}$ is an example for the identity relation on a finite set. The line $y = x$ is a visualization for $\Delta_A = \{(x, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$, an example of an infinite identity relation.
5. Let $A \neq \emptyset$ be any set. The relation $\mathcal{R} = A \times A = \{(a, b) \in A \times A : a, b \in A\}$ is reflexive, symmetric, and transitive. It is not antisymmetric for any A having more than one element. Let $a \neq b$ be elements in A, according to the definition of $\mathcal{R}$, both (a, b) and (b, a) belong to $\mathcal{R}$, but $a \neq b$, which implies that $\mathcal{R}$ is not antisymmetric. Clearly, as $(a, b) \in \mathcal{R}$ for all $a, b \in A$, then $\mathcal{R}$ is a connex relation.
6. Let $A = \mathbb{N}$ and $\mathcal{R} = \left\{(x, y) \in \mathbb{N}^2 : y = x + 1\right\}$. The relation $\mathcal{R}$ is not reflexive, not symmetric, and not transitive. As $\mathcal{R}$ is not reflexive, it is not a connex relation.
7. Let $A = \mathbb{R}$ and $\mathcal{R} = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\right\}$. The relation $\mathcal{R}$ is not reflexive since $2 \in A$, but $(2, 2) \notin \mathcal{R}$ ($2^2 + 2^2 = 8 \neq 1$). It is symmetric, for if $(x, y) \in \mathcal{R}$ then $x^2 + y^2 = 1$. i.e., $y^2 + x^2 = 1$ and $(y, x) \in \mathcal{R}$. The relation $\mathcal{R}$ is not antisymmetric as both $(1, 0), (0, 1) \in \mathcal{R}$ but $0 \neq 1$. Finally, it is not transitive as $(1, 0), (0, -1) \in \mathcal{R}$, but $(1, -1) \notin \mathcal{R}$. Clearly, it is not a connex relation (Fig. 1.6).

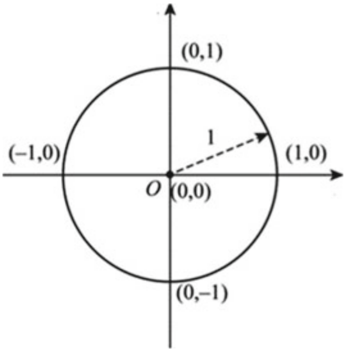


Fig. 1.6 Graph of $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$

1.4 Types of Binary Relations on Sets

A relation can be classified depending on its properties. In this book, we will encounter specific types of relations, such as equivalence and order relations. Readers can refer to (Halmos, 2013) for more details regarding the types of relations.

Definition 1.4.1 (*Types of relations*) Let A be a set and $\mathcal{R}$ be a relation on A. The relation $\mathcal{R}$ is said to be

1. An equivalence relation if $\mathcal{R}$ is reflexive, symmetric, and transitive.
2. A partial order relation if $\mathcal{R}$ is reflexive, antisymmetric, and transitive.
3. A total order relation if $\mathcal{R}$ is antisymmetric, transitive, and a connex relation.

As any connex relation is reflexive, a total order relation must be a partial order relation. By order relation, we mean a partial order relation.

The identity relation (Example 1.3.7(4)) is the canonical example of an equivalence relation, where for any $a, b \in A$, $(a, b) \in \mathcal{R}$ if and only if $a = b$. The partial order relation generalizes the concept of ordering or arranging the elements of a set. For $a, b \in A$, the pair (a, b) belongs to a partial order relation means that one of the elements precedes the other in the order. The word "partial" indicates that not every pair of elements in A are related, i.e., if a and b are arbitrary elements in A, then the partial order relation does not require (a, b) or (b, a) to be $\mathcal{R}$. In contrast, due to the connexity property, the total order relation requires that either $(a, b) \in \mathcal{R}$ or $(b, a) \in \mathcal{R}$ for each $a, b \in A$. i.e., in a total order relation, any two elements in A are comparable. The set endowed with a total order relation is called a chain. For order relations, the notation $\leq$ is usually used instead of $\mathcal{R}$, and the notation $a \leq b$ is used instead of $a\mathcal{R}b$.

Example 1.4.2

1. In Example 1.3.7,
   - The relation $\emptyset$ in (1) is an equivalence relation, a partial order, and a total order relation.

- The set $\emptyset$ in (2) and the relation in (3) are not reflexive; hence these relations are neither equivalence nor order relations.
- The relation Δ_A in (4) is an equivalence relation and a partial order relation. If $|A| \geq 2$, we pick $a, b \in A$ such that $a \neq b$. Since neither (a, b) nor (b, a) belongs to Δ_A, then Δ_A cannot be a total order relation for any set that contains more than one element.
- The relation in (5) is an equivalence relation, it is not an order relation since it is not antisymmetric.
- The relation in (6) is neither an equivalence relation nor an order relation. This result remains true if $\mathbb{N}$ is replaced with $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$.
- The relation in (7) is not reflexive, so it is neither equivalence nor order relation.

2. Let $A = \mathbb{R}$, and $\mathcal{R}$ be the natural order on $\mathbb{R}$. i.e., $a\mathcal{R}b \Leftrightarrow a \leq b$ for all $a, b \in \mathbb{R}$. It is straightforward to verify that $\mathcal{R}$ is reflexive, antisymmetric, and transitive. The relation $\mathcal{R}$ is not symmetric. For any two distinct real numbers, one must be greater than the other. Hence, the natural order is a total (hence, a partial) order relation, but not an equivalence relation.

Definition 1.4.3 Let A be a nonempty set and $\leq$ be a partial order relation on A. For any nonempty subset B of A,

1. an element $a \in A$ is called a lower bound of B if $a \leq b$ for all $b \in B$,
2. an element $d \in A$ is called an upper bound of B if $b \leq d$ for all $b \in B$,
3. the set B is called bounded below (bounded above) if B has a lower bound (an upper bound),
4. the set B is called bounded if it is bounded below and above; otherwise, it is called unbounded.

Definition 1.4.4 Let A be a nonempty set and $\leq$ be a partial order relation on A. For any nonempty subset B of A,

1. an element $c \in B$ is called minimal in B if for all $b \in B$, $b \leq c \Rightarrow c = b$,
2. an element $c \in B$ is called the minimum of B if $c \leq b$ for all $b \in B$,
3. an element $d \in B$ is called maximal in B if for all $b \in B$, $d \leq b \Rightarrow d = b$,
4. an element $d \in B$ is called the maximum of B if $b \leq d$ for all $b \in B$.

Note that if we read $c \leq b$ as c is less than or equal to b, then

in the above definition, (1) states that $c \in B$ is minimal if c is less than or equal to every element in B that is comparable with c. Item (2) states that $c \in B$ is minimum if c is less than or equal to every element in B. Thus, the minimum is always a minimal element, the maximal and maximum elements can be similarly distinguished, and the maximum element is always maximal. The converse is not true, as shown in the following example.

Example 1.4.5 Let $A = \{a, b, c\}$.

1. Let $\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}$. The relation $\mathcal{R}$ is a partial order relation on A (Check!). Clearly, b is a maximal element in A, but is not maximum, since there exists an element $c \in A$ such that $c \nleq b$. The element c is also maximal.
2. Let $\mathcal{R} = \{(a, a), (b, b), (c, c), (b, c), (a, c)\}$. The relation $\mathcal{R}$ is a partial order relation on A (Check!). The element b is a minimal element in A that is not minimum, since there exists an element $a \in A$ such that $a \nleq c$. The element a is also minimal.
3. Let $\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)\}$. It is easy to check that c is a maximal and maximum element in A, and a is minimal and minimum.

Proposition 1.4.6 *Let A be a nonempty set and $\leq$ be a partial order relation on A. If B is a nonempty subset of A, then B has at most one maximum and one minimum element. If $\leq$ is a total order relation on B, then a minimal (res. maximal) is the minimum (res. maximum) element in B.*

Next, we focus on equivalence relations. Recall the definition of a partition of a set given in Definition 1.1.16. We show that any equivalence relation results in a partition of the underlying set (Theorem 1.4.10 below). We begin with the following definition.

Definition 1.4.7 (*Equivalence classes*) Let A be a nonempty set and $\mathcal{R}$ be an equivalence relation on A. For all $a \in A$, the equivalence class of a, denoted by $[a]_{\mathcal{R}}$ or simply $[a]$, is the set of elements of A that are related to a via $\mathcal{R}$. That is,

$$\begin{aligned}[a]_{\mathcal{R}} &= \{b \in A : (a, b) \in \mathcal{R}\} = \{b \in A : (b, a) \in \mathcal{R}\} \\ &= \{b \in A : a\mathcal{R}b\} = \{b \in A : b\mathcal{R}a\}.\end{aligned}$$

Two elements of the set A are called equivalent if and only if they belong to the same equivalence class, i.e., if and only if they are related by $\mathcal{R}$. The set of all equivalence classes for all elements in A is called equivalence classes of $\mathcal{R}$.

Example 1.4.8

1. Let $A = \{1, 2, 3\}$ and $\mathcal{R}_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$. The relation $\mathcal{R}_1$ is an equivalence relation (Verify!). The equivalence classes are Fig 1.7 visualizes the equivalence class for each element in A.

$$[1] = \{1, 2\} = [2] \text{ and } [3] = \{3\}$$

2. Let $A = \{1, 2, 3, 4\}$ and $\Delta_A = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$. As explained in Example 1.3.7, the relation Δ_A is an equivalence relation. The equivalence classes are

$$[1] = \{1\}, [2] = \{2\}, [3] = \{3\}, \text{ and } [4] = \{4\}.$$

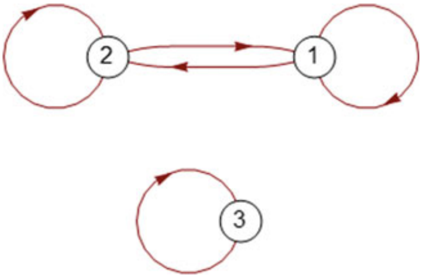


Fig. 1.7 Equivalence classes of $\mathcal{R}_1$

In general, the equivalence class of an element in a set A, endowed with Δ_A, consists of one element $[a] = \{a\}$, see also Fig. 1.8.

Proposition 1.4.9 *Let A be a nonempty set and $\mathcal{R}$ be an equivalence relation on A. For all $a, b \in A$, the following statements are satisfied:*

1. $a \in [a]$.
2. $b \in [a]$ if and only if $[a] = [b]$.
3. $[a] \cap [b] \neq \emptyset$ if and only if $[a] = [b]$.
4. If $(a, b) \notin \mathcal{R}$, then $[a] \cap [b] = \emptyset$.

Item (3) in the above proposition states that any two equivalence classes are either equal or disjoint. This is an important fact for proving the following theorem.

Theorem 1.4.10 *Let A be a nonempty set. The equivalence classes of any equivalence relation on A form a partition of A.*

Example 1.4.11 Let $A = \mathbb{Z}$ and $\mathcal{R} = \left\{(a, b) \in \mathbb{Z}^2 : (a - b)/3 \in \mathbb{Z}\right\}$. The relation $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$ and satisfies the following properties:

- Reflexive: For all $a \in \mathbb{Z}$, $((a - a)/3) = 0 \in \mathbb{Z}$, which implies that $(a, a) \in \mathcal{R}$.
- Symmetric: Assume that $(a, b) \in \mathcal{R}$ for arbitrary integers a and b. According to the definition of $\mathcal{R}$, $(a - b)/3 \in \mathbb{Z}$, which is equivalent to $(b - a)/3 = -(a - b)/3 \in \mathbb{Z}$. Hence, $(b, a) \in \mathcal{R}$.
- Transitive: Assume that $(a, b) \in \mathcal{R}$ and $(b, c) \in \mathcal{R}$ for arbitrary integers a, b, and c. According to the definition of $\mathcal{R}$, both $(a - b)/3$ and $(b - c)/3 \in \mathbb{Z}$. Consequently,

$$\frac{a-c}{3} = \frac{a-b}{3} + \frac{b-c}{3} \in \mathbb{Z}.$$

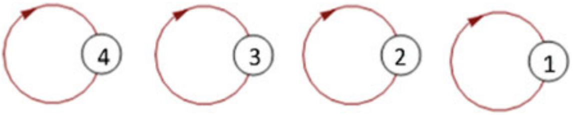


Fig. 1.8 Equivalence classes of Δ_A

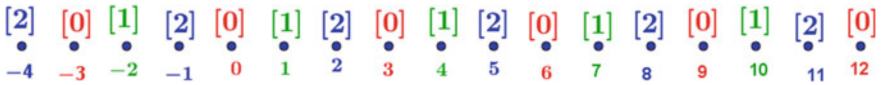


Fig. 1.9 Equivalence classes of $\mathcal{R}$ on A

Therefore, the relation $\mathcal{R}$ is an equivalence relation. For any $a \in \mathbb{Z}$, the equivalence class of a is

$$[a] = \{b \in \mathbb{Z} : (a, b) \in \mathcal{R}\} = \left\{b \in \mathbb{Z} : \frac{a-b}{3} \in \mathbb{Z}\right\} = \left\{b \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \ni \frac{\mathrm{a}-\mathrm{b}}{3} = \mathrm{k}\right\}$$
$$= \{b \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \ni \mathrm{b} = \mathrm{a} - 3\mathrm{k}, \mathrm{k} \in \mathbb{Z}\} = \mathrm{a} + \{3l : l \in \mathbb{Z}\} = \mathrm{a} + 3\mathbb{Z}.$$

For example,

$$[0] = 0 + 3\mathbb{Z} = \{\ldots - 6, -3, 0, 3, 6, \ldots\}, [1] = 1 + 3\mathbb{Z} = \{\ldots - 5, -2, 1, 4, 7, \ldots\}$$
$$[2] = 2 + 3\mathbb{Z} = \{\ldots - 4, -1, 2, 5, 8, \ldots\}, [3] = 3 + 3\mathbb{Z} = \{\ldots - 3, 0, 3, 6, 9, \ldots\} = [0]$$

By Proposition 1.4.9 (3),
$\ldots = [-6] = [-3] = [0] = [3] = [6] = \ldots =$ multiple of 3
$\ldots = [-5] = [-2] = [1] = [4] = [7] = \ldots =$ (multiple of 3) + 1.
$\ldots = [-4] = [-1] = [2] = [5] = [8] = \ldots =$ (multiple of 3) + 2 (Fig. 1.9).

To show that these classes are the only equivalent classes for the relation $\mathcal{R}$, let m be an arbitrary element in $\mathbb{Z}$. Confine m between two consecutive multiples of 3, i.e., find n such that

$$3n \le m < 3(n+1) = 3n + 3$$

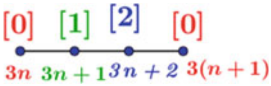
The possible values for the integer m are

$m = 3n \in 3\mathbb{Z} = [0]$, $m = 3n + 1 \in 3\mathbb{Z} + 1 = [1]$, or $m = 3n + 2 \in \mathbb{Z} + 2 = [2]$.

This indicates that at most three equivalence classes exist, namely: [0], [1], [2], see Fig 1.10. According to Proposition 1.4.9 (4), as (0, 1), (0, 2), and (1, 2) are not elements of $\mathcal{R}$, the three equivalence classes are disjoint. The set of equivalence classes of $\mathcal{R}$ is $\{[0], [1], [2]\} = \{[6], [-8], [-4]\} = \ldots$ etc.

In the previous example, using an equivalence relation on $\mathbb{Z}$, the set $\mathbb{Z}$ was divided into three disjoints parts. By defining another similar equivalence relation on $\mathbb{Z}$, the set $\mathbb{Z}$ can be divided into another number of sets. For example, the relation $\mathcal{R} = \left\{(a, b) \in \mathbb{Z}^2 : (a - b)/9 \in \mathbb{Z}\right\}$ on $\mathbb{Z}$ divides $\mathbb{Z}$ into nine disjoint sets. In general, for any $n \in \mathbb{Z}^*$, the relation

Fig. 1.10 Only three different equivalence classes of $\mathcal{R}$



$$\mathcal{R} = \left\{(a, b) \in \mathbb{Z}^2 : \frac{a-b}{n} \in \mathbb{Z}\right\}$$

divides $\mathbb{Z}$ into n disjoint sets in the form $m + n\mathbb{Z}$, where $m = 0, 1, 2, \ldots, n-1$ (Exercise 1.19).

Example 1.4.12 Let $\mathbb{Z}^*$ be the set of nonzero integers and

$$A = \mathbb{Z} \times \mathbb{Z}^* = \{(m, n) : m, n \in \mathbb{Z} \wedge n \neq 0\}.$$

On A, define the relation $\sim$ as $(m, n) \sim (r, s) \Leftrightarrow ms = nr$. The relation $\sim$ satisfies the following properties:

1. Reflexive: For an arbitrary element $(m, n) \in A$, the integers m, n satisfy $mn = nm$, which implies that $(m, n) \sim (m, n)$.
2. Symmetric: Assume that $(m, n), (r, s) \in A$ are arbitrary elements such that $(m, n) \sim (r, s)$, then

$$(m, n) \sim (r, s) \Rightarrow ms = nr \Rightarrow rn = sm \Rightarrow (r, s) \sim (m, n).$$

3. Transitive: Suppose $(m, n), (r, s), (k, l)$ are arbitrary elements in A such that $(m, n) \sim (r, s)$ and $(r, s) \sim (k, l)$. Therefore, m, n, r, s, k, l are integers where $n, s, l \neq 0$, and

$$(m, n) \sim (r, s) \text{ and } (r, s) \sim (k, l) \Rightarrow ms = nr \wedge rl = sk.$$

Multiplying both sides of $ms = nr$ by l and both sides of $rl = sk$ by n yields

$$msl = nrl \text{ and } nrl = nsk$$

which implies that $msl = nsk$. As $s \neq 0$, dividing both sides of $msl = nsk$ by s yields $ml = nk$. Thus, $(m, n) \sim (k, l)$, and $\sim$ is transitive.

Thus, the relation $\sim$ is an equivalence relation. By definition, the equivalence class of (m, n) is given by

$$[(m, n)] = \{(r, s) \in A : (m, n) \sim (r, s)\} = \{(r, s) \in A : ms = nr\}.$$

If (m, n) is identified with the rational fraction m/n, then $[(m, n)]$ is identified with the set of all equivalent fractions to m/n. In fact, the set of rational fractions $\mathbb{Q}$ is defined as the set of equivalence classes of the relation $\sim$.

$$\mathbb{Q} = \{[(m, n)] : m, n \in \mathbb{Z} \wedge n \neq 0\} := \{m/n : m, n \in \mathbb{Z} \wedge n \neq 0\}.$$

The set $\mathbb{Q}^* = \mathbb{Q} \backslash [(0, n)]$ is identified with $\{m/n : m, n \in \mathbb{Z} \wedge m, n \neq 0\}$.

If A is any nonempty set and $\mathcal{C}$ is any partition of A, a relation $\mathcal{R}$ on A can be defined as follows:

$(a, b) \in \mathcal{R}$ if and only if a, b belong to the same element (set) of $\mathcal{C}$.

It is straightforward to verify that the relation $\mathcal{R}$ is an equivalence relation. The equivalence class of any element a in A is $[a] = \{b \in A : (a, b) \in \mathcal{R}\} = \{b \in A : a, b$ belong to the same set in $\mathcal{C}\} = E$

where E is the element in $\mathcal{C}$ containing a.

Proposition 1.4.13 *Let A be a nonempty set. Any partition $\mathcal{C}$ of A defines an equivalence relation on A whose equivalence classes are the elements of $\mathcal{C}$.*

Corollary 1.4.14 *Let A be a nonempty set. There exists a one to one corresponding between the set of equivalence relations on A and the set partitions of A.*

Next, we provide examples of relations defined on the set of equivalence classes. If A is a nonempty set, $\mathcal{R}$ is an equivalence relation on A, and $\mathcal{C} = \{[a] : a \in A\}$ is the set of equivalence classes of $\mathcal{R}$, then a relation $\mathcal{R}'$ can be defined from $\mathcal{C}$ to a given set B, i.e.,

$$\mathcal{R}' \subseteq \{([a], b) \in \mathcal{C} \times B : a \in A, b \in B\}$$

A relation on the set of equivalence classes $\mathcal{C}$ is in the form

$$\mathcal{R}' \subseteq \{([a], [b]) \in \mathcal{C} \times \mathcal{C} : a, b \in A\}$$

Example 1.4.15

1. Consider the relation in Example 1.4.11 and its equivalence classes $\mathcal{C} = \{[0], [1], [2]\}$. The set

$$\mathcal{R}' = \{([0], 1), ([5], 2), ([12], 3)\} \text{ and } \mathcal{R}'' = \{([0], 1), ([5], 2), ([4], 3)\}$$

are relations from $\mathcal{C}$ to the set $\{1, 2, 3\}$. The sets

$$\mathcal{S}' = \{([0], [1]), ([5], [-4]), ([12], [-7])\},$$
$$\mathcal{S}'' = \{([0], [1]), ([5], [-4]), ([12], [-8])\}$$

are relations on $\mathcal{C}$.

2. Consider the equivalence relation in Example 1.4.12 and its equivalence classes

$\mathbb{Q} = \{[(m, n)] : m, n \in \mathbb{Z} \wedge n \neq 0\}$. The set $\mathcal{J} = \{([(m, n)], m) : m, n \in \mathbb{Z} \wedge n \neq 0\}$ forms a relation from $\mathbb{Q}$ to $\mathbb{Z}$. The set $\mathcal{T} = \mathbb{Q}^* \times \mathbb{Q}^* = \{([(m, n)], [(r, s)]) : m, n, r, s \in \mathbb{Z}^*\}$ is a relation on $\mathbb{Q}^*$.

1.5 Functions

In this section, a specific type of relations, called functions, is examined. The importance of studying functions springs from their presence and role in almost every branch of mathematics. The symbol f, the first letter of function, is used instead of $\mathcal{R}$ to denote a relation that is a function.

Definition 1.5.1 Let A and B be any sets and $f \subseteq A \times B$ be a relation from A to B. The relation f is said to be a function on A if for each element $a \in A$, there exists a unique element $b \in B$ such that $(a, b) \in f$, i.e., the conditional statement

$$a \in A \Rightarrow \exists\, !\, b \in B \text{ such that } (a, b) \in f$$

is true for all $a \in A$. The notation $\exists\, !$ indicates uniqueness.

The notation $f : A \to B$ denotes that f is a function from A to B, and the notation $b = f(a)$ is used instead of $(a, b) \in f$. Note that the uniqueness requirement in this definition is equivalent to the following statement:

$$a_1 = a_2 \Rightarrow f(a_1) = f(a_2) \text{ for all } a_1, a_2 \in A.$$

Remark 1.5.2 If $\mathcal{R}$ is an equivalence relation on A, and $f : \{[a] : a \in A\} \to B$ is a function on the set of all equivalence classes of $\mathcal{R}$, then uniqueness requirement means that the definition of f does not depend on the representatives used for the equivalence class of a, i.e., if a and b are elements in A such that $[a] = [b]$, then their images under f must be equal. This is called well-defined property of f, i.e., a function f from $\{[a] : a \in A\}$ to B must satisfy that

$$a_1 \mathcal{R} a_2 \Rightarrow f([a_1]) = f([a_2]) \quad \forall a_1, a_2 \in A$$

In general, if the domain of f involves equivalence classes (e.g., $f : \mathcal{A} \to B$, where $\mathcal{A}$ is a set defined using equivalence classes), then the well-defined property must be verified. For more explanation, see the Example 1.5.6 (4–9).

Definition 1.5.3 Let A and B be any sets, $f : \mathcal{A} \to B$ be a function from A to B, and A_1 be any subset of A. The restriction of f on A_1, denoted by $f_{|A_1}$, is the map from A_1 to B defined by $f_{|A_1}(a) = f(a)$ for all $a \in A_1$.

As for any other relation on sets (Definition 1.3.3), the following definition holds:

Definition 1.5.4 Let A and B be any two sets and $f : A \to B$ be a function.

- The set A is called the domain of f, denoted by $D(f)$, and B is called the codomain of f.
- The element $b \in B$ such that $b = f(a)$ is called the image of a under f or the value of a.
- The set of all images of A is $f(A) = \{f(a) : a \in A\}$, which is called the range of f, denoted by $Rang(f)$.
- If $b \in B$, then the preimage (inverse image) of b under f is the set

$$f^{-1}(b) = \{a \in A : b = f(a)\}.$$

- If $Y \subseteq B$, then the preimage (inverse image) of Y under f is the set

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\}.$$

Remark 1.5.5

1. To calculate $f^{-1}(Y)$, it is easier to
   - calculate $f^{-1}(\{b\}) = \{x : f(x) = b\}$ for all $b \in Y$, then
   - use the equality $f^{-1}(Y) = \bigcup_{b \in Y} f^{-1}(\{b\})$.
2. If a function is defined on a subset of $\mathbb{R}$ as an algebraic expression $f(x)$ in a variable x, the domain of f is taken to be all possible values x, where the expression is valid. For example, the domain of $f(x) = \frac{x^2+1}{x^2-3x+2}$ is $\mathbb{R}\backslash\{1, 2\}$.

Example 1.5.6 Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4\}$.

1. The relation $f = \{(a, 1), (b, 1), (c, 1), (d, 2)\}$ from A to B is a function whose domain is A, and the image of each element in A is given as

$$f(a) = 1, f(b) = 1, f(c) = 1, \text{ and } f(d) = 2.$$

2. The relation $g = \{(a, 1), (b, 1), (a, 2), (c, 3), (d, 1)\}$ from A to B is not a function, as both $(a, 1)$ and $(a, 2)$ are in g but $1 \neq 2$.
3. The relation $h = \{(a, 2), (b, 3), (c, 4)\}$ from A to B is not a function, as it is not defined for every element in A.
4. The relation $\mathcal{R}'$ in Example 1.4.15 is not a function. It is not defined for every element in $\mathcal{C}$ ($\{[0], [5], [12]\} = \{[0], [2]\} \neq \mathcal{C}$), and it is not well-defined since $[0] = [12]$, but $1 \neq 3$.
5. The relation $\mathcal{R}''$ in Example 1.4.15 represents a function on $\mathcal{C}$; it is defined for every element in $\mathcal{C}$ ($\{[0], [5], [4]\} = \{[0], [1], [2]\}$). Since $[0] \neq [5]$, $[0] \neq [4]$ and $[4] \neq [5]$, there are no equal equivalence classes in the domain of $\mathcal{R}''$.
6. The relation $\mathcal{S}'$ in Example 1.4.15 is not a function. It is not defined for every element in $\mathcal{C}$, and it is not well-defined since $[0] = [12]$ but $[1] \neq [-7]$.
7. The relation $\mathcal{S}''$ in Example 1.4.15 is not a function. Note that [0] and [12] are the only equal equivalence classes in the domain of $\mathcal{S}''$, and as their images under $\mathcal{S}''$ ([1] and [−8], respectively) are equal, then $\mathcal{S}''$ is well-defined. However, it is not a function on $\mathcal{C}$ as it is not defined for every element in $\mathcal{C}$.
8. The relation $\mathcal{J}$ in Example 1.4.15 is defined for every element in $\mathbb{Q}$, but it is not well-defined since $[(2, 4)] = [(1, 2)]$, but their images under $\mathcal{J}$ are not equal.
9. The relation $\mathcal{T}$ in Example 1.4.15 is defined for every element in $\mathbb{Q}^*$, but it is not well-defined since every element in $\mathbb{Q}^*$ is an image of all other elements in $\mathbb{Q}^*$. For example, $[(1, 2)]$ has infinitely many different images under $\mathcal{T}$.

Example 1.5.7 Let $f : \{1, 2, 3, 4, 5, 6\} \to \{a, b, c, d\}$ be the function

$$f = \{(1, a), (2, b), (3, a), (4, b), (5, c), (6, d)\}$$

The images of the elements in $\{1, 2, 3, 4, 5, 6\}$ are given by

$$f(1) = a,\ f(2) = b,\ f(3) = a,\ f(4) = b,\ f(5) = c,\ f(6) = d$$

Therefore, $Rang(f) = \{a, b, c, d\}$. If $X = \{1, 3, 6\}$, then the image of X is

$$f(X) = \{f(1), f(3), f(6)\} = \{a, d\}.$$

If $Y = \{a, b\}$, the preimage (inverse image) of Y is

$$f^{-1}(Y) = f^{-1}(\{a\}) \cup f^{-1}(\{b\}) = \{1, 3\} \cup \{2, 4\} = \{1, 2, 3, 4\}.$$

Example 1.5.8

1. Consider the identity relation on a nonempty set A, defined by $\Delta_A = \{(a, a) : a \in A\}$. Clearly, for each $a \in A$ there exists a unique element a in A such that $\Delta_A(a) = a$. Therefore, Δ_A is a function on A. This function is called the identity function on A, and usually written as $I : A \rightarrow A$ such that $I(a) = a$.
2. Let A be any set and $B \subseteq A$. The inclusion map of B, denoted by $\iota_B : B \rightarrow A$ and defined by $\iota_B(a) = a$ for all $a \in B$, is a function from B to A. In fact, the map ι_B is the restriction of the identity function Δ_A on the subset B.
3. The relations

$$f = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\right\} \text{ and } h = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2 - 5\right\}$$

are functions on $\mathbb{R}$ (Check!). Geometrically, the function f is the parabola x^2, and h is the same parabola shifted 5 units downwards.
4. The relation $f = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\right\}$ is not a function, as both $(0, 1)$ and $(0, -1)$ belong to f, and $1 \neq -1$. The equation $x^2 + y^2 = 1$ implies that $y = \pm\sqrt{1 - x^2}$. This means that every element x such that $x \notin \{-1, 1\}$ is related to two elements in the codomain, which violates the uniqueness condition.
5. The relation $\left\{(x, y) \in \mathbb{R} \times [0, \infty) : x^2 + y^2 = 1\right\}$ retains the uniqueness condition in the definition of functions, but it is not defined for every element of $\mathbb{R}$. For example, $(3, y)$ does not belong to the relation for any y in $(0, \infty)$, and thus, the relation is not a function.
6. The relation $\left\{(x, y) \in [-1, 1] \times [0, \infty) : x^2 + y^2 = 1\right\}$ defines a unique element $\sqrt{1 - x^2}$ in $[0, \infty)$ for every element in $[-1, 1]$. Therefore, this relation is a function that represents the top semicircle of the unit circle. Such a relation can be easily expressed as $f(x) = \sqrt{1 - x^2}$, where $-1 \leq x \leq 1$.
7. The relation $\{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x + 1\}$ defines a unique element $x + 1$ in $\mathbb{R}$ for every element $x \in \mathbb{R}$. Therefore, this relation is a function on $\mathbb{R}$ that is written as $f(x) = x + 1$.

Example 1.5.9 Let $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z} \wedge n \neq 0\}$ (Example 1.4.12). Define

$$\begin{array}{lll} f : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} & \text{and } g : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} & \text{where} \\ f(a/b,\ c/d\ ) = \frac{ad+cb}{bd} & g(a/b,\ c/d\ ) = \frac{ac}{bd} & \end{array}$$

Both f and g are functions on $\mathbb{Q} \times \mathbb{Q}$. To show this, let $(a/b, c/d)$ be an arbitrary element in $\mathbb{Q} \times \mathbb{Q}$. Since both $b \neq 0$ and $d \neq 0$, then $bd \neq 0$. Therefore, both $f(a/b, c/d)$ and $g(a/b, c/d)$ belong to $\mathbb{Q}$. To verify the uniqueness requirement, assume that $(a/b, c/d)$ and $\left(a'/b', c'/d'\right)$ are two elements in $\mathbb{Q} \times \mathbb{Q}$ such that $(a/b, c/d) = \left(a'/b', c^{'}/d'\right)$. It is necessary to show that $f(a/b, c/d) = f\left(a'/b', c^{'}/d'\right)$ and $g(a/b, c/d) = g\left(a'/b', c^{'}/d'\right)$. As $a/b = a'/b'$ and $c/d = c^{'}/d'$, then $ab' = a'b$ and $cd' = c'd$ (Example 1.4.12). Thus,

$$\begin{aligned} (ad + cb)\left(b'd'\right) &= adb'd' + cbb'd' \\ &= \left(ab'\right)\left(dd'\right) + \left(cd'\right)\left(bb'\right) \\ &= \left(a'b\right)\left(dd'\right) + \left(c'd\right)\left(bb'\right) \\ &= \left(a'd'\right)(bd) + \left(c'b'\right)(bd) \\ &= (a'd' + c'b')(bd) \end{aligned}$$

According to the definition of the equivalence relation (Example 1.4.12),

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{bd}$$

Similarly,

$$ac\left(b'd'\right) = ab'\left(cd'\right) = a'b\left(c'd\right) = a'c'(bd)$$

which implies that

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

as required.

Functions can be expressed as equations, tables, or graphs. The functions in Example 1.5.8(3) and (6) are expressed as equations. If the domain of a function is a finite set, the function can be presented in tabular form. In this representation, the inputs and the outputs are listed in different columns. For example, the function in Example 1.5.6 (1) can be represented as in Table 1.1.

If $f : A \times B \to C$ is a function in which A and B are both finite, then the outputs of f can be presented in a tabular form. If $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_m\}$, and $f : A \times B \to C$ is a function, then the outputs of f can be listed as in Table 1.2.

Table 1.1 Representation of the function in Example 1.5.6 (1)

x	$f(x)$	$(x, f(x))$
a	1	$(a, 1)$
b	1	$(b, 1)$
c	1	$(c, 1)$
d	2	$(d, 2)$

Table 1.2 Tabular representation of function on finite domain and codomain

f	a_1	a_2	$\cdots$	a_n
b_1	$f(a_1, b_1)$	$f(a_2, b_1)$	$\cdots$	$f(a_n, b_1)$
b_2	$f(a_1, b_2)$	$f(a_2, b_2)$	$\cdots$	$f(a_n, b_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
b_m	$f(a_1, b_m)$	$f(a_2, b_2)$	$\cdots$	$f(a_n, b_m)$

If the domain is a subset of the real numbers $\mathbb{R}$, or a subset of the plane $\mathbb{R}^2$, then f can be graphically visualized. The graph of a function f from A to B is the set $\{(x, f(x)) : x \in A\}$. To learn more about graphing functions, the reader can refer to (Hungerford & Shaw, 2009).

Definition 1.5.10 (Piecewise defined function) A function defined by multiple expressions is called a piecewise defined function, or simply a piecewise function. Each expression is applied to a certain part of the domain.

The following are examples of piecewise functions:

$$f(x) = \begin{cases} 2 & x \geq 7 \\ -x^2 + 1 & x < 7 \end{cases} \qquad g(x) = \begin{cases} x & x > 0 \\ 5 & x = 0 \\ -1 & x < 0 \end{cases} \qquad h(x) = |x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Definition 1.5.11 (*Composition of functions*) Let A, B, H and K be any sets. Let $f : A \to B$ and $g : H \to K$ be two functions such that $Rang(f) \subseteq D(g)$. The composition of f and g is the function.

$$g \circ f : A \longrightarrow K, \text{ where } g \circ f(x) = g(f(x)).$$

It is left to the reader (Exercise 1.21) to verify that a composition of two functions is a function.

Example 1.5.12 Let $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x - 1$, and let $g : \mathbb{R} \to \mathbb{R}$, where $g(x) = x^2$. The corresponding compositions are.

$$g \circ f(x) = g(f(x)) \underset{g(z)=z^2}{=} (f(x))^2 \underset{f(x)=x-1}{=} (x-1)^2 = x^2 - 2x + 1.$$

and

$$f \circ g(x) = f(g(x)) \underset{f(z)=z-1}{=} g(x) - 1 = x^2 - 1.$$

Clearly, $g \circ f$ and $f \circ g$. are not equal.

Note that for $g \circ f$ to be defined, the range of f must be a subset of the domain of g. Otherwise, the composition cannot be defined. For example, if $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x - 1$ and $g : \left(\mathbb{R}^+ \cup \{0\}\right) \to \mathbb{R}$ is defined by $g(x) = \sqrt{x}$, then the composition $g \circ f$ cannot be donfined at $x = 0$ (Verify!).

The following proposition can be obtained by applying the composition of two functions twice.

Proposition 1.5.13 *Let A, B and C be any three sets. If $f : A \to B$, $g : B \to C$, and $h : C \to D$ are three functions such that $Rang(f) \subseteq D(g)$ and $Rang(g) \subseteq D(h)$, then*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Definition 1.5.14 (Injective and surjective functions) Let A and B be two sets. Let $f : A \to B$ be a function. The map f is called

1. Injective (one-to-one) if $x \neq y \Rightarrow f(x) \neq f(y)$ for all $x, y \in A$. Equivalently,

$$f(x) = f(y) \Rightarrow x = y \text{ for all } x, y \in A.$$

2. Surjective (onto) if for each $y \in B$, there exists an $x \in A$ such that $f(x) = y$.
3. Bijective if f is both injective and surjective.

Example 1.5.15

1. The map $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x$, is an injective and a surjective map, so it is bijective.
2. The map $g : \mathbb{R} \to \mathbb{R}$, where $g(x) = x^2$, is neither injective nor surjective. However, we can obtain injective or surjective functions from g by restricting the domain or codomain. For example,
   - The map $g_1 : \mathbb{R} \to \mathbb{R}^+$, where $g_1(x) = x^2$, is surjective but not injective.
   - The map $g_2 : \mathbb{R}^+ \to \mathbb{R}$, where $g_2(x) = x^2$, is injective but not surjective.
   - The map $g_3 : \mathbb{R}^+ \to \mathbb{R}^+$, where $g_3(x) = x^2$, is both injective and surjective. Therefore, this map is bijective.

For the proof of the following lemma, see Exercise 1.6.

Lemma 1.5.16 *Let A and B be two finite sets such that $|A| = |B|$, and let $f : A \to B$ be a function. The map f is injective if and only if it is surjective.*

Example 1.5.17 For $n \in \mathbb{N}$, let $s, t \in \{1, 2, \ldots, n\}$ and $\mathcal{R}_{s,t} : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ be defined as

$$\mathcal{R}_{s,t}(k) = \begin{cases} k \; k \neq s \wedge k \neq t \\ t \;\; k = s \\ s \;\; k = t \end{cases}$$

Clearly, the map $\mathcal{R}_{\mathrm{s,t}}$ is defined for any element in $\{1, 2, \ldots, n\}$, and any element in the domain has a unique image under $\mathcal{R}_{\mathrm{s,t}}$. Hence, it is a function on $\{1, 2, \ldots, n\}$. To show that $\mathcal{R}_{\mathrm{s,t}}$ is an injective map, let k, k' be elements in $\{1, 2, \ldots, n\}$ such that $\mathcal{R}_{s,t}(k) = \mathcal{R}_{s,t}\big(k'\big)$.

- If $k \neq s \wedge k \neq t$, then $k = \mathcal{R}_{s,t}(k) = \mathcal{R}_{s,t}\big(k'\big)$, which implies that $k = k'$.
- If $k = s$, then $t = \mathcal{R}_{s,t}(k) = \mathcal{R}_{s,t}\big(k'\big)$, which implies that $k' = s = k$.
- If $k = t$, then $s = \mathcal{R}_{s,t}(k) = \mathcal{R}_{s,t}\big(k'\big)$, which implies that $k' = t = k$.

In all cases $k' = k$. Thus, $\mathcal{R}_{s,t}$ is injective. By Lemma 1.5.16, the map $\mathcal{R}_{s,t}$ is also surjective.

The map $\mathcal{R}_{s,t}$ permutes the two elements s and t.Consequently, it is known as a "transposition". The following proposition is proved in Chap 6.

Proposition 1.5.18 *Any bijective map on* $\{1, 2, \ldots, n\}$ *is a composition of transpositions.*

Definition 1.5.19 (*Invertible function*) Let A and B be two sets. A function $f : A \to B$ is said to be invertible if there exists a function $g : B \to A$ such that $g \circ f = \iota_A$ and $f \circ g = \iota_B$. The map g is called the inverse of f and is denoted by f^{-1}.

The conditions $g \circ f = \iota_A$ and $f \circ g = \iota_B$ means $(a, b) \in f \Leftrightarrow (b, a) \in g$. This relation can be intuitively expressed as follows: if f connects a to b, then g returns b to its preimage a, and vice versa. There are many examples of noninvertible functions. For example, the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not invertible. If f was invertible, then there would exist $g : \mathbb{R} \to \mathbb{R}$ such that

$$f \circ g(x) = (g(x))^2 = x$$

which implies that $g(x) = \pm\sqrt{x}$, i.e., g takes either the value of $\sqrt{x}$ or $-\sqrt{x}$, and thus, is not a function. In addition, g is not defined for the negative real numbers.

Theorem 1.5.20 Let $f : A \to B$ be a function. The map f is invertible if and only if it is a bijective map.

According to the Theorem above, to show that a map $f : A \to B$ is bijective, it suffices to show that there exists a map $g : B \to A$ such that $g \circ f = \iota_A$ and $f \circ g = \iota_B$ (Exercise 1.8).

Example 1.5.21

1. Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x + 1$, then f is a bijective map and is thus invertible. To find its inverse, let $y = f(x)$, and solve for x as follows: $y = 2x + 1 \Leftrightarrow x = (y - 1)/2$. Interchanging x and y yields $y = (x - 1)/2$. Hence, the inverse of $f(x)$ is the map $g(x) = (x - 1)/2$. It can be verified that $f \circ g(x) = x = g \circ f(x)$. Therefore, g is the inverse of f.
2. Let $f : \mathbb{R} \to [-1, 1]$ be defined as $f(x) = \cos x$. Since $\cos\left(\frac{\pi}{4}\right) = \cos\left(\frac{-\pi}{4}\right)$, then f is not one to one, hence it is not invertible. However, if the domain of $\cos x$ is restricted to be $0 \leq x \leq \pi$, then $\cos x$ will be invertible, with the inverse $g(x) = \cos^{-1} x$. The domain of g is $[-1, 1]$.

1.6 Matrices

This section focuses on matrices, a type of maps that can be presented using arrays. Many functions on matrices, such as matrix addition and matrix multiplication are defined and briefly discussed. For additional information and proofs, the reader can refer to (Burton, 2007) and (Hartman, 2011).

Definition 1.6.1 Let $m, n \in \mathbb{N}$, and let K be any set. A K-matrix of type $m \times n$ (read m by n) is a map

$$A : \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \to K$$

that assigns an element a_{ij} in K for each $(i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$.

Such a map can be presented as a rectangular array with m rows and n columns in the following form:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

where $A((i, j)) = a_{ij} \in K$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$.

If there is no risk of ambiguity, a K-matrix is simply referred to as a matrix. If a formula for the elements a_{ij} is given, the matrix can be written as $\left(a_{ij}\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ or simply $\left(a_{ij}\right)$. Here, the elements a_{ij} are called the entries of the matrix A, and the integers m and n are called the dimensions of the matrix A. A matrix that consists of m rows and n columns is called an $m \times n$ matrix. The set of all $m \times n$ matrices with entries in K is denoted by $\mathcal{M}_{mn}(K)$. The set $\mathcal{M}_{nn}(K)$ can be abbreviated to $\mathcal{M}_n(K)$. A matrix in $\mathcal{M}_n(K)$ is called a square matrix of dimension n. The entries a_{ii} in a square matrix are called diagonal entries.

Example 1.6.2

1. The set $\mathcal{M}_{3\times 2}(\mathbb{Z})$ consists of all 3×2 matrices with integers entries.
2. The set $\mathcal{M}_{5\times 1}(\mathbb{R})$ consists of all 5×1 matrices with real entries, and such matrices have the form

$$\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ a_{41} \\ a_{51} \end{pmatrix}$$

where a_{i1} is an element in $\mathbb{R}$. This matrix can be considered an element in $\mathbb{R}^5$. In fact, there exists a bijection map between $\mathcal{M}_{5\times 1}(\mathbb{R})$ and $\mathbb{R}^5$. In general, an $n \times 1$ matrix consists of one column in the form

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{(n-1)1} \\ a_{n1} \end{pmatrix}$$

This matrix can be identified with an element in $\mathbb{R}^n$.
3. A $1 \times n$ matrix consisting of one row can be expressed as

$$\begin{pmatrix} a_{11} \; a_{12} \cdots a_{1(n-1)} \; a_{1n} \end{pmatrix}$$

and identified with an element in $\mathbb{R}^n$.
4. The set $\mathcal{M}_7(\mathbb{C})$ consists of all square matrices of dimension 7 with complex entries.
5. Let $X = \{a, b, c\}$. The set $\mathcal{M}_{3\times 2}(\mathcal{P}(X))$ consists of all 3×2 matrices whose entries are subsets of X. An example of a matrix in $\mathcal{M}_{3\times 2}(\mathcal{P}(X))$ is

$$\begin{pmatrix} \{a, b\} & \{b, c\} \\ \emptyset & \{b\} \\ \{a, c\} & \{a\} \end{pmatrix}$$

Definition 1.6.3 Let $n \in \mathbb{N}$, and let $K \neq \emptyset$ be a subset of $\mathbb{C}$ such that K contains 0 and 1. Let $\mathcal{M}_n(K)$ be the set of square matrices of dimension n over K.

1. A matrix $\left(a_{ij}\right) \in \mathcal{M}_n(K)$ with entries $a_{ij} = 0$ whenever $i \neq j$ can be expressed as

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

This matrix is called a diagonal matrix. The set of all diagonal matrices in $\mathcal{M}_n(K)$ is denoted by $D(K)$. A diagonal matrix with all diagonal entries are equal to 1 is called a unit matrix, denoted by I_n.

$$I_n = \left(a_{ij}\right) \text{ where } a_{ij} = \begin{cases} 1 \, if \; i = j \\ 0 \, if \; i \neq j \end{cases}$$

A notable example of diagonal matrices is the subset $\{A \in \mathcal{M}_n(\mathbb{C}) : A = \lambda I_n\}$ in which all the diagonal elements are equal.

2. A matrix $\left(a_{ij}\right) \in \mathcal{M}_n(K)$ with entries $a_{ij} = 0$ whenever $i > j$ can be expressed as

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & a_{24} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & a_{34} & \cdots & a_{3n} \\ \vdots & \vdots & 0 & a_{44} & \cdots & a_{4n} \\ 0 & 0 & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

This matrix is called an upper triangular matrix. The set of all upper triangle matrices over K is denoted by $U(K)$. i.e.,

$$U(K) = \left\{\left(a_{ij}\right) \in \mathcal{M}_n(K) : a_{ij} = 0 \quad \forall \; i > j\right\}$$

3. A matrix $\left(a_{ij}\right) \in \mathcal{M}_n(K)$ with all its entries $a_{ij} = 0$ whenever $i < j$ is in the form

$$\begin{pmatrix} a_{11} & 0 & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & 0 & \cdots & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \cdots & a_{nn} \end{pmatrix}.$$

This matrix is called a lower triangular matrix. The set of all lower triangle matrices over K is denoted by $L(K)$. i.e.,

$$L(K) = \{(a_{ij}) \in \mathcal{M}_n(K) : a_{ij} = 0 \quad \forall\ i < j\}.$$

In the following, we define several algebraic operations on matrices. For the remainder of this chapter, the set K denotes a nonempty subset of the complex numbers $\mathbb{C}$ such that.

1. K contains 0 and 1.
2. K is closed under the usual addition on $\mathbb{C}$, the usual multiplication on $\mathbb{C}$, and the conjugation.

Definition 1.6.4 Let $m, n \in \mathbb{N}$. Let $\mathcal{M}_{mn}(K)$ be the set of $m \times n$ matrices with K-entries. Let $A = (a_{ij})$ and $B = (b_{ij})$ be two matrices in $\mathcal{M}_{mn}(K)$.

1. For any $c \in K$, the multiplication of the matrix A by any constant c is the matrix cA obtained from A by multiplying each entry by c, i.e., $cA = (ca_{ij})$.
2. The addition of A and B is the matrix $A + B$ obtained from A and B by adding the entries of A and B that have the same indices i and j. That is,

$$A + B = (a_{ij} + b_{ij})$$

where $a_{ij} + b_{ij}$ is the usual sum of the complex numbers a_{ij} and b_{ij}.

Note that matrices with two different dimensions cannot be added. For example, a 2 × 3 matrix and a 4 × 7 matrix cannot be added. Therefore, matrix addition is defined only for matrices with the same dimensions.

Example 1.6.5

1. The matrices

$$A = \begin{pmatrix} 2 & -3 & 7 \\ 3 & 2 & 4 \end{pmatrix}, B = \begin{pmatrix} -3 & 5 & -5 \\ -1 & 2 & -2 \end{pmatrix}$$

are elements in $\mathcal{M}_{2\times3}(\mathbb{Z})$. Multiplying these matrices by 2 and 0 respectively, yields

$$2A = 2\begin{pmatrix} 2 & -3 & 7 \\ 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 4 & -6 & 14 \\ 6 & 4 & 8 \end{pmatrix}, 0B = 0\begin{pmatrix} -3 & 5 & -5 \\ -1 & 2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The sum $A + B$ is $\begin{pmatrix} -1 & 2 & 2 \\ 2 & 4 & 2 \end{pmatrix}$.

2. The matrices

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are elements in $\mathcal{M}_{2\times 2}(\mathbb{C})$. Any matrix $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ in $\mathcal{M}_{2\times 2}(\mathbb{C})$ can be expressed using such matrices, as follows:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22} = \sum_{i=1}^{2}\sum_{j=1}^{2} a_{ij}E_{ij}.$$

3. In general, a matrix $\left(a_{ij}\right)$ in $\mathcal{M}_{mn}(\mathbb{C})$ can be expressed as

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}$$

where $E_{ij} = (a_{kl})$ in $\mathcal{M}_{m\times n}(\mathbb{C})$ with $a_{kl} = \begin{cases} 1 \; if \; k = i \wedge l = j \\ 0 \quad \text{elsewhere} \end{cases}$

Definition 1.6.6 Let $m, n, l \in \mathbb{N}$. Let $A = \left(a_{ij}\right) \in \mathcal{M}_{mn}(K)$ and $B = \left(b_{ij}\right) \in \mathcal{M}_{nl}(K)$. The product of A and B is the matrix $AB \in \mathcal{M}_{ml}(K)$, defined as $\left(c_{ij}\right)$, where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

In this definition, the entry c_{ij} is formed using the i-th row in A and the j-th column in B entries. i.e.,

$$c_{ij} = \left(a_{i1} \; a_{i2} \ldots \; a_{in}\right) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{rj} \end{pmatrix} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Note that matrix multiplication can be performed if and only if the number of columns in the left matrix equals the number of rows in the right matrix. The multiplication of square matrices is only defined if the two matrices have the same dimension. If A is an $m \times n$ matrix and B is an $n \times l$ matrix, then their product $A \cdot B$ is an $m \times l$ matrix. We will also use AB to denote the multiplication $A \cdot B$ of any two matrices A and B.

Example 1.6.7

1. Let $A = \begin{pmatrix} 1 & -3 \\ 4 & 1 \\ 0 & 7 \end{pmatrix} \in \mathcal{M}_{3\times 2}(\mathbb{Z})$ and $B = \begin{pmatrix} 2 & 6 & 7 \\ -3 & 2 & 4 \end{pmatrix} \in \mathcal{M}_{2\times 3}(\mathbb{Z})$.

$$AB = \begin{pmatrix} 11 & 0 & -5 \\ 5 & 26 & 32 \\ -21 & 14 & 28 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}) \text{ and } BA = \begin{pmatrix} 26 & 49 \\ 5 & 39 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}).$$

2. Let $A = \begin{pmatrix} 1 & 5 \\ 6 & -1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z})$ and $B = \begin{pmatrix} 6 & 1 & 0 \\ -2 & 3 & 3 \end{pmatrix} \in \mathcal{M}_{2\times 3}(\mathbb{Z})$.

   $AB = \begin{pmatrix} -4 & 16 & 15 \\ 38 & 3 & -3 \end{pmatrix} \in \mathcal{M}_{2\times 3}(\mathbb{Z})$ and BA is not possible.

3. Let $E_{ij} \in \mathcal{M}_{mn}(\mathbb{C})$ and $E_{ks} \in \mathcal{M}_{nl}(\mathbb{C})$ be defined as in Example 1.6.5 (3). It is straightforward to show that $E_{ij}E_{ks} = \delta_{jk}E_{is}$, where $\delta_{jk} = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases}$.

Proposition 1.6.8 *Let $m, n \in \mathbb{N}$. The matrix addition $+ : \mathcal{M}_{mn}(K) \times \mathcal{M}_{mn}(K) \to \mathcal{M}_{mn}(K)$ and the matrix multiplication $\cdot : \mathcal{M}_n(K) \times \mathcal{M}_n(K) \to \mathcal{M}_n(K)$ are both functions.*

Proof Let $(A, B) \in \mathcal{M}_{mn}(K) \times \mathcal{M}_{mn}(K)$ be an arbitrary element. As all elements in $\mathcal{M}_{mn}(K)$ are of the same type, then the addition of A and B is defined. To verify the uniqueness requirement, assume that (A, B) and (A', B') are elements in $\mathcal{M}_{mn}(K) \times \mathcal{M}_{mn}(K)$ such that $(A, B) = (A', B')$. According to the equality of the order pairs, $A = A'$ and $B = B'$, which implies that.

$$+(A, B) = A + B = A' + B' = +(A', B')$$

Thus, the matrix addition identifies a unique element in $\mathcal{M}_{mn}(K)$ for each pair of matrices in $\mathcal{M}_{mn}(K) \times \mathcal{M}_{mn}(K)$.

For the matrix multiplication, if $(A, B) \in \mathcal{M}_n(K) \times \mathcal{M}_n(K)$, then A and B are square matrices of the same dimension. The multiplication of A and B is defined and yields a square matrix of dimension n. To verify the uniqueness requirement, assume that (A, B) and (A', B') are elements in $\mathcal{M}_n(K) \times \mathcal{M}_n(K)$ such that $(A, B) = (A', B')$. According to the equality of the order pairs, $A = A'$ and $B = B'$, which implies that $a_{ik} = a^{'}_{ik}$ and $b_{kj} = b^{'}_{kj}$ for all $1 \leq i, j \leq n$, i.e.,

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a^{'}_{ik}b^{'}_{kj}$ is the ij-entry in the multiplication $A'B'$.

Thus,

$$\cdot(A, B) = AB = A'B' = \cdot(A', B')$$

Therefore, the matrix multiplication identifies a unique element in $\mathcal{M}_n(K)$ for each pair of matrices in $\mathcal{M}_n(K) \times \mathcal{M}_n(K)$. ■

Proposition 1.6.9 *Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all square matrices of dimension n.*

1. *The multiplication of two diagonal matrices is a diagonal matrix. If A and B are diagonal matrices, then $AB = BA$.*
2. *The multiplication of two upper matrices is an upper matrix.*
3. *The multiplication of two lower matrices is a lower matrix.*

Proof

1. Assume that A and B are arbitrary matrices in $D(K)$. The multiplication $A \cdot B$ is $\left(c_{ij}\right)$ where

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

For $s \neq t$, $a_{st} = b_{st} = 0$, which implies that for $i \neq j$,

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \underset{k \neq i \Rightarrow a_{ik}=0}{=} a_{ii} b_{ij} \underset{i \neq j \Rightarrow b_{ij}=0}{=} 0$$

i.e., AB is a diagonal matrix. Similarly, BA is a diagonal matrix. The diagonal entries in AB are

$$c_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} \underset{k \neq i \Rightarrow a_{ik}=0}{=} a_{ii} b_{ii}$$

which are also the diagonal entries in BA as

$$\sum_{k=1}^{n} b_{ik} a_{ki} \underset{k \neq i = b_{ik}=0}{=} b_{ii} a_{ii} = a_{ii} b_{ii}$$

2. Assume that A and B are arbitrary matrices in $U(K)$. The multiplication AB is (c_{ij}) where

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

As for $s > t$, $a_{st} = b_{st} = 0$, then for $i > j$

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \underset{k < i \Rightarrow a_{ik}=0}{=} \sum_{k=i}^{n} a_{ik} b_{kj} \underset{k \geq i > j \Rightarrow b_{kj}=0}{=} 0.$$

That is, AB is an upper matrix.

3. Similar to (2). ■

Many functions that can be defined on matrices, several of which are introduced below.

Definition 1.6.10 (*The conjugate map*) Let $m, n \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K. Define the map

$$\begin{aligned}\mathcal{M}_{mn}(K) &\longrightarrow \mathcal{M}_{mn}(K)\\ (a_{ij}) &\mapsto (\overline{a}_{ij})\end{aligned}$$

where $\overline{a}_{ij}$ is the complex conjugate of a_{ij}. This map is called the conjugate map. The conjugate of a matrix A is denoted by $\overline{A}$.

It is clear that for any matrix $A \in \mathcal{M}_{mn}(\mathbb{R})$, $A = \overline{A}$. The conjugate of a matrix over $\mathbb{C}$ can be computed using the conjugates of complex numbers as in the following example:

$$\text{If } A = \begin{pmatrix} 1+3i\ 2 & 2-i \\ 5i & -1\ 6+7i \end{pmatrix} \in \mathcal{M}_{2\times 3},\ \text{then } \overline{A} = \begin{pmatrix} 1-3i\ 2 & 2+i \\ -5i & -1\ 6-7i \end{pmatrix}$$

The complex conjugate of a complex number $x + iy$ is $x - iy$. The following propositions are straightforward.

Proposition 1.6.11 *Let $m, n, l \in \mathbb{N}$. Let $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K, and $\mathcal{M}_{nl}(K)$ be the set of all $n \times l$ matrices over K. For $A \in \mathcal{M}_{mn}(K)$ and $B \in \mathcal{M}_{nl}(K)$,*

$$\overline{\overline{A}} = A, \quad \text{and} \quad \overline{AB} = \overline{A}\,\overline{B}$$

Proposition 1.6.12 *Let $m, n \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices overK. The conjugate map is a function on $\mathcal{M}_{mn}(K)$.*

The second example of a function on matrices is the transpose map, which exchanges the rows of a matrix with its columns.

Definition 1.6.13 (The transpose map) Let $m, n \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K. The map

$$\begin{aligned}T : \mathcal{M}_{mn}(K) &\longrightarrow \mathcal{M}_{nm}(K)\\ (a_{ij}) &\mapsto (a_{ji})\end{aligned}$$

is called the transpose map. The transpose of a matrix A is denoted by A^T.

The reader can easily check that $(8)^T = (8)$, $(1\ 2)^T = \begin{pmatrix}1\\2\end{pmatrix}$, $\begin{pmatrix}1\ 2\\3\ 4\end{pmatrix}^T = \begin{pmatrix}1\ 3\\2\ 4\end{pmatrix}$, and

$$\begin{pmatrix} 1 & -3 \\ 4 & 1 \\ 0 & 7 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 & 0 \\ -3 & 1 & 7 \end{pmatrix}$$

Proposition 1.6.14 *Let $m, n \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K. The transpose map is a function from $\mathcal{M}_{mn}(K)$ to $\mathcal{M}_{nm}(K)$, which satisfies the following statements:*

1. $\left(A^T\right)^T = A$
2. *For all* $\alpha \in \mathbb{C}$, $(\alpha A)^T = \alpha A^T$
3. $(A + B)^T = A^T + B^T$

for any $A, B \in \mathcal{M}_{mn}(K)$.

Proposition 1.6.15 *Let $m, n, l \in \mathbb{N}$. For any $A \in \mathcal{M}_{mn}(K)$ and $B \in \mathcal{M}_{nl}(K)$,*

$$(AB)^T = B^T A^T.$$

Definition 1.6.16 (*The Hermitian conjugate map*) Let $m, n \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K. The map

$$\begin{aligned} * : \mathcal{M}_{mn}(K) &\longrightarrow \mathcal{M}_{nm}(K) \\ \left(a_{ij}\right) &\mapsto \left(\overline{a}_{ji}\right) \end{aligned}$$

is called the Hermitian conjugate map. The entry $\overline{a}_{ji}$ is the element in K obtained by taking the conjugate of the element a_{ji} in the transpose matrix of (a_{ij}). The Hermitian conjugate of a matrix A is denoted by A^*.

For any $n \in \mathbb{N}$, the Hermitian conjugate of I_n is I_n. The Hermitian conjugate map is a composition of the conjugate and the transpose maps ($A^* = \overline{A}^T$ for any matrix A in $\mathcal{M}_{mn}(K)$). Therefore, the Hermitian conjugate is a function. It is also known by conjugate transpose, or Hermitian transpose map. The following proposition is straightforward.

Proposition 1.6.17 *Let $m, n, l \in \mathbb{N}$ and $\mathcal{M}_{mn}(K)$ be the set of all $m \times n$ matrices over K. For $A \in \mathcal{M}_{mn}(K)$ and $B \in \mathcal{M}_{nl}(K)$.*

$$\left(A^*\right)^* = A, \quad (AB)^* = B^* A^*.$$

The following functions are defined only on square matrices.

Definition 1.6.18 (*The trace map*) Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. The trace map is defined as

$$\begin{aligned} \text{trace: } \mathcal{M}_n(K) &\longrightarrow \mathbb{C} \\ A &\mapsto \sum_{i=1}^{n} a_{ii} \end{aligned}$$

Proposition 1.6.19 *Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. The $trace : \mathcal{M}_n(K) \to \mathbb{C}$ is a function that satisfies the following statements:*

1. $\text{trace}\left(A^T\right) = \text{trace}(A)$
2. $\text{trace}(A + B) = \text{trace}(A) + \text{trace}(B)$
3. $\text{trace}(AB) = \text{trace}(BA)$

for all $A, B \in \mathcal{M}_n(K)$.

Definition 1.6.20 (*The determinant map*) Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. Let $\det : \mathcal{M}_n(K) \to \mathbb{C}$ be the recursive map defined for square matrices as

1. $\det((c)) = c$(determinant of 1×1 matrix is the entry of such matrix).
2. For any $A \in \mathcal{M}_n(K)$, such that $n \geq 2$,

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A_{ik})$$

where i is any integer such that $1 \leq i \leq n$, and A_{ik} is the matrix obtained from A by deleting row i and column k.

In some linear algebra books, the notation $|A|$ is used instead of $\det(A)$. Throughout this book, $\det(A)$ is used to denote the determinant of A

Remarks 1.6.21 In the abovementioned definition, a fixed row i is chosen, and the entries of the row are used to compute the determinant of the matrix A. The determinant can also be defined using a fixed column j and the entries of this column, as follows:

- $\det((c)) = c$ (determinant of 1×1 matrix is the entry of such matrix).
- For any $A \in \mathcal{M}_n(K)$ such that $n \geq 2$,

$$\det(A) = \sum_{k=1}^{n} (-1)^{j+k} a_{kj} \det\left(A_{kj}\right)$$

where j is any integer such that $1 \leq j \leq n$, and A_{kj} is the matrix obtained from A by deleting row k and column j.

Example 1.6.22

1. Consider an arbitrary matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathcal{M}_2(K)$. To find the determinant of A, either a row or a column must be selected. Using the first row, we have

$$\det(A) = \sum_{k=1}^{2} (-1)^{1+k} a_{1k} \det(A_{1k}) = (-1)^2 a \det((d)) + (-1)^3 b \det((c))$$

$$= ad - bc$$

For example,
$\det\left(\begin{pmatrix} 2 & 7 \\ -3 & 5 \end{pmatrix}\right) = 10 - (-21) = 31$ and

$$\det\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = \cos\theta^2 + \sin\theta^2 = 1 \text{ for any angle } \theta.$$

2. Consider an arbitrary matrix $A = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix}$ in $\in \mathcal{M}_3(K)$. To compute the determinant of A, either a row or a column must be selected. Choosing the first column this time,

$$\det(A) = \sum_{k=1}^{n} (-1)^{1+k} a_{k1} \det(A_{k1})$$

i.e., $\det(A)$ is

$$(-1)^2 x_1 \det\left(\begin{pmatrix} y_2 & z_2 \\ y_3 & z_3 \end{pmatrix}\right) - x_2 \det\left(\begin{pmatrix} y_1 & z_1 \\ y_3 & z_3 \end{pmatrix}\right) + x_3 \det\left(\begin{pmatrix} y_1 & z_1 \\ y_2 & z_2 \end{pmatrix}\right)$$

$$= x_1(y_2z_3 - z_2y_3) - x_2(y_1z_3 - z_1y_3) + x_3(y_1z_2 - z_1y_2).$$

Notably, the choice of the column or row in calculating the determinant determines the ease of the calculation. For example, the second row is the optimal choice to calculate the determinant of

$$\begin{pmatrix} 1 & 5 & 1 \\ 2 & 0 & 0 \\ 3 & 2 & 7 \end{pmatrix}$$

because the second row contains many zero entries. Using the second row, we obtain

$$\det\begin{pmatrix} 1 & 5 & 1 \\ 2 & 0 & 0 \\ 3 & 2 & 7 \end{pmatrix} = -2\det\left(\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}\right) + 0 + 0 = -2(35 - 2) = -66$$

Proposition 1.6.23 *Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. Let $A, B \in \mathcal{M}_n(K)$ be arbitrary matrices. The map* $\det : \mathcal{M}_n(K) \to \mathbb{C}$ *is a function that satisfies*

1. $\det(A) = \det(A^T)$
2. $\det(kA) = k^n \det(A)$
3. $\det(A \cdot B) = \det(A) \cdot \det(B)$.

The abovementioned functions are used to create special subsets of $\mathcal{M}_n(K)$. These subsets have important applications in algebra and other mathematical fields. We briefly mention them below.

Definition 1.6.24 Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K.

1. A matrix $A \in \mathcal{M}_n(K)$ is called an orthogonal matrix if $A \cdot A^T = A^T \cdot A = I_n$. The subset of all orthogonal matrices is denoted by $O(n, K)$, or simply, $O(n)$. i.e.,

$$O(n) = \left\{A \in \mathcal{M}_n(K) : A \cdot A^T = A^T \cdot A = I_n\right\}.$$

2. A matrix $A \in \mathcal{M}_n(K)$ is called a unitary matrix if $A \cdot A^* = A^* \cdot A = I_n$. The subset of all unitary matrices is denoted by $U(n, K)$, or simply $U(n)$. i.e.,

$$U(n) = \left\{A \in \mathcal{M}_n(K) : A \cdot A^* = A^* \cdot A = I_n\right\}.$$

Notation 1.6.25 Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K.

1. The set of all matrices in $\mathcal{M}_n(K)$ whose determinant is not zero is denoted by $GL(n, K)$ or $GL_n(K)$. i.e.,

$$GL_n(K) = \{A \in \mathcal{M}_n(K) : \det(A) \neq 0\}.$$

2. The set of all matrices in $\mathcal{M}_n(K)$ whose determinant equals 1 is denoted by $SL(n, K)$ or $SL_n(K)$. i.e.,

$$SL_n(K) = \{A \in \mathcal{M}_n(K) : \det(A) = 1\}.$$

In the following, we discuss the invertibility of a square matrix. The invertibility of a matrix is not defined if the matrix is not a square matrix.

Definition 1.6.26 (Invertible matrices) Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. Let A be a matrix in $\mathcal{M}_n(K)$. The matrix A is said to be invertible if there exists a matrix $B \in \mathcal{M}_n(K)$ such that $AB = BA = I_n$. The matrix B (if it exists) is called the inverse of A and is denoted by A^{-1}.

Not every matrix in $\mathcal{M}_n(K)$ is invertible. For example, the zero matrix $0_n = (0)$ belongs to $\mathcal{M}_n(K)$, but no matrix in $\mathcal{M}_n(K)$ satisfies $0_n B = B\, 0_n = I_n$. Therefore,

$$\begin{aligned} \mathcal{M}_n(K) &\longrightarrow \mathcal{M}_n(K) \\ A &\mapsto A^{-1} \end{aligned}$$

is not a function on $\mathcal{M}_n(K)$. To define a formula for the inverse of an invertible matrix, the following definition is needed.

Definition 1.6.27 Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. The adjugate matrix of a matrix A in $\mathcal{M}_n(K)$ is the matrix computed from A as follows:

$$\mathrm{Adj}(A) = \left((-1)^{i+j} A_{ij}\right)^T$$

where A_{ij} is the determinant of the matrix obtained from A by deleting the i th row and the j th columnn.

Proposition 1.6.28 *Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. A matrix A in $\mathcal{M}_n(K)$ is invertible if and only if $det(A) \neq 0$. In this case,*

$$A^{-1} = \frac{1}{\det(A)} \mathrm{Adj}(A)$$

where $Adj(A)$ is the adjugate matrix of A.

Proposition 1.6.29 *Let $n \in \mathbb{N}$ and $\mathcal{M}_n(K)$ be the set of all $n \times n$ matrices over K. If A and B are invertible matrices in $\mathcal{M}_n(K)$, then $(AB)^{-1} = B^{-1}A^{-1}$.*

1.7 Geometric Transformations and Symmetries in the Plane

The rotation and reflection are two important basic transformations that operate on a plane (generally in $\mathbb{R}^n$). This section will study R_θ, the rotation around the origin with angle θ, and l_θ, the reflection of a line passing through the origin, inclined at an angle θ from the x-axis. Any other rotation or reflection of a line (in the plane) can be defined using either R_θ or l_θ. Readers can refer to (Boyd & Vandenberghe, 2018) for more details regarding geometric transformations and vectors in the plane. As mentioned in Example 1.6.2, there exists a correspondence between the points in $\mathbb{R}^n$ and the $n \times 1$ matrices with real entries. By restricting the study to $\mathbb{R}^2$, this correspondence can be expressed in the following lemma.

Lemma 1.7.1 *The map.*

$$\begin{aligned} g : \mathbb{R}^2 &\longrightarrow \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\} \\ (x, y) &\mapsto \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

is a bijection map identifying the points in $\mathbb{R}^2$ with the matrices in $\mathcal{M}_{2\times 1}(\mathbb{R})$.

Using this lemma, any function on the plane can be defined directly on the matrices $\mathcal{M}_{2\times 1}(\mathbb{R})$.

Reminder 1.7.2 Any point P in the plane can be represented using at least two coordinate systems of the plane:

1. The Cartesian coordinates of $P = (x, y)$, where x and y are given by the projections of the point P on the x-axis and y-axis, respectively.
2. The polar coordinates of $P = (r, \psi)$, where r is the distance from P to the origin of the plane, and ψ is the angle that the line $\overrightarrow{OP}$ makes with x-axis.

The relations between the two representations are given by the following equations

$$x = r\cos\psi,\ y = r\sin\psi,\ r^2 = x^2 + y^2,\ y = x\tan\psi$$

Recall that a rotation around the origin with an angle θ in the plane changes the polar coordinates of a point from (r, ψ) to $(r, \psi + \theta)$. According to the next proposition, a rotation by θ around the origin is represented by a matrix multiplication, which will be denoted by R_θ. The matrix R_θ is called the rotation matrix by θ.

Proposition 1.7.3 *The rotation of the point* (x, y) *in the plane around the origin with an angle* θ *is equivalent to the function.*

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto R_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

where $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

Proof Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation by an angle θ around the origin. The rotation f moves the point $(x, y) = (rcos\psi, rsin\psi)$ to $\left(x', y'\right) = (r\cos(\psi + \theta), r\sin(\psi + \theta))$. Thus, the coordinates after the rotation are

$$x' = r\cos(\psi + \theta) = (r\cos\psi)\cos\theta - (r\sin\psi)\sin\theta = x\cos\theta - y\sin\theta$$

and

$$y' = r\sin(\psi + \theta) = (r\cos\psi)\sin\theta + (r\sin\psi)\cos\theta = x\sin\theta + y\cos\theta.$$

These equations can be expressed as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

The following proposition matches the expected geometrical fact that “rotation by an angle θ followed by rotation by an angle β is equivalent to a rotation by $\theta+\beta$ ”. ■

Proposition 1.7.4 *Let θ and β be any two angles. Then,*

$$R_{\theta+\beta} = R_\theta R_\beta = R_\beta R_\theta .$$

Proof According to the identities for the trigonometric functions,

$$R_{\theta+\beta} = \begin{pmatrix} \cos(\theta+\beta) & -\sin(\theta+\beta) \\ \sin(\theta+\beta) & \cos(\theta+\beta) \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta\cos\beta - \sin\theta\sin\beta & -(\sin\theta\cos\beta + \cos\theta\sin\beta) \\ \sin\theta\cos\beta + \cos\theta\sin\beta & \cos\theta\cos\beta - \sin\theta\sin\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} = R_\theta R_\beta .$$

Similarly, $R_{\beta+\theta} = R_\beta R_\theta$. The result follows as $\theta+\beta = \beta+\theta$. ■

Example 1.7.5

1. According to Proposition 1.7.3,
   - The rotation matrix by 0 is $R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.
   - The rotation matrix by $\frac{\pi}{2}$ is $R_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
   - The rotation matrix by π is $R_\pi = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$.

     R_n can also be computed using Proposition 1.7.4, to obtain the same answer.
   - Proposition 1.7.4 can be used to obtain
     - $R_{3\pi/2} = R_{\pi/2}R_\pi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,
     - $R_{2\pi} = R_{\pi/2}R_{3\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. Similarly, $R_{\pi/3} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$, $R_{2\pi/3} = R_{\pi/3}R_{\pi/3} = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$
   - $R_\pi = R_{\pi/3}R_{2\pi/3} = -I_2$,,
   - $R_{4\pi/3} = R_{\pi/3}R_\pi = -R_{\pi/3}$,,
   - $R_{5\pi/3} = R_{\pi/3}R_{4\pi/3} = -R_{2\pi/3}$, and
   - $R_{2\pi} = R_{\pi/3}R_{5\pi/3} = R_0$.

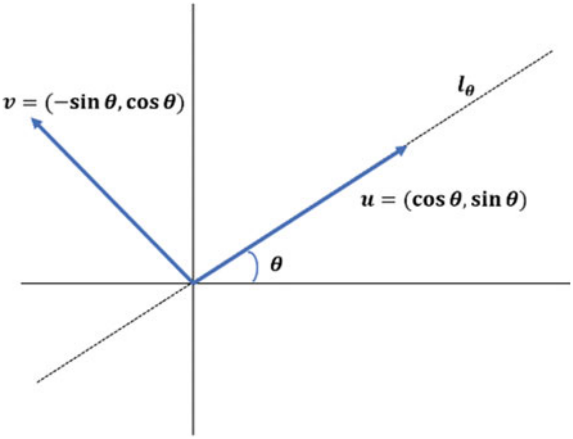

$\boldsymbol{v} = (-\sin\boldsymbol{\theta}, \cos\boldsymbol{\theta})$
$\boldsymbol{l_\theta}$
$\boldsymbol{u} = (\cos\boldsymbol{\theta}, \sin\boldsymbol{\theta})$
$\boldsymbol{\theta}$

Fig. 1.11 Rotating u by $\pi/2$

To find a matrix that represents a reflection around a line l_θ passing the origin and making an angle θ with the x-axis, we need an expression for the unit vector in the direction of l_θ. Recall that if l_θ makes an angle θ with the x-axis, then the coordinates for the unit vector u on l_θ are $(\cos\theta, \sin\theta)$, which can be identified with $u = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$. The unit vector v that is perpendicular to l_θ can be obtained by rotating u with $\frac{\pi}{2}$ see Fig. 1.11. According to Proposition 1.7.3,

$$v = R_{\pi/2}\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}.$$

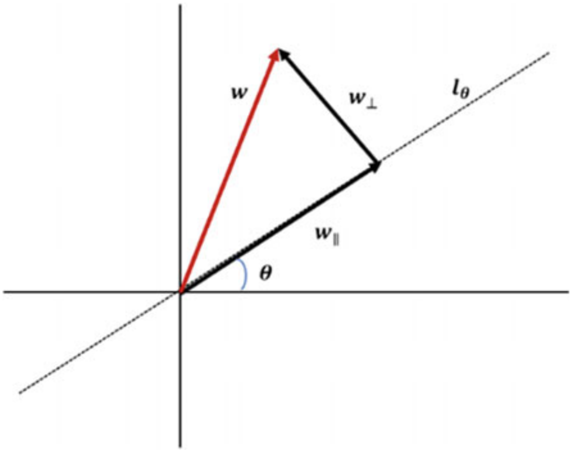
Proposition 1.7.6 *Let l_θ be the straight line that passes the origin and makes an angle θ with the x-axis. The reflection of the point (x, y) around l_θ in the plane is equivalent to the function.*

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto l_\theta \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

where $l_\theta = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$.

Proof Let $w = \begin{pmatrix} x \\ y \end{pmatrix}$ be a point in the plane, then w can be expressed as a line vector that starts from the origin and passes the point w. Such a vector is the sum of two vectors $w = w_\parallel + w_\perp$ where $w_\parallel$ is in the direction of l_θ and $w_\perp$ is perpendicular direction on l_θ (Fig. 1.12). i.e.,

Fig. 1.12 Vector $w = w_{\|} + w_{\perp}$



- $w_{\|} = \langle w, u\rangle u = (x\cos\theta + y\sin\theta)\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix} = \begin{pmatrix}x\cos^2\theta + y\sin\theta\cos\theta\\ x\sin\theta\cos\theta + y\sin^2\theta\end{pmatrix}$.
- $w_{\perp} = \langle w, v\rangle v = (-x\sin\theta + y\cos\theta)\begin{pmatrix}-\sin\theta\\ \cos\theta\end{pmatrix} = \begin{pmatrix}x\sin^2\theta - y\sin\theta\cos\theta\\ -x\sin\theta\cos\theta + y\cos^2\theta\end{pmatrix}$ where $\langle w, u\rangle$ and $\langle w, v\rangle$ are the inner products of w with u and v, respectively (Boyd & Vandenberghe, 2018).

The reflection of w around l_θ is the point $w^{'} = w_{\|} - w_{\perp}$ (Fig.1.13). Therefore,

$$\begin{aligned}
w' &= w_{\|} - w_{\perp}\\
&= \begin{pmatrix}x\cos^2\theta + y\sin\theta\cos\theta\\ x\sin\theta\cos\theta + y\sin^2\theta\end{pmatrix} - \begin{pmatrix}x\sin^2\theta - y\sin\theta\cos\theta\\ -x\sin\theta\cos\theta + y\cos^2\theta\end{pmatrix}\\
&= \begin{pmatrix}x\left(\cos^2\theta - \sin^2\theta\right) + 2y\sin\theta\cos\theta\\ 2x\sin\theta\cos\theta + y\left(\sin^2\theta - \cos^2\theta\right)\end{pmatrix}\\
&= \begin{pmatrix}x\cos 2\theta + y\sin 2\theta\\ x\sin 2\theta - y\cos 2\theta\end{pmatrix} = \begin{pmatrix}\cos 2\theta & \sin 2\theta\\ \sin 2\theta & -\cos 2\theta\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}.
\end{aligned}$$

The above proposition shows that the reflection about a straight line that passes through the origin and makes the angle θ with the x-axis can be represented by a matrix multiplication. This matrix is called the reflection matrix about l_θ and is denoted by l_θ. Applying the reflection about the line l_θ twice returns each point to itself. That is, ${l_\theta}^2 = I_2$

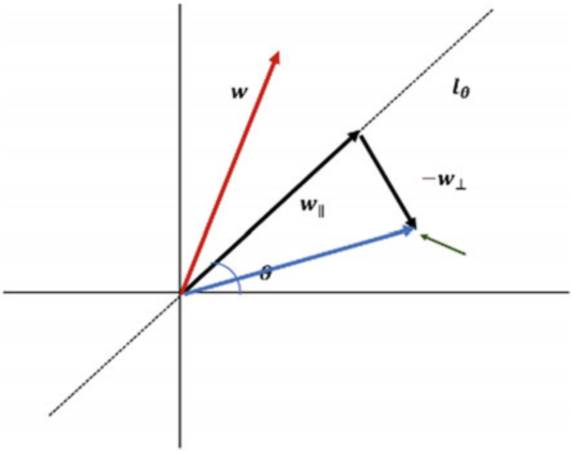


Fig. 1.13 Reflection of w around l_θ

Proposition 1.7.7 *For angles θ and β the following identities hold:*

1. $R_{\theta+\beta} = R_\theta R_\beta = R_\beta R_\theta$.
2. $l_\theta l_\theta = R_0$.
3. $l_\theta l_\beta = R_{2(\theta-\beta)}$.
4. $R_\theta l_\beta = l_{\beta+\frac{\theta}{2}}$.
5. $l_\beta R_\theta = l_{\beta-\frac{\theta}{2}}$.
6. $\left(l_\beta R_\theta\right)^2 = \left(R_\theta l_\beta\right)^2 = R_0$

Proof The first identity is the result in Proposition 1.7.4. Items (2) and (3) can be easily verified using Proposition 1.7.3, and 1.7.6, matrix multiplication, and trigonometric identities. To show (4), we first replace θ by $\frac{\theta}{2}+\beta$ in (3) to obtain $l_{\frac{\theta}{2}+\beta} l_\beta = R_\theta$. Using this identity and the identity in (2), we get

$$R_\theta l_\beta = \left(l_{\frac{\theta}{2}+\beta} l_\beta\right) l_\beta = l_{\frac{\theta}{2}+\beta}$$

To obtain the identity in (5), we compute $l_\beta l_{\beta-\frac{\theta}{2}}$ using the identity in (3) to get

$$l_\beta l_{\beta-\frac{\theta}{2}} = R_\theta$$

Using this identity and the identity in (2), we get

$$l_\beta R_\theta = l_\beta \left(l_\beta l_{\beta-\frac{\theta}{2}}\right) = l_{\beta-\frac{\theta}{2}}$$

The last equality follows directly from (2), (4), and (5). ■

The geometric interpretation for the relation in (3) is that a reflection about l_θ followed by a reflection about l_β is equivalent to a rotation with an angle that is double the angle between l_θ and l_β. This aspect can be explained as follows.

It is straightforward to show, using Proposition 1.7.6, that a refection about l_θ maps a point (r, α) to the point $(r, 2\theta - \alpha)$. Therefore, applying another reflection l_θ leads to

$$(r, \alpha)l_\beta \to (r, 2\beta - \alpha)l_\theta \to (r, 2\theta - (2\beta - \alpha)) = (r, 2(\theta - \beta) + \alpha)$$

.i.e., the composition of l_θ and l_β is a rotation by angle $2(\theta - \beta)$.

Example 1.7.8 By using the abovementioned notation,

$$l_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \text{ and } l_{\pi/4} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\left(l_{\pi/4}\right)^2 = l_{\pi/4}l_{\pi/4} = I_2, \quad l_{\pi/4}R_{\pi/2} = l_0, \text{ and } l_{\pi/3} = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

From now on, a rotation by angle θ is identified with its rotation matrix R_θ. A reflection about the line that passes through the origin and makes an angle θ with x-axis is identified with its reflection matrix l_θ. Therefore, R_θ (similarly, l_θ) represents both the matrix and the symmetry represented by the matrix.

Let $n \in \mathbb{N}$ such that $n \geq 3$. Consider a regular (sides of equal lengths and equal interior angles) n-polygon. There exist $2n$ types of symmetries for such a polygon: rotations about the center by an angle moving each vertex to the next vertex, reflections about the lines that pass the center of the polygon and the vertices, reflections about the lines that pass the center of the polygon and divide opposite sides of the polygon into equal halves, and their compositions. For example, see Fig. 1.14. The following steps can be implemented to identify such symmetries.

1. Select one of the vertices, and number it as vertex 1.
2. Identify the center of the polygon with the origin of the plane such that the line passes the center and vertex 1 lies on the x-axis.

As the polygon is regular, the required symmetries are

- the rotations by the angles $0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2(n-1)\pi}{n}$,
- the reflections about lines passing the origin and making angles $0, \frac{\pi}{n}, \frac{2\pi}{n}, \frac{3\pi}{n}, \ldots, \frac{(n-1)\pi}{n}$ with the x-axis, and
- any compositions of these.

According to a Propositions 1.7.3 and 1.7.6, these symmetries can be represented by the matrices

$$R_0, R_{\frac{2\pi}{n}}, R_{\frac{4\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}, l_0, l_{\frac{\pi}{n}}, \ldots, l_{\frac{(n-1)\pi}{n}}$$

and any matrix resulting by their multiplications. Note that l_θ and $l_{\pi+\theta}$ represent the same line of symmetry. This can be checked easily using the result of Proposition 1.7.6.

Example 1.7.9 (The symmetries of a Square) Consider a square with the center at the origin and one of its vertices on the x-axis. The symmetries of the square are represented by $R_0 = I_2$, $R_{\pi/2}$, R_π, $R_{3\pi/2}$, l_0, $l_{\pi/4}$,$l_{\pi/2}$,$l_{3\pi/4}$ and the products of any of these matrices. The equations in Proposition 1.7.7 easily shows that these are all the different symmetries of the square. The following table is obtained using Proposition 1.7.7. Note that $l_0 = l_\pi$ as they represent the same line. Similarly, $l_{\pi/4} = l_{5\pi/4}$, $l_{\pi/2} = l_{3\pi/2}$ and $l_{3\pi/4} = l_{7\pi/4}$ (see Fig. 1.15 and Table 1.3).

The next example pertains to a polygon with an odd number of vertices.

Example 1.7.10 (The symmetries of a Pentagon) Consider a pentagon with the center at the origin, and one of its vertices on the x-axis. The symmetries of the pentagon are represented by

$$R_0 = I_2,\ R_{2\pi/5},\ R_{4\pi/5},\ R_{6\pi/5},\ R_{8\pi/5}, l_0, l_{\pi/5}, l_{2\pi/5}, l_{3\pi/5}, l_{4\pi/5}$$

and their products. The equations in Proposition 1.7.7 shows that these are all the different symmetries of the regular pentagon (Fig. 1.16).

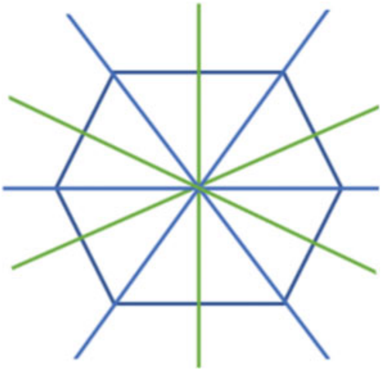


Fig. 1.14 Regular 6-polygon

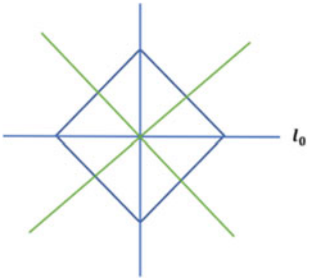


Fig. 1.15 Regular 4-polygon

Table 1.3 Composition of the symmetries of a square

$\cdot$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$	l_0
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	$l_{\pi/2}$	$l_{3\pi/4}$	l_0	$l_{\pi/4}$
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π	$l_{3\pi/4}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$
l_0	l_0	$l_{3\pi/4}$	$l_{\pi/2}$	$l_{\pi/4}$	R_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$
$l_{\pi/4}$	$l_{\pi/4}$	l_0	$l_{3\pi/4}$	$l_{\pi/2}$	$R_{\pi/2}$	R_0	$R_{3\pi/2}$	R_π
$l_{\pi/2}$	$l_{\pi/2}$	$l_{\pi/4}$	l_0	$l_{3\pi/4}$	R_π	$R_{\pi/2}$	R_0	$R_{3\pi/2}$
$l_{3\pi/4}$	$l_{3\pi/4}$	$l_{\pi/2}$	$l_{\pi/4}$	l_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$	R_0

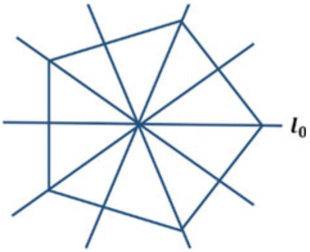


Fig. 1.16 Regular 5-polygon

Summary 1.7.11 Let $n \in \mathbb{N}$ such that $n \geq 3$. The symmetries of the regular n-polygon are

- n rotations, each of which shifts each vertex to the next vertex position,
- n reflections, each of which pertain to the line passing the center and making an angle $\frac{\pi k}{n}$, where $k = 0, 1, \ldots, n-1$,
- any compositions of these entities.

Using Proposition 1.7.7 and $= l_\theta l_{\pi+\theta}$, one can easily show that the product of any two of these matrices

$$R_0, R_{\frac{2\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}, l_0, l_{\frac{\pi}{n}}, l_{\frac{2\pi}{n}} \cdots, l_{\frac{(n-1)\pi}{n}}$$

is again one of the matrices listed above.

Corollary 1.7.12 *Let $n \in \mathbb{N}$ such that $n \geq 3$. The set.*

$$\left\{R_0, R_{\frac{2\pi}{n}}, \ldots, R^n_{\frac{2(n-1)\pi}{n}}, l_0, l_{\frac{\pi}{n}}, l_{\frac{2\pi}{n}} \ldots, l_{\frac{(n-1)\pi}{n}}\right\}$$

contains all the different symmetries of the regular n-polygon.

The following picture shows the effects of all the possible symmetries of an octagon (Fig. 1.17).

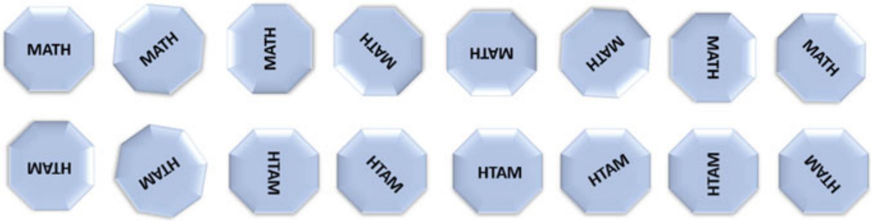


Fig. 1.17 Symmetries of regular 8-polygon

Exercises

Solved Exercises

1.1 Show that any nonempty finite subset of $\mathbb{Z}$ has unique minimum and maximum elements.

Solution: Let $n \in \mathbb{N}$ and $A = \{a_1, a_2, \ldots, a_n\}$ be a nonempty finite subset of $\mathbb{Z}$. Using mathematical induction on n, we show that A has minimum and maximum elements. i.e., we show that there exist $x, y \in A$ such that $x \leq a \leq y$ for all $a \in A$.

Base step: if $n = 1$, then $A = \{a_1\}$ for some integer $a_1 \in \mathbb{Z}$. As $a_1 \leq a_1 \leq a_1$, then by letting $x = y = a_1$, the statement is true for $n = 1$.

Inductive step: assume that the statement is true for n. That is, any subset of $\mathbb{Z}$ that contains n elements must have minimum and maximum elements. Let $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$ be a subset of $\mathbb{Z}$ with $n + 1$ elements. Let $B = A \backslash \{a_{n+1}\} = \{a_1, a_2, \ldots, a_n\}$ be a subset that only contains n elements. According to the induction hypothesis, B has minimum and maximum elements. i.e., there exist $x, y \in B$ such that $x \leq a_i \leq y$ for all $a_i \in B \subseteq A$. Three possibilities can be listed for a_{n+1}:

$$a_{n+1} \leq x, x \leq a_{n+1} \leq y, \text{ or } y \leq a_{n+1}$$

- If $a_{n+1} \leq x$, then $a_{n+1} \leq x \leq a_i \leq y$ for all $a_i \in A$, $1 \leq i \leq n$. Thus, a_{n+1} is a minimum element of A and y is a maximum element.
- If $x \leq a_{n+1} \leq y$, then $x \leq a_i \leq y$ for all $a_i \in A$, $1 \leq i \leq n + 1$. Thus, x is a minimum element of A and y is a maximum of A.
- If $y \leq a_{n+1}$ then $x \leq a_i \leq y \leq a_{n+1}$ for all $a_i \in A$, $1 \leq i \leq n$. Thus, x is a minimum element of A while a_{n+1} is a maximum element of A.

In all three cases, A has minimum and maximum elements. Therefore, according to the principle of mathematical induction, the statement is true for any $n \in \mathbb{N}$. The uniqueness follows as the relation $\leq$ is a total order relation on $\mathbb{Z}$.

1.2 Let A be any set. Consider the identity relation on A that is defined in Example 1.3.7 (4). Show that

i Any subset of Δ_A is a transitive relation on A.

ii A relation $\mathcal{R}$ on A is both symmetric and antisymmetric if and only if $\mathcal{R}$ is a subset of the identity relation Δ_A.

Solution

i. Let $\mathcal{R}$ be any subset of Δ_A and $(a, b), (b, c) \in \mathcal{R}$, then $a = b$ and $b = c$. Therefore, $(a, c) = (a, b) \in \mathcal{R}$, and $\mathcal{R}$ is transitive.

ii. Assume that $\mathcal{R}$ is a relation on A such that $\mathcal{R}$ is both symmetric and antisymmetric. Let (a, b) be an arbitrary element in $\mathcal{R}$. Since $\mathcal{R}$ is symmetric, the ordered pair (b, a) must also be in $\mathcal{R}$. However, since $\mathcal{R}$ is antisymmetric, then $a = b$, and thus, $\mathcal{R} \subseteq \Delta_A$. For the other direction, if $\mathcal{R} \subseteq \Delta_A$, any element in $\mathcal{R}$ is in the form (a, a) for some $a \in A$. That is, $\mathcal{R} = \{(a, a) \in A \times A : a \in B\}$ for some $B \subseteq A$. i.e., $\mathcal{R} = \Delta_B$ for some subset B. By Example 1.3.7 (4), $\mathcal{R}$ is both symmetric and antisymmetric.

1.3 Let $\mathcal{R}$ be a relation on $\mathbb{Z}$ defined as $a\mathcal{R}b$ if and only if $a - b$ is divisible by 2. Determine whether $\mathcal{R}$ is reflexive, symmetric, antisymmetric, and/or transitive. What type of relation is $\mathcal{R}$?

Solution:

$\mathcal{R}$ is reflexive: since $a - a = 0$ and $0 = 0 \cdot 2$ is divisible by 2, and $a\mathcal{R}a$.

$\mathcal{R}$ is symmetric: if $a\mathcal{R}b$, then $a - b$ is divisible by 2. i.e., there exists $k \in \mathbb{Z}$ such that $a - b = 2k$. This implies that $b - a = 2(-k)$ is divisible by 2. i.e., $b\mathcal{R}a$.

$\mathcal{R}$ is not antisymmetric: $2\mathcal{R}4$ and $4\mathcal{R}2$ (Check!), but $2 \neq 4$.

$\mathcal{R}$ is transitive: if $a\mathcal{R}b$ and $b\mathcal{R}c$, then there exist $k, h \in \mathbb{Z}$ such that

$$a - b = 2k \text{ and } b - c = 2h.$$

Therefore,
$a - c = (a - b) + (b - c) = 2k + 2h = 2(k + h)$ is divisible by 2
i.e., $a\mathcal{R}c$, and thus, $\mathcal{R}$ is transitive.

1.4 Consider the set of positive integers $\mathbb{N}$, and let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Define

$$\mathcal{R} = \left\{(x + 2, x + 3) \in \mathbb{N}^2 : x \in A\right\}.$$

Here $\mathcal{R}$ is a relation on $\mathbb{N}$. Determine the domain and the range of $\mathcal{R}$. What is the domain and range of $\mathcal{R}$ if A is replaced by $\mathbb{N}$?

Solution: The relation $\mathcal{R}$ can be expressed as follows:

$$\mathcal{R} = \{(2, 3), (3, 4), (4, 5), (5, 6), (6, 7), (7, 8), (8, 9), (9, 10), (10, 11), (11, 12), (12, 13)\}$$

Therefore,

$$D(\mathcal{R}) = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Rang(\mathcal{R}) = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$$

If A is replaced by $\mathbb{N}$, then the domain and the range would be the following infinite sets

$$D(\mathcal{R}) = \{3, 4, 5, 6, 7, \ldots\}, \quad Rang(\mathcal{R}) = \{4, 5, 6, 7, 8, \ldots\}$$

1.5 Let $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \times \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let

$$\mathcal{R} = \left\{((x, y), (u, v)) \in A^2 : 3x + y \leq 3u + v\right\}$$

be a relation on A. Determine whether $\mathcal{R}$ is an equivalence, a partial order, or a total order relation.

Solve the question with $\mathcal{R} = \left\{((x, y), (u, v)) \in A^2 : 11x + y \leq 11u + v\right\}$ as well.

Solution: The properties of $\mathcal{R}$ can be checked as follows:

Reflexivity: since $3x + y \leq 3x + y$, we have $((x, y), (x, y)) \in \mathcal{R}$ for each $(x, y) \in A$. i.e., $\mathcal{R}$ is reflexive.

Symmetry: since $((0, 0), (1, 2)) \in \mathcal{R}$ and $((1, 2), (0, 0)) \notin \mathcal{R}$, the relation $\mathcal{R}$ is not symmetric.

Antisymmetry: since both $((0, 4), (1, 1))$ and $((1, 1), (0, 4))$ are elements in $\mathcal{R}$ and $(0, 4) \neq (1, 1)$, $\mathcal{R}$ is not antisymmetric.

Transitivity: If both $((x, y), (u, v))$ and $((u, v), (z, w))$ are elements in $\mathcal{R}$, then

$3x + y \leq 3u + v$ and $3u + v \leq 3z + w$.

This implies that $3x + y \leq 3z + w$ and $((u, v), (z, w)) \in \mathcal{R}$. So, $\mathcal{R}$ is transitive.

Therefore, $\mathcal{R}$ is not an equivalence or an order relation.

If $\mathcal{R} = \left\{((x, y), (u, v)) \in A^2 : 11x + y \leq 11u + v\right\}$, the abovementioned reasons can be used to show that $\mathcal{R}$ is reflexive, not symmetric and transitive. $\mathcal{R}$ is antisymmetric because if $((x, y), (u, v))$ and $((u, v), (x, y))$ are both elements in $\mathcal{R}$, then $11x + y = 11u + v$ implying that $v - y = 11(x - u)$ is a multiple of 11. That is, there exists $q \in \mathbb{Z}$ such that $v - y = 11q$. Since both y and v belong to A, we have $|v - y| \leq 10$. So, zero is the only possible value of q. i.e., $v = y$, and $x = u$. Therefore, $(x, y) = (u, v)$, and $\mathcal{R}$ is antisymmetric. Hence, $\mathcal{R}$ is a partial order relation. To show that $\mathcal{R}$ is a total order relation, assume that (x, y) and (u, v) are two elements in A. Since $11x + y$ and $11u + v$ are elements in $\mathbb{N}$, they are comparable. i.e., either $11x + y \leq 11u + v$ or $11u + v \leq 11x + y$. In general, $\mathcal{R} = \left\{((x, y), (u, v)) \in A^2 : kx + y \leq ku + v\right\}$ is a total order relation whenever $k > 10$.

1.6 Let A and B Be two finite sets such that $|A| = |B|$ and $f : A \to B$ be a function. Show that the map f is injective if and only if f is surjective.

Solution: Assume that $|A| = |B| = n$. Let $B = \{b_1, \cdots, b_n\}$, where $b_1, \cdots, b_n$ are distinct elements in B. For all $1 \leq i \leq n$, let $A_i = \{a \in A : f(a) = b_i\}$ and $k_i = |A_i|$, the number of elements in A_i. The sets

$\{A_i, 1 \leq i \leq n\}$ form a partition of A (Check!). Therefore,

$$n = |A| = k_1 + \cdots + k_n$$

Note that,

- the function f is surjective if and only if $A_i \neq \varnothing$ for all $1 \leq i \leq n$, that is, if and only if $k_i \geq 1$ for all $1 \leq i \leq n$.
- the function f is injective if and only if for all $1 \leq i \leq n$, the set A_i contains at most one element. That is, if and only if $k_i \leq 1$ for all $1 \leq i \leq n$.

If f is injective, then $k_i \leq 1$ for all $1 \leq i \leq n$, so $k_i \in \{0, 1\}$. Since the sum $k_1 + \cdots + k_n = n$, then $\mathrm{k_i} = 1$ for all $1 \leq i \leq n$. Therefore, f is surjective.

For the other direction, suppose f is surjective, then $k_i \geq 1$ for all $1 \leq i \leq n$. Let $l_i = k_i - 1 \geq 0$. Here,

$$n = k_1 + \cdots + k_n = (1 + l_1) + \cdots + (1 + l_n) = \underbrace{1 + \cdots + 1}_{n \text{ times}} + l_1 + \cdots + l_n.$$

Therefore, $n = n + (l_1 + \cdots + l_n)$ and $l_1 + \cdots + l_n = 0$. Since $l_i \geq 0$ for all $1 \leq i \leq n$, then $l_i = 0$ for all $1 \leq i \leq n$, and $k_i = 1$ for all $1 \leq i \leq n$. Hence, f is injective.

1.7 Consider the following relations:

1. $\mathcal{R} = A \times B$ where $A = \emptyset$ and B is any nonempty set.
2. $\mathcal{S} = A \times B$ where $B = \emptyset$ and A is any nonempty set.
3. $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 - x^2 = 1\}$.
4. $g = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 - y^2 = 1\right\}$.

Determine whether each relation is a function.

Solution:

1. If $A = \emptyset$, then $\mathcal{R} = A \times B = \emptyset$ for any nonempty set B. Since there are no elements in A, then the conditional statement

$$(a \in A \Rightarrow \exists\,!\, b \in B \text{ such that } (a, b) \in \mathcal{R})$$

is true. Therefore, $\mathcal{R}$ is a function.

2. Assume that $B = \varnothing$, and A is a nonempty subset. If $\mathcal{S}$ is a function, then for each $a \in A$ there exists $b \in B$ such that $(a, b) \in \mathcal{S}$, which contradicts that B is empty, So, $\mathcal{S}$ is not a function.
3. For each $x \in \mathbb{R}$, there exist two ordered pairs in f. Namely, $(x, \sqrt{1 + x^2})$ and $(x, -\sqrt{1 + x^2})$ preventing f from being a function (Fig. 1.18). If we restrict the codomain to only the nonnegative real numbers, and define f as

$$f = \left\{(x, y) \in \mathbb{R} \times \left(\mathbb{R}^+ \cup \{0\}\right) : y^2 - x^2 = 1\right\}$$

then f would assign only one image for each x in $\mathbb{R}$, and thus, it is a function on $\mathbb{R}$.

4. The relation $g = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 - y^2 = 1\right\}$ is not a function because the ordered pairs $\left(x, \sqrt{x^2-1}\right)$ and $(x, -\sqrt{x^2-1})$ are both in g. Even if we restrict the codomain to the nonnegative real numbers, the relation would not be a function on $\mathbb{R}$, because not every element in the domain has an image. If x is any real number such that $|x| < 1$, then there is no y such that $(x, y) \in g$ since that would give $1 + y^2 = x^2 < 1$, which implies that $y^2 < 0$. Thus, for x with $|x| < 1$, no image exists under g and g is not a function (Fig. 1.19).

1.8 Let $f : A \to B$ Be a Function. Prove that the Map f is Invertible if and Only if It is a Bijective Map.

Solution:

Assume that f is invertible and $g : B \to A$ is the inverse function of f. If $f(a) = f(b)$, applying g on both sides of the equation yields

$$a = g(f(a)) = g(f(b)) = b$$

which means that f is injective. Let $b \in B$ be an arbitrary element, and $a = g(b)$. Then

$$f(a) = f(g(b)) = f \circ g(b) = \iota_B(b) = b.$$

So, f is surjective. Therefore, f is bijective.

For the other direction, assume that f is bijective, and let

$$g = \{(b, a) : (a, b) \in f\} \subseteq B \times A.$$

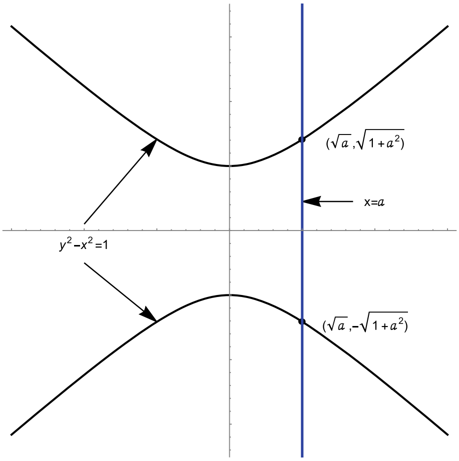


Fig. 1.18 Graph of $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 - x^2 = 1\}$

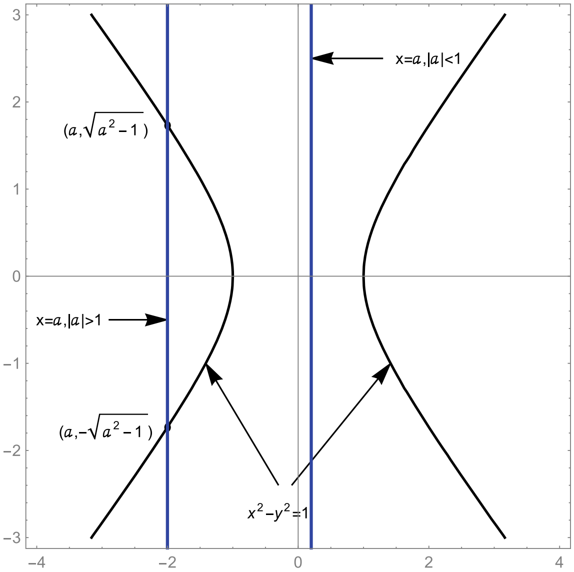


Fig. 1.19 Graph of $g = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 - y^2 = 1\}$

We show that $g : B \to A$ is a function such that $g \circ f = \iota_A$ and $f \circ g = \iota_B$. Let $b \in B$ be an arbitrary element. Since f is surjective (onto), there exists $a \in A$ such that $f(a) = b$. i.e., $(a, b) \in f$, so $(b, a) \in g$. That is, g is defined for each element in B.

To show the uniqueness of images of elements in B under g, let (b, a_1) and (b, a_2) be two elements in g, so (a_1, b) and (a_2, b) belong to f. Since f is injective (one-to-one), then $a_1 = a_2$, as required. We still need to show that for all $a \in A$, $g \circ f(a) = a$ and for all $b \in B$, $f \circ g(b) = b$. Let $a \in A$, since f is defined for all elements of A, then there exists a unique element $b \in B$ such that $(a, b) \in f$ i.e., $(b, a) \in g$. Therefore,

$$g \circ f(a) = g(f(a)) = g(b) = a.$$

Since a is an arbitrary element in A, then $g \circ f = \iota_A$. Similarly, according to the surjectivity of f, for each $b \in B$ there exists $a \in A$ such that $(a, b) \in f$. This implies that $(b, a) \in g$. i.e.,

$$f \circ g(b) = f(g(b)) = f(a) = b.$$

Since b is an arbitrary element in B, then $f \circ g = \iota_B$.

1.9 Let $n \in \mathbb{N}$, K be any subset of $\mathbb{C}$, and $A \in \mathcal{M}_n(K)$ be an invertible matrix. Show that

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)}$$

and $\det(A) = \det\left(A^{-1}\right)$ if and only if $\det(A) \in \{1, -1\}$.

Solution: If $A \in \mathcal{M}_n(K)$ is an invertible matrix, then there exists $A^{-1} \in \mathcal{M}_n(K)$ such that

$$AA^{-1} = I_n$$

Therefore,

$$\det(A)\det\left(A^{-1}\right) = \det\left(AA^{-1}\right) = \det(I_n) = 1$$

The result now follows. Moreover, we have

$$\det(A) = \det\left(A^{-1}\right) \Leftrightarrow \det(A) = \frac{1}{\det(A)} \Leftrightarrow (\det(A))^2 = 1 \Leftrightarrow \det(A) \in \{1, -1\}$$

1.10 Compute all possible symmetries of a regular triangle and list their multiplications.

Solution: According to Corollary 1.7.12, the set.

$$\left\{R_0, R_{2\pi/3}, R_{4\pi/3}, l_o, l_{\pi/3}, l_{2\pi/3}\right\}$$

contains all the symmetries of the regular triangle. Using the relations in Proposition 1.7.7, and,

$$l_\theta = l_{\pi+\theta}$$

we obtain the following Table 1.4 that contains all their compositions.

Unsolved Exercises

Table 1.4 Compositions of the symmetries of a regular triangle

·	R_0	$R_{2\pi/3}$	$R_{4\pi/3}$	l_0	$l_{\pi/3}$	$l_{2\pi/3}$
R_0	R_0	$R_{2\pi/3}$	$R_{4\pi/3}$	l_0	$l_{\pi/3}$	$l_{2\pi/3}$
$R_{2\pi/3}$	$R_{2\pi/3}$	$R_{4\pi/3}$	R_0	$l_{\pi/3}$	$l_{2\pi/3}$	l_0
$R_{4\pi/3}$	$R_{4\pi/3}$	R_0	$R_{2\pi/3}$	$l_{2\pi/3}$	l_0	$l_{\pi/3}$
l_0	l_0	$l_{2\pi/3}$	$l_{2\pi/3}$	R_0	$R_{4\pi/3}$	$R_{2\pi/3}$
$l_{\pi/3}$	$l_{\pi/3}$	l_0	$l_{2\pi/3}$	$R_{2\pi/3}$	R_0	$R_{4\pi/3}$
$l_{2\pi/3}$	$l_{2\pi/3}$	$l_{\pi/3}$	l_0	$R_{4\pi/3}$	$R_{2\pi/3}$	R_0

1.11 Let Δ denote the symmetric difference defined in Definition 1.1.8. Show that $(A\Delta B)\Delta C = A\Delta(B\Delta C)$ for any sets A, B and C.

1.12 Let r be a real number such that $0 < r < 1$. Show that

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

for every integer n such that $n \geq -1$.

1.13 Show that $2^{n+2} + 3^{2n+1}$ is divisible by 7 for every nonnegative integer n.

1.14 Show that if $x \in \mathbb{R}$, $x > -1$, then $(1 + x)^n \geq 1 + nx$ for every integer n such that $n \geq 0$.

1.15 For each of the following relations

1. $\mathcal{R} = \left\{(x, y) \in \mathbb{Z}^2 : x + y < 5\right\}$,
2. $\mathcal{T} = \{(x, y) \in \mathbb{N}^2 : x + y > 1\}$, and
3. $\mathcal{V} = \left\{(x, y) \in \mathbb{Z}^2 : x + y \text{ is even}\right\}$,

determine whether the relation is reflexive, symmetric, antisymmetric, or transitive.

1.16 Let A be a nonempty set. For any relations $\mathcal{R}$ and $\mathcal{T}$ on A, the composition relation is defined as

$$\mathcal{R}\circ\mathcal{T} = \left\{(a, c) \in A^2 : \exists\, b \in A, (a, b) \in \mathcal{T} \wedge (b, c) \in \mathcal{R}\right\}$$

Show that if $\mathcal{R}$ and $\mathcal{T}$ are equivalence relations on A, then $\mathcal{R} \circ \mathcal{T}$ is an equivalence relation on A if and only if $\mathcal{R} \circ \mathcal{T} = \mathcal{T} \circ \mathcal{R}$.

1.17 Let $A = \mathbb{Z}\backslash\{0\}$ and $\mathcal{R} = \left\{(x, y) \in A^2 : xy > 0\right\}$ be a relation on A. Determine whether $\mathcal{R}$ is an equivalence relation.

1.18 Let $A = \mathbb{Z}\backslash\{0\}$ and $\mathcal{R} = \left\{(x, y) \in A^2 : x|y\right\}$ be a relation on A. Show that $\mathcal{R}$ is a partial order relation. Is $\mathcal{R}$ a total order relation?

1.19 Let $n \in \mathbb{N}$ and $\mathcal{R} = \left\{(a, b) \in \mathbb{Z}^2 : \frac{b-a}{n} \in \mathbb{Z}\right\} = \left\{(a, b) \in \mathbb{Z}^2 : n|(b - a)\right\}$.

a. Show that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.
b Show that the equivalence classes of $\mathcal{R}$ can be expressed as $m + n\mathbb{Z}$, where $m = 0, 1, 2, \ldots, n - 1$.

1.20 Consider the set of integers $\mathbb{Z}$. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the maps defined by

$$f(a, b) = a + b, g(a, b) = ab$$

Show that f and g define functions on $\mathbb{Z}$.

1.21 Show that the composition of two functions is a function, and the composition of two bijective maps is a bijective map. Show that the inverse of a bijective map is bijective.

1.22 Determine whether the functions

a. $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^2 - 5$
b. $g : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, where $g(x) = \frac{1}{x} + 2$

are injective or surjective. Find the domains and ranges of these functions.

1.23 Let A and B Be Two Sets and $f{:}A{\to}B$ Be a Function. Show that

$$\iota_B \circ f = f \circ \iota_A = f$$

where i_A and i_B are the inclusion functions of A and B respectively.

1.24 Let A and B be two sets and $f : A \to B$ be a Function. Show that

- f is injective if and only if for any $H \subseteq A$, $f^{-1}(f(H)) = H$.
- f is surjective if and only if for any $K \subseteq B$, $f\big(f^{-1}(K)\big) = K$.

where $f(H)$ denotes the image of H under f, and $f^{-1}(K)$ is the preimage of K.

1.25 Let $f : \mathbb{C} \to \mathbb{C}$ be the map takes $z = x+iy$ to its complex conjugate $\overline{z} = x-iy$. Show that the map f is a bijective function, and for all $z, z_1, z_2 \in \mathbb{C}$

$$\bar{\bar{z}} = z, \quad \text{and} \quad \overline{z_1 z_2} = \bar{z_1}\ \bar{z_2}$$

1.26 Show that the multiplication of diagonal matrices is commutative.

1.27 Show that if A is an upper or a lower tringle matrix, then the determinant of A is the product of its diagonal entries. i.e.,

$$det(A) = \prod_{i=1}^{n} a_i = a_{11}\ a_{22} \ldots\ldots a_{nn}.$$

1.28 List all possible symmetries for a regular octagon and the compositions of any two of these symmetries.

References

Boyd, S., & Vandenberghe, L. (2018). *Introduction to applied linear algebra vectors, matrices, and least squares*. Cambridge University Press.

Burton, D. M. (2007). *Elementary number theory*. MacGraw-Hill.

Halmos, P. (2013). *Naive set theory*. Springer.

Hammack, R. (2013). *Book of Proof*. Creative Commons.

Hartman, G. (2011). *Fundamentals of Matrix Algebra*. Creative Commons.

Hungerford, T., & Shaw, D. (2009). *Contemporary precalculus: A graphing approach* (5th ed.). Thomson Higher Education.

Printer, C. C. (2014). *A book of set theory*. Dover Publications INC.

Chapter 2
Algebraic Operations on Integers

Counting began with the positive integers $\mathbb{N} = \{1, 2, 3, \ldots\}$. The counterparts of these numbers, the negative numbers, and the zero were later introduced to form the integers. Namely, the integers can be expressed as

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Any integer has two parts, sign and magnitude. The sign of an integer is either positive, negative, or neutral (if the integer equals zero). The magnitude of an integer a is mathematically defined as the absolute value of a, i.e.,

$$|a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$$

In this chapter, we study the basic operations on integers, and present several fundamental results. In Sect. 2.1, the quotient–remainder theorem is discussed and illustrated. The divisibility of integers and basic results are illustrated in Sect. 2.2. In Sect 2.3, the common divisor and the greatest common divisor are defined and discussed. In Sect. 2.4, the Euclidean algorithm for computing the greatest common divisor is studied. The Bézout's lemma and methods of writing the common divisor as a linear combination of the integers are studied in Sect. 2.5. Section 2.6 is devoted to relatively prime numbers and their properties, and Sect. 2.7 is devoted to the common multiples of integers. The fundamental theorem of arithmetic and the prime numbers are considered in Sect. 2.8. The last section is divided into two parts pertaining to applications of the Euclidean algorithm. The first part pertains to testing the primality of an integer, and the second discusses the computation of the greatest common divisor and the least common multiple. The readers can refer to (Burton, 2007) for the results presented in this chapter and their proofs.

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_2

2.1 Basic Algebraic Operations on Integers

Four basic operations can be performed on integers: addition, subtraction, multiplication, and division. We assume that the reader is familiar with these fundamental, their properties, and the usual methods used to compute them. Since the addition (subtraction) of two integers a and b defines a unique element $a + b$ $(a - b)$ in $\mathbb{Z}$ for each $a, b \in \mathbb{Z}$, then the addition (subtraction) forms a function on $\mathbb{Z}$. Note that the subtraction is not a function on $\mathbb{N}$ as a subtraction of two elements in $\mathbb{N}$ is not necessarily in $\mathbb{N}$. The multiplication (product) of two integers is defined using the addition operation. If a and b are two positive integers, the multiplication of a and b, denoted by $a \times b$, refers to the addition of a to itself b times, and vice versa, i.e., for two positive integers a and b, $a \times b = \underbrace{a + a + a + \cdots + a}_{b \text{ times}}$. The definition of multiplication for any integers can be generalized as follows:

Let a and b be two nonzero integers. The multiplication of a and b is defined as the integer whose absolute value is $|a| \times |b|$ and whose sign is determined by the following rule:

$$\mathrm{Sign}(a \times b) = \begin{cases} + & \mathrm{Sign}(a) = \mathrm{Sign}(b) \\ \\ - & \mathrm{Sign}(a) \neq \mathrm{Sign}(b) \end{cases}$$

If either a or b is zero, then $a \times b = 0$.

Proposition 2.1.1 *The three operations of addition, subtraction, and multiplication are functions on the set of integers $\mathbb{Z}$. Only addition and multiplication form functions on $\mathbb{N}$. Subtraction is not a function on $\mathbb{N}$.*

The rest of this section discusses dividing two integers. If a and b are two positive integers, the quotient of a and b is the maximum number of times one can subtract b from a without obtaining a negative result. The value that remains in a afterward is called the remainder. For example, the quotient of 7 and 2 is 3, as one can subtract 2 three times from 7 without obtaining a negative result, and the remainder is 1. The operation of finding the quotient and remainder is called division. The quotient-remainder theorem, stated below, shows the existence and uniqueness of the quotient and remainder of any two integers, with the restriction that the divisor is nonzero. Dividing by zero is always undefined.

Theorem 2.1.2 (Quotient-remainder theorem) *Let $a, b \in \mathbb{Z}$ and $b \neq 0$. There exist unique elements $q, r \in \mathbb{Z}$ such that $a = qb + r$, where $0 \leq r < |b|$.*

Definition 2.1.3 Let $a, b \in \mathbb{Z}$, $b \neq 0$, and q, r be as in Theorem 2.1.2. The number q is called the quotient of a by b, and r is called the remainder. The numbers a and b are called the dividend and the divisor, respectively.

To find the numbers q and r in dividing 39 by 5 (for example), one starts by listing the multiples of 5 that are not greater than 39 in increasing order.

$$0, 5, 10, 15, 20, 25, 30, 35$$

As the largest of these is $35 = 5 \times 7$, then $q = 7$, and the remainder $r = 39 - 7 \times 5 = 4$. This method of finding q and r is not practical when q is large. The quotient and the remainder of two positive integers are usually found using the division algorithm (long division). The long division can only be carried out on positive integers, the quotient and the remainder for dividing integers a and b can be obtained from long division of the positive integers $|a|$ and $|b|$ using the steps outlined below.

An algorithm to find the quotient and the remainder:

To find the quotient q and remainder r of dividing a by b where $b \neq 0$, use the long division to divide $|a|$ and $|b|$ to obtain Q and R, such that $|a| = Q|b| + R$ where $0 \leq R < |b|$.

1. If $a > 0$ and $b > 0$, let $q = Q$ and $r = R$.
2. If $a > 0$ and $b < 0$, let $q = -Q$ and $r = R$ ($a = Q|b| + R = (-Q)b + R$).
3. If $a < 0$ and $b > 0$, then $a = -|a| = -Qb - R$.
   (a) If $R = 0$, let $q = -Q$ and $r = 0$
   (b) If $R \neq 0$, let $q = -Q - 1$ and $r = b - R$ ($a = (-Q - 1)b + (b - R)$).
4. If $a < 0$ and $b < 0$, then $a = -|a| = -Q|b| - R = Qb - R$.
   (a) If $R = 0$, let $q = Q$ and $r = 0$
   (b) If $R \neq 0$, let $q = Q + 1$ and $r = |b| - R$ ($a = (Q + 1)b + |b| - R$).

It is left to the reader to verify that in all cases, the equation $a = qb + r$, where $0 \leq r < |b|$, holds. As $r = a - qb$, the remainder forms a linear combination of a and b. For a nonzero integer b, the remainder r of dividing any integer by b satisfies $0 \leq r < |b|$. Hence, the set of positive integers that are less than $|b|$ contains all possible remainders that result from dividing by b. For example, $\{0, 1, 2, 3, 4\}$ contains all remainders of 5, while $\{0, 1, 2, 3, 4, 5, 6, 7\}$ contains the remainders of -8.

Definition 2.1.4 Let $b \in \mathbb{Z}$ such that $b \neq 0$. The set $\{0, 1, 2, \ldots |b| - 1\}$ is called the set of remainders of b.

Example 2.1.5 To find the quotient and remainder of dividing a by b, where

i. $a = 123, b = 21$, ii. $a = 123, b = -21$, iii. $a = -123, b = 21$, iv. $a = -123, b = -21$

we apply long division on the positive integers $|123|$ and $|21|$ to obtain

$$123 = 5 \cdot 21 + 18, \text{ i.e., } \; Q = 5 \text{ and } R = 18.$$

Therefore, by applying the algorithm described above, we obtain

i. For $a = 123, b = 21$, the quotient is 5, and the remainder is 18.
ii. For $a = 123, b = -21$, the quotient is -5, and the remainder is 18.
iii. For $a = -123, b = 21$, the quotient is -6, and the remainder is 3.
iv. For $a = -123, b = -21$, the quotient is 6, and the remainder is 3.

2.2 Divisibility of Integers

This section studies the notion of divisibility, which is almost equivalent to division with a zero remainder, the only exceptions to this equivalence is when determining divisibility by zero. We state and prove several results that are needed for subsequence chapters.

Definition 2.2.1 Let $a, b \in \mathbb{Z}$. We say b divides a, denoted by $b|a$, if there exists $c \in \mathbb{Z}$ such that $a = bc$. In this a case, we say a is divisible by b, we also say a is a multiple of b.

Lemma 2.2.2 *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. The integer a is divisible by b if and only if the remainder of dividing a by b is zero.*

Proof Assume that $a, b \in \mathbb{Z}$. By Theorem 2.1.2, there exist two integers q and r such that $a = qb + r$ and $0 \leq r < |b|$. In this equation, $r = 0$ if and only if $a = qb$. ■

Definition 2.2.3 For an integer a,

1. The set $\mathrm{Div}(a) = \{b \in \mathbb{Z} : b|a\}$ is called the divisors of a.
2. The set $\mathrm{Mult}(a) = \{c \in \mathbb{Z} : a|c\}$ is called the multiples of a.

For example:

$$\mathrm{Div}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}, \mathrm{Mult}(12) = \{0, \pm 12, \pm 24, \pm 36, \ldots\} = 12\mathbb{Z}.$$
$$\mathrm{Div}(13) = \{\pm 1, \pm 13\}, \mathrm{Mult}(13) = \{0, \pm 13, \pm 26, \pm 39, \ldots\} = 13\mathbb{Z}.$$
$$\mathrm{Div}(15) = \{\pm 1, \pm 3, \pm 5, \pm 15\}, \mathrm{Mult}(15) = \{0, \pm 15, \pm 30, \pm 45, \ldots.\} = 15\mathbb{Z}.$$

Although division by zero is not defined, the first item in the following proposition shows that zero can be divided by, and is thus a multiple of, any integer.

Proposition 2.2.4

1. *Any integer is a divisor of zero, and zero is the only multiple of zero, i.e.,*

$$\mathrm{Div}(0) = \mathbb{Z} \text{ and } \mathrm{Mult}(0) = \{0\} \quad (a|0 \text{ for any } a \in \mathbb{Z}, \text{ and } 0|a \Rightarrow a = 0).$$

2. *The only divisors of* 1 *and of* -1 *are* 1 *and* -1. *Any integer is a multiple of* 1 *and of* -1, *i.e.,*

$$\mathrm{Div}(1) = \mathrm{Div}(-1) = \{\pm 1\} \text{ and } \mathrm{Mult}(1) = \mathrm{Mult}(-1) = \mathbb{Z}.$$

$$(1|a \text{ for any } a \in \mathbb{Z},\ -1|a \text{ for any } a \in \mathbb{Z}, \text{ and } a|1 \Rightarrow a = \pm 1).$$

3. *Any integer is a divisor and a multiple of itself, i.e.,*

$$a \in \mathrm{Div}(a) \text{ and } a \in \mathrm{Mult}(a) \text{ for any integer } a. \quad (a|a \text{ for any } a \in \mathbb{Z}).$$

4. *For an integer a,* $Mult(a) = a\mathbb{Z} = \{ab : b \in \mathbb{Z}\}$. *(In particular,* $Mult(0) = \{0\} = 0\mathbb{Z}$*).*

Proof

1. Let $a \in \mathbb{Z}$ be an arbitrary element. As the equation $0 \times a = 0$ holds for a, we have $a|0$, i.e., a belongs to $\mathrm{Div}(0)$, which implies that $\mathbb{Z} \subseteq \mathrm{Div}(0)$. As $\mathrm{Div}(0) \subseteq \mathbb{Z}$, then $\mathrm{Div}(0) = \mathbb{Z}$.

   If $0|a$, then there exists $b \in \mathbb{Z}$ such that $a = 0 \times b$, which implies that $a = 0$, and thus, $\mathrm{Mult}(0) = \{0\}$.
2. If $a|1$, then there exists $b \in \mathbb{Z}$ such that $1 = ab$. The only possible integer solutions for this equation are $a = 1, b = 1$ and $a = -1, b = -1$, and thus $a = \pm 1$. Since any integer a can be written as $a = a \times 1$, we have $1|a$ and $\mathrm{Mult}(1) = \mathbb{Z}$. Similar results hold for $\mathrm{Div}(-1)$ and $\mathrm{Mult}(-1)$.
3. Let a be any integer. The equation $a = a \times 1$ implies $a|a$, thereby implying both results in this item.
4. As ab is a multiple of a for any $b \in \mathbb{Z}$, then $a\mathbb{Z} \subseteq \mathrm{Mult}(a)$. In the other direction, by definition, any multiple of a is an element in $a\mathbb{Z}$. ■

Note that for any integer $a \neq 0$, the set of multiples of a, $\mathrm{Mult}(a)$, is an infinite subset of $\mathbb{Z}$.

Proposition 2.2.5 *Let a and b be two integers.*

1. *The integer b divides a if and only if −b divides a if and only if b divides −a, i.e.,*

$$b \in \mathrm{Div}(a) \Leftrightarrow -b \in \mathrm{Div}(a) \Leftrightarrow b \in \mathrm{Div}(-a).$$

   Hence, $\mathrm{Div}(a) = \mathrm{Div}(-a)$.
2. *If* $a \neq 0$, *and b divides a, then* $|b| \leq |a|$ *(The magnitude of the divisor cannot exceed that of the dividend).*
3. *If* $a|b$ *and* $b|a$, *then* $|b| = |a|$ *and vice versa (If two integers divide each other, then they may differ only in sign).*

Proof

1. The integer b divides a if and only if there exists $c \in \mathbb{Z}$ such that $a = b \times c = (-b) \times (-c)$ if and only if $-b|a$. For the second statement, $b|a$ if and only if there exists $c \in \mathbb{Z}$ such that $a = b \times c$, if and only if there exists $c \in \mathbb{Z}$ such that $-a = b \times (-c)$, if and only if there exists $d = -c \in \mathbb{Z}$ such that $-a = b \times d$, this is if and only if $b|(-a)$.
2. Assume $a \neq 0$ and $b|a$, then there exists $c \in \mathbb{Z}$ such that $a = bc$ and $c \neq 0$. Hence, $|a| = |bc| = |b||c| \geq |b| \cdot 1 = |b|$ ($|c| \geq 1$ since $c \neq 0$).
3. If $a = 0$ or $b = 0$, then by item (1) in Proposition 2.2.4, both a and b equal to zero, and thus, $|a| = 0 = |b|$. If $a \neq 0$ and $b \neq 0$, by item (2), $|a| \leq |b|$ and $|b| \leq |a|$. Therefore, $|a| = |b|$. ■

Remark 2.2.6

- Proposition 2.2.5 (2) implies that the set of divisors of any nonzero integer a, $\text{Div}(a)$, is a finite set bounded by $-|a|$ and $|a|$.

$$(a \neq 0 \Rightarrow \text{Div}(a) \subseteq \{-|a|, -|a|+1, \ldots, 0, \ldots, |a|-1, |a|\})$$

- Since $a \in \text{Div}(a)$ (Proposition 2.2.4 (3)) and $\text{Div}(a) = \text{Div}(-a)$ (Proposition 2.2.5), then $-a \in \text{Div}(a)$.

Proposition 2.2.7 *Let a, b, and c be any integers.*

1. *If $b|a$ and $a|c$, then $b|c$ (The divisibility relation is transitive).*
2. *If $b|a$ and $b|c$, then $b|(xa + yc)$ for any $x, y \in \mathbb{Z}$ (A divisor for two integers divides any linear combination of them).*
3. *If $a \neq 0$, then $ab|ac$ if and only if $b|c$.*

Proof

1. Assume that $b|a$ and $a|c$, then there exist $m, n \in \mathbb{Z}$ such that $a = mb$ and $c = na$. Therefore, $c = n(mb) = (nm)b$ and $b|c$.
2. Assume that $b|a$ and $b|c$, then there exist $m, n \in \mathbb{Z}$ such that $a = mb$ and $c = nb$. Therefore, $xa + yc = x(mb) + y(nb) = (xm + yn)b$. Since $xm + yn$ is an integer, then $b|(xa + yc)$.
3. Assume that $a \neq 0$. The integer b divides c if and only if there exists $d \in \mathbb{Z}$ such that $c = bd$ if and only if there exists $d \in \mathbb{Z}$ such that $ac = abd$, this is, if and only if $ab|ac$ ■

Example 2.2.8

1. We can show that 1 is the only positive integer that divides both 231 and 10 as follows: Assume that a is a positive integer that divides both 231 and 10. Using long division, the following mathematical statement can be obtain

$$231 = (23 \times 10) + 1$$

i.e.

$$231 - (23 \times 10) = 1.$$

Therefore, 1 is a linear combination of 231 and 10. As a divides 231 and 10, by Proposition 2.2.7 (2), a divides 1. Therefore, by Proposition 2.2.4 (2), the integer a is either 1 or -1. Since $a > 0$, then a must be 1.

2. We show that the integers 1 and 2 are the only positive integers that divide both 40 and 26 as follows: Assume that a is a positive integer such that a divides both 40 and 26. By applying long division for dividing 40 by 26, one gets

$$40 = (1 \times 26) + 14, \text{ i.e., } 40 - (1 \times 26) = 14.$$

Therefore, 14 is a linear combination of 40 and 26. As a divides 40 and 26, by Proposition 2.2.7 (2), a divides 14, i.e., a divides both 14 and 26. Repeating the same process with the numbers 14 and 26, one obtains $12 = 26 - (1 \times 14)$ and $a|12$. Repeating the same process one more time for 12 and 14, one obtains $2 = 14-(1 \times 12)$, and thus, $a|2$. By Proposition 2.2.5 (2), $|a| \leq |2| = 2$. Therefore, $a = \pm 1$ or $a = \pm 2$. As a is positive integer, then $a = 1$ or $a = 2$.

Remark 2.2.9 In Example 2.2.8 (2), the process continued until the remainder divides the smaller integer. If we applied the long division one more time and obtained a linear combination from 12 and 2, then we get $0 = 12 - (2 \times 6)$, which yields $a|0$. Since all integers divide 0, then a cannot be determined in such case. Hence, it is necessary to terminate the process at certain stage, i.e., when the remainder divides the smaller integer.

2.3 Common Divisors of Integers

This section defines the common divisors of given integers. Several essential properties of common divisors are examined, and the greatest common divisor is introduced.

Definition 2.3.1 (*Common Divisor*) Let $a, b, c \in \mathbb{Z}$. If c divides both a and b, then c is called a common divisor of a and b. The set of all common divisors of a and b is denoted by $D(a, b)$. i.e., $D(a, b) = \{c \in \mathbb{Z} : c|a \wedge c|b\}$.

For any integers a and b, $D(a, b) = D(b, a)$. As $1 \in D(a, b)$, then $D(a, b)$ is a nonempty subset of $\mathbb{Z}$.

Definition 2.3.2 Let $a_1, a_2, \ldots, a_n$ be any integers. If c divides a_i for each $1 \leq i \leq n$, then c is said to be a common divisor of $a_1, a_2, \ldots, a_n$. The set of all common divisors of $a_1, a_2, \ldots, a_n$ is denoted by $D(a_1, a_2, \ldots, a_n)$, i.e.,

$$D(a_1, a_2, \ldots, a_n) = \{c \in \mathbb{Z} : c|a_i \ \ \forall\ 1 \leq i \leq n\}.$$

As $1 \in D(a_1, a_2 \ldots a_n)$, then $D(a_1, a_2 \ldots a_n)$ is a nonempty subset of $\mathbb{Z}$. An integer a is a common divisor of any finite subset of $a\mathbb{Z}$. For example, 2 is a common divisor of any finite subset of even integers, and 3 is a common divisor of any subset of $3\mathbb{Z}$.

Lemma 2.3.3 *For any* $a \in \mathbb{Z}$,

$$D(a, a) = D(a, 0) = \text{Div}(a).$$

In particular, $D(0, 0) = \mathbb{Z}$.

Proof By definition, $D(a, a) = \{c \in \mathbb{Z} : c|a\} = \text{Div}(a)$. It is clear that $D(a, 0) \subseteq \text{Div}(a)$. For the other direction, if $c \in \text{Div}(a)$, then $c|a$. Since all integers divide 0 (Proposition 2.2.4 (1)), then $c \in D(a, 0)$. Therefore, $D(a, 0) = \text{Div}(a)$. The last statement follows as $\text{Div}(0) = \mathbb{Z}$. ■

Lemma 2.3.4 *If* $a, b \in \mathbb{Z}$ *then*

1. $D(a, b) = D(|a|, |b|)$.
2. $D(a, b) = D(a - qb, b)$ for any $q \in \mathbb{Z}$.

Proof By Proposition 2.2.5 (1), $\text{Div}(c) = \text{Div}(-c)$ for any integer c. Hence,

$$D(a, b) = D(-a, b) = D(a, -b) = D(-a, -b).$$

The result follows as $|c|$ is either c or $-c$ for any $c \in \mathbb{Z}$. For the second statement, assume that $q \in \mathbb{Z}$. If $c \in D(a, b)$, then by Proposition2.2.7 (2), c divides any linear combination of a and b. In particular, c divides $a - qb$, i.e., $c \in D(a - qb, b)$. For the other direction, let $c \in D(a - qb, b)$. As c divides both $a - qb$ and b, it divides their linear combination $(a - qb) + qb = a$. That is, $c|a$, and $c \in D(a, b)$. ■

As $D(0, 0) = \mathbb{Z}$, then $D(0, 0)$ is an unbounded set. However, if $a \neq 0$ or $b \neq 0$, then any element c in $D(a, b)$ must satisfy $-|a| \leq c \leq |a|$ or $-|b| \leq c \leq |b|$ (Remark 2.2.6). Therefore, if $a \neq 0$ or $b \neq 0$, then for any c in $D(a, b)$, the following inequality holds

$$\max\{-|a|, -|b|\} \leq c \leq \min\{|a|, |b|\}.$$

This discussion can be summarized as follows:

Lemma 2.3.5 *Let* $a, b \in \mathbb{Z}$ *such that* $a \neq 0$ *or* $b \neq 0$. *The set* $D(a, b)$ *is a nonempty finite subset of* $\mathbb{Z}$ *bounded below by max*$\{-|a|, -|b|\}$ *and above by min*$\{|a|, |b|\}$. *The set* $D(0, 0) = \mathbb{Z}$ *is an unbounded set.*

The following corollary is a direct result for Lemma 2.3.5 and Exercise 1.1.

Corollary 2.3.6 *Let $a, b \in \mathbb{Z}$ such that $a \neq 0$ or $b \neq 0$. The set $D(a, b)$ of all common divisors of a and b has a unique maximum element.*

In general, if $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that they are not all zeros. The set $D(a_1, a_2 \ldots a_n)$ of all common divisor of $a_1, a_2, \ldots, a_n$ has a unique maximum element.

Definition 2.3.7 Let a and b be integers such that at least one of them is not zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is defined as the maximum element in $D(a, b)$. The greatest common divisor of zero and zero, $\gcd(0, 0)$, is not defined.

In general,

Definition 2.3.8 Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that they are not all zeros. The greatest common divisor of $a_1, a_2, \ldots, a_n$, denoted by $\gcd(a_1, \ldots, a_n)$, is defined as the maximum element in $D(a_1, a_2, \ldots, a_n)$.

Remark 2.3.9 Let a and b are integers such that at least one of them is not zero. Since $D(a, b) = D(b, a)$, the maximum elements of the two sets are equal, i.e., $\gcd(a, b) = \gcd(b, a)$.

Corollary 2.3.10 *Let a and b be integers such that $a \neq 0$ or $b \neq 0$. Then,*

1. $\gcd(a, b) \geq 1$ *and* $\gcd(a, b) = \gcd(|a|, |b|)$.
2. *For any $q \in \mathbb{Z}$, the integers $a - qb$ and b are not both zero, and*

$$\gcd(a, b) = \gcd(a - qb, b)$$

   (i.e., *the greatest common divisor of two integers does not change if we replace one of the integers by the remainder of their division*).
3. *If $b|a$, then* $\gcd(a, b) = |b|$. *In particular, if $a \neq 0$, then* $\gcd(a, 0) = |a|$.

Proof Since $1 \in D(a, b)$, we have $\gcd(a, b) \geq 1$. As $D(a, b) = D(|a|, |b|)$, the maximum elements of the two sets are equal. For the second statement, assume q to be any integer. If both b and $a - qb$ are zero, then $a = (a - qb) + qb = 0 + 0 = 0$, which contradicts the corollary's assumption. Hence, b and $a - qb$ cannot be both zero. The equality in (2) follows as $\mathrm{D}(a, b) = \mathrm{D}(a - qb, b)$ (Lemma 2.3.4). For the last statement, assume that $b|a$, then $|b| \in D(a, b)$. The result follows by Lemma 2.3.5 as any element in $D(a, b)$ is less than or equal to $|b|$. ■

2.4 Euclidean Algorithm (Euclid's Algorithm)

The Euclidean algorithm, or Euclid's algorithm can be used to determine the greatest common divisor of two integers. As $\gcd(a, b) = \gcd(|a|, |b|)$ (Corollary 2.3.10),

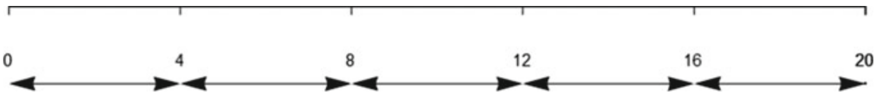


Fig. 2.1 The integer 4 measures 20

we only consider nonnegative integers in applying the Euclidean algorithm. The method was established by the Greek mathematician Euclid (300 BC). In that period, mathematics focused on geometry. Mathematicians described positive integers as lengths of intervals (sticks). Hence, the statement "*b* divides *a*" was expressed as "*b* measures *a*", which means that stick *b* could be used to measure *a*. The following illustration shows how 4 measures 20 (Fig. 2.1).

The Greeks called the common divisor, the common measure. The problem was to determine the largest common measure that can be used to measure lengths (sticks) *a* and *b*. Euclid adopted the idea of using the shorter stick, let us say *b*, to measure the longer stick *a*. If the measurement could be performed, then *b* is the required largest common measure. However, this scenario is not always possible. For example, 9 is not a suitable candidate for the scale measurement of the lengths 24 and 9. A stick with length of 9 cannot be used to measure 24 as there will be part with length 6 that cannot be measured by 9 (Figs. 2.2 and 2.3).

Remarkably, Euclid noticed that the required scale measurement for 24 and 9 must also measure the remainder 6. Thus, instead of using sticks of length 24 and 9, Euclid had many sticks of length 9 and one stick of length 6. To measure these sticks, it is necessary to use a scale measurement that can measure 9 and 6. Hence, the problem of finding the largest scale measurement for 24 and 9 turns into a problem of finding the largest scale measurement for 9 and 6. Applying the same process on lengths 9 and 6, it is necessary to determine the largest scale measurement that can measure 6 and 3. Since 3 can measure 6, then 3 is the largest common measurement for 3

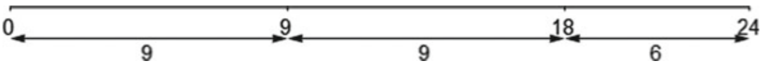


Fig. 2.2 The integer 9 does not measure 24

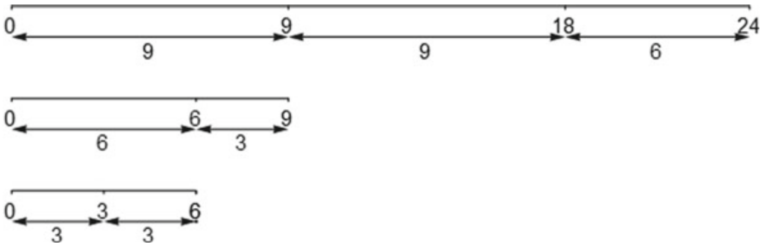
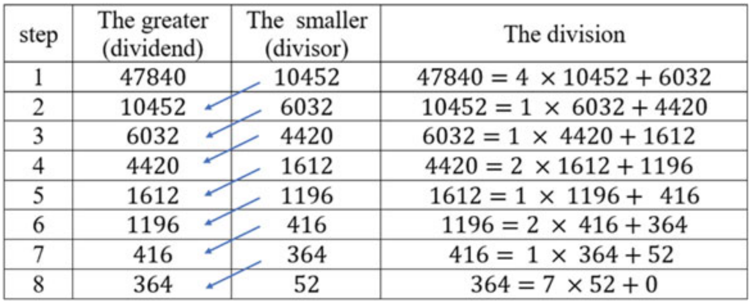


Fig. 2.3 The largest common measurement that measures 3, 6, 9, and 24

Table 2.1 The Euclidean algorithm's steps to find the common divisor of 47840 and 10452



step	The greater (dividend)	The smaller (divisor)	The division
1	47840	10452	47840 = 4 × 10452 + 6032
2	10452	6032	10452 = 1 × 6032 + 4420
3	6032	4420	6032 = 1 × 4420 + 1612
4	4420	1612	4420 = 2 × 1612 + 1196
5	1612	1196	1612 = 1 × 1196 + 416
6	1196	416	1196 = 2 × 416 + 364
7	416	364	416 = 1 × 364 + 52
8	364	52	364 = 7 × 52 + 0

and 6. Therefore, 3 is the largest common measurement that can be used to measure 3, 6, 9, and 24. This method to find the greatest common divisor for two integers is known as the Euclidean algorithm.

Euclidean Algorithm 2.4.1 The greatest common divisor of two positive integers can be computed using the following steps:

1. Determine the greater integer, call it a, and label the other integer b.
2. Divide a by b and determine the remainder r.
3. If $r \neq 0$, replace a by b, and replace b by r.
4. Repeat steps (2) and (3) until $r = 0$.
5. Return the last value of b.

The outcome of the Euclidean algorithm is the greatest common divisor of the two integers.

Example 2.4.2 Table 2.1 summarizes the steps of the Euclidean algorithm to find the common divisor of 47840 and 10452. According to the Euclidean algorithm, the greatest common divisor is 52.

The next goal is to show that the output of the Euclidean algorithm is the greatest common divisor of the two input integers. To better understand the applied algorithm, we analyze it for positive integers a and b as follows: let a and b be any positive integers such that $a \geq b$. Let $a = a_0,\ b = b_0$ and apply the Euclidean algorithm on a_0 and b_0. The process generates the following equations:

$$a_0 = q_0 b_0 + r_0 \text{ such that } q_0, r_0 \in \mathbb{Z} \text{ and } 0 \leq r_0 < b_0$$

$$(\text{If } r_0 \neq 0,\ \text{ let } a_1 = b_0, b_1 = r_0 \text{ and apply the division algorithm on } a_1, b_1)$$

$$a_1 = q_1 b_1 + r_1 \text{ such that } q_1, r_1 \in \mathbb{Z} \text{ and } 0 \leq r_1 < b_1 = r_0$$

$$(\text{If } r_1 \neq 0, \text{ let } a_2 = b_1, b_2 = r_1 \text{ and apply the division algorithm on } a_2, b_2)$$

$$a_2 = q_2 b_2 + r_2 \text{ such that } q_2, r_2 \in \mathbb{Z} \text{ and } 0 \leq r_2 < b_2 = r_1$$

$$\vdots\ \vdots \qquad\qquad \vdots\ \ \vdots\ \vdots$$

$$(\text{If } r_{k-1} \neq 0, \text{ let } a_k = b_{k-1}, b_k = r_{k-1}, \text{ and apply the division algorithm on } a_k, b_k)$$

$$a_k = q_k b_k + r_k \text{ such that } q_k, b_k \in \mathbb{Z} \text{ and } 0 \leq r_k < b_k = r_{k-1}$$

$$\vdots\ \vdots \qquad\qquad \vdots\ \ \vdots\ \vdots$$

The algorithm iterates until $a_n = q_n b_n + r_n$ such that q_n, $b_n \in \mathbb{Z}$ and $r_n = 0$. Then, the process is terminated, yielding b_n as the output.

Remark 2.4.3 Applying the Euclidean algorithm on two positive integers generates a list of.

1. Decreasing nonnegative integers r_k, where $0 \leq k \leq n$, and $r_n = 0$.
2. Equations $a_k = q_k b_k + r_k$ such that $q_k, r_k \in \mathbb{Z}$, and $0 \leq r_k < b_k$, $0 \leq k \leq n$, where for each $k \geq 1$, $a_k = b_{k-1}$ and $b_k = r_{k-1}$.

The process used in the Euclidean algorithm is implemented by applying long division (division algorithm) in each step. By Corollary 2.3.10 (2), the greatest common divisor does not change in each step. For each k, $a_k = b_{k-1}$ and $b_k = r_{k-1}$, which implies that

$$\begin{aligned}\gcd(a_k, b_k) = \gcd(b_k, a_k) &= \gcd(r_{k-1}, b_{k-1}) \\ &= \gcd(a_{k-1} - q_{k-1}b_{k-1}, b_{k-1}) = \gcd(a_{k-1}, b_{k-1}).\end{aligned}$$

That is, the greatest common divisor is preserved in each step during the process of applying the Euclidean algorithm, as proven in the following lemma.

Lemma 2.4.4 *Let $a, b \in \mathbb{N}$ such that $a \geq b$. In applying the Euclidean algorithm on a and b,*

$$\gcd(a, b) = \gcd(a_k, b_k)$$

for all $0 \leq k \leq n$. The integers a_k, and b_k are defined in the Euclidean algorithm.

Proof Following the algorithm, let $a = a_0$ and $b = b_0$. The result is obtained using the mathematical induction on k.

- If $k = 0$, then $\gcd(a, b) = \gcd(a_0, b_0)$ as required.

- Assume that the equality holds for $k-1$, i.e., $\gcd(a, b) = \gcd(a_{k-1}, b_{k-1})$.
- Using Corollary 2.3.10 (2) and the argument after Remark 2.4.3, one can show that $\gcd(a_k, b_k) = \gcd(a_{k-1}, b_{k-1})$. By induction hypothesis, this is equal to $\gcd(a, b)$ as required.

By the abovementioned steps, and the principle of mathematical induction, the result holds for any k such that $0 \le k \le n$. ■

Corollary 2.4.5 *Let $a, b \in \mathbb{N}$, such that $a \ge b$. The returned integer after applying the Euclidean algorithm on a and b is their greatest common divisor.*

Proof By Lemma 2.4.4, $\gcd(a, b) = \gcd(a_k, b_k)$ for all $0 \le k \le n$. In particular,

$$\gcd(a, b) = \gcd(a_n, b_n).$$

Using the result of Corollary 2.3.10 (2), we obtain

$$\begin{aligned}\gcd(a, b) &= \gcd(a_n, b_n) = \gcd(b_n, a_n - q_n b_n)\\ &= \gcd(b_n, r_n) = \gcd(b_n, 0) = b_n. \qquad ■\end{aligned}$$

In the following example, the Euclidean algorithm is applied to find the greatest common divisor of 57970 and 10353.

$$\begin{aligned}\gcd(47840, 10452) &= \gcd(10452, 6032) = \gcd(6032, 4420)\\ &= \gcd(4420, 1612) = \gcd(1612, 1196) = \gcd(1196, 416)\\ &= \gcd(416, 364) = \gcd(364, 52) = \gcd(52, 0) = 52.\end{aligned}$$

2.5 Bézout's Lemma (Bézout's Identity)

As shown in Proposition 2.2.7 (2), a divisor for two integers also divides any linear combination of them. Therefore, the greatest common divisor of two integers divides any linear combination of these integers. Furthermore, as we show below, the greatest common divisor of two integers is the only positive divisor that can be expressed as a linear combination of the two integers. The idea is attributed to the French mathematician É. Bézout.

Theorem 2.5.1 (Bézout's lemma) *For any $a, b \in \mathbb{Z}$, such that $a \neq 0$ or $b \neq 0$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$ i.e., $\gcd(a, b)$ can be written as a linear combination of a and b.*

A generalization of Bézout's lemma (Exercise 2.9) is the following.

Theorem 2.5.2 *Let $a_1, a_2, \ldots, a_k$ be integers at least one of which is nonzero. There exist $x_i \in \mathbb{Z}$, $1 \le i \le k$ such that $\gcd(a_1, a_2, \ldots, a_k) = x_1 a_1 + x_2 a_2 + \cdots + x_k a_k$.*

Recall that in computing $\gcd(a, b)$, we built a sequence of long divisions $a_i = q_i b_i + r_i$, where $a_0 = a, b_0 = b$, and for each $2 \le i \le k$, $a_i = b_{i-1}, b_i = r_{i-1}$ with, in the final step, $r_k = 0$, i.e., b_k a divisor of a_k (Remark 2.4.3). We showed that $\gcd(a, b) = b_k = \gcd(a_i, b_i)$ for $1 \le i \le k$. Next, we discuss two methods used to write the greatest common divisor of two numbers as a linear combination of these numbers. The two methods utilize the same steps that were used in the Euclidean algorithm to determine the gcd. In backward substitution method, we start with the step before the last $a_{k-1} = q_{k-1}b_{k-1} + b_k$, which since $\gcd(a, b) = b_k$, can be rewritten as

$$\gcd(a, b) = a_{k-1} - q_{k-1}b_{k-1}$$

yielding the gcd as a linear combination of a_{k-1} and b_{k-1}. Having managed to write

$$\gcd(a, b) = x_i a_i + y_i b_i, \text{ where } 1 < i \le k - 1. \tag{2.1}$$

Since $b_i = r_{i-1} = a_{i-1} - q_{i-1}b_{i-1}$ and $a_i = b_{i-1}$, we can by substituting for b_i and $a_i = b_{i-1}$ at (2.1) getting the following expression

$$\gcd(a, b) = x_i b_{i-1} + y_i (a_{i-1} - q_{i-1}b_{i-1}) = x_{i-1}a_{i-1} + y_{i-1}b_{i-1}$$

Continuing this process, we finally obtain $\gcd(a, b) = x_1 a + y_1 b$.

Example 2.5.3 (Backward substitution) According to Example 2.4.2, the greatest common divisor of $a = 47840$ and $b = 10452$ is 52. Consider the list of equations used to find the $\gcd(a, b)$ in Example 2.4.2. Starting with step 7, we rewrite it as

$$52 = (1 \times 416) - (1 \times 364).$$

This equation expresses 52 as a linear combination, but not that of a and b. According to step 6, $364 = 1196 - (2 \times 416)$**,** which implies that

$$\begin{aligned} 52 &= (1 \times 416) - (1 \times (1196 - (2 \times 416))) \\ &= (-1 \times 1196) + (3 \times 416). \end{aligned}$$

This process only takes us one step up (closer to a and b). Repeating the same process with step 5, we obtain $416 = 1612 - (1 \times 1196)$, which implies that

$$\begin{aligned} 52 &= (-1 \times 1196) + (3 \times 416) = (-1 \times 1196) + 3(1612 - (1 \times 1196)) \\ &= (3 \times 1612) - (4 \times 1196). \end{aligned}$$

See Table 2.2.

Again, using the equation in step 4 to substitute $1196 = 4420 - (2 \times 1612)$ yields

$$52 = (3 \times 1612) - (4 \times 1196)$$

Table 2.2 The Euclidean algorithm applied to 47840 and 10452

1	$47840 = 4 \times 10452 + 6032$
2	$10452 = 1 \times 6032 + 4420$
3	$6032 = 1 \times 4420 + 1612$
4	$4420 = 2 \times 1612 + 1196$
5	$1612 = 1 \times 1196 + 416$
6	$1196 = 2 \times 416 + 364$
7	$416 = 1 \times 364 + 52$
8	$364 = 7 \times 52 + 0$

$$\begin{aligned} &= (3 \times 1612) - (4 \times (4420 - (2 \times 1612))) \\ &= (-4 \times 4420) + (11 \times 1612). \end{aligned}$$

Using the equation in step 3, to substitute $1612 = 6032 - (1 \times 4420)$ yields

$$\begin{aligned} 52 &= (-4 \times 4420) + (11 \times 1612) \\ &= (-4 \times 4420) + (11 \times (6032 - (1 \times 4420))) \\ &= (11 \times 6032) + (-15 \times 4420). \end{aligned}$$

Using the equation in step 2, to substitute $4420 = 10{,}452 - (1 \times 6032)$ implies that

$$\begin{aligned} 52 &= (11 \times 6032) + (-15 \times 4420) \\ &= (11 \times 6032) + (-15 \times (10452 - (1 \times 6032))) \\ &= (-15 \times 10452) + (26 \times 6032). \end{aligned}$$

Using step 1 to substitute $6032 = 47840 - (4 \times 10452)$, which finally yields

$$\begin{aligned} 52 &= (-15 \times 10452) + (26 \times 6032) \\ &= (-15 \times 10353) + (26 \times (47840 - (4 \times 10452))) \\ &= (26 \times 47840) + (-119 \times 10452). \end{aligned}$$

This expression is the required linear combination for $\gcd(a, b)$.

The method used in solving Example 2.5.3 involves processing the steps in the Euclidean algorithm in the reverse order (backwards). Another method, used to express the $\gcd(a, b)$ as linear combinations of a and b, applies the process of the Euclidean algorithm in normal order (forwards) starting from the first equation in the algorithm and working toward the last one. Ignoring the trivial and easily handled cases, where one of the two numbers is a multiple of the other, or where the remainder of the first division is the greatest common divisor, the forward method starts at the first two divisions and express their remainder as a linear combination of a and b.

$$r_1 = a_1 - q_1 b_1 = a - q_1 b = x_1 a + y_1 b$$

and

$$r_2 = a_2 - q_2 b_2 = b_1 - q_2 r_1 = b - q_2(a - q_1 b) = x_2 a + y_2 b.$$

Having expressed r_j, the remainder in step j as a linear combination $r_j = x_j a + y_j b$ of a and b for all $1 \leq j < i$, where $3 \leq i < k - 1$, substituting the last two obtained expressions yields

$$a_i = b_{i-1} = r_{i-2} = x_{i-2} a + y_{i-2} b \text{ and } b_i = r_{i-1} = x_{i-1} a + y_{i-1} b$$

and then

$$r_i = a_i - q_i b_i = (x_{i-2} a + y_{i-2} b) - q_i (x_{i-1} a + y_{i-1} b) = x_i a + y_i b.$$

In the step $i = k - 1$, the desired expression for $r_{k-1} = x_{k-1} a + y_{k-1} b$ is obtained.

Example 2.5.4 (Forward substitution) Consider the list of equations used to find the $\gcd(a, b)$ in Example 2.4.2. We start by writing the first two remainders as linear combinations of a and b

$$6032 = (1 \times 47840) - (4 \times 10452)$$

and

$$\begin{aligned} 4420 &= 10452 - (1 \times 6032) \\ &= 10452 - (1 \times ((1 \times 47840) - (4 \times 10452))) \\ &= (-1 \times 47840) + (5 \times 10452). \end{aligned}$$

Subsequently, we use the last two obtained expressions for remainders to express the new remainder as a linear combination of a and b. From line 3, using the last two expressions obtained above, we have

$$\begin{aligned} 1612 &= 6032 - (1 \times 4420) \\ &= ((1 \times 47840) - (4 \times 10452)) - (1 \times ((-1 \times 47840) + (5 \times 10452))) \\ &= (2 \times 47840) - (9 \times 10452). \end{aligned}$$

From line 4, using the last two expressions obtained, we have

$$\begin{aligned} 1196 &= 4420 - (2 \times 1612) \\ &= ((-1 \times 47840) + (5 \times 10452)) - (2 \times ((2 \times 47840) - (9 \times 10452))) \\ &= (-5 \times 47840) + (23 \times 10452). \end{aligned}$$

From line 5 using the last two expressions obtained, we have

$$\begin{aligned}416 &= 1612 - (1 \times 1196)\\ &= ((2 \times 47840) - (9 \times 10452)) - (1 \times ((-5 \times 47840) + (23 \times 10452)))\\ &= (7 \times 47840) - (32 \times 10452).\end{aligned}$$

Repeating the process with line 6 we obtain

$$\begin{aligned}364 &= 1196 - (2 \times 416)\\ &= ((-5 \times 47840) + (23 \times 10452)) - (2 \times ((7 \times 47840) - (32 \times 10452)))\\ &= (-19 \times 47840) + (87 \times 10452).\end{aligned}$$

Finally, using line 7 we obtained the desired expression

$$\begin{aligned}52 &= 416 - (1 \times 364)\\ &= ((7 \times 47840) - (32 \times 10452)) - (1 \times ((-19 \times 47840) + (87 \times 10452)))\\ &= (26 \times 47840) + (-119 \times 10452).\end{aligned}$$

We terminate this process since we obtained 52 as a linear combination of a, b. We end this section by listing several corollaries of Bézout's lemma.

Corollary 2.5.5 *Let $a, b \in \mathbb{Z}$ such that at least one of them is nonzero. The greatest common divisor of a and b is the only positive common divisor of a and b that can be written as a linear combination of them.*

Proof Let c be a common divisor of a and b that can be written as a linear combination of a and b. As the $\gcd(a, b)$ divides both a and b, then by Proposition 2.2.7 (2), $\gcd(a, b)$ divides c. Similarly, since $\gcd(a, b)$ is a linear combination of a and b (Bézout's lemma), and c divides both a and b, then by Proposition 2.2.7 (2), c divides $\gcd(a, b)$. According to Proposition 2.2.5 (3),

$$\gcd(a, b) = |\gcd(a, b)| = |c|. \quad \text{Thus } c = \pm\gcd(a, b). \qquad \blacksquare$$

The proof of Corollary 2.5.5 shows a stronger result than the statement in Corollary 2.5.5. It shows that the only common divisors of a and b that can be written as a linear combination of a and b are $\gcd(a, b)$ and $-\gcd(a, b)$. The following corollary is a direct result of Corollary 2.5.5, and Bézout's lemma. The corollary follows from 1 being a common divisor for any two integers.

Corollary 2.5.6 *Let $a, b \in \mathbb{Z}$ such that they are not both zero, then*

$$\gcd(a, b) = 1 \text{ if and only if there exist } x, y \in \mathbb{Z} \text{ such that } xa + yb = 1.$$

Corollary 2.5.7 *Let $a, b \in \mathbb{Z}$ such that they are not both zero. If $c \in \mathbb{Z}$ is a nonzero integer, then*

1. $c|a \wedge c|b \Rightarrow c|\gcd(a, b)$ *(Any divisor for two integers divides their* gcd*).*
2. $c|ab \wedge \gcd(a, c) = 1 \Rightarrow c|b$.
3. $c|a \wedge b|a \wedge \gcd(b, c) = 1 \Rightarrow bc|a$.

Proof

1. Since c divides a and b, it divides any linear combination of them (Proposition 2.2.7 (2)), Bézout's lemma implies the result.
2. Assume that $c|ab \wedge \gcd(a, c) = 1$. According to Bézout's lemma, there exist x, y $\in \mathbb{Z}$ such that $xc + ya = 1$. By multiplying both sides by b, we obtain $x(cb) + y(ab) = b$. As $c|cb$ and $c|ab$, then by Proposition 2.2.7 (2), c divides b.
3. Assume that $c|a$, $b|a$ and $\gcd(b, c) = 1$. Since $c|a$, then $a = qc$ for some integer q, thus $b|qc$. However, as $\gcd(b, c) = 1$, then by (2), $b|q$. Therefore, there exists $z \in \mathbb{Z}$ such that $q = zb$. Hence,

$$a = qc = (zb)c = z(bc).$$

That is, bc divides a. ■

2.6 Relatively Prime Integers

For nonzero integers, the term "relatively prime" means that they have no common divisor with a magnitude larger than 1. If the integers a and b do not belong to $\{0, \pm 1\}$, then being relatively prime guarantees that neither of them divides the other.

Definition 2.6.1 Let $a, b \in \mathbb{Z}$ such that they are not both zero. The integers a and b are called relatively prime (or coprime) if $\gcd(a, b) = 1$.

According to Corollary 2.5.6, two integers are relatively prime if and only if 1 can be written as a linear combination of them. From this, it follows that the relatively prime relation is symmetric. It is not transitive relation on the set of integers, as $\gcd(4, 7) = 1$ and $\gcd(7, 8) = 1$, but $\gcd(4, 8) = 4 \neq 1$. Clearly, the relatively prime relation is not reflexive.

Proposition 2.6.2 *Let $a, b, c \in \mathbb{Z}$. If a, b are relatively prime, and a, c are relatively prime, then a and bc are relatively prime* ($\gcd(a, b) = 1, \gcd(a, c) = 1 \Rightarrow \gcd(a, bc) = 1$).

Proof Assume that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. According to Corollary 2.5.6, there exist $x, y \in \mathbb{Z}$ such that $xa + yb = 1$, and there exist $u, v \in \mathbb{Z}$ such that $ua + vc = 1$. Hence,

$$(xa + yb)(ua + vc) = (xua + xvc + ybu)a + (yv)bc = 1.$$

i.e., there exists $k = xua + xvc + ybu$, and $l = yv$ such that $ka + l(bc) = 1$. The result follows by Corollary 2.5.6. ■

Proposition 2.6.3 *Let $a, b \in \mathbb{Z}$ such that they are not both zero. The integers $a/gcd(a, b)$ and $b/gcd(a, b)$ cannot both be zero and are relatively prime.*

Proof Let $a_1 = a/\text{gcd}(a, b)$ and $b_1 = b/\text{gcd}(a, b)$. Since $\text{gcd}(a, b)$ divides both a and b, both a_1 and b_1 are integers. Moreover, they are not both zero since a and b are not both zero. Suppose that a_1 and b_1 have a common divisor $d > 1$, i.e.,

$$\exists\, a_2, b_2 \in \mathbb{Z} \ni\ a_1 = da_2 \ \wedge\ b_1 = db_2 \ \text{ where } \ d > 1.$$

Therefore,

$$a = \text{gcd}(a, b)a_1 = \text{gcd}(a, b)(da_2) = (\text{gcd}(a, b)d)a_2$$

and

$$b = \text{gcd}(a, b)b_1 = \text{gcd}(a, b)(db_2) = (\text{gcd}(a, b)d)b_2.$$

Thus, $\text{gcd}(a, b)d$ is a common divisor of a and b, and

$$\text{gcd}(a, b)d > \text{gcd}(a, b) \cdot 1 = \text{gcd}(a, b)$$

contradicting the definition of gcd as the largest common divisor. ■

Corollary 2.6.4 *For any $a, b \in \mathbb{Z}$ that are not both zero, there exist two integers d, t such that $a = d\ \text{gcd}(a, b)$, $b = t\ \text{gcd}(a, b)$ and $\text{gcd}(d, t) = 1$.*

Proposition 2.6.5 *Let $a, b \in \mathbb{Z}$ such that they are not both zero.*

1. The linear Diophantine equation $xa + yb = d$ has integer solutions if and only if $\text{gcd}(a, b)|d$.
2. If there is an integer solution of $xa + yb = d$, then there are infinitely many solutions. Namely, if (x_0, y_0) is an integer solution for $xa + yb = d$, the solutions of the equation are

$$x = x_0 + \frac{b}{\text{gcd}(a, b)}t,\ \ y = y_0 - \frac{a}{\text{gcd}(a, b)}t, \quad t \in \mathbb{Z}.$$

Example 2.6.6 To determine whether the equation $49x + 14y = 35$ has an integer solution, one finds that $\text{gcd}(49, 14) = 7$. Since 7 divides 35, the equation $49x + 14y = 35$ has integer solutions. To determine a solution, we write 7 as a linear combination of 49 and 14 to obtain

$$(1 \times 49) - (3 \times 14) = 7.$$

Multiplying both sides by $5(= 35/\text{gcd}(49, 14))$ yields

$$5 \times 49 - 15 \times 14 = 35.$$

Therefore, $x_0 = 5$, $y_0 = -15$ is a solution for the given equation. The other solutions are $x = 5 + (14/7)t,\ y = -15 - (49/7)t$, where $t \in \mathbb{Z}$.

The following definition is a generalization of the concept of relatively prime.

Definition 2.6.7 Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}^*$. The integers $a_1, a_2, \ldots a_k$ are called pairwise relatively prime (pairwise coprime) if $\gcd\big(a_i, a_j\big) = 1$ for all $1 \le i \ne j \le k$.

Proposition 2.6.8 *Let* $a_1, a_2, \ldots, a_n \in \mathbb{Z}^*$ *and* $s \in \mathbb{N}$. *For any* $b \in \mathbb{Z}$, *if* $\gcd(b, a_i) = 1$ *for all* $1 \le i \le s$, *then* $\gcd(b, a_1 \cdot a_2 \cdot \cdots \cdot a_s) = 1$.

Proof The proof is by mathematical induction on s.

- The statement is true for $s = 1$, as by assumption, $\gcd(b, a_1) = 1$.
- Assume that the statement is true for $s = k$.
- Let $s = k + 1$, and assume that $\gcd(b, a_i) = 1$ for all i such that$1 \le i \le k + 1$. By induction hypothesis, $\gcd(b, a_1 \cdot \cdots \cdot a_k) = 1$ and $\gcd(b, a_{k+1}) = 1$, so by Proposition 2.6.2,

$$\gcd(b, a_1 \cdot a_2 \cdot \cdots \cdot a_{k+1}) = \gcd(b, (a_1 \cdot a_2 \cdot \cdots \cdot a_k) \cdot a_{k+1}) = 1.$$

By mathematical induction, the statement is true for all $s \in \mathbb{N}$. ■

Corollary 2.6.9 *Let* $a_1, a_2, \ldots, a_n \in \mathbb{Z}^*$ *such that* $a_1, a_2, \ldots a_n$ *are pairwise relatively prime. For each* $1 \le i \le n$, $\gcd(a_i, a_1 \cdot a_2 \cdot a_{i-1} \cdot a_{i+1} \cdots \ \cdots a_n) = 1$.

The following statement is a generalization of part (3) in Corollary 2.5.7.

Proposition 2.6.10 *Let* $a_1, a_2, \ldots, a_n \in \mathbb{Z}^*$, *where* $a_1, a_2, \ldots, a_n$ *are pairwise relatively prime. Let* $M \in \mathbb{Z}$. *If* $a_i | M$ *for all* $1 \le i \le n$, *then* $(a_1 \cdot a_2 \cdots a_n) | M$.

2.7 Common Multiples of Integers

In this section, the common multiples of two integers are defined, and several basic properties of these multiples are stated.

Definition 2.7.1 Let $a, b \in \mathbb{Z}$. A common multiple of a and b is an integer c such that c is divisible by both a and b, i.e., $a|c$ and $b|c$. The set of common multiples of a and b is denoted by $M(a, b)$. Therefore, $M(a, b) = \{c \in \mathbb{Z} : a|c \wedge b|c\}$.

For any two integers a, b, the set $M(a, b)$ is nonempty as for any $q \in \mathbb{Z}$, $abq \in M(a, b)$).

Definition 2.7.2 Let $a_1, a_2, \ldots, a_n$ be integers. A common multiple of $a_1, a_2, \ldots, a_n$ is an integer c such that c is divisible by each of these integers. The set of common multiples of $a_1, a_2, \ldots, a_n$ is denoted by $M(a_1, a_2, \ldots, a_n)$, i.e.,

$$M(a_1, a_2 \ldots a_n) = \{c \in \mathbb{Z} : a_i | c \ \ \forall\ 1 \leq i \leq n\}.$$

An example of a common multiple is the number billion, 10^9. This number is a common multiple of each of $1, 10, 100, \ldots, 10^9$ and $-1, -10, -100, \ldots, -10^9$.

Proposition 2.7.3 *For any integer a,*

$$M(a, 0) = \{0\} \text{ and } M(a, a) = Mult(a) = a\mathbb{Z}.$$

Proof As $0|0$ and $a|0$ for any $a \in \mathbb{Z}$ (Proposition 2.2.4 (1)), $0 \in M(a, 0)$. Moreover, as zero is the only multiple of zero (Proposition 2.2.4 (1)), $M(a, 0) \subseteq \{0\}$. Thus, $M(a, 0) = \{0\}$. The second statement follows by the definition. ■

Proposition 2.7.4 *For any $a, b \in \mathbb{Z}$,*

1. *$M(a, b)$ is a nonempty subset of integers that is infinite if both a and b are not zeros.*
2. *$M(a, b) = M(b, a)$.*
3. *$M(a, b) = M(|a|, |b|)$.*

Proof The set $M(a, b)$ contains $ab\mathbb{Z} = \{(ab)q : q \in \mathbb{Z}\}$, and thus, it is a nonempty set. If both a, b are not zero, then $ab\mathbb{Z}$ is an infinite set, and so is $M(a, b)$. The second statement follows immediately from the definition. Finally, as $x|c \iff -x|c$, then.

$$M(a, b) = M(-a, b) = M(a, -b) = M(-a, -b).$$

The required conclusion follows by choosing the appropriate sign. ■

Note that c is a common multiple of a and b if and only if $-c$ is a common multiple of them. For any nonzero integers a and b, let $M(a, b)^+$ be the set of positive common multiples of a and b. Since $M(a, b)^+$ contains $|a||b|$, the set $M(a, b)^+$ is nonempty, bounded below by zero. Therefore, $M(a, b)^+$ contains a least element.

Definition 2.7.5 Let $a, b \in \mathbb{Z}$. The least common multiple of a and b, denoted $\operatorname{lcm}(a, b)$, is defined as the least element in the set $M(a, b)^+$ when a and b are both nonzero. If either a or b is zero, the least common multiple is defined to be zero.

The next proposition yields a formula to calculate the least common multiple for two integers using their greatest common divisor.

Proposition 2.7.6 *Let $a, b \in \mathbb{Z} \setminus \{0\}$. The least common multiple of a and b is*

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Remark 2.7.7 The relation in Proposition 2.7.6 implies many similarities between the gcd and lcm for two integers. For example, the commutativity of the gcd (Remark 2.3.9) is implied for the lcm as well, i.e., $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$.

Proposition 2.7.8 *Let $a, b \in \mathbb{N}$. The maps*

$$\begin{aligned} f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad &\wedge \quad g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ \textit{defined by } f(a, b) = \gcd(a, b) \quad &\quad g(a, b) = \operatorname{lcm}(a, b) \end{aligned}$$

for all $a, b \in \mathbb{N}$, form functions on $\mathbb{N}$.

Proof Let (a, b) be any element in $\mathbb{N} \times \mathbb{N}$. As both gcd and lcm are defined for any positive integers and are both positive integers (Corollary 2.3.10 (1) and Proposition 2.7.6), then $f(a, b)$ and $g(a, b)$ define an element in $\mathbb{N}$. The uniqueness of the gcd implies that $f(a, b)$ is a unique element in $\mathbb{N}$. Proposition 2.7.6 then implies that $g(a, b)$ is also a unique element in $\mathbb{N}$. ■

2.8 Prime Numbers and the Fundamental Theorem of Arithmetic

In this section, we examine a special subset of integers known as prime numbers. The fundamental theorem of arithmetic is stated and proved. We restrict our study to positive integers $\mathbb{N}$.

Definition 2.8.1 The integer p > 1 is called a prime if the only positive divisors of p are p and 1.

That is, p is a prime if and only if $\operatorname{Div}(p)$ is exactly the set $\{\pm 1, \pm p\}$ (Definition 2.2.3). Note that, by definition, the integer 1 is not a prime. The integers

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

are examples of prime numbers. In dealing with small integers, it is relatively easy to decide whether the given number is a prime by checking its divisibility by each integer that is less than or equal to it. However, for large numbers, no convenient method exists for checking primality. For any integer a and a prime p, if $p|a$, then by Corollary 2.3.10 (3), $\gcd(a, p) = |p| = p$. If p $\nmid$ a, then the common divisors of p and a are only $\{\pm 1\}$, which implies the following lemma.

Lemma 2.8.2 *If $a \in \mathbb{Z}$, and p is prime, then*

$$\gcd(a, p) = \begin{cases} p & \text{if } p|a \\ 1 & \text{if } p \nmid a \end{cases}$$

Proposition 2.8.3 (Euclid's Lemma) *Let $n \in \mathbb{N}$, and p be a prime number. If $a_1, a_2, \dots, a_n$ are integers such that $p|(a_1 \cdot a_2 \cdot \cdots \cdot a_n)$, then $p|a_j$ for some j, where $1 \leq j \leq n$ (If a prime divides a multiplication of integers, then it divides at least one of them).*

Proof The proof is conducted by induction on n. If $n = 1$, the statement is obviously true. Assume that the statement is true for $n = k$. Let $n = k + 1$ and assume that $p|(a_1 \cdot a_2 \cdot \cdots\cdots \cdot a_{k+1})$. If $p|a_{k+1}$, the result follows by taking $j = k + 1$. If $p \nmid a_{k+1}$, then by Lemma 2.8.2, $\gcd(p, a_{k+1}) = 1$. Thus, by Corollary 2.5.7 (2), p must divide $a_1 \cdot a_2 \cdots\cdots a_k$. By induction hypothesis, there exists j, $1 \leq j \leq k < k + 1$ such that $p|a_j$. Thus, by induction, the result is true for all positive integers. ■

The above lemma is not true if one does not assume that p is a prime number. For example, $6|(9 \times 2)$, but 6 does not divide 9 or 2. Therefore, the assumption that p is a prime in Euclid's lemma is essential.

Corollary 2.8.4 Let p, q be prime numbers. If $p|q^n$ for some $n \in \mathbb{N}$, then $p = q$.

Proof Assume that $p\left|\left(\underbrace{q \cdot q \cdot \cdots \cdot q}_{n\ times}\right)\right.$. Euclid's lemma (Proposition 2.8.3) implies that p divides q. As the only divisors of q are $\{\pm 1, \pm q\}$ and $p > 1$, then $p = q$. ■

Proposition 2.8.5 *Let $s \in \mathbb{N}$, and $p, p_1, p_2, \dots, p_s$ be a set of prime integers. Let $k_1, \dots, k_s$ be nonnegative integers. If $p|\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}\right)$, then $p = p_i$ for some $1 \leq i \leq s$.*

Proof Assume that $p|\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}\right)$. According to Euclid's lemma (Proposition 2.8.3), there exists i, $1 \leq i \leq s$ such that $p|p_i^{k_i}$. If $k_i = 0$, then $p|1$, which contradicts that p is prime, so $k_i \in \mathbb{N}$. Corollary 2.8.4 then implies the result. ■

By the transitivity of divisibility (Proposition 2.2.7 (1)), and Proposition 2.8.5, the following result can be easily proved.

Corollary 2.8.6 *Let $s \in \mathbb{N}$, and $p_1, p_2, \dots, p_s$ be a set of prime integers. Let $k_1, \dots, k_s$ be nonnegative integers. If n is an integer such that $n|\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}\right)$, then $\{p_1, p_2, \dots, p_s\}$ contains all the prime divisors of n.*

Next, we state and prove the fundamental theorem of arithmetic.

Theorem 2.8.7 (Fundamental theorem of arithmetic) *Any positive integer greater than 1 can be uniquely, up to reordering, written as a product of prime numbers, i.e., For all $n \in \mathbb{N}\backslash\{1\}$, there exist $s \in \mathbb{N}$ and a set of prime integers $p_1, p_2, \dots, p_s$ such that*

$$n = p_1 \cdot p_2 \cdots p_s.$$

Proof The existence is shown by the strong induction on n. The base step is for $n = 2$. As 2 is a product of only one prime number, the statement is true at $n = 2$. For the inductive step, assume that $n > 2$ is a positive integer and that any positive integer k less than n is a product of primes. For n, we have two possibilities:

- If n is a prime number, then n is a product of primes.
- If n is not prime, then there exist $a, b \in \mathbb{N}$ such that $n = ab$ and $1 < a, b < n$. By the induction hypothesis, both a and b is a product of prime numbers, so n is.

Thus, in both cases n is a product of primes and by induction, the statement is true for any positive integer $n > 1$.

We prove uniqueness by using strong induction on n. The uniqueness statement is true for the integer 2, which can be uniquely written as a product of one prime. Assume that the uniqueness statement is true for all integers $k < n$. For n, assume that there exist $s, t \in \mathbb{N}$ such that

$$n = p_1 \cdot p_2 \cdots p_s \quad \text{and} \quad n = q_1 \cdot q_2 \cdots q_t$$

where $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_t$ are two sets of primes. We have the following two cases:

- If $t = 1$ or $s = 1$, then n would be a prime and the two factorizations of n are equal.
- If $t \geq 2$ and $s \geq 2$, since p_1 divides $n = q_1 \cdot q_2 \cdots q_t$, then by Euclid's lemma (Proposition 2.8.3), there exists $1 \leq j \leq s$ such that $p_1 | q_j$. Therefore, $p_1 = q_j$ (Corollary 2.8.4). By rearranging $q_1 \cdot q_2 \cdots q_t$ if necessary, we can assume that $p_1 = q_1$. Let $m = n/p_1 = p_2 \cdot p_3 \cdots p_s = q_2 \cdot q_3 \cdots q_t$. The integer m is less than n, so by induction hypothesis, the two factorizations $p_2 \cdot p_3 \cdots p_s$ and $q_2 \cdot q_3 \cdots q_t$ have the same number of factors and the same primes up to a rearrangement. Thus, the same applies to the factorizations $n = p_1 \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_t$. ■

In writing any positive integer n as a product of prime numbers, the fundamental theorem does not assert that the primes are necessarily distinct. For example, in $8 = 2 \times 2 \times 2$, all factors are the same prime 2. It sometimes convenient to group the prime factors into powers of distinct primes and write

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}$$

where $p_1, p_2, \ldots, p_s$ are distinct primes. The exponent k_i is called the multiplicity of p_i. Note that $1 = p_1^0 \cdot p_2^0 \cdots p_s^0$ for any prime p_i. The integer 1 is a finite product of primes with zero exponents. Theorem 2.8.7 can be restated as follows:

Theorem 2.8.8 *Let $n \in \mathbb{N} \backslash \{1\}$. There exist $s \in \mathbb{N}$, $k_1, k_2, \ldots, k_s \in \mathbb{N} \cup \{0\}$, and a set of distinct prime integers $p_1, p_2, \ldots, p_s$ such that*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}.$$

Corollary 2.8.9 *Any positive integer greater than* 1 *is a product of its prime divisors, taking their multiplicity into account.*

Proof Let n be a positive integer greater than 1, and Q be the set of all prime divisors of n. According to Theorem 2.8.8, there exist $s \in \mathbb{N}$, $k_1, k_2, \ldots, k_s \in \mathbb{N} \cup \{0\}$ and a set of prime integers $p_1, p_2, \ldots, p_s$ such that $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_s^{k_s}$. The goal is to show that $Q = \{p_1, p_2, \ldots, p_s\}$. One inclusion is given by Corollary 2.8.6, as the set Q is contained in the set$\{p_1, p_2, \ldots, p_s\}$, i.e.,

$$Q \subseteq \{p_1, p_2, \ldots, p_s\}.$$

On the other hand, for each i, $1 \leq i \leq s$, the integer p_i divides $p_i^{k_i}$. Hence, it divides n which implies that $\{p_1, p_2, \ldots, p_s\} \subseteq Q$. ■

For example, $1440 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5$. Therefore, $1440 = 2^5 3^2 5^1 = 2^5 3^2 5^1 7^0$.

Definition 2.8.10 Let $n \in \mathbb{N} \backslash \{1\}$. The expression $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$ in Theorem 2.8.8 is called the prime factorization of n. The integers $p_1, p_2, \ldots, p_s$ are called the prime factors of n.

Let m and n be two positive integers, and $p_1, p_2, \ldots, p_s$ be all the prime factors of m and n, i.e., $p_1, p_2, \ldots, p_s$ is formed by joining the prime factors of each of m and n. One can write n using $p_1, p_2, \ldots, p_s$ as $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, where $k_i \geq 0$ and $k_i = 0$ if p_i does not appear in the prime factorization of n. Similarly, $m = p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s}$, where $l_i \geq 0$ and $l_i = 0$ if p_i does not appear in the prime factorization of m. This remark leads to the following result.

Lemma 2.8.11 *Any positive integers m, n can be expressed using the same prime factors. The prime factorizations of m and n only differ in their exponents.*

Example 2.8.12 Consider the two integers $40 = 2^3 5^1$ and $84 = 2^2 3^1 7^1$. The prime factors of 40 and 84 are 2, 3, 5, 7. Expressing the prime factorizations of 40 and 84 using the same prime factors can be obtained by writing $40 = 2^3 3^0 5^1 7^0$ and $84 = 2^2 3^1 5^0 7^1$.

2.9 Applications of the Fundamental Theorem of Arithmetic

This section contains two applications of the results shown in Sect. 2.8. The first one provides a primality test. The second provides an easy method to compute the greatest common divisor and the least common multiple of two integers without applying the Euclidean algorithm.

Application I. Test of primality of an integer *n*.

As mentioned in the beginning of the last section, primality tests are difficult. However, several results help with testing primality of small numbers. Proposition 2.9.3 shows that to test the primality of an integer it suffices to test its divisibility by all the prime integers less than its square root. We begin with the following lemma.

Lemma 2.9.1 *Let $n \in \mathbb{N}$. If n is not a prime number, then there exists a prime p such that*

$$p \leq \sqrt{n} \quad \text{and} \quad p|n.$$

Proof Assume that n is not a prime. According to Theorem 2.8.7, there exist prime numbers $p_1, p_2, p_3, \dots, p_k$ such that $n = p_1p_2p_3 \dots p_k$. Since n is not prime, k must be greater than 1. By reordering (if needed), assume that $p_1 \leq p_2 \leq \cdots \leq p_k$. Hence,

$$n = p_1p_2p_3 \dots p_k \geq p_1p_2 \geq p_1^2$$

From which it follows $p = p_1 \leq \sqrt{n}$. ■

Example 2.9.2

1. Consider the integer 8, we have 2 divides 8, and $2 < \sqrt{8} \simeq 2.828$.
2. Consider the integer 33, we have 3 divides 33, and $3 < \sqrt{33} \simeq 5.745$.
3. The integer 1223 is a prime number. If not, then by Lemma 2.9.1, there exists a prime number p such that $p|1233$ and $p < \sqrt{1233} \simeq 35.11$. The primes that are less than 35 are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

As none of these integers divides 1223, thus 1223 must be a prime.

Proposition 2.9.3 *Let $n \in \mathbb{N}\backslash\{1\}$. If there exists $b \in \mathbb{N}$ such that $b^2 > n$, and n is not divisible by any prime less than b, then n is a prime.*

Proof If n is not prime, then there exists a prime p such that $p|n$ and $p \leq \sqrt{n}$ (Lemma 2.9.1). Therefore, there exists a prime p less than b and $p|n$, which contradicts the assumption. So, n must be a prime. ■

Remark 2.9.4 The result in Proposition 2.9.3 helps establish the following test to determine if a given number n is a prime:

1. Find an integer b such that $b^2 > n$.
2. Let S be the set of all the primes p_i, such that $p_i < b$.
3. Only one of the following cases holds:
   - $n \in S$, in which case n is prime.
   - $n \notin S$, and thus, one of the two following cases holds:

– n is not divisible by any p_i in the list, and thus, n is prime (Proposition 2.9.3).
– there exists p_i in S such that $p_i|n$, and thus, n is not prime.

Example 2.9.5

1. To determine whether 47 is prime, we look for a squared number bigger than 47. Since $7^2 = 49 > 47$, the list of all the primes that are less than 7 is $\{2, 3, 5\}$, and testing the divisibility of 47 by these numbers, we find that 47 is not divisible by any number in this list, thus by Proposition 2.9.3, 47 is a prime.
2. To determine whether 91 is prime, we look for a squared number bigger than 91. Since $10^2 = 100 > 91$, the list of all the primes that are less than 10 is $\{2, 3, 5, 7\}$, and testing the divisibility of 91 by these numbers, we find that 91 is divisible by 7, and thus is not a prime.

The method used above is not practical when the number under examination is large. For example, computer software (uses the primality test algorithms) are the best tools to check the primality of 34527569473879. More examples are described in Sect. 10.2.1.

Application II: The greatest common divisor and the least common multiple (Revisited)

In this section, the prime factorizations of two integers are used to find their greatest common divisor and the least common multiple. Although this method is rarely easier than the Euclidean algorithm 2.4.1, it provides a solution method for problems that cannot be readily solved using the Euclidean algorithm. Recall that the same prime factors can be used in factoring any pair of positive integers (Lemma 2.8.11).

Lemma 2.9.6 *Let $n, m \in \mathbb{N}$. Let $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$ and $m = p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s}$ be the prime factorizations of n and m, respectively with $k_i, l_i \geq 0$. Then*

$$m|n \Longleftrightarrow l_i \leq k_i \text{ for each } 1 \leq i \leq s.$$

Proof Assume that $l_i \leq k_i$ for each $1 \leq i \leq s$ and rewrite n as

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s} = p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s} \cdot p_1^{k_1-l_1} \cdot p_2^{k_2-l_2} \cdots p_s^{k_s-l_s}.$$

Let $r = \mathrm{p}_1^{\mathrm{k}_1-\mathrm{l}_1} \cdot \mathrm{p}_2^{\mathrm{k}_2-\mathrm{l}_2} \cdots \mathrm{p}_\mathrm{s}^{\mathrm{k}_\mathrm{s}-\mathrm{l}_\mathrm{s}}$. As $0 \leq k_i - l_i$ for each $0 \leq i \leq s$, then r is an integer and $n = mr$. Therefore, $m|n$. For the other direction, assume that $m|n$. For each $1 \leq i \leq s$, $p_i^{l_i}$ divides m, hence $p_i^{l_i}$ divides n ($p_i^{l_i}|m$ and $m\Big|n \Rightarrow p_i^{l_i}\Big|n$). If for some $1 \leq i_0 \leq s$ we have $l_{i_0} > k_{i_0}$, then as $p_{i_0}^{l_{i_0}}$ divides n, there exists $r \in \mathbb{Z}$ such that $n = p_{i_0}^{l_{i_0}} r$. Dividing both sides of the equation by $p_{i_0}^{k_{i_0}}$ yields

$$np_{i_0}^{-k_{i_0}} = p_1^{k_1} \cdot p_2^{k_2} \cdots p_{i_0-1}^{k_{i_0-1}} \cdot p_{i_0+1}^{k_{i_0+1}} \cdots p_s^{k_s} = \prod_{\substack{1 \leq i \leq s \\ i \neq i_0}} p_i^{k_i} = p_{i_0}^{l_{i_0}-k_{i_0}} r$$

Since $l_{i_0} - k_{i_0} > 0$, we have p_{i_0} divides the right side of the equation above. So, p_{i_0} divides $\prod_{\substack{1 \leq i \leq s \\ i \neq i_0}} p_i^{k_i}$. Thus, by Proposition 2.8.5, there exists $i \neq i_0$, $0 \leq i \leq s$, such that $p_{i_0} = p_i$, which contradicts that $p_1, p_2, \ldots, p_s$ are distinct. Therefore, $l_i \leq k_i$ for each $1 \leq i \leq s$. ■

Theorem 2.9.7 *Let $n, m \in \mathbb{N}$. Let $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$ and $m = p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s}$ with $l_i, k_i \geq 0$ be the prime factorizations of n and m respectively. The* gcd *and* lcm *of n and m are*

$$\gcd(m, n) = p_1^{\min(l_1,k_1)} \cdot p_2^{\min(l_2,k_2)} \cdots p_s^{\min(l_s,k_s)}$$

$$\operatorname{lcm}(m, n) = p_1^{\max(l_1,k_1)} \cdot p_2^{\max(l_2,k_2)} \cdots p_s^{\max(l_s,k_s)}.$$

Proof If $\gcd(m, n) = 1$, then there exists no common prime factor between n and m. Thus, in the given factorizations of n and m, for each $1 \leq i \leq s$ either $k_i = 0$ or $l_i = 0$. Therefore,

$$\gcd(m, n) = 1 = p_1^0 \cdot p_2^0 \cdots p_s^0 = p_1^{\min(l_1,k_1)} \cdot p_2^{\min(l_2,k_2)} \cdots p_s^{\min(l_s,k_s)}.$$

If $\gcd(m, n) \neq 1$, set

$$c = p_1^{\min(l_1,k_1)} \cdot p_2^{\min(l_2,k_2)} \cdots p_s^{\min(l_s,k_s)}.$$

As $\min(l_i, k_i) \leq k_i$ and $\min(l_i, k_i) \leq l_i$, then by Lemma 2.9.6, the integer c divides both n and m. Hence, the integer c divides their gcd (Corollary 2.5.7), i.e., $c|\gcd(m, n)$. On the other hand, as $\gcd(m, n)$ divides $p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, then by Corollary 2.8.6, the set $\{p_1, p_2, \ldots, p_s\}$ contains all the prime divisors of $\gcd(m, n)$. Therefore, by Corollary 2.8.9,

$$\gcd(m, n) = p_1^{j_1} \cdot p_2^{j_2} \cdots p_s^{j_s} \text{ for some } j_i \geq 0, 1 \leq i \leq s.$$

For each i, the integer $j_i \leq l_i$ and $j_i \leq k_i$. Therefore, $j_i \leq \min(k_i, l_i)$ for each 1 ≤ i ≤ s. By Lemma 2.9.6, $\gcd(m, n)|c$. Since $\gcd(m, n)$ and c are positive integers that divide each other, then by Proposition 2.2.5 (3),

$$\gcd(m, n) = |\gcd(m, n)| = |c| = c.$$

For the second equality, as

$\operatorname{lcm}(m, n) = \frac{nm}{\gcd(m,n)}$ (Proposition 2.7.6)
and $a + b = \min(a, b) + \max(a, b)$ for any $a, b \in \mathbb{N}$, then

$$\begin{aligned}
\operatorname{lcm}(m, n) &= \frac{p_1^{l_1} \cdot p_2^{l_2} \cdots p_s^{l_s} \cdot p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}}{p_1^{\min(l_1,k_1)} \cdot p_2^{\min(l_2,k_2)} \cdots p_s^{\min(l_s,k_s)}} \\
&= \frac{p_1^{l_1+k_1} \cdot p_2^{l_2+k_2} \cdots p_s^{l_s+k_s}}{p_1^{\min(l_1,k_1)} \cdot p_2^{\min(l_2,k_2)} \cdots p_s^{\min(l_s,k_s)}} \\
&= p_1^{l_1+k_1-\min(l_1,k_1)} \cdot p_2^{l_2+k_2-\min(l_2,k_2)} \cdots p_s^{l_s+k_s-\min(l_s,k_s)} \\
&= p_1^{\max(l_1,k_1)} \cdot p_2^{\max(l_2,k_2)} \cdots p_s^{\max(l_s,k_s)}.
\end{aligned}$$

■

Example 2.9.8 The prime factorizations of 198 and 174 can be expressed as

$$174 = 2^1 3^1 29^1,\ 198 = 2^1 3^2 11^1.$$

These equations can be modified to write the prime factorizations of 198 and 174 with common prime factors

$$174 = 2^1 3^1 11^0 29^1,\ 198 = 2^1 3^2 11^1 29^0.$$

According to Theorem 2.9.7

$$\gcd(174, 198) = 2^1 3^1 11^0 29^0 = 6$$

$$\operatorname{lcm}(174, 198) = 2^1 3^2 11^1 29^1 = 5742.$$

Once the prime factorizations of the two integers m, n are known, then using Theorem 2.9.7 is straightforward. However, this is not always the case. Computing the $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ by finding the prime factorizations of m and n is usually more difficult than using the division method in the Euclidean algorithm. The prime factorization method is practical and preferred in cases in which the expressions of m and n are given in exponent forms.

Example 2.9.9 In finding the greatest common divisor and least common multiple of

$$m = 60^{67} \times 28^{144} \text{ and } n = 123^{201}$$

calculating the greatest common divisor using the Euclidean algorithm would involve division of very large integers. The solution can be more easily (and feasibly) obtained using Theorem 2.9.7.

$$m = 60^{67} \times 28^{144} = \left(2^2 3^1 5^1\right)^{67} \times \left(2^2 7^1\right)^{144}$$

$$= 2^{134}3^{67}5^{67} \times 2^{288}7^{144} = 2^{422}3^{67}5^{67}7^{144}$$

and $n = 123^{201} = (3^1 41^1)^{201} = 3^{201}41^{201}$.

Writing m and n using common prime factors yields

$$m = 2^{422}3^{67}5^{67}7^{144}41^0, n = 2^0 3^{201}5^0 7^0 41^{201}.$$

Theorem 2.9.7 now can be applied to obtain

$$\gcd(m, n) = 3^{67} \text{ and } \operatorname{lcm}(m, n) = 2^{422}3^{201}5^{67}7^{144}41^{201}.$$

Theorem 2.9.12 *Let $m_1, m_2, \ldots, m_n$ be positive integers. For each $1 \le j \le n$, let $m_j = p_1^{k_{j1}} \cdot p_2^{k_{j2}} \cdots p_s^{k_{js}}$, where $k_{ji} \ge 0$ is the prime factorization of m_j. The gcd and lcm of m_j, $1 \le j \le n$ are*

$$\gcd(m_1, m_2, \ldots, m_n) = p_1^{\min(k_{11}, k_{21}, \ldots, k_{n1})} \cdot p_2^{\min(k_{12}, k_{22}, \ldots, k_{n2})} \cdots p_s^{\min(k_{1s}, k_{2s}, \ldots, k_{ns})}$$

$$\operatorname{lcm}(m_1, m_2, \ldots, m_n) = p_1^{\max(k_{11}, k_{21}, \ldots, k_{n1})} \cdot p_2^{\max(k_{12}, k_{22}, \ldots, k_{n2})} \cdots p_s^{\max(k_{1s}, k_{2s}, \ldots, k_{ns})}.$$

Exercises

Solved Exercises

2.1 Show that the square of any odd integer n is of the form $n^2 = 8m + 1$ for some integer m.

Solution

Assume that n is an odd integer. Applying the quotient-remainder theorem to n and 2, we write $n = 2q + r$ for some $q \in \mathbb{Z}$ and $r = 0$ or $r = 1$. Since n is odd, then the only possible value of r is 1. Thus, $n = 2q + 1$ for some $q \in \mathbb{Z}$, and

$$n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$$

- If $q = 2k$ is an even integer, then $n^2 = 8k(q + 1) + 1 = 8m + 1$, where $m = k(q + 1) \in \mathbb{Z}$.
- If q is odd, then $q + 1 = 2k$ is an even integer, which implies that $n^2 = 4q(2k) + 1 = 8m + 1$, where $m = qk \in \mathbb{Z}$.

2.2 Show that the cube of any integer n has one of the following forms

$$9m, 9m + 1, \text{ or } 9m + 8 \text{ for some } m \in \mathbb{Z}.$$

Solution

Applying the quotient-remainder theorem to n and 3, we obtain

$$n = 3q, n = 3q + 1, \text{ or } n = 3q + 2, \text{ where } q \in \mathbb{Z}.$$

- If $n = 3q$, then $n^3 = 27q^3 = 9\big(3q^3\big) = 9m$, where $m = 3q^3 \in \mathbb{Z}$.
- If $n = 3q + 1$, then

$$n^3 = 27q^3 + 27q^2 + 9q + 1 = 9\big(3q^3 + 3q^2 + q\big) + 1 = 9m + 1,$$
$$\text{where } m = 3q^3 + 3q^2 + q \in \mathbb{Z}.$$

- If $n = 3q + 2$, then

$$n^3 = 27q^3 + 54q^2 + 36q + 8 = 9\big(3q^3 + 6q^2 + 4q\big) + 8 = 9m + 8,$$
$$\text{where } m = 3q^3 + 6q^2 + 4q \in \mathbb{Z}.$$

2.3 Let a, b, c be elements in $\mathbb{Z}$. Show that if $c|a + b$ and $\gcd(a, b) = 1$, then $\gcd(a, c) = \gcd(b, c) = 1$.

Solution

Assume that $c|a + b$ and $\gcd(a, b) = 1$. Since $\gcd(a, b) = 1$, at least one of a or b is nonzero.

- If $c = 0$, since only number divisible by zero is zero, then $a + b = 0$, and thus, $a = -b$. Thus,

$$1 = \gcd(a, b) = \gcd(a, -a) = |a|$$

which implies that $a, b \in \{1, -1\}$ and thus, $\gcd(a, c) = \gcd(b, c) = 1$.

- If $c \neq 0$, then it is not divisible by zero, so $\gcd(a, c) = d \geq 1$. Since $d|c$ and $c|a + b$ by the transitivity of divisibility, we obtain $d|a + b$. Since $d|a$, then by Proposition 2.2.7, $d|(a + b - a) = b$. As d divides both a and b, by Corollary 2.5.6, $d|\gcd(a, b) = 1$. Therefore, $d = 1$. Similarly, $\gcd(b, c) = 1$.

2.4 Find all positive integers n such that $n|(3n + 4)$.

Solution

Assume that $n|(3n+4)$. Since $n|3n$, then n divides 4 (as $4 = (3n + 4) - 3n$ is a linear combination of $3n + 4$ and n). Since the positive divisors of 4 are 1, 2, and 4, then these are all the possible values of n.

2.5 Find all integers n such that $(2n + 5)/(3n + 2)$ is an integer.

Solution

Assume that n is an integer such that $(2n + 5)/(3n + 2)$ is an integer. This means that $(3n + 2)$ divides $(2n + 5)$. Since $3n + 2$ divides itself, then

$$(3n + 2) \mid [3(2n + 5) - 2(3n + 2)] = 11.$$

As the only divisors of 11 are $\pm 1, \pm 11$, we obtain that $3n+2 \in \{\pm 1, \pm 11\}$. Thus, there are only four possible values for $3n + 2$,

- $3n + 2 = 1$, which has no integer solution since $\frac{-1}{3} \notin \mathbb{Z}$.
- $3n + 2 = -1$, which implies that $n = -1 \in \mathbb{Z}$.
- $3n + 2 = 11$, which implies $n = 3 \in \mathbb{Z}$.
- $3n + 2 = -11$, which has no integer solution since $\frac{-13}{3} \notin \mathbb{Z}$.

Therefore, $n = 3$ and $n = -1$ are the only possible integer values for n.

2.6 Let $a, b, c \in \mathbb{Z}$ such that a, b are not both zero. Show that

i. If $c \neq 0$, then $D(ac, bc) = \{dk : d \in D(a, b) \wedge k|c\}$.
ii. For $c > 0$, $\gcd(ac, bc) = c\gcd(a, b)$.

Solution

i. If $d \in D(a, b) \wedge k|c$, then $dk|ac \wedge dk|ab$. Hence, $dk \in D(ac, bc)$. For the other direction, assume that $x \in D(ac, bc)$, and let $k = \gcd(x, c)$. By applying Corollary 2.6.4 to x and c, we obtain that there exist $d, t \in \mathbb{Z}$ such that

$$x = kd, \;\; c = kt \;\text{ and }\; \gcd(d, t) = 1.$$

Since $x|ac$, then $kd|akt$, and thus, $d|at$. As $\gcd(d, t) = 1$, it follows that $d|a$. Similarly, $d|b$. That is, $x = dk$, where $d \in D(a, b)$ and $k|c$. Therefore,

$$x \in \{dk : d \in D(a, b) \;\wedge\; k|c\} \text{ and } D(ac, bc) = \{dk : d \in D(a, b) \;\wedge\; k|c\}.$$

ii. By the result in (i), $\gcd(ac, bc) = dk$, where $d \in D(a, b)$ and $k|c$. Thus, dk divides $\gcd(a, b)c = c \gcd(a, b)$, i.e.,

$$\gcd(ac, bc) \leq c \gcd(a, b).$$

On other hand, as $\gcd(a, b)$ divides both a and b, then $c \gcd(a, b)$ divides both ca and cb which implies that $c \gcd(a, b)$ divides their greatest common divisor, $\gcd(ac, bc)$, i.e., $c \gcd(a, b) \leq \gcd(ac, bc)$. Therefore,

$$\gcd(ac, bc) = c \gcd(a, b).$$

The assumption that $c > 0$ is necessary for keeping $\gcd(ac, bc)$ nonnegative.

2.7 Let a, b be two integers such that both are not zero. Show that if $\gcd(a, b) = 1$, then $\gcd\big(a^2, b\big) = 1 = \gcd\big(a^2, b^2\big)$.

Solution

Assume that $\gcd(a, b) = 1$. According to Bézout's lemma (Theorem 2.5.1), there exist $x, y \in \mathbb{Z}$ such that $1 = xa + yb$. Therefore,

$$(xa + yb)^2 = x^2a^2 + 2\,xa\,yb + y^2b^2 = 1.$$

This implies that

$$\big(2\,xay + y^2b\big)b + x^2a^2 = 1 \qquad (*)$$

- This equality and Corollary 2.5.6 imply that $\gcd\big(a^2, b\big) = 1$.
- By rewriting $(*)$ as $\big(2\,xay + y^2b\big)b = 1 - x^2a^2$ and squaring both sides, we obtain

$$(2\,xay + y^2b)^2 b^2 = (1 - x^2a^2)^2 = 1 - 2x^2a^2 + x^4a^4.$$

Rearranging the equation yields

$$(2x^2 - x^4a^2)a^2 + (2\,xay + y^2b)^2 b^2 = 1.$$

Let $u = 2x^2 - x^4a^2$ and $v = (2\,xay + y^2b)^2$. Hence, there exist $u, v \in \mathbb{Z}$ such that $ua^2 + vb^2 = 1$, which by Corollary 2.5.6 implies that $\gcd\big(a^2, b^2\big) = 1$.

2.8 Let $n \in \mathbb{N}$, such that $n \geq 3$. Let $a_1, \ldots, a_n$ be any integers that are not all zeros. Show that for each $1 \leq i \leq n$,

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i).$$

Solution

Assume that $a_1, \ldots, a_n$ are any integers that are not all zeros. Pick i such that $1 \leq i \leq n$. Since $\gcd(a_1, \ldots, a_n) | a_j$ for each $j \neq i$, $1 \leq j \leq n$, then

$$\gcd(a_1, \ldots, a_n) | \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n).$$

As $\gcd(a_1, \ldots, a_n)|a_i$, then

$$\gcd(a_1, \ldots, a_n)|\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i)$$

which implies that

$$\gcd(a_1, \ldots, a_n) \leq \gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i).$$

On other hand, as $\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i)$ divides $\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ and $\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)|a_j$ for each $j \neq i$, thus by transitivity,

$$\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i)|a_j \text{ for each } j \neq i, 1 \leq j \leq n.$$

As also $\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i)|a_i$, then

$$\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i)|\gcd(a_1, \ldots, a_n)$$

which implies that

$$\gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i) \leq \gcd(a_1, \ldots, a_n).$$

Therefore,

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i).$$

2.9 Generalization of Bézout's Lemma: Let $a_1, \ldots, a_n$ be any integers that are not all zeros. Show that there exist integers $x_1, \ldots, x_n$ such that

$$\gcd(a_1, \ldots, a_n) = x_1a_1 + \cdots + x_na_n$$

Solution

We prove the result using induction on n.

Base step: If $n = 2$, then the result is Bézout's lemma.

Inductive step: Suppose the result is true for n, that is, if $a_1, \ldots, a_n$ are integers that are not all zeros, then there exist integers $x_1, \ldots, x_n$ such that

$$\gcd(a_1, \ldots, a_n) = x_1a_1 + \cdots + x_na_n.$$

For $n + 1$, assume that $a_1, \ldots, a_n, a_{n+1}$ are integers that are not all zeros. By Exercise 2.8, we have

$$\gcd(a_1, a_2, \ldots, a_n, a_{n+1}) = \gcd\big(\gcd(a_1, a_2, \ldots, a_n), a_{n+1}\big).$$

By Bézout's lemma, there exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a_1, a_2, \ldots, a_n, a_{n+1}) = x \gcd(a_1, a_2, \ldots, a_n) + y\, a_{n+1}.$$

By induction assumption, there exist integers $x_1, \ldots, x_n$ such that

$$\gcd(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n.$$

Therefore,

$$\begin{aligned}\gcd(a_1, a_2, \ldots, a_n, a_{n+1}) &= x(x_1 a_1 + \cdots + x_n a_n) + y a_{n+1}\\ &= (x x_1) a_1 + \cdots + (x x_n) a_n + y\, a_{n+1}.\end{aligned}$$

as required.

2.10 List the first four positive common multiples of 10 and 25 and find lcm(25, 10).

Solution

The positive multiples of 10 are:

$$10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, 120, 130, \ldots$$

The positive multiples of 25 are:

$$25, 50, 75, 100, 125, 150, 175, 200, 225, 250, \ldots$$

Therefore, the first four positive common multiples of 10 and 25 are 50, 100, 150, 200 and the least common multiple is 50.

2.11 Show that $\gcd(p, 1-p) = \gcd\big(p^2, 1-p\big) = 1$ for any prime p.

Solution

Since $1 \times p + 1 \times (1-p) = 1$ and $1 \times p^2 + (1+p) \times (1-p) = 1$, by Corollary 2.5.5, we obtain $\gcd(p, 1-p) = 1$ and $\gcd\big(p^{2,} 1-p\big) = 1$.

2.12 Let $m \in \mathbb{N}$, and $p_1, \ldots, p_n$ be the distinct prime divisors of m. Let $k_1, \ldots, k_n$ be nonnegative integers such that $m = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ is the prime factorization of m. Show that

$$\text{if } m_i = m/p_i^{k_i} = \prod_{j \neq i} p_j^{k_j}, \text{ then } \gcd(m_1, \ldots, m_n) = 1.$$

Solution

Let $\gcd(m_1, \ldots, m_n) = c$. If $c \neq 1$, then there exists a prime p such that $p|c$. As $c|m_i$ for each $1 \leq i \leq n$, we have $p|m_i$ for each $1 \leq i \leq n$. So, p is a prime divisor of m_i, and thus, a member of $\{p_j : j \neq i\}$. Hence, p belongs to the intersection of these sets which is empty. Since the assumption that $c \neq 1$ leads to a contradiction we must have $c = 1$.

2.13 Prove that 509 is a prime number.

Solution

Assume that 509 is not a prime. By Lemma 2.9.1, there exists a prime number p such that $p \mid 509$ and $p < \sqrt{509} \cong 22.56$. As the prime numbers that are less than 22 are 2, 3, 5, 7, 11, 13, 17, 19, and none of them divide 509, then 509 is a prime.

Unsolved Exercises

2.14 Show that any integer n can be written as one of the following forms:

$$n = 5q, n = 5q + 1, n = 5q + 2, n = 5q + 3, \text{ or } n = 5q + 4$$

for some $q \in \mathbb{Z}$

2.15 Prove that for any integer n, the integer $n^2 - n + 3$ is odd.

2.16 Let n be an integer. Show that n^4 is of the form $5k$, *or* $5k + 1$ for some integer k.

2.17 Let a, b be integers that are not both zero. Show that $\gcd(a, b)$ is the only divisor of a, b that is divisible by any other common divisor of a and b, i.e., if $d|a$, $d|b$ and $c|d$ for all $c \in D(a, b)$, then $d = \gcd(a, b)$.

2.18 Let $a, b, c \in \mathbb{Z}$ such that one of a, b is not zero. Show that if $c \neq 0$, then

$$\gcd(ca, cb) = |c| \gcd(a, b) \text{ and } \operatorname{lcm}(ca, cb) = |c| \operatorname{lcm}(a, b).$$

2.19 Show that $\gcd(a, a + 1) = 1$ for any integer a.

2.20 Let $n \in \mathbb{N}$, such that $n \geq 3$. Let $a_1, \ldots, a_n$ be any integers that are not all zero. Show that for each $1 \leq i \leq n.$,

$$\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n), a_i).$$

2.21 Determine whether the equation $23x + 12y = 134$ has an integer solution. If so, find all possible solutions.

2.22 Using Proposition 2.6.2 and mathematical induction, show that for any integers a, b, if $\gcd(a, b) = 1$, then $\gcd\big(a, b^k\big) = 1$ for each $k \geq 1$.

2.23 Find the integer b such that $\gcd(45, b) = 3$ and $\operatorname{lcm}(45, b) = 405$.

2.24 Let c be an integer and $a_1, a_2, \ldots, a_n$ be a set of integers such that $a_i|c \ \forall\, 1 \leq i \leq n$. Show that $\gcd(a_1, a_2, \ldots, a_n)|c$ and $\operatorname{lcm}(a_1, a_2, \ldots, a_n)|c$.

2.25 Let d be an integer and $a_1, a_2, \ldots, a_n$ be a set of integers such that $d|a_i$ $\forall\, 1 \leq i \leq n$. Show that $d|\gcd(a_1, a_2, \ldots, a_n)$ and d$|\operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

2.26 Prove that the only prime that can be expressed as $n^2 - 4$ is 5.

2.27 Prove that 1063 is a prime number.

2.28 Determine whether 97, 257 and 103 are primes.

Reference

Burton, D. M. (2007). *Elementary number theory*. MacGraw-Hill.

Chapter 3
The Integers Modulo *n*

In this chapter, for each positive integer n, a set of integers is defined. Such a set is called the “integers modulo n” or “the residue classes mod n” and denoted by $\mathbb{Z}_n$. Like any other algebraic structure, many operations are defined and performed on the integers modulo n. Section 3.1 describes, in detailed, the structure of $\mathbb{Z}_n$, Sect. 3.2 presents several examples of functions defined on $\mathbb{Z}_n$. Section 3.3 is devoted to the study of the basic operations (addition and multiplication) on $\mathbb{Z}_n$. The presentation of these operations using tables is given and discussed in Sect. 3.4. In Sect. 3.5, an alternative new formula for integers modulo n was introduced. Such formula utilizes solving the linear equations on $\mathbb{Z}_n$, which are defined and studied in Sect. 3.6. For more information about integers modulo n, see (Bloch, 2000).

3.1 Structure of Integers Modulo *n*

For a positive integer n, the structure of the integers modulo n is based on a partition of $\mathbb{Z}$ into n disjoint subsets, with each subset representing an integer modulo n. This partition is performed by introducing an equivalence relation on $\mathbb{Z}$ using n, resulting in a partition into equivalence classes of this relation (Fig. 3.1).

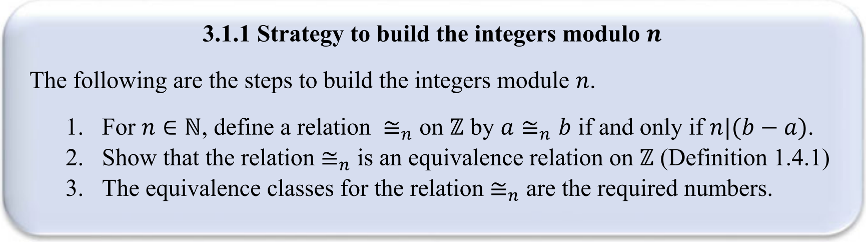
Definition 3.1.2 For each $n \in \mathbb{N}$, define the relation modulo n, denoted by $\cong_n$, on $\mathbb{Z}$ by

$$a \cong_n b \Longleftrightarrow n|(b-a) \text{ for any } a, b \in \mathbb{Z}.$$

The mathematical statement $a \cong_n b$ is read as “a congruent to b modulo n”. If n is obvious from the context, the symbol $\cong$ can be used instead of $\cong_n$ to simplify notation. The statement $a \ncong_n b$ is the negation of $a \cong_n b$ and is read as “a is not congruent to b modulo n”.

It can be easily verified that for $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$,

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_3



3.1.1 Strategy to build the integers modulo n

The following are the steps to build the integers module n.

1. For $n \in \mathbb{N}$, define a relation $\cong_n$ on $\mathbb{Z}$ by $a \cong_n b$ if and only if $n|(b-a)$.
2. Show that the relation $\cong_n$ is an equivalence relation on $\mathbb{Z}$ (Definition 1.4.1)
3. The equivalence classes for the relation $\cong_n$ are the required numbers.

Fig. 3.1 Strategy to build the integers modulo n

1. $a \cong_n b$ if and only if $\exists\, q \in \mathbb{Z} \ni b - a = qn$
2. If $a \cong_n b$, then $a \cong_m b$ for each $m \in \mathbb{Z}$ such that $m|n$ (It follows by the transitive property of divisibility).

One can easily check that the following statements are correct.

$$\begin{array}{rrrr}
5 \cong_4 1, & -17 \cong_8 7, & 119 \not\cong_{59} 2, & 23 \cong_4 -5 \\
119 \cong_2 1, & 100 \cong_3 -26, & 89 \cong_{17} 55, & 456 \cong_2 4 \\
5 \cong_{11} -6, & 436 \cong_{436} 0, & 436 \not\cong_3 0, & 436 \cong_2 8 \\
29 \cong_{12} 5, & 81 \cong_{35} 11, & 111 \cong_{16} -33, & -100 \cong_9 -1
\end{array}$$

Note that the relation $\mathcal{R}$ in Example 1.4.11 is the relation $\cong_3$. According to this the strategy, and Example 1.4.11, the integers modulo 3 are [0], [1], [2]. The next proposition lists some important properties of the relation $\cong_n$.

Proposition 3.1.3 *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$.*

1. *If $a \cong_n b$, then $ra \cong_n rb$ and $ra \cong_{rn} rb$ for each $r \in \mathbb{Z}$.*
2. *If $a \cong_n b$, then $ar \cong_n br$ and $ar \cong_{rn} br$ for each $r \in \mathbb{N}$.*
3. *If $ra \cong_n rb$, for some $r \in \mathbb{N}$, then $a \cong_{\frac{n}{\gcd(n,r)}} b$. If $\gcd(r, n) = 1$, then $a \cong_n b$.*
4. *If $ar \cong_n br$, for some $r \in \mathbb{N}$, then $a \cong_{\frac{n}{\gcd(n,r)}} b$. If $\gcd(r, n) = 1$, then $a \cong_n b$.*

Proof If $a \cong_n b$, there exists $q \in \mathbb{Z}$ such that $b - a = qn$. Multiplying both sides of the equation by r, one obtains $rb - ra = rqn = (rq)n = q(rn)$. Therefore, $ra \cong_n rb$ and $ra \cong_{rn} rb$. Similarly, the second statement can be derived. For (3), assuming that $ra \cong_n rb$, there exists $q \in \mathbb{Z}$ such that $rb - ra = qn$. Dividing both sides by $\gcd(r, n)$, yields the following equation

$$\frac{r}{\gcd(r,n)}(b-a) = q\frac{n}{\gcd(r,n)}.$$

So,

$$\left(\frac{n}{\gcd(r,n)}\right) \Big| \left(\frac{r}{\gcd(r,n)}(b-a)\right).$$

According to Proposition 2.6.3, $\gcd\left(\frac{n}{\gcd(r,n)}, \frac{r}{\gcd(r,n)}\right) = 1$. Hence, Corollary 2.5.7 (2) implies that

$$\left(\frac{n}{\gcd(r,n)}\right)|(b-a).$$

Item (4) can be proved in similar manner. ■

Example 3.1.4

1. As $5 \cong_3 2$, then $60 = 5 \times 12 \cong_{36} 2 \times 12 = 24$, i.e., $60 \cong_{36} 24$.
2. As $42 \cong_7 14$, then $126 = 42 \times 3 \cong_{21} 14 \times 3 = 42$, i.e., $126 \cong_{21} 42$.
3. Since $4 \times 7 = 28 \cong_6 16 = 4 \times 4$ and $(6/\gcd(6,4)) = 3$, applying Proposition 3.1.3 (3) with $r = 4$ yields $7 \cong_3 4$.
4. Since $6 \times 21 = 126 \cong_{21} 42 = 6 \times 7$ and $(21/\gcd(21,6)) = 3$, applying Proposition 3.1.3 (3) with $r = 6$ yields $21 \cong_7 7$.
5. Since $2 \times 21 = 42 \cong_7 14 = 2 \times 7$ and $(7/\gcd(7,2)) = 7$, applying Proposition 3.1.3 (3) with $r = 2$ yields $21 \cong_7 7$.
6. Since $42 \cong_4 50$, then $2 \times 21 = 42 \cong_4 50 = 2 \times 25$. Hence, applying Proposition 3.1.3 (3) with $r = 2$ yields $21 \cong_2 25$ (note $(4/\gcd(4,2)) = 2$).

Proposition 3.1.5 *Let $n \in \mathbb{N}$. The relation $\cong_n$ is an equivalence relation on $\mathbb{Z}$.*

Proof For all $a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot n$ and $0 \in \mathbb{Z}$, i.e., $a \cong_n a$. Hence, $\cong_n$ is reflexive. Assume that $a \cong_n b$ for some $a, b \in \mathbb{Z}$. By definition of $\cong_n$, there exists $q \in \mathbb{Z}$ such that $b - a = nq$, i.e., there exists $q \in \mathbb{Z}$ such that $a - b = nl, l = -q \in \mathbb{Z}$, which implies that $b \cong_n a$ and $\cong_n$ is symmetric. To verify the transitivity, assume that $a, b, c \in \mathbb{Z}$ such that $a \cong_n b$, $b \cong_n c$. By Definition 3.1.2, there exist $q_1, q_2 \in \mathbb{Z}$ such that $b - a = nq_1 \wedge c - b = nq_2$. Thus,

$$c - a = (c - b) + (b - a) = n(q_1 + q_2) = nq$$

where $q = q_1 + q_2 \in \mathbb{Z}$. Thus, $a \cong_n c$, and the relation $\cong_n$ is transitive. According to Definition 1.4.1, the relation $\cong_n$ is an equivalence relation on $\mathbb{Z}$. ■

Next, we compute the equivalence classes of the equivalence relation $\cong_n$. Recall the definition of equivalence classes (Definition 1.4.7).

Lemma 3.1.6 *Let $n \in \mathbb{N}$, and $a \in \mathbb{Z}$. The equivalence class of $\cong_n$ that contains a is $a + n\mathbb{Z}$.*

Proof Let $a \in \mathbb{Z}$. By Definition 1.4.7, the equivalence class of $\cong_n$ that contains a is

$$\begin{aligned}
[a]_n &= \{b \in \mathbb{Z} : a \cong_n b\} = \{b \in \mathbb{Z} : n|(b-a)\} \\
&= \{b \in \mathbb{Z} : \exists\, q \in \mathbb{Z} \wedge b - a = nq\} \\
&= \{a + nq : q \in \mathbb{Z}\} = a + n\mathbb{Z}.
\end{aligned}$$

■

It can be easily verified that for any $n \in \mathbb{N}$,

1. $[a]_n = [b]_n \Leftrightarrow a \cong_n b \Leftrightarrow n|(b-a)$ for any $a, b \in \mathbb{Z}$.
2. For any $q, r \in \mathbb{Z}$, $[qn + r]_n = [r]_n$. In particular, $[qn]_n = [0]_n = [n]_n$.

Proposition 3.1.7 *Let $n \in \mathbb{N}$. There are exactly n distinct equivalence classes of the relation $\cong_n$, namely, $[0]_n, [1]_n, \ldots, [n-1]_n$.*

Proof Let $a \in \mathbb{Z}$. According to the quotient-remainder theorem (Theorem 2.1.2) applied on a and n, there exist $q, r \in \mathbb{Z}$ such that $a = qn + r$, $0 \le r < n$, i.e., there exist $q, r \in \mathbb{Z}$ such that

$[a]_n = [qn + r]_n = [r]_n, 0 \le r < n.$

Therefore, the set $\{[r]_n : r \in \mathbb{Z}, 0 \le r < n\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ contains all the equivalent classes of the relation $\cong_n$. To show that these classes are distinct, assume that there exist $r_1, r_2 \in \mathbb{Z}$ such that $0 \le r_1, r_2 < n$ and $[r_1]_n = [r_2]_n$. Without loss of generality, assume that $r_1 \le r_2$. Hence,

$$[r_1]_n = [r_2]_n \Rightarrow r_1 \cong_n r_2 \Rightarrow r_2 - r_1 = qn, \quad q \in \mathbb{Z}.$$

Since $0 \le r_2 - r_1 \le r_2 < n$, then $|q|n = |r_2 - r_1| = r_2 - r_1 < n$. Therefore, $|q| < 1$. Since q is an integer, $q = 0$, which implies that $r_2 - r_1 = 0$ and $r_1 = r_2$. ■

If there is no ambiguity, we omit the index n in $[a]_n$ and write $[a]$ instead of $[a]_n$.

Definition 3.1.8 Let $n \in \mathbb{N}$. The set of all equivalence classes of $\cong_n$, denoted by $\mathbb{Z}_n$, is called the integers modulo n or the residue classes mod n. i.e.,

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

The element $[a]$ in $\mathbb{Z}_n$ is called the class of a modulo n.

For any $n \in \mathbb{Z}$, the set $\mathbb{Z}_n$ forms a partition for $\mathbb{Z}$ into n disjoint subsets (Theorem 1.4.10), as illustrated in the next example.

Example 3.1.9 Every element in $\mathbb{Z}_n$ is of the form $m + n\mathbb{Z}$ for some $0 \le m \le n-1$ (Definition 3.1.2, Exercise 1.19), i.e., the set $\mathbb{Z}_n$ contains only n elements with every element having infinitely many representations. For example,

1. The set $\mathbb{Z}_2$ consists of two elements $[0]$ and $[1]$, with $[0] = 0 + 2\mathbb{Z} = 2\mathbb{Z}$(even integers) and $[1] = 1 + 2\mathbb{Z}$ (odd integers).
2. In $\mathbb{Z}_9 = \{[0], [1], \ldots, [8]\}$,

   a. $[0] = 0 + 9\mathbb{Z} = \{0 + 9q : q \in \mathbb{Z}\} = \{\ldots, -18, -9, 0, 9, 18, \ldots\}$,
   b. $[7] = 7 + 9\mathbb{Z} = \{7 + 9q : q \in \mathbb{Z}\} = \{\ldots, -11, -2, 7, 16, 25, \ldots\}$,
   c. $[18] = [2 \times 9] = [0] = 0 + 9\mathbb{Z} = \{\ldots, -18, -9, 0, 9, 18, \ldots\}$,
   d. $[25] = [2 \times 9 + 7] = [7] = 7 + 9\mathbb{Z}$,
   e. $[-100] = [-9 \times 12 + 8] = [8] = 8+9\mathbb{Z} = \{\ldots, -10, -1, 8, 17, 26, \ldots\}$,
   f. $[1105] = [122 \times 9 + 7] = [7] = 7 + 9\mathbb{Z}$.

3. In $\mathbb{Z}_{15} = \{[0], [1], \ldots, [14]\}$,

    a. $[45] = [15 \times 3] = [0] = 15\mathbb{Z}$,
    b. $[3021] = [15 \times 201 + 6] = [6] = 6 + 15\mathbb{Z}$,
    c. $[246] = [15 \times 16 + 6] = [6] = 6 + 15\mathbb{Z}$,
    d. $[-3] = [15 \times (-1) + 12] = [12] = 12 + 15\mathbb{Z}$,
    e. $[-1004] = [15 \times (-67) + 1] = [1] = 1 + 15\mathbb{Z}$,
    f. $[21] = [15 \times 1 + 6] = [6] = 6 + 15\mathbb{Z}$,
    g. $[-21] = [15 \times (-2) + 9] = [9] = 9 + 15\mathbb{Z}$.

3.2 Functions on the Integers Modulo *n*

Let $n \in \mathbb{N}$. Since $\mathbb{Z}_n$ consists of equivalence classes, one must be careful when defining functions on $\mathbb{Z}_n$, and must verify that the function is well-defined (Sect. 1.5).

Example 3.2.1

1. On $\mathbb{Z}_5$, define the relation $f \subseteq \mathbb{Z}_5 \times \{-1, 1\}$ given by $f([a]) = (-1)^a$. Since $[0] = [5]$ in $\mathbb{Z}_5$ and $f([0]) = 1 \neq -1 = f([5])$, then f is not well-defined. Therefore, f is not a function on $\mathbb{Z}_5$.
2. Let $n \in \mathbb{N}$. Define $g : \mathbb{Z} \to \mathbb{Z}_n$ by $g(a) = [a]$ for all $a \in \mathbb{Z}$. One can easily verify that g is a function on $\mathbb{Z}$, as follows: if $a \in \mathbb{Z}$, then by the quotient-remainder theorem (Theorem 2.1.2) applied on a and n, there exist unique elements $q, r \in \mathbb{Z}$ such that

$$a = qn + r, 0 \leq r < n.$$

Therefore,

$$[a] = [qn + r] = [r] \in \mathbb{Z}_n$$

i.e., for each element in $\mathbb{Z}$, there exists a unique image in $\mathbb{Z}_n$ under g, so g is a function on $\mathbb{Z}$.

Example 3.2.3

1. Let $f : \mathbb{Z}_3 \to \mathbb{Z}_6$ be defined as $f([a]_3) = [a]_6$. The relation f is not well-defined. Since $[0]_3 = [3]_3$, but $f([0]_3) = [0]_6 \neq [3]_6 = f([3]_3)$.
2. To verify that $g : \mathbb{Z}_{12} \to \mathbb{Z}_{60}$ defined by $g([a]_{12}) = [5a]_{60}$ is a well-defined map, assume that $[a]_{12} = [b]_{12}$, then

$$\begin{aligned}[a]_{12} = [b]_{12} &\Rightarrow 12 | (b - a) \Rightarrow b - a = 12q, \quad q \in \mathbb{Z} \\ &\Rightarrow 5b - 5a = 60q, \quad q \in \mathbb{Z} \\ &\Rightarrow 60 | (5b - 5a) \Rightarrow [5a]_{60} = [5b]_{60} \Rightarrow g([a]_{12}) = g([b]_{12}).\end{aligned}$$

3. Let $h : \mathbb{Z}_4 \to \mathbb{Z}_{11}$ be defined by $h([a]_4) = [7a]_{11}$. The relation h is not well-defined, as the elements $[0]_4 = [4]_4$, while $h([0]_4) = [0]_{11} \neq [28]_{11} = h([4]_4)$.

Example 3.2.4 Let $m, n, k \in \mathbb{N}$. Define $f : \mathbb{Z}_n \to \mathbb{Z}_m$ as

$$[x]_n \mapsto [kx]_m$$

then, f is a well-defined map if and only if m divides kn. We show the two directions as follows:

Assume that f is a well-defined map. As $[0]_n = [n]_n$ then $[0]_m = f([0]_n) = f([n]_n) = [kn]_m$, which means that $m|(kn - 0)$. For the other direction, assume that m divides kn, i.e., there exists $l \in \mathbb{Z}$ such that $kn = ml$. If $a, b \in \mathbb{Z}$ with $[a]_n = [b]_n$, then

$$\begin{aligned}
[a]_n = [b]_n &\Rightarrow n|(b-a) \Rightarrow b - a = nq, \quad q \in \mathbb{Z}\\
&\Rightarrow kb - ka = knq, \qquad\qquad q \in \mathbb{Z}\\
&\Rightarrow kb - ka = mlq = m(lq), \quad q, l \in \mathbb{Z}\\
&\Rightarrow m|(kb - ka) \Rightarrow [ka]_m = [kb]_m\\
&\Rightarrow f([a]_n) = f([b]_n).
\end{aligned}$$

and f is well-defined.

The reader may notice that if m does not divide kn, then the zero element in the domain can be selected to show that $f : \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $f([a]_n) = [ka]_m$ is not well-defined. For if m does not divide kn, then kn is not a multiple of m which implies that $[kn]_m \neq [0]_m$. Therefore, $[0]_n = [n]_n$, but $f([0]_n) = [0]_m \neq [kn]_m = f([n]_n)$.

3.3 Algebraic Operations the Integers Modulo *n*

In this section, algebraic operations like addition and multiplication on $\mathbb{Z}_n$ are defined and discussed. We advise the reader to review Sect. 1.3 regarding relations on a set.

Definition 3.3.1 Let $n \in \mathbb{N}$. The addition and multiplication relations on $\mathbb{Z}_n \times \mathbb{Z}_n$ are defined as:

$$\begin{array}{lll}
\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n & \otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n & \\
[a] \oplus_n [b] = [a+b] & [a] \otimes_n [b] = [ab] & \text{for all} [a], [b] \in \mathbb{Z}_n.
\end{array}$$

where $a + b$ and ab denote the addition and multiplication of integers, respectively, on a and b.

Note that in the above definition, the notation $[a] \oplus_n [b]$ and $[a] \otimes_n [b]$ are used instead of $\oplus_n([a], [b])$ and $\otimes_n([a], [b])$, respectively.

Proposition 3.3.2 *Let $n \in \mathbb{N}$. The relations $\oplus_n$ and $\otimes_n$, defined in Definition 3.3.1, are functions on $\mathbb{Z}_n$.*

Proof First, we verify that the result of applying each operation on two elements of $\mathbb{Z}_n$ is an element of $\mathbb{Z}_n$. Let $[a], [b] \in \mathbb{Z}_n$ be arbitrary elements. According to the quotient-remainder theorem (Theorem 2.1.2), there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $a + b = q_1 n + r_1$ and $ab = q_2 n + r_2$, where $0 \leq r_1, r_2 < n$. Therefore,

$$[a] \oplus_n [b] = [a + b] = [r_1] \in \mathbb{Z}_n \text{ and } [a] \otimes_n [b] = [ab] = [r_2] \in \mathbb{Z}_n.$$

To verify that the operations are well-defined, assume that $a, b, c, d \in \mathbb{Z}$ such that

$$[a] = [c] \;\wedge\; [b] = [d].$$

According to the definition of the relation modulo n, there exist $q_1, q_2 \in \mathbb{Z}$ such that

$$a - c = q_1 n, \;\; b - d = q_2 n.$$

Hence,

$$(a + b) - (c + d) = (a - c) + (b - d) = (q_1 + q_2)n$$

where $q_1 + q_2 \in \mathbb{Z}$, and

$$\begin{aligned} ab - cd &= ab - ad + ad - cd = a(b - d) + (a - c)d \\ &= (aq_2 + q_1 c)n \end{aligned}$$

where $aq_2 + q_1 c \in \mathbb{Z}$. Therefore,

$$\begin{aligned} &[a + b] = [c + d] \text{ and [ab] = [cd], which implies that} \\ &[a] \oplus_n [b] = [c] \oplus_n [d] \text{ and } [a] \otimes_n [b] = [c] \otimes_n [d]. \end{aligned}$$

■

Definition 3.3.3 The maps $\oplus_n$ and $\otimes_n$ on $\mathbb{Z}_n$, are called the addition modulo n, and multiplication modulo n, respectively.

Example 3.3.4

1. Considering the set $\mathbb{Z}_{13}$, the reader may easily verify that

$$\begin{aligned} &[2] \oplus_{13} [7] = [9], [12] \oplus_{13} [10] = [22] = [9], [8] \oplus_{13} [9] = [17] = [4], \\ &[2] \otimes_{13} [7] = [14] = [1], [12] \otimes_{13} [10] = [120] = [3], [8] \otimes_{13} [9] = [72] = [7]. \end{aligned}$$

2. Considering the set $\mathbb{Z}_6$, the reader may easily verify that

$$\begin{gathered}[2] \oplus_6 [15] = [17] = [5], \quad [-5] \oplus_6 [1] = [-4] = [2], \quad [2] \oplus_6 [4] = [6] = [0],\\ [13] \oplus_6 [-4] = [9] = [3], \quad [2] \otimes_6 [7] = [14] = [2], \quad [2] \otimes_6 [7] = [2] \otimes_6 [1] = [2],\\ [2] \otimes_6 [3] = [6] = [0], \quad [-5] \otimes_6 [4] = [-20] = [4].\end{gathered}$$

Note that $[2] \otimes_6 [3] = [0]$ is an example for multiplying two nonzero elements that could be zero. This example is not encountered the multiplication of integers. The example shows that the multiplication of modulo n has different rules than those of the multiplication of integers.

Proposition 3.3.5 *Let n be an integer such that $n > 1$, and $[a] \in \mathbb{Z}_n$.*

There exists [b] $\in \mathbb{Z}_n$ *such that* $[a] \otimes_n [b] = [1]$ *if and only if* $\gcd(a, n) = 1$.

Proof Assume that $[a]\in \mathbb{Z}_n$. By applying Bézout's lemma (Theorem 2.5.1) to a and n, we have

$$\begin{aligned}\gcd(a, n) = 1 &\Leftrightarrow \text{there exist } b, q \in \mathbb{Z} \text{ such that } ab + nq = 1\\ &\Leftrightarrow \text{there exist } b, q \in \mathbb{Z} \text{ such that } nq = 1 - ab\\ &\Leftrightarrow \text{there exist } b, q \in \mathbb{Z} \text{ such that } n|(1 - ab)\\ &\Leftrightarrow [ab] = [1] \Leftrightarrow [a] \otimes_n [b] = [1].\end{aligned}$$

■

Definition 3.3.6 Let n be an integer such that $n > 1$, and $[a] \in \mathbb{Z}_n$. If there exists [b] $\in \mathbb{Z}_n$ such that $[a] \otimes_n [b] = [1]$, then $[b]$ is called the multiplicative inverse of $[a]$, denoted by $[a]^{-1}$. If no such $[b]$ exists, we say $[a]$ is not invertible or that $[a]^{-1}$ is not defined.

Definition 3.3.7 Let $n \in \mathbb{N}$, $k \in \mathbb{Z}$, and $[a] \in \mathbb{Z}_n$. For $k > 0$, $k[a]$, and $[a]^k$ are defined as follows

$$k[a] = \underbrace{[a] \oplus_n [a] \oplus_n \cdots \oplus_n [a]}_{k \text{ times}}$$
$$[a]^k = \underbrace{[a] \otimes_n [a] \otimes_n \cdots \otimes_n [a]}_{k \text{ times}}$$

$0[a]$ and $[a]^0$ are defined as [0] and [1], respectively. For $k < 0$,

- $k[a]$ is defined as follows:

$$k[a] = \underbrace{[-a] \oplus_n [-a] \oplus_n \cdots \oplus_n [-a]}_{-k \text{ times}}$$

- $[a]^k$ is only defined if $[a]$ has a multiplicative inverse. In this case,

$$[a]^k = \underbrace{[a]^{-1} \otimes_n [a]^{-1} \otimes_n \cdots \otimes_n [a]^{-1}}_{-k \text{ times}}.$$

According to the definition of addition and multiplication modulo n, for any $k \geq 0$,

$$k[a] = [ka] \text{ and } [a]^k = [a^k].$$

Note that the equality $[a]^k = [a^k]$ is usually not true for $k < 0$ even when of $[a]^{-1}$ is defined (Exercise). The following propositions are easy to verify using the definition.

Proposition 3.3.8 *Let $n \in \mathbb{N}$, then $n[a] = [0]$ for any $a \in \mathbb{Z}$. If $[a], [b] \in \mathbb{Z}_n$ and $[a] = [b]$, then $[a]^k = [b]^k$ for any $k \in \mathbb{N} \cup \{0\}$.*

Proposition 3.3.9 *Let $n \in \mathbb{N}$ and $[a] \in \mathbb{Z}_n$. For any $k_1, k_2 \in \mathbb{Z}$,*

1. $(k_1 + k_2)[a] = k_1[a] \oplus_n k_2[a]$.
2. *If $k_1, k_2 \geq 0$, then $[a]^{(k_1+k_2)} = [a]^{k_1} \otimes_n [a]^{k_2}$ and $\left([a]^{k_1}\right)^{k_2} = [a]^{k_1 k_2}$.*

Example 3.3.10

1. In $\mathbb{Z}_9$,

   a. $3[3] = [3] \oplus_9 [3] \oplus_9 [3] = [6] \oplus_9 [3] = [9] = [0]$, or simply, $3[3] = [3 \times 3] = [9] = [0]$.
   b. $[3]^3 = [3] \otimes_9 [3] \otimes_9 [3] = [9] \otimes_9 [3] = [0] \otimes_9 [3] = [0]$, or simply, $[3]^3 = \left[3^3\right] = [27] = [0]$.
   c. $4[2] = [2] \oplus_9 [2] \oplus_9 [2] \oplus_9 [2] = [8]$, or simply, $4[2] = [4 \times 2] = [8]$.
   d. $[7]^4 = [7] \otimes_9 [7] \otimes_9 [7] \otimes_9 [7] = [49] \otimes_9 [49] = [4] \otimes_9 [4] = [16] = [7]$, or simply, $[7]^4 = \left[7^4\right] = [2401] = [7]$.

2. In $\mathbb{Z}_{10}$,

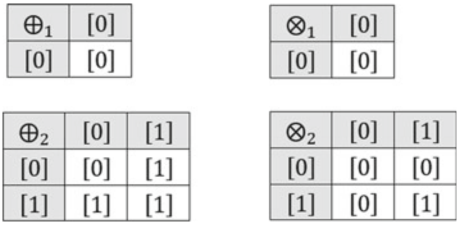
   a.
$$\begin{aligned} -322[2]^{13} &= -322\big([2]^4 \otimes_{10} [2]^4 \otimes_{10} [2]^4 \otimes_{10} [2]^1\big) \\ &= -322([6] \otimes_{10} [6] \otimes_{10} [6] \otimes_{10} [2]) = -322([6] \otimes_{10} [2]) \\ &= -322([2]) = -(32 \times 10 + 2)[2] = -(32 \times 10[2] \oplus_{10} 2[2]) \\ &= -(32 \times [0] \oplus_{10} 2[2]) = -([0] \oplus_{10} 2[2]) = -[4] = [-4] = [6]. \end{aligned}$$

   We can also compute it as follows:

$$\begin{aligned} [2]^{13} = [2]^5 \otimes_{10} [2]^5 \otimes_{10} [2]^3 &= [2] \otimes_{10} [2] \otimes_{10} [8] = [4] \otimes_{10} [8] = [2] \\ \text{and } -322[2]^{13} &= -322[2] = -[644] = -[4] = [6]. \end{aligned}$$

   b. $[2]^{-322} = \left([2]^{-1}\right)^{322}$ is not defined.

Table 3.1 Addition and multiplication tables for $\mathbb{Z}_1$ and $\mathbb{Z}_2$



$\oplus_1$	[0]
[0]	[0]

$\otimes_1$	[0]
[0]	[0]

$\oplus_2$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[1]

$\otimes_2$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

c. $[3]^2 = [3] \otimes_{10} [3] = [9]$, $[3]^3 = [9] \otimes_{10} [3] = [27] = [7]$, and $2[3]^2 = 2[9] = [18] = [8]$.

d. $$\begin{aligned} -42[3]^7 &= -42\big([3]^3 \otimes_{10} [3]^3 \otimes_{10} [3]\big) = -42([7] \otimes_{10} [7] \otimes_{10} [3]) \\ &= -42([9] \otimes_{10} [3]) = -42[7] = [6]. \end{aligned}$$

e. $[4]^{-42} = \big([4]^{-1}\big)^{42}$ is not defined.

f. Since $[5]^k = [5]$ in $\mathbb{Z}_{10}$ for any $k \in \mathbb{N}$ (Check!), then $[5]^{2063} = [5]$, and

$$\begin{aligned} 2063[5]^3 &= 2063[5] = (206 \times 10 + 3)[5] \\ &= (206 \times 10)[5] + (3)[5] \\ &= [0] + (3)[5]{=}[5]. \end{aligned}$$

3.4 The Addition Modulo *n* and Multiplication Modulo *n* Tables

As $\mathbb{Z}_n$ is a finite set, the addition and multiplication modulo n on $\mathbb{Z}_n$ can be represented using tables (Sect. 1.5). Theoretically, these tables can be built for any positive integer n, however, this process is impractical when n is large.

Example 3.4.1 The following tables pertain to the addition and multiplication on $\mathbb{Z}_n$ for several chosen integers n (Tables 3.1, 3.2 and 3.3).

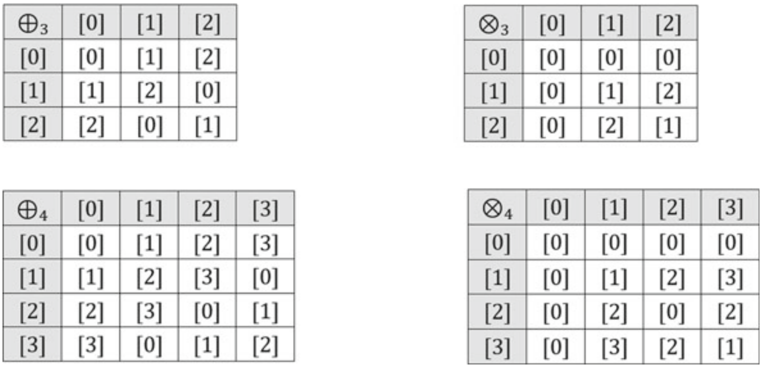
3.5 Use of the "mod *n*" Formula

In this section, we present a different but equivalent notation for the congruent formula $a \cong_n b$. The introduced notation is "$a \equiv b$ mod n", which is called the mod n formula. This change in notation helps deal with linear equations on $\mathbb{Z}_n$ defined in the next section. As $a \cong_n b$ means that $[a]_n = [b]_n$, then we obtain

$$a \equiv b \bmod n \Leftrightarrow a \cong_n b \Leftrightarrow [a]_n = [b]_n.$$

Recall that $[a]_n$ is an element in $\mathbb{Z}_n$.

Table 3.2 Addition and multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$



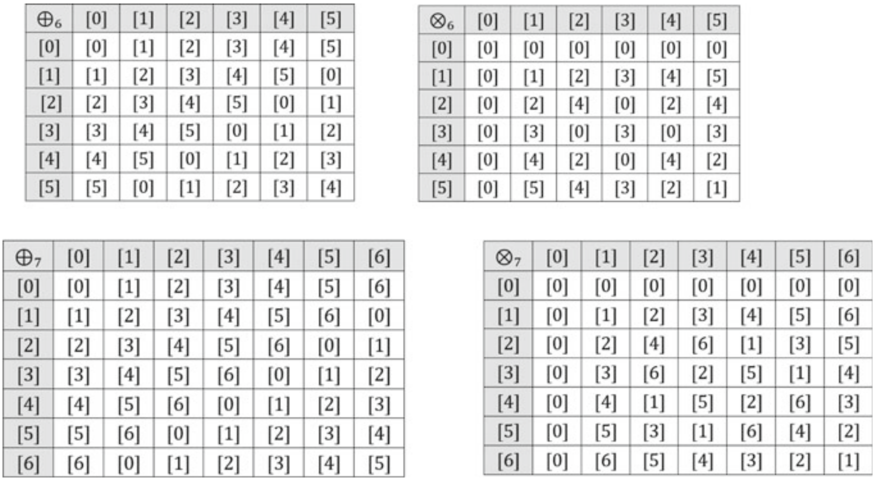
$\oplus_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\otimes_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\oplus_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\otimes_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Table 3.3 Addition and multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$



$\oplus_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\otimes_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\oplus_7$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

$\otimes_7$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Example 3.5.1 In the following statements, the congruent formulas are rewritten as mod n formulas, and vice versa.

$$7 \equiv 31 \bmod 8 \Leftrightarrow [7]_8 = [31]_8$$
$$23 \equiv -3 \bmod 13 \Leftrightarrow [23]_{13} = [-3]_{13}$$
$$a \equiv 5 \bmod 13 \Leftrightarrow [a]_{13} = [5]_{13}$$

Example 3.5.2 The following mathematical statements can be easily verified.

1. $119 \equiv 1 \bmod 2$ $(119 - 1 = 118$ and $2|118)$.
2. $119 \equiv 1 \bmod 59$ $(119 - 1 = 118$ and $59|118)$.
3. $23 \equiv -1 \bmod 6$ $(24 = 23 - (-1)$ and $6|24)$.

4. $89 \equiv 55 \bmod 17$ $(34 = 89 - 55$ and $17|34)$.
5. $100 \equiv -20 \bmod 24$ $(120 = 100 - (-20)$ and $24|120)$.

To simplify the use of the mod n formula, we rewrite all the previous results and definitions with both formulas:

Definition 3.5.3 For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$,

$$a \equiv b \bmod n \Leftrightarrow a \cong_n b \Leftrightarrow [a]_n = [b]_n.$$

The properties of the equivalence relation modulo n, stated in Propositions 3.1.5 and 3.1.3 can be expressed as follows:

Lemma 3.5.4 *For $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$,*

1. $a \equiv a \bmod n$ *(mod n is reflexive).*
2. $a \equiv b \bmod n \Leftrightarrow b \equiv a \bmod n$ *(mod n is symmetric).*
3. $a \equiv b \bmod n, b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$ *(mod n is transitive).*

Proposition 3.5.5 *For $r, n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$*

1. $a \equiv b \bmod n \Rightarrow ra \equiv rb \bmod n.$
2. $a \equiv b \bmod n \Rightarrow ra \equiv rb \bmod rn.$
3. $a \equiv b \bmod n \Rightarrow ar \equiv br \bmod n.$
4. $a \equiv b \bmod n \Rightarrow ar \equiv br \bmod rn.$
5. $ra \equiv rb \bmod n \Rightarrow a \equiv b \bmod \left(\frac{n}{\gcd(n,r)}\right).$
6. $ar \equiv br \bmod n \Rightarrow a \equiv b \bmod \left(\frac{n}{\gcd(n,r)}\right).$

The well-defined property of addition and multiplication modulo n in Proposition 3.3.2 can be rewritten as:

Proposition 3.5.6 *Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv c \bmod n$ and $b \equiv d \bmod n$, then*

$$a + b \equiv c + d \bmod n \text{ and } ab \equiv cd \bmod n.$$

Proposition 3.3.8 can be restated as follows:

Lemma 3.5.7 *Let $n \in \mathbb{N}$. If $a, b \in \mathbb{Z}$ such that $a \equiv b \bmod n$, then $a^k \equiv b^k \bmod n \ \ \forall k \in \mathbb{N}$.*

Example 3.5.8 To show that $(17)^6 - 1$ is divisible by 7, one needs to prove that $17^6 \equiv 1 \bmod 7$. The integer 17^6 is a large number, but one can avoid computing it by using Lemma 3.5.7, and the transitivity property of mod 7 as follows:

As $17 \equiv 3 \bmod 7$, using Lemma 3.5.7, yields $17^6 \equiv 3^6 \bmod 7$. Since $3^6 = 9^3$ and $9 \equiv 2 \bmod 7$, then $3^6 = 9^3 \equiv 2^3 \bmod 7$. Applying the transitivity property of mod 7, yields $17^6 \equiv 2^3 \bmod 7$. However, $2^3 = 8 \equiv 1 \bmod 7$, which implies (by property of mod 7) that $17^6 \equiv 1 \bmod 7$, as required.

Another way to show that $17^6 \equiv 1 \bmod 7$ is by using Proposition 3.5.6 as follows:

Since $17 \equiv 3 \bmod 7$, then applying Proposition 3.5.6, yields $17 \times 17 \equiv 3 \times 3 \bmod 7$. That is, $17^2 \equiv 9 \bmod 7$. However, since $9 \equiv 2 \bmod 7$, then by the transitive property of mod 7, one gets $17^2 \equiv 2 \bmod 7$. Therefore, $17^3 = 17^2 \times 17 \equiv 2 \times 3 = 6 \bmod 7 \Rightarrow 17^3 \equiv 6 \bmod 7$. Applying Proposition 3.5.6 again yields $17^6 = 17^3 \times 17^3 \equiv 6 \times 6 = 36 \equiv 1 \bmod 7$, as required.

Example 3.5.9

1. One can show that the product of any three consecutive positive integers is divisible by 6 as follows: Suppose $D = n(n+1)(n+2)$ for some positive integer n. Since either n or $n+1$ is even, then D is an even integer, i.e., D is divisible by 2. We show that 3 divides D by examining n and the elements of $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

   - If $n \in [0]$, then $n \equiv 0 \bmod 3$. Thus, n is divisable by 3 and $3|D$.
   - If $n \in [1]$, then $n \equiv 1 \bmod 3$. Thus, $n+2$ is divisable by 3 and $3|D$.
   - If $n \in [2]$, then $n \equiv 2 \bmod 3$. Thus, $n+1$ is divisable by 3 and $3|D$.

   In all cases, D is divisible by 3. Since$2|D$, $3|D$, and $\gcd(2, 3) = 1$, by Corollary 2.5.7 (3), $6|D$.
2. For all $n \in \mathbb{N}$, as $n^3 - n = n\big(n^2 - 1\big) = (n-1)n(n+1)$ is a product of three consecutive numbers, then by item 1, one obtains $6|(n^3 - n)$, i.e., $n^3 \equiv n \bmod 6$.
3. For all $n \in \mathbb{N}$, $5n^3 + n$ is divisible by 6. To Show this, we use that $n^3 \equiv n \bmod 6$ to obtain $5n^3 \equiv 5n \bmod 6$. As $5n \equiv -n \bmod 6$, by the transitive property of mod 6,

   $$5n^3 \equiv 5n \equiv -n \bmod 6.$$

   Therefore, $6|(5n^3 + n)$ and $5n^3 + n$ is divisible by 6.

In cryptography, one needs to compute the class of $a^b \bmod n$ for very large numbers a, b and n. In these applications computing a^b is not practical. Let's illustrate a possible strategy with an example.

Example 3.5.10 To compute $67^{789} \bmod 100$, we start with the exponent and repeat diving by 2 (with remainder) to get

$$\begin{aligned} &789 = 394 \times 2 + 1, \quad 394 = 2 \times 197, \quad 197 = 2 \times 98 + 1, \\ &98 = 2 \times 49, \quad 49 = 2 \times 24 + 1, \quad 24 = 2 \times 12, \\ &12 = 2 \times 6, \quad 6 = 2 \times 3, \quad 3 = 2 \times 1 + 1. \end{aligned}$$

We compute classes modulo 100 starting with the last division and work our way up as follow:

$$
\begin{aligned}
&67^2 \equiv 89 \bmod 100,\\
&67^3 \equiv 67^2 \times 67^1 \equiv 89 \times 67 \equiv 63 \bmod 100,\\
&67^6 \equiv \left(67^3\right)^2 \equiv 63 \times 63 \equiv 69 \bmod 100,\\
&67^{12} \equiv \left(67^6\right)^2 \equiv 69 \times 69 \equiv 61 \bmod 100,\\
&67^{24} \equiv \left(67^{12}\right)^2 \equiv 61 \times 61 \equiv 21 \bmod 100,\\
&67^{49} \equiv \left(67^{24}\right)^2 \times 67 \equiv 21 \times 21 \times 67 \equiv 47 \bmod 100,\\
&67^{98} \equiv \left(67^{49}\right)^2 \equiv 47 \times 47 \equiv 9 \bmod 100,\\
&67^{197} \equiv \left(67^{98}\right)^2 \times 67 \equiv 9 \times 9 \times 67 \equiv 27 \bmod 100,\\
&67^{394} \equiv \left(67^{197}\right)^2 \equiv 27 \times 27 \equiv 29 \bmod 100, \text{ and}\\
&67^{789} \equiv \left(67^{394}\right)^2 \times 67 \equiv 29 \times 29 \times 67 \equiv 47 \bmod 100.
\end{aligned}
$$

Note that

- Although 67^{789} has more than 1000 digits, we only used, in above computation, numbers less than 100 and exponents 1 or 2.
- One can choose to begin by dividing on any number rather than 2, however, this might complicate the computation as the exponents that appear in the computations will contain numbers more than 2.

3.6 Linear Equations on the Integers Modulo *n*

As in the case of integers, linear equations can be defined on $\mathbb{Z}_n$ using the addition and multiplication modulo n.

Definition 3.6.1 Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$.

1. The general form of a linear equation with one variable on $\mathbb{Z}_n$ is

$$([a] \otimes_n [x]) \oplus_n [b] = [c].$$

2. A solution of $([a] \otimes_n [x]) \oplus_n [b] = [c]$ is an element $[x_0] \in \mathbb{Z}_n$ such that

$$([a] \otimes_n [x_0]) \oplus_n [b] = [c].$$

Remark 3.6.2

$$
\begin{aligned}
([a] \otimes_n [x]) \oplus_n [b] = [c] &\Leftrightarrow ([ax]) \oplus_n [b] = [c]\\
&\Leftrightarrow [ax + b] = [c]\\
&\Leftrightarrow ax + b \equiv c \mod n.
\end{aligned}
$$

Thus, the equation in Definition 3.6.1 (1) can be rewritten as $ax + b \equiv c \bmod n$, which simplifies the notations.

Example 3.6.3 Consider the equation $4x + 2 \equiv 10 \bmod 12$.

1. The class 2 mod 12 is a solution for the equation, since

$$4 \cdot 2 + 2 = 8 + 2 = 10 \equiv 10 \bmod 12.$$

   Equivalently, we can write $[2] \in \mathbb{Z}_{12}$ is a solution for $([4] \otimes_{12} [x]) \oplus_{12} [2] = [10]$.
2. The classes 5 mod 12 and 8 mod 12 are also solutions for the equation as

$$4 \cdot 5 + 2 = 20 + 2 = 22 \equiv 10 \bmod 12$$

   and

$$4 \cdot 8 + 2 = 32 + 2 = 34 \equiv 10 \bmod 12.$$

3. The class 7 mod 12 is not a solution for the equation, since

$$4 \cdot 7 + 2 = 28 + 2 = 30 \not\equiv 10 \bmod 12.$$

Note that the symbol $=$ means equality, while the symbol $\equiv$ means equality modulo n or equivalence.

Example 3.6.4

1. Considering all the elements of $\mathbb{Z}_8$, one can determine [3] is the only solution in $\mathbb{Z}_8$ for the equation $[x] \oplus_8 [2] = [5]$. Although finding a solution for such an equation in $\mathbb{Z}_8$ seems easy, it is impractical to examine all the elements in cases involving a large $\mathbb{Z}_n$. The equation $[x] \oplus_8 [2] = [5]$ can be solved without examining all the elements in $\mathbb{Z}_8$ by using the form in Remark 3.6.2 and Proposition 3.5.6.

$$\begin{aligned} x + 2 \equiv 5 \bmod 8 &\Rightarrow x + 2 - 2 \equiv 5 - 2 \bmod 8 \\ &\Rightarrow x \equiv 3 \bmod 8. \end{aligned}$$

   Therefore, [3] is a solution in $\mathbb{Z}_8$.

   Note that the second method is not applicable to the more general equation $ax + b \equiv c \bmod n$. To obtain solutions to this more general equation, the results in Proposition 3.6.7 below are needed.
2. To find a solution for $x + 7 \equiv 3 \bmod 8$, we add -7 to both sides, to obtain $x \equiv -4 \bmod 8$. Since $4 \equiv -4 \bmod 8$, then by the transitive property of mod 8, $x \equiv 4 \bmod 8$, and [4] is a solution to the equation $[x] \oplus_8 [7] = [3]$ in $\mathbb{Z}_8$.
3. The equation $3x - 2 \equiv 5 \bmod 9$ has no solution in $\mathbb{Z}_9$. If a mod 9 was a solution, then

$$\begin{aligned} 3a - 2 \equiv 5 \bmod 9 &\Rightarrow 3a - 2 + 2 \equiv 5 + 2 \bmod 9 \\ &\Rightarrow 3a \equiv 7 \bmod 9 \Rightarrow \exists\, a \in \mathbb{Z} \ni 9 | (3a - 7). \end{aligned}$$

As $3|9$, then by transitivity of divisibility, we obtain $\exists\ a \in \mathbb{Z} \ni 3|(3a-7)$. Since$3|3a$, then 3 divides 7 (since 7 is a linear combination of $(3a-7)$ and $3a$), which contradicts that 7 is a prime number. Therefore, no solution to this equation exists in $\mathbb{Z}_9$.

4. To find a solution in $\mathbb{Z}_{15}$ for the equation $3x+7 \equiv 1 \bmod 15$, we follow the same steps as in the last two examples:

$$3x+7 \equiv 1 \bmod 15 \Rightarrow 3x \equiv -6 \bmod 15 \Rightarrow 3x \equiv 9 \bmod 15$$
$$\Rightarrow x \equiv 3 \bmod 15.$$

Thus, [3] is a solution for the given equation in $\mathbb{Z}_{15}$. This solution is not the only solution to this equation since [8] and [13] are also solutions to the same equation in $\mathbb{Z}_{15}$.

Note that a linear equation on $\mathbb{Z}_n$ in one variable may have more than one solution. This differs from that of equations on the integers, where a linear equation in one variable has at most one solution. Corollary 3.6.6 provides the necessary conditions for $ax+b \equiv c \bmod n$ to have a solution, and Proposition 3.6.7 determines all possible solutions of this equation in $\mathbb{Z}_n$ if they exist. We begin with the following lemma.

Lemma 3.6.5 *Let $n \in \mathbb{N}$ and a, c be integers. The equation $ax \equiv c \bmod n$ has a solution if and only if $\gcd(a,n)|c$.*

Proof The equation $ax \equiv c \bmod n$ has a solution if and only if there exists $[b] \in \mathbb{Z}_n$ such that

$$ab \equiv c \bmod n$$

i.e., if and only if $ab - c = qn$ for some $q, b \in \mathbb{Z}$. In other words, if and only if

$$ab + qn = c \text{ for some } b, q \in \mathbb{Z}$$

i.e., if and only if the equation $ax + ny = c$ has integer solutions. According to Proposition 2.6.5 (1), this holds if and only if $\gcd(a,n)|c$. ■

Applying the result of Lemma 3.6.5 on $ax \equiv (c-b) \bmod n$, yields

Corollary 3.6.6 *Let $n \in \mathbb{N}$, and a, b, c be any integers. The equation $ax+b \equiv c \bmod n$ has a solution if and only if $\gcd(a,n)|(c-b)$.*

Proposition 3.6.7 *Let $n \in \mathbb{N}$ and a, b, c be integers. If $[x_0] \in \mathbb{Z}_n$ is a solution to the equation $ax+b \equiv c \bmod n$, then the set*

$$\left\{\left[x_0 + \frac{n}{\gcd(a,n)}t\right] : t \in \mathbb{Z}\right\}$$

contains all possible solutions for the equation $ax+b \equiv c \bmod n$ in $\mathbb{Z}_n$. The subset

$$A = \left\{ \left[x_0 + \frac{n}{\gcd(a,n)} t \right] : t \in \mathbb{Z}, 0 \leq t < \gcd(a,n) \right\}$$

forms all distinct solutions in $\mathbb{Z}_n$.

Proof If $[x_0] \in \mathbb{Z}_n$ such that $ax_0 + b \equiv c \mod n$, then for any $t \in \mathbb{Z}$,

$$\begin{aligned} a\left(x_0 + \frac{n}{\gcd(a,n)} t \right) + b &= (ax_0 + b) + \left(\frac{at}{\gcd(a,n)} \right) n \\ &\equiv c + 0 = c \bmod n. \end{aligned}$$

Hence, $x_0 + (n/\gcd(a,n))t$ is a solution for this equation for all $t \in \mathbb{Z}$. If x_1 is also a solution for the equation $ax + b \equiv c \bmod n$, then

$$ax_0 + b \equiv c \bmod n, \ ax_1 + b \equiv c \bmod n.$$

By transitive property of mod n, $ax_1 + b \equiv ax_0 + b \bmod n$, which implies that

$$ax_1 \equiv ax_0 \bmod n.$$

According to Proposition 3.1.3, $x_1 \equiv x_0 \bmod (n/\gcd(a,n))$. Thus, there exists $t \in \mathbb{Z}$ such that

$$x_1 - x_0 = t(n/\gcd(a,n)).$$

Therefore,

$$x_1 = x_0 + (n/\gcd(a,n))t \text{ for some } t \in \mathbb{Z}.$$

To demonstrate that A contains all the different solutions, one must show that

- A contains all the solutions for the given equation.
- All elements in A are distinct.

as follows:

Assume that $t \in \mathbb{Z}$ is an arbitrary integer. By applying the quotient-remainder theorem (Theorem 2.1.2) on t and $\gcd(a,n)$, there exist two integers q, r such that

$$t = q \gcd(a,n) + r, \quad 0 \leq r < \gcd(a,n).$$

Therefore,

$$\begin{aligned} \left[x_0 + \frac{n}{\gcd(a,n)} t \right] &= \left[x_0 + \frac{n}{\gcd(a,n)} (q \gcd(a,n) + r) \right] \\ &= \left[x_0 + nq + \frac{n}{\gcd(a,n)} r \right] = \left[x_0 + \frac{n}{\gcd(a,n)} r \right] \oplus_n [nq] \end{aligned}$$

$$= \left[x_0 + \frac{n}{\gcd(a,n)}r\right] \oplus_n [0] = \left[x_0 + \frac{n}{\gcd(a,n)}r\right] \in A.$$

To show that all elements in A are different, let $t_1, t_2 \in \mathbb{Z}$ such that $0 \le t_1, t_2 < \gcd(a,n)$ and

$$\left[x_0 + \frac{n}{\gcd(a,n)}t_1\right] = \left[x_0 + \frac{n}{\gcd(a,n)}t_2\right]$$

converting this equation to the mod n formula yields

$$x_0 + \frac{n}{\gcd(a,n)}t_1 \equiv x_0 + \frac{n}{\gcd(a,n)}t_2 \bmod n$$

which implies that

$$\frac{n}{\gcd(a,n)}t_1 \equiv \frac{n}{\gcd(a,n)}t_2 \bmod n.$$

Multiplying both sides of the statement by $\gcd(a,n)$ (Proposition 3.1.3), one obtains

$$nt_1 \equiv nt_2 \bmod (n\gcd(a,n)).$$

This statement implies that $n(t_2 - t_1) = qn \gcd(a,n)$ for some $q \in \mathbb{Z}$. i.e., $(t_2 - t_1) = q \gcd(a,n)$. That is, $\gcd(a,n)$ divides $|t_2 - t_1|$. As both t_1, t_2 are nonnegative integers that are less than $\gcd(a,n)$, so $|t_2 - t_1| < \gcd(a,n)$, and thus $|t_2 - t_1|$ must be zero. Therefore, $t_1 = t_2$, and all elements in A are distinct. ■

Although the last proposition appears similar to Proposition 2.6.5, the reader should note that Proposition 2.6.5 pertain to a linear equation on $\mathbb{Z}$ in two variables x and y, whereas this proposition is an equation in one variable. Moreover, once a solution for $ax + b \equiv c \bmod n$ has been obtained, the integers b and c are not relevant anymore. The integers a and n determine the other solutions. Note also that the statement in Proposition 3.6.7 implies that if a solution to the equation $ax + b \equiv c \bmod n$ exists in $\mathbb{Z}_n$, then the number of distinct solutions for the equation equals to $\gcd(a,n)$.

Example 3.6.8 To find all possible solutions for the equation $2x \equiv 3 \bmod 5$ in $\mathbb{Z}_5$, one computes $\gcd(5,2)$. As $\gcd(5,2) = 1$ divides 3, then by Lemma 3.6.5, the given equation has a solution in $\mathbb{Z}_5$. Proposition 3.6.7 ensures that there is only one solution (at $t = 0$). We present two methods to find it.

Method 1:

The equation $2x \equiv 3 \bmod 5$ is equivalent to $[x] \otimes_5 [2] = [3]$. By substituting all elements of $\mathbb{Z}_5$ in $[x] \otimes_5 [2] = [3]$, the solution $[x]$ can be sequentially determined, as indicated in Table 3.4.

Table 3.4 The solutions for the equation $2x \equiv 3 \bmod 5$

$[x] = [0]$	$[0] \otimes_5 [2] = [0] \neq [3]$	[0] is not a solution
$[x] = [1]$	$[1] \otimes_5 [2] = [2] \neq [3]$	[1] is not a solution
$[x] = [2]$	$[2] \otimes_5 [2] = [4] \neq [3]$	[2] is not a solution
$[x] = [3]$	$[3] \otimes_5 [2] = [1] \neq [3]$	[3] is not a solution
$[x] = [4]$	$[4] \otimes_5 [2] = [3]$	[4] is a solution

Thus, $[x] = [4]$ is the required solution.

Method 2**:**

As $\gcd(5, 2) = 1$, then by Bézout's lemma (Theorem 2.5.1) using backward substitution

$$1 = \gcd(5, 2) = 5 \times 1 - 2 \times 2.$$

Multiply both sides of the equation by 3 to obtain $3 = 5 \times 3 + 2 \times (-6)$. Apply the relation mod 5 on both sides to get $2 \times (-6) \equiv 3 \bmod 5$. Since $-6 = 4$ in $\mathbb{Z}_5$,

$$3 \equiv 2 \times 4 \bmod 5.$$

Therefore, $[x] = [4]$ is the solution of the given equation in $\mathbb{Z}_5$.

Example 3.6.9 To find all possible solutions for the equation $12x \equiv 6 \bmod 27$ in $\mathbb{Z}_{27}$, one must compute $\gcd(12, 27)$. Using the Euclidean Algorithm 2.4.1, the $\gcd(12, 27) = 3$. As $3|6$, there exist three distinct solutions for $12x \equiv 6 \bmod 27$ in $\mathbb{Z}_{27}$ (Lemma 3.6.5 and Proposition 3.6.7). By Bézout's lemma (Theorem 2.5.1), and backward substitution,

$$\gcd(12, 27) = 3 = 27 + 12 \times (-2).$$

By multiplying both sides of the equation by 2, one obtains $6 = 27 \times 2 + 12 \times (-4)$. Applying the relation mod27 to both sides yields $6 \equiv 12 \times (-4) \bmod 27$. Since $-4 \equiv 23$ in $\mathbb{Z}_{27}$, then $6 \equiv 12 \times 23 \bmod 27$ and $[x] = [23]$ is a solution for the given equation in $\mathbb{Z}_{27}$. According to Proposition 3.6.7, the distinct solutions for $12x \equiv 6 \bmod 27$ are

$$23 + 9t \bmod 27, \ 0 \leq t < 3.$$

Therefore, the distinct solutions for the given equation in $\mathbb{Z}_{27}$ are

$$[23], \quad [23 + 9] = [32] = [5], \quad [23 + 18] = [41] = [14].$$

Exercises

Solved Exercises

3.1. Let $a, b, c \in \mathbb{Z}$ and n be positive integers such that $a \cong_n b$. Without using the well-defined property of $\oplus_n$ and $\otimes_n$, show that

1. $a + c \cong_n b + c,\ a - c \cong_n b - c.$
2. $ac \cong_n bc.$

Solution:

Assume that $a \cong_n b$.

1. $a \cong_n b \Leftrightarrow n|(b-a) \Leftrightarrow$ there exists $q \in \mathbb{Z}$ such that $b - a = qn$

$$\Leftrightarrow \text{there exists } q \in \mathbb{Z} \text{ such that } b + c - (a + c) = q\,n$$
$$\Leftrightarrow n|(b + c - (a + c)) \Leftrightarrow a + c \cong_n b + c.$$

The second statement follows as $a - c = a + (-c)$, and $b - c = b + (-c)$.

2. $a \cong_n b \Leftrightarrow n|(b-a) \Leftrightarrow$ there exists $q \in \mathbb{Z}$ such that $b - a = qn$

$$\Leftrightarrow \text{there exists } q \in \mathbb{Z} \text{ such that } bc - ac = q\,n\,c$$
$$\Leftrightarrow n|(bc - ac)$$
$$\Leftrightarrow ac \cong_n bc.$$

3.2. Find a positive integer n that satisfies:

i. $347 \cong_n 340.$
ii. $27 \equiv 17 \bmod n.$

Solution:

Using the relations in Definition 3.1.2, we obtain.

i. $347 \cong_n 340 \Leftrightarrow n|(340 - 347) \Leftrightarrow n|7$. As the only divisors of 7 are 1 and 7, then $n = 1$ or $n = 7$.
ii. $27 \equiv 17 \mod n \Leftrightarrow n|(17 - 27) \Leftrightarrow n|(-10)$. As the positive divisors of -10 are 1, 2, 5 and 10, then these are all possible values of n.

3.3. Let m, n, q be integers such that $mq \cong n \bmod q^2$. Show that $q|n$.

Solution:

Assume that $mq \cong n \bmod q^2$. By Definition 3.1.2, $q^2|(n - mq)$, and thus, there exists $s \in \mathbb{Z}$ such that $n - mq = \mathrm{s}\, q^2$, i.e., $n = sq^2 + mq = q(sq + m)$ for some $s \in \mathbb{Z}$. Therefore, $q|n$.

3.4. Show that the following relations are not well-defined. Give examples to support your answer.

- $f : \mathbb{Z}_6 \to \mathbb{Z}_5$ defined by $f([a]_6) = [3a]_5$.
- $g : \mathbb{Z}_4 \to \mathbb{Z}_8$ defined by $g([a]_4) = [a]_8$.
- $h : \mathbb{Z}_6 \to \mathbb{Z}_{10}$ defined by $h([a]_6) = [2a]_{10}$.

Solution:

According to the result of Example 3.2.4, all the above relations are not well-defined.

- For f, the classes $[0]_6$ and $[6]_6$ are equal, however

$$f([0]_6) = [0]_5 \neq [3]_5 = f([6]_6).$$

Also, $[1]_6$ and $[7]_6$ are equal in $\mathbb{Z}_6$, but their images are not (Check!).

- For g, the classes $[0]_4$ and $[4]_4$ are equal, however

$$g([0]_4) = [0]_8 \neq [4]_8 = f([4]_4).$$

Also, $[2]_4$ and $[6]_4$ are equal in $\mathbb{Z}_4$, but their images are not (Check!).

- For h, the classes $[0]_6$ and $[6]_6$ are equal, however

$$h([0]_6) = [0]_{10} \neq [2]_{10} = f([6]_6).$$

Also, $[5]_6$ and $[-1]_6$ are equal in $\mathbb{Z}_6$, but their images are not (Check!).

3.5. Give an example for an integer n and two nonzero elements $[a], [b] \in \mathbb{Z}_n$ such that

$$[a] \oplus_n [b] = [0] \text{ and } [a] \otimes_n [b] = [0].$$

Solution:

One can obtain an example by choosing $n = 4$, $[a] = [2]$, and $[b] = [2]$.

3.6. Let a be any integer. Show that either $a^2 \equiv 0 \bmod 4$ or $a^2 \equiv 1 \bmod 4$.

Solution:

Assume that a is any integer. By applying the quotient-remainder theorem to a and 2, we obtain $a = 2q + r$ for some $q \in \mathbb{Z}$ and $r = 0, 1$.

- If $r = 0$, then $a = 2q$ and $a^2 = 4q^2 \equiv 0 \bmod 4$.
- If $r = 1$, then $a = 2q + 1$, and

$$a^2 = 4q^2 + 4q + 1 = 4\big(q^2 + q\big) + 1 \equiv 1 \bmod 4.$$

3.7. Let a, b, r be integers and p be a prime such that $p \nmid r$. Show that if $ra \equiv rb \bmod p$ then $a \equiv b \bmod p$.

Solution:

Assume that $ra \equiv rb \bmod p$. Since $p \nmid r$ and p is a prime, then $\gcd(p, r) = 1$. According to Proposition 3.5.5 (5), $a \equiv b \bmod p$.

3.8. Show that 41 divides $2^{20} - 1$.

Solution:

To solve the question, we must show that $2^{20} \equiv 1 \bmod 41$. We start by listing 2^k for some k, to get

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32, \quad 2^6 = 64.$$

We terminate the process at 2^6, as 41 is between 2^5 and 2^6. Since $41 = 2^5 + 9$, then $2^5 \equiv -9 \bmod 41$. According to Lemma 3.5.7,

$$\begin{aligned} 2^{20} &= (2^5)^4 \equiv (-9)^4 \bmod 41 \\ &\equiv 81 \times 81 \bmod 41. \end{aligned}$$

As $81 \equiv -1 \bmod 41$, then by Lemma 3.5.4 (3),

$$2^{20} \equiv (-1) \times (-1) \equiv 1 \bmod 41.$$

3.9. Let p be a prime number. Find the solutions for $x^2 \equiv x \bmod p$ in $\mathbb{Z}_p$, if there are any.

Solution:

If $x^2 \equiv x \bmod p$, then $p|x^2 - x$, i.e., $p|x(x-1)$. According to Euclid's lemma (Proposition 2.8.3), $p|x$ or $p|(x-1)$.

- If $p|x$, then there exists $q \in \mathbb{Z}$ such that $x = qp \equiv 0 \bmod p$.
- If $p|(x-1)$, then there exists $q \in \mathbb{Z}$ such that $x - 1 = qp \equiv 0 \bmod p$. i.e., $x \equiv 1 \bmod p$.

Therefore, the only possible values of x in $\mathbb{Z}_p$ are [0] and [1].

3.10. Find all distinct solutions for the following equations in $\mathbb{Z}_5$.

$$[3] \otimes_5 [x] = [1], \quad x \equiv 3 \bmod 5, \quad 2x \equiv 4 \bmod 5.$$

Solution:

For any $a \neq 5q, q \in \mathbb{Z}$, we have $\gcd(a, 5) = 1$. Therefore, all the given equations have only one solution in $\mathbb{Z}_5$ (Proposition 3.6.7). Since $\mathbb{Z}_5$ contains only five elements, all the elements of $\mathbb{Z}_5$ can be examined to determine the possible solution.

- For $[3] \otimes_5 [x] = [1]$:

  According to the computations in Table 3.5, [2] is the required solution for $[3] \otimes_5 [x] = [1]$ in $\mathbb{Z}_5$.
- For $x \equiv 3 \bmod 5$: Considering all elements in $\mathbb{Z}_5$, 3 is the only element in $\{0, 1, 2, 3, 4\}$ that satisfies the equation $x \equiv 3 \bmod 5$. Therefore, [3] is the required solution for $x \equiv 3 \bmod 5$ in $\mathbb{Z}_5$.
- For $2x \equiv 4 \bmod 5$:

  According to the computations in Table 3.6, $[x] = [2]$ is a solution for the given equation in $\mathbb{Z}_5$.

3.11. Find all the distinct solutions for the following equation in $\mathbb{Z}_{10}$.

$$2x \equiv 7 \bmod 10, \quad [x] \otimes_{10} [1] = [6],$$

Table 3.5 The solution for $[3] \otimes_5 [x] = [1]$

$[x] = [0]$	$[3] \otimes_5 [0] = [0] \neq [1]$	[0] is not a solution
$[x] = [1]$	$[3] \otimes_5 [1] = [3] \neq [1]$	[1] is not a solution
$[x] = [2]$	$[3] \otimes_5 [2] = [1]$	[2] is a solution
$[x] = [3]$	$[3] \otimes_5 [3] = [4] \neq [1]$	[3] is not a solution
$[x] = [4]$	$[3] \otimes_5 [4] = [2] \neq [1]$	[4] is not a solution

Table 3.6 The solution for $2x \equiv 4 \bmod 5$

$[x] = [0]$	$[2] \otimes_5 [0] = [0] \neq [4]$	[0] is not a solution
$[x] = [1]$	$[2] \otimes_5 [1] = [2] \neq [4]$	[1] is not a solution
$[x] = [2]$	$[2] \otimes_5 [2] = [0]$	[2] is a solution
$[x] = [3]$	$[2] \otimes_5 [3] = [1] \neq [4]$	[3] is not a solution
$[x] = [4]$	$[2] \otimes_5 [4] = [3] \neq [4]$	[4] is not a solution

$$[5] \otimes_{10} [x] = [0], \quad 3x \equiv 5 \bmod 10.$$

Solution:

Using the result of Lemma 3.6.5 and Proposition 3.6.7,

- As $\gcd(2, 10) = 2$ and $2 \nmid 7$, no solution for $2x \equiv 7 \bmod 10$ exists in $\mathbb{Z}_{10}$.
- Clearly, [6] is a solution for the equation $[x] \otimes_{10} [1] = [6]$. As $\gcd(1, 10) = 1$, there exists one solution for $[x] \otimes_{10} [1] = [6]$ in $\mathbb{Z}_{10}$. Therefore, [6] is the only possible solution in $\mathbb{Z}_{10}$.
- As $\gcd(5, 10) = 5$ and $5 | 0$, there exist five solutions for $[5] \otimes_{10} [x] = [0]$ in $\mathbb{Z}_{10}$. Checking all the elements in $\mathbb{Z}_{10}$, one obtains that

$$[0], [2], [4], [6], [8]$$

  are the only possible solutions in $\mathbb{Z}_{10}$.
- Finally, as $\gcd(3, 10) = 1$, there exists one solution for $3x \equiv 5 \bmod 10$ in $\mathbb{Z}_{10}$. Checking all the elements in $\mathbb{Z}_{10}$, one finds that [5] is the only possible solution in $\mathbb{Z}_{10}$.

3.12. Let $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$. Show that for any $a, b \in \mathbb{Z}$, the equations

$$x \equiv a \bmod p \text{ and } x \equiv b \bmod q$$

have a common solution.

Solution:

By Bézout's lemma (Theorem 2.5.1), there exist $u, v \in \mathbb{Z}$ such that $up + vq = 1$. i.e.

$$up \equiv 1 \bmod q \quad \text{and} \quad vq \equiv 1 \bmod p$$

which implies that for any integers a, b,

$$bup \equiv b \bmod q \text{ and } vaq \equiv a \bmod p.$$

Let $x = avq + bup \in \mathbb{Z}$, then $x \equiv avq \bmod p$ and $x \equiv bup \bmod q$.

As $vaq \equiv a \bmod p$ and $bup \equiv b \bmod q$, by transitivity, we obtain

$$x \equiv a \bmod p \text{ and } x \equiv b \bmod q$$

i.e., x is a common solution.

Unsolved Exercises

3.13. Find a positive integer n such that

i. $54 \cong_n 76$.
ii. $27 \equiv 10 \bmod n$.

3.14. Show that 97 divides $2^{48} - 1$.

3.15. Verify the following statements

$$\begin{array}{rrr} 7 \equiv 0 \bmod 7, & 29 \equiv 3 \bmod 13, & 119 \equiv 19 \bmod 4, \\ 6 \equiv -5 \bmod 11, & 456 \equiv 4 \bmod 2, & 121 \equiv 71 \bmod 5, \\ -4 \equiv 23 \bmod 27, & 436 \equiv 0 \bmod 436, & 436 \equiv 0 \bmod 3. \end{array}$$

3.16. List all the elements of $\mathbb{Z}_{13}$ and $\mathbb{Z}_8$. Give examples of functions $f : \mathbb{Z}_{13} \to \mathbb{Z}_8$ and $g : \mathbb{Z}_8 \to \mathbb{Z}_{13}$.

3.17. Determine whether the following are functions:

- $f : \mathbb{Z}_5 \to \mathbb{Z}_{10}$, where $f([a]_5) = [6a]_{10}$
- $f : \mathbb{Z}_4 \to \mathbb{Z}_6$, where $f([a]_4) = [3a]_6$
- $f : \mathbb{Z}_7 \to \mathbb{Z}_{12}$, where $f([a]_7) = [a]_{12}$
- $f : \mathbb{Z}_{12} \to \mathbb{Z}_7$, where $f([a]_{12}) = [a]_7$

3.18. Let k be any integer. Is $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ defined by $f([a]_8) = [ka]_4$ a function? Explain your answer.

3.19. Let $f : \mathbb{Z}_4 \to \mathbb{Z}_8$, where $f([a]_4) = [ka]_8$. List all integers k that render f well-defined.

3.20. Let $m, n \in \mathbb{N}$ such that $m > n$. Does $f : \mathbb{Z}_n \to \mathbb{Z}_m$, where $f([a]_n) = [a]_m$ form a function? Explain your answer.

3.21. Write the addition and multiplication tables for the additive groups $\mathbb{Z}_7$, $\mathbb{Z}_{10}$.

3.22. Let $m, n \in \mathbb{N}$ such that $n|m$. Show that for any integers a, b

$$a \equiv b \bmod m \Rightarrow a \equiv b \bmod n.$$

3.23. Find the solutions of the following equations if any exist:

- $3x + 3 \equiv 1 \bmod 9$.
- $12x - 10 \equiv 2 \bmod 7$.
- $[6] \otimes_3 [x] \oplus_3 [10] = [20]$.
- $[7] \otimes_6 [x] = [3]$.

Reference

Bloch, E. D. (2000). *Proofs and fundamentals: A first course in abstract mathematics.* Birkhaeuser.

Chapter 4
Semigroups and Monoids

This chapter examines semigroups and monoids, studies their basic properties, and presents several examples. The first section defines binary operations and presents several examples and results. Moreover, properties of binary operations such as associativity and commutativity are studied, and the notion of the identity element is introduced. The section provides the preliminary knowledge for studying Sect. 4.2, which discusses semigroups, and their stronger version, monoids. Section 4.3 defines and describes the set of invertible elements in a monoid, which paves the way for defining groups in Chap. 5, that contains the core of our study. The last and shortest section of this chapter discusses the notion of idempotent elements. The main result of Sect. 4.4 is presented in Proposition 4.4.5, which states that the identity element is the only idempotent invertible element in a monoid. Following most mathematicians, we use the letter G to denote a set whenever we discuss semigroups or monoids.

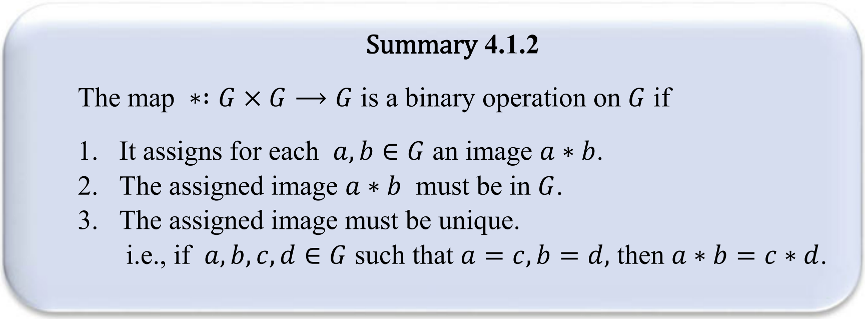
4.1 Binary Operations on Sets

In this section, we define and study binary operations on sets and highlight several of their algebraic properties.

Definition 4.1.1 Let G be any set. A binary operation $*$ on G means a function $* : G \times G \to G$.

The symbols $+$, $\cdot$, $\bullet$, $*$, and similar symbols are used to denote binary operations instead of the usual notation for functions. Thus, $a*b$ is used instead of $*(a, b)$ to denote the result of the operation, and $(G, *)$ is used to denote a set G equipped with a binary operation $*$. Recall that the map $* : G \times G \to G$ is a function if each element (a, b) in $G \times G$ has a unique image $a * b$ in G (Definition 1.5.1) (Fig. 4.1).

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_4



Summary 4.1.2

The map $*: G \times G \longrightarrow G$ is a binary operation on G if

1. It assigns for each $a, b \in G$ an image $a * b$.
2. The assigned image $a * b$ must be in G.
3. The assigned image must be unique.
   i.e., if $a, b, c, d \in G$ such that $a = c, b = d$, then $a * b = c * d$.

Fig. 4.1 The binary operation definition

Example 4.1.3

1. The map $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$$a * b = a + b$$

forms a function on $\mathbb{Z}$ (Sect. 2.1). Therefore, the addition of integers forms a binary operation on $\mathbb{Z}$.

2. The map $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$$a * b = \frac{a + b}{a - b}$$

is not a function on $\mathbb{Z}$, since $a * a$ is not defined for any integer a. Therefore, the above expression does not define a binary operation on $\mathbb{Z}$.

3. The map $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$a * b = a - b$$

is not a function on $\mathbb{N}$, as $2 * 7 = -5 \notin \mathbb{N}$. Indeed, the image $a * b$ does not belong to $\mathbb{N}$ when $b \geq a$. Thus, subtraction is not a binary operation on $\mathbb{N}$. However, the above expression defines a binary operation on $\mathbb{Z}$.

4. Let $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$ and $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$. Define $* : \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^*$ by

$$\frac{a}{b} * \frac{c}{d} = \frac{a+c}{bd} \quad a, b, c, d \in \mathbb{Z}^*.$$

This relation is not a function on $\mathbb{Q}^*$. For each $a, b \in \mathbb{Z}^*$,

$$\frac{a}{b} * -\frac{a}{b} = \frac{0}{b^2} = 0 \notin \mathbb{Q}^*.$$

Therefore, $*$ is not a binary operation on $\mathbb{Q}^*$. Another reason for not being a binary operation is that this relation is not well-defined as $1/3 = 2/6$, while

$$\frac{1}{3}*\frac{4}{7} = \frac{5}{21} \neq \frac{6}{42} = \frac{2}{6}*\frac{4}{7}.$$

5. Let $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ be defined as

$$\frac{a}{b} * \frac{c}{d} = \frac{a+c}{bd} \quad a, c \in \mathbb{Z}, \ \ b, d \in \mathbb{Z}^*.$$

The relation $*$ is not well-defined for the same reason given in (4). Thus, it is not binary operation.

6. The map $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by

$$\frac{a}{b} * \frac{c}{d} = \frac{ad+bc}{bd} \quad a, c \in \mathbb{Z}, \quad b, d \in \mathbb{Z}^*$$

is a function on $\mathbb{Q}$ (Example 1.5.9). Therefore, $*$ is a binary operation on $\mathbb{Q}$.

Definition 4.1.4 Let G be a set with a subset $B \subseteq G$, and $*$ be a binary operation on G. The set B is said to be closed under $*$ if $a * b \in B$ for all $a, b \in B$.

Example 4.1.5

1. Since the sum of two even integers is an even integer, the subset of all even integers of $\mathbb{Z}$ is closed under the addition.
2. For $n \in \mathbb{Z}$, consider $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\} \subseteq \mathbb{Z}$. For any $a, b \in n\mathbb{Z}$, there exists $m_1, m_2 \in \mathbb{Z}$, such that $a = nm_1$ and $b = nm_2$. Thus,

$$a + b = nm_1 + nm_2 = n(m_1 + m_2) \in n\mathbb{Z}.$$

Therefore, $n\mathbb{Z}$ is closed under the addition on $\mathbb{Z}$.

3. Consider $\mathbb{N}$, the subset of all positive integers in $\mathbb{Z}$. The set $\mathbb{N}$ is not closed under the subtraction on $\mathbb{Z}$. For example, both 2 and 3 are positive integers, but $2 - 3 = -1 \notin \mathbb{N}$.

Proposition 4.1.6 *Let G be a set with $B \subseteq G$, and $*$ be a binary operation on G. The operation $*$ is a binary operation on B if and only if B is closed under $*$.*

Proof If $*$ is a binary operation on B, then B is closed under $*$(by the definition of a binary operation). For the other direction, assume that B is closed under $*$, and let $a, b \in B$ be arbitrary elements. Since $*$ is an operation on G, the image $a * b$ is defined and unique, it belongs to B since B is closed under $*$, i.e., the operation $*$ forms a binary operation on B. ■

Next, we define and examine several properties of binary operations.

Definition 4.1.7 Let $*$ be a binary operation on G.

1. The operation $*$ is said to be associative if $a * (b * c) = (a * b) * c \;\; \forall\, a, b, c \in G$.
2. The operation $*$ is said to be commutative if $a * b = b * a \;\; \forall\, a, b \in G$.

Proposition 4.1.8 *Let G be a set and $B \subseteq G$. Let $*$ be a binary operation on G and B be closed under $*$. If the operation $*$ is an associative (commutative) operation on G, then it is an associative (commutative) operation on B. That is, B inherits the associativity (commutative property) from G.*

Proof The operation $*$ is a binary operation on B (Proposition 4.1.6). If $a, b, c \in B$, then $a, b, c \in G$. By associativity of $*$ on G, one finds that $a * (b * c) = (a * b) * c$, where both sides of the equation are in B. Similarly, for the commutativity, if a, b are elements in B, then they are elements in G and $a * b = b * a$, where both sides of the equation are in B. ■

Example 4.1.9 Let $*$ be defined for all $a, b \in \mathbb{Z}$ by $a * b = ab - a - b$. The operation $*$ forms a binary commutative and not an associative operation on $\mathbb{Z}$. For if $a, b \in \mathbb{Z}$, then the image $a * b$ defines a unique element in $\mathbb{Z}$. Hence, $*$ is a binary operation on $\mathbb{Z}$. The relation is commutative because for any $a, b \in \mathbb{Z}$,

$$a * b = ab - a - b = ba - b - a = b * a.$$

To show that $*$ is not associative, consider the three integers 2, 3, 4. It is easy to verify that

$$3 * (4 * 2) = 1 \neq 3 = (3 * 4) * 2.$$

Therefore, $*$ is not associative.

If G is a set with a binary operation $*$, then one can discuss the existence of an identity element in G. This element may or may not exist in G.

Definition 4.1.10 Let G be a set and $*$ be a binary operation on G.

1. An element $e_l \in G$ is called a left identity with respect to $*$ if

$$e_l * a = a \text{ for all } a \in G.$$

2. An element $e_r \in G$ is called a right identity with respect to $*$ if

$$a * e_r = a \text{ for all } a \in G.$$

3. An element $e \in G$ is called an identity with respect to $*$ if

$$a * e = e * a = a \text{ for all } a \in G.$$

If the operation $*$ is the only operation defined on G and there is no risk of ambiguity, we can drop the words "with respect to $*$" when discussing identity element.

Remark 4.1.11 If the operation $*$ is commutative on G, it is enough to check for the existence of a left or a right identity. For if e_l is a left identity of G and $*$ is commutative, then

$$a * e_l = e_l * a = a \quad \forall\, a \in G.$$

i.e., e_l is also a right identity. Likewise for a right identity in G.

Example 4.1.12

1. Let $+$ be the sum operation defined on the integers $\mathbb{Z}$. For each $a \in \mathbb{Z}$,

$$a + 0 = a = 0 + a,$$

which implies that 0 is an identity element for $(\mathbb{Z}, +)$. Similarly, 0 is an identity element for $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$. The subset $\mathbb{N}$ has no identity element with respect to the sum operation $+$. For if $\mathbb{N}$ has an identity with respect to $+$, then it must be zero, which does not belong to $\mathbb{N}$.

2. Let $\cdot$ be the multiplication operation defined on the positive integers $\mathbb{N}$. For each $a \in \mathbb{N}$, $a \cdot 1 = a = 1 \cdot a$, which implies that 1 is an identity element for $(\mathbb{N}, \cdot)$. Similarly, 1 is an identity element for $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$.
3. Let $-$ be the subtraction operation defined on the integers $\mathbb{Z}$. The subtraction is a binary operation on $\mathbb{Z}$ (Example 4.1.3 (3)). It can be easily verified that $\mathbb{Z}$ has the zero as a right identity with respect to $-$ but no left identity exists.

Example 4.1.13 Let $*$ be the binary operation defined on $\mathbb{Z}$ by $a * b = ab - a - b$ for each $a, b \in \mathbb{Z}$. (Example 4.1.9). No element in $\mathbb{Z}$ can serve as a left identity, for if e_l is a left identity in $(\mathbb{Z}, *)$, then $b = e_l * b$ for all $b \in \mathbb{Z}$. In particular,

$$1 = e_l * 1 = e_l - e_l - 1 = -1.$$

which contradicts $1 \neq -1$. Since $*$ is a commutative operation, no right identity exists in $(\mathbb{Z}, *)$, and consequently, no identity element exists in $(\mathbb{Z}, *)$.

Example 4.1.14 Let G be a set containing at least two elements. For each $a, b \in G$, define $a * b$ as the element on the left side of $*$, i.e., $a * b = a$. Clearly, $*$ is a function (and thus a binary operation) on G. As $a * (b * c) = a * b = a = a * c = (a * b) * c$ for all $a, b, c \in G$, thus $*$ is an associative operation on G. The operation $*$ is noncommutative, as for any $a \neq b$, $a * b = a \neq b = b * a$. If $c \in G$ is an arbitrary element, then c satisfies $a * c = a \quad \forall\, a \in G$. Therefore, c is a right identity, i.e., any element in G is a right identity. However, the set G has no left identity, since if d is an element in G, such that $x = d * x$ for all $x \in G$, then by the definition of the operation $*$, we have $x = d * x = d$, i.e., $x = d$ for any $x \in G$, and G has only one element.

The above examples demonstrate that the set G may have a left (right) identity or may not. If G has both left and right identities, then they must be equal. If e_l, e_r are left and right identities of G, respectively, then by Definition 4.1.10 (1-2),

$$e_l \underset{e_r \text{ is a right identity}}{=} e_l * e_r \underset{e_l \text{ is a left identity}}{=} e_r .$$

Moreover, if G has the two identity elements $e, e' \in G$, then by Definition 4.1.10 (3),

$$e \underset{e' \text{ is an identity}}{=} e * e' \underset{e \text{ is an identity}}{=} e' .$$

These results are stated in the following lemma and corollary.

Lemma 4.1.15 *Let G be a set and $*$ be a binary operation on G. If G has right and left identities, then they coincide.*

Corollary 4.1.16 (The uniqueness of the identity). *Let G be a set and $*$ be a binary operation on G. An identity of G (if it exists) is unique.*

To emphasize the uniqueness of the identity, if $(G, *)$ has an identity element, we call it the identity element of G, and we use e to denote the identity.

4.2 Semigroups and Monoids

In this section, we define the semigroups and monoids, and we present several examples of both. An important of a semigroup, known by the transformation semigroup is also defined.

Definition 4.2.1

1. A semigroup is a set G equipped with an associative binary operation $*$. If the operation $*$ is commutative, $(G, *)$ is called a commutative semigroup.

2. A monoid is a semigroup $(G, *)$ that contains an identity element. If the operation $*$ is commutative, $(G, *)$ is called a commutative monoid.

Remark 4.2.2 In a semigroup $(G, *)$, changing the operation application order of $*$ on any finite sequence of elements of G (that contains more than two elements) does not change the value of the expression. For example,

$$a_1 * (a_2 * (a_3 * a_4)) = (a_1 * a_2) * (a_3 * a_4) = a_1 * (a_2 * a_3) * a_4$$

for any a_1, a_2, a_3, a_4 elements of G. Note that only the operation application order is changed, whereas the order of the elements themselves remains unchanged. In general, if $a_1, a_2, \dots, a_n$ are elements in a semigroup G, as long as the same order of the elements is maintained, applying the operations in any order yields the same element of G. We usually omit the parentheses between the elements and write $a*b*c$ to denote any of the sides of the equation in Definition 4.1.7 (1).

Notation 4.2.3: Let $n \in \mathbb{N}$, and $(G, *)$ be semigroups and $a_1, a_2, \dots, a_n$ be elements of G. The notation $a_1 * a_2 * \cdots * a_n$ is used to denote the value obtained by applying the operations in any order. If $a_i = a$ for all $1 \leq i \leq n$, we denote $\underbrace{a * a * \cdots * a}_{n \text{ times}}$ by a^n.

Proposition 4.2.4 *Let* $(G, *)$ *be a commutative semigroup. For any bijection map* f *on the finite set* $\{1, 2, \dots, n\}$,

$$a_1 * a_2 * \cdots * a_n = a_{f(1)} * a_{f(2)} * \cdots * a_{f(n)}.$$

i.e., in a commutative semigroup, one can apply the operation in any arbitrary order for the elements.

Proof Let f be any bijection map on $\{1, 2, \dots, n\}$. The map f can be expressed as a composition of adjacent transpositions $\mathcal{R}_{s,s+1}$ for some s where $1 \leq s \leq n-1$ (Proposition 1.5.18). Hence, it suffices to show the assertion for $f = \mathcal{R}_{s,s+1}$, $1 \leq s \leq n-1$, where

$$\mathcal{R}_{s,s+1} : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$$

$$\mathcal{R}_{s,s+1}(k) = \begin{cases} k & k \neq s \wedge k \neq s+1 \\ s+1 & k = s \\ s & k = s+1. \end{cases}$$

If $f = \mathcal{R}_{\mathrm{s,s+1}}$, then

$$\begin{aligned} a_{f(1)} * a_{f(2)} * \cdots * a_{f(n)} &= a_1 * a_2 * \cdots a_{s-1} * a_{s+1} * a_s * \cdots * a_n \\ &= (a_1 * a_2 * \cdots a_{s-1}) * (a_{s+1} * a_s) * (\cdots * a_n) \\ &= (a_1 * a_2 * \cdots a_{s-1}) * (a_s * a_{s+1}) * (\cdots * a_n) \end{aligned}$$

$$= a_1 * a_2 * \cdots a_{s-1} * a_s * a_{s+1} * \cdots * a_n$$
$$= a_1 * a_2 * \ldots * a_n.$$

■

Example 4.2.5

1. Let $+, \cdot$ be the usual addition and multiplication on the integers. Then $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \cdot)$ are commutative semigroups. All these semigroups except $(\mathbb{N}, +)$ are monoids. The zero serves as identity element in $(\mathbb{Z}, +)$, whereas 1 is the identity element in $(\mathbb{N}, \cdot)$, and $(\mathbb{Z}, \cdot)$.
2. Let $+, \cdot$ be the usual sum and multiplication defined on the set of rational numbers. Then $(\mathbb{Q}, +)$ and $(\mathbb{Q}, \cdot)$ are commutative monoids. The zero and 1 serve as identity elements in $(\mathbb{Q}, +)$ and $(\mathbb{Q}, \cdot)$, respectively.
3. Let $+, \cdot$ be the usual sum and multiplication defined on the set of real numbers. Then $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$ are commutative monoids. The zero and 1 serve as identity elements in $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$, respectively.
4. Let $+, \cdot$ be the usual sum and multiplication defined on the set of complex numbers. Then $(\mathbb{C}, +)$ and $(\mathbb{C}, \cdot)$ are commutative monoids. The zero and 1 serve as identity elements in $(\mathbb{C}, +)$ and $(\mathbb{C}, \cdot)$, respectively.
5. Let $-$ be the usual subtraction defined on the set of integers. In this case, $(\mathbb{Z}, -)$ is not a semigroup, and thus not a monoid. The operation $-$ is not associative on $\mathbb{Z}$. For example,

$$(3-2)-1 = 0 \neq 2 = 3-(2-1) \text{ and } 3-2 = 1 \neq -1 = 2-3.$$

6. Let $-$ be the usual subtraction defined on the set of complex numbers. This operation is not associative, thus $(\mathbb{C}, -)$ is not a semigroup and not a monoid. Clearly, the operation $-$ is not commutative on $\mathbb{C}$.
7. Let $m, n \in \mathbb{N}$ and $+$ be the addition operation defined on the matrices $\mathcal{M}_{mn}(\mathbb{C})$. This operation is an associative commutative binary operation on $\mathcal{M}_{mn}(\mathbb{C})$, and thus $(\mathcal{M}_{\mathrm{mn}}(\mathbb{C}), +)$ is a commutative semigroup. Proposition 4.3.14 shows that $(\mathcal{M}_{\mathrm{mn}}(\mathbb{C}), +)$ is a monoid.
8. Let $m, n \in \mathbb{N}$ and let $-$ be the subtraction operation defined on the matrices $\mathcal{M}_{\mathrm{mn}}(\mathbb{C})$. As in the case of addition, one can easily show that the subtraction of matrices is a binary operation on $\mathcal{M}_{mn}(\mathbb{C})$. However, the subtraction is not associative, and hence $\mathcal{M}_{mn}(\mathbb{C})$ is not a semigroup under subtraction. Clearly, this operation is not commutative.
9. Let $n \in \mathbb{N}$, and let $\cdot$ be the matrix multiplication defined on $\mathcal{M}_{\mathrm{n}}(\mathbb{C})$. The matrix multiplication is associative and not a commutative binary operation on $\mathcal{M}_{\mathrm{n}}(\mathbb{C})$. Therefore, $(\mathcal{M}_{\mathrm{n}}(\mathbb{C}), \cdot)$ is a semigroup, that is not commutative. Proposition 4.3.15 shows that $(\mathcal{M}_{\mathrm{n}}(\mathbb{C}), \cdot)$ is a monoid.
10. Consider the empty set $\emptyset$. On $\emptyset$, consider the empty relation $f = \emptyset \subseteq \emptyset \times \emptyset$. As f is a function on $\emptyset$, it is a binary operation and vacuously satisfies the conditions of associativity and commutativity. Therefore, $\emptyset$ is a commutative semigroup. This semigroup is not a monoid as it does not contain an identity element.

Example 4.2.6 Let $*$ be defined on the real numbers $\mathbb{R}$ by

$$a * b = ab/5 \quad a, b \in \mathbb{R}.$$

$(\mathbb{R}, *)$ is a commutative semigroup. To verify this, let a, b be arbitrary elements in $\mathbb{R}$. Clearly, $a * b$ defines a unique element that belongs to $\mathbb{R}$, i.e., the operation $*$ is a binary operation on $\mathbb{R}$. For associativity, let a, c, b be arbitrary elements in $\mathbb{R}$. Since

$$a * (b * c) = a * \left(\frac{bc}{5}\right) = \frac{a(bc)}{25} = \frac{(ab)c}{25} = \left(\frac{ab}{5}\right) * c = (a * b) * c,$$

then $(\mathbb{R}, *)$ is a semigroup. Moreover,

$$a * b = ab/5 = ba/5 = b * a \text{ for any } a, b \in \mathbb{R}.$$

Thus, $*$ is commutative. To check if $(\mathbb{R}, *)$ contains an identity element, assume that e is the identity element in $\mathbb{R}$, i.e., $e * a = a * e = a$ for any element a in $\mathbb{R}$. If $a \neq 0$, then

$$e * a = a \Leftrightarrow \frac{ea}{5} = a \Leftrightarrow \frac{e}{5} = 1 (a \neq 0) \Leftrightarrow e = 5.$$

If $a = 0$, then $5 * 0 = \frac{5 \times 0}{5} = 0$. Therefore, 5 is an element in $\mathbb{R}$ that satisfies $5 * a = a$ for any element a in $\mathbb{R}$. As $*$ is a commutative operation, 5 also satisfies $a * 5 = a$, and $(\mathbb{R}, *)$ is a monoid whose identity element is 5.

Example 4.2.7 Let $*$ and $\bullet$ be the binary operations defined on the positive integers $\mathbb{N}$ by

$$a * b = \gcd(a, b)$$

$$a \bullet b = \operatorname{lcm}(a, b)$$

for all $a, b \in \mathbb{N}$. Both $(\mathbb{N}, *)$ and $(\mathbb{N}, \bullet)$ are examples of commutative semigroups. As both operations are functions on $\mathbb{N}$ (Proposition 2.7.8), they both form binary operations on $\mathbb{N}$. The discussions in Remark 2.3.9 and Remark 2.7.7 demonstrate that both operations are commutative. To show that $*$ is associative, let $a, b, c \in \mathbb{N}$ be arbitrary elements. Apply the result of Exercises 2.8 ($n = 3$) and the commutative property of $*$ to obtaim

$$\begin{aligned} a * (b * c) &= \gcd(a, \gcd(b, c)) = \gcd(\gcd(b, c), a) = \gcd(b, c, a) \\ &= \gcd(a, b, c) = \gcd(\gcd(a, b), c) = (a * b) * c. \end{aligned}$$

Similarly, using the result of Exercise 2.20, the operation $\bullet$ is also associative. Therefore, both $(\mathbb{N}, *)$ and $(\mathbb{N}, \bullet)$ are semigroups. The semigroup $(\mathbb{N}, *)$ has no identity element. For if k is an integer such that $\gcd(a, k) = a$ for all $a \in \mathbb{N}$, then $a|k$ for all $a \in \mathbb{N}$, i.e., $\mathbb{N} \subseteq \operatorname{Div}(k)$. Remark 2.2.6 and Proposition 2.2.4 (1) imply that $k = 0$. Hence, the zero is the only integer satisfying $a * 0 = a$ for any $a \in \mathbb{N}$. Since $0 \notin \mathbb{N}$, then $(\mathbb{N}, *)$ has no identity element. For the operation $\bullet$, as $1 \in \mathbb{N}$ and $a \bullet 1 = \operatorname{lcm}(a, 1) = a$ for each $a \in \mathbb{N}$, then 1 is the identity element in $(\mathbb{N}, \bullet)$, and $(\mathbb{N}, \bullet)$ is a monoid.

Definition 4.2.8 Let A be a nonempty set. The set A^A is defined to be the set of all functions from A to A, i.e., $A^A = \{f : A \to A, f \quad \text{is a function}\}$.

Proposition 4.2.9 *If A is a nonempty set, and $\circ$ is the composition of functions defined on A^A, then $\left(A^A, \circ\right)$ is a monoid. This monoid is noncommutative for any A with more than one element.*

Proof The composition of two functions from A to A is a function from A to A (Exercise 1.21), thus the map

$$\circ : A^A \times A^A \to A^A \quad \text{where}$$

$$f \circ g(x) = f(g(x)) \;\; \forall\, x \in A$$

defines a binary operation on A^A. The operation is associative since

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$$

and

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

The identity map $I_A : A \to A$, where $I_A(x) = x \quad \forall\, x \in A$ is an element in A^A and satisfies

$$I_A \circ f(x) = f \circ I_A(x) = f(x) \;\; \forall\, x \in A \;\text{ and }\; \forall\, f \in A^A.$$

Therefore, I_A serves as an identity element in $\left(A^A, \circ\right)$. If A has only one element, then A^A has only the identity function and composition is commutative. If a and b are two different elements in A, then by defining the functions $f : A \to A$, $f(x) = a$ for all $x \in A$, and $g : A \to A$, $g(x) = b$ for all $x \in A$, one can easily show that $f \circ g(x) = a \neq b = g \circ f(x)$ for all x in A. Thus, the composition is not commutative in this case. ■

The monoid in Proposition 4.2.9 is known by the transformation (composition) semigroup.

4.3 Invertible Elements in Monoids

In this section, we assume that G is a monoid (semigroup with an identity element). We define and study the subset of the invertible elements in G. We observe that each element in this set is paired with another element, called its inverse.

Definition 4.3.1 Let G be a set equipped with a binary operation $*$, and e be an identity element in G. Let $a, b \in G$,

1. b is said to be a left inverse of a if $b * a = e$.
2. b is said to be a right inverse of a if $a * b = e$.
3. b is said to be an inverse of a if b is a left and right inverse of a. i.e., $a * b = b * a = e$.

Remark 4.3.2 If the binary operation $*$ is commutative on G, then the existence of one-sided inverse guarantees the existence of both one-sided inverses. For if b is a left inverse and $*$ is commutative, then $a * b = b * a = e$, which means that b is a right inverse, and thus, an inverse. Likewise for a right inverse.

Let G be a monoid and $a \in G$. If $b_l \in G$ is a left inverse of a, and $b_r \in G$ is a right inverse of a, then by Definition 4.3.1,

$$\begin{aligned} b_l = b_l * e = b_l * (a * b_r) &= (b_l * a) * b_r \\ &= e \cdot b_r = b_r \end{aligned}$$

which means that the left and right inverse (if they both exist) are equal. This leads to the following result.

Lemma 4.3.3 *Let $(G, *)$ be a monoid, and $a \in G$. If a has a left and right inverse in G, then they coincide.*

Corollary 4.3.4 *Let $(G, *)$ be a monoid, and $a \in G$. An inverse element of a (if it exists) is unique. The inverse of a is denoted as a^{-1}.*

Proof Let b, c be two inverses of a in G. According to Definition 4.3.1,

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

■

Let $G = \{a, b, c\}$ and $* : G \times G \to G$ be defined as in Table 4.1. One can easily verify that $*$ is a binary operation on G. The element a is the identity element (Check!). The element b satisfies

$$(b * b) * c = b * c = a \neq b = b * a = b * (b * c),$$

which shows that $(G, *)$ is not a semigroup. This leads the following remark.

Table 4.1 The operation on G

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

Remark 4.3.5 The results in Lemma 4.3.3, and Corollary 4.3.4 are satisfied only if G is a semigroup and are not guaranteed for any binary operation on set G.

Definition 4.3.6 Let $(G, *)$ be a monoid and $a \in G$. The element a is said to be invertible in G if it has an inverse in G, that is, if there exists $b \in G$ such that

$$a * b = b * a = e.$$

where e is the identity element in G. The set of all invertible elements in $(G, *)$ is denoted by $\mathrm{Inv}((G, *))$, or simply, $\mathrm{Inv}(G)$ if the operation $*$ is not ambiguous, i.e.,

$$\begin{aligned}\mathrm{Inv}(G) &= \{a \in G : a \text{ is invertible}\}\\ &= \{a \in G : \exists\, b \in G \ni \mathrm{a} * \mathrm{b} = \mathrm{b} * \mathrm{a} = \mathrm{e}\}.\end{aligned}$$

Note that G^* is used to denote the set of invertible elements in G in some of algebra books. In this book, we use $\mathrm{Inv}(G)$ as mentioned above and reserve the notation K^* to denote $K\backslash\{0\}$, where $K \subseteq \mathbb{C}$.

Proposition 4.3.7 *Let $(G, *)$ be a monoid, and $a, b \in G$ be arbitrary elements in G.*

1. If $a \in G$ is invertible in G, then a^{-1} is invertible in G and $\left(a^{-1}\right)^{-1} = a$.
2. If $a, b \in G$ are invertible in G, then $a * b$ is invertible in G and

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

Proof The first statement follows directly from Definition 4.3.1(3), and

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

For the second statement, assume that a, b are invertible elements in G. The result follows as

$$\left(b^{-1} * a^{-1}\right) * (a * b) = b^{-1} * \left(a^{-1} * a\right) * b = b^{-1} * e * b = b^{-1} * b = e$$

and

$$(a * b) * \left(b^{-1} * a^{-1}\right) = a * \left(b * b^{-1}\right) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

The result in item 2 means that the subset $\mathrm{Inv}(G)$ is closed under $*$. Therefore, the result in Proposition 4.1.6 yields: ■

Corollary 4.3.8 *Let* $(G, *)$ *be a monoid. The set* $\mathrm{Inv}(G)$ *of all invertible elements in* G *forms a monoid with respect to* $*$.

The following generalization of Proposition 4.3.7 can be easily proved using mathematical induction on n.

Proposition 4.3.9 *Let* $(G, *)$ *be a monoid and* $a_1, a_2, \ldots, a_n$ *be invertible elements in* G. *The element* $a_1 * a_2 * \cdots * a_n$ *is invertible in* G *and*

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_1^{-1}.$$

Proposition 4.3.10 *Let* $(G, *)$ *be a monoid and* a *be an invertible element in* G. *The left and right cancellation laws hold for* a, i.e., *for all* b, c *in* G, *the following statements hold*:

1. $b * a = c * a \Rightarrow b = c$.
2. $a * b = a * c \Rightarrow b = c$.

Proof Assume that a is an invertible element in G, and $b * a = c * a$. By multiplying both sides of the equation on the right by a^{-1}, one obtains $(b * a)*a^{-1} = (c * a)*a^{-1}$, which implies that $b = c$. The second part of the proposition is proved in similar manner. ■

Example 4.3.11 Consider the monoid $(\mathbb{Z}, +)$, where $+$ is the addition operation on integers. Every element in $\mathbb{Z}$ is invertible. For if $a \in \mathbb{Z}$, then $-a \in \mathbb{Z}$, satisfies

$$a + (-a) = (-a) + a = 0.$$

Similarly, every element in $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ is invertible. i.e.,

$$\mathrm{Inv}((\mathbb{Z}, +)) = \mathbb{Z},\ \mathrm{Inv}((\mathbb{Q}, +)) = \mathbb{Q},\ \mathrm{Inv}((\mathbb{R}, +)) = \mathbb{R},\ \mathrm{Inv}((\mathbb{C}, +)) = \mathbb{C}.$$

Note that $\mathbb{N}$ has no identity with respect to the sum operation; hence, there is no point to look for invertible elements in $(\mathbb{N}, +)$.

Example 4.3.12

1. In the monoid $(\mathbb{N}, \cdot)$, where $\cdot$ is multiplication of integers, the only invertible element in $(\mathbb{N}, \cdot)$ is 1, i.e., $\mathrm{Inv}((\mathbb{N}, \cdot)) = \{1\}$. The inverse of 1 is itself.
2. In the monoid $(\mathbb{Z}, \cdot)$, where $\cdot$ is multiplication of integers, the invertible elements are 1 and -1, with each being the inverse of itself. If a is an invertible element in $\mathbb{Z}$ with an inverse b, then by Definition 4.3.1, $a \cdot b = 1$. Therefore, $|a \cdot b| = |a| \cdot |b| = 1$, which implies that $|a| = |b| = 1$. Hence, $a \in \{1, -1\}$, and $\mathrm{Inv}((\mathbb{Z}, \cdot)) = \{1, -1\}$.

3. In the monoid $(\mathbb{Q}, \cdot)$, where $\cdot$ is multiplication of rational numbers, any nonzero element in $\mathbb{Q}$ is invertible. If $a \in \mathbb{Q}$ is a nonzero element in $\mathbb{Q}$, then $1/a$ is an element in $\mathbb{Q}$ that satisfies $a \cdot (1/a) = (1/a) \cdot a = 1$. The zero is not invertible. Therefore, $\text{Inv}((\mathbb{Q}, \cdot)) = \mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$.
4. Similar to (3), every nonzero element a in $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ is invertible with an inverse $1/a$, where $\cdot$ is multiplication of real and complex numbers, respectively. i.e., $\text{Inv}((\mathbb{R}, \cdot)) = \mathbb{R}^* = \mathbb{R}\backslash\{0\}$ and $\text{Inv}((\mathbb{C}, \cdot)) = \mathbb{C}^* = \mathbb{C}\backslash\{0\}$.

Example 4.3.13 Let $(\mathbb{R}, *)$ be the monoid defined in Example 4.2.6, i.e.,

$$a * b = \frac{ab}{5}\ a, b \in \mathbb{R}.$$

To find the invertible elements in $\mathbb{R}$, assume that $a \in \mathbb{R}$. Consider the following two cases:

– If $a \neq 0$, then for any b in $\mathbb{R}$,

$$a * b = 5 \Leftrightarrow \frac{ab}{5} = 5 \Leftrightarrow b = \frac{25}{a}.$$

As $25/a \in \mathbb{R}$, the element a has a right inverse in $\mathbb{R}$. The element $25/a \in \mathbb{R}$ is a left inverse ($*$ is commutative). Hence, a is invertible, with $a^{-1} = 25/a$. One can easily check that $a * (25/a) = (25/a) * a = 5$.

– If $a = 0$, then $0 * b = 0 \neq 5$ for all elements b in $\mathbb{R}$. Thus, 0 is not invertible.

Therefore, the set of invertible elements in $(\mathbb{R}, *)$ are $\text{Inv}(\mathbb{R}) = \mathbb{R}^* = \mathbb{R}\backslash\{0\}$.

Proposition 4.3.14 *Let $m, n \in \mathbb{N}$, and let $\mathcal{M}_{mn}(\mathbb{C})$ be the set of all $m \times n$ matrices with complex coefficients. Let $+$ be defined on $\mathcal{M}_{mn}(\mathbb{C})$ as the sum of matrices. The set*

$$(\mathcal{M}_{mn}(\mathbb{C}), +)$$

is a commutative monoid, and every element in $\mathcal{M}_{mn}(\mathbb{C})$ is invertible.

Proof The sum of matrices is a function from $\mathcal{M}_{mn}(\mathbb{C}) \times \mathcal{M}_{mn}(\mathbb{C})$ to $\mathcal{M}_{mn}(\mathbb{C})$ (Proposition 1.6.8), and thus the sum of matrices is a binary operation on $\mathcal{M}_{mn}(\mathbb{C})$. Assume that $A = \left(a_{ij}\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, $B = \left(b_{ij}\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, and $C = \left(c_{ij}\right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ are elements in $\mathcal{M}_{mn}(\mathbb{C})$. According to the definition of $+$,

$$\begin{aligned} A + (B + C) &= \left(a_{ij}\right) + \left(\left(b_{ij}\right) + \left(c_{ij}\right)\right) \\ &= \left(a_{ij}\right) + \left(b_{ij} + c_{ij}\right) = \left(a_{ij} + \left(b_{ij} + c_{ij}\right)\right) \end{aligned}$$

$$\begin{aligned}&=\big((a_{ij}+b_{ij})+c_{ij}\big)=\big(a_{ij}+b_{ij}\big)+\big(c_{ij}\big)\\&=\big(\big(a_{ij}\big)+\big(b_{ij}\big)\big)+\big(c_{ij}\big)=(A+B)+C.\end{aligned}$$

Therefore, $+$ is an associative operation on $\mathcal{M}_{mn}(\mathbb{C})$. For the commutativity,

$$A+B=\big(a_{ij}+b_{ij}\big)=\big(b_{ij}+a_{ij}\big)=B+A$$

is satisfied for all $A, B \in \mathcal{M}_{mn}(\mathbb{C})$. Therefore, $(\mathcal{M}_{mn}(\mathbb{C}), +)$ is a commutative semigroup.

Let $0_{mn} = (0) = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$. The matrix $0_{mn} \in \mathcal{M}_{mn}(\mathbb{C})$, and satisfies that for each $A = \big(a_{ij}\big)$ in $\mathcal{M}_{mn}(\mathbb{C})$,

$$A+0_{mn}=\big(a_{ij}+0\big)=A=\big(0+a_{ij}\big)=0_{mn}+A.$$

Thus, 0_{mn} is the identity element in $(\mathcal{M}_{mn}(\mathbb{C}), +)$.

For any $A = \big(a_{ij}\big) \in \mathcal{M}_{mn}(\mathbb{C})$, let $B = \big(-a_{ij}\big)$. The matrix B is an element of $\mathcal{M}_{mn}(\mathbb{C})$ that satisfies

$$A+B=\big(a_{ij}+\big(-a_{ij}\big)\big)=0_{mn}=\big(-a_{ij}+a_{ij}\big)=B+A.$$

Therefore, B is the inverse of A with respect to $+$. Consequently, every element in $\mathcal{M}_{mn}(\mathbb{C})$ is invertible. ■

For $m, n \in \mathbb{N}$, the multiplication of two matrices in $\mathcal{M}_{mn}(\mathbb{C})$ is not defined unless $m = n$. Recall that we use the notation AB to denote the multiplication $A \cdot B$.

Proposition 4.3.15 Let $n \in \mathbb{N}$, and let $\mathcal{M}_n(\mathbb{C})$ be the set of all $n \times n$ matrices with complex coefficients. Let $\cdot$ be matrix multiplication on $\mathcal{M}_n(\mathbb{C})$. The set

$$(\mathcal{M}_n(\mathbb{C}), \cdot)$$

is a noncommutative monoid, where every matrix in $\mathcal{M}_n(\mathbb{C})$ with a nonzero determinant is invertible.

Proof As the matrix multiplication is a function on $\mathcal{M}_n(\mathbb{C})$ (Proposition 1.6.8), it is a binary operation on $\mathcal{M}_n(\mathbb{C})$. To show that $\cdot$ is an associative operation, let $A_1 = \big(a^1_{ij}\big)$, $A_2 = \big(a^2_{ij}\big)$, and $A_3 = \big(a^3_{ij}\big)$ be matrices in $\mathcal{M}_n(\mathbb{C})$, where $1 \leq i, j \leq n$. According to the definition of matrix multiplication (Definition 1.6.6),

$$A_1A_2=\big(c_{ij}\big)\text{where } c_{ij}=\sum_{l=1}^{n}a^1_{il}a^2_{lj}$$

$$A_2A_3 = \big(d_{ij}\big)\text{where } d_{ij} = \sum_{k=1}^{n} a^2_{ik}a^3_{kj}.$$

Hence,

$$\begin{aligned} A_1(A_2A_3) = A_1\big(d_{ij}\big) &= \sum_{l=1}^{n} a^1_{il}d_{lj} = \sum_{l=1}^{n} a^1_{il}\sum_{k=1}^{n} a^2_{lk}a^3_{kj} \\ &= \sum_{l=1}^{n}\sum_{k=1}^{n} a^1_{il}(a^2_{lk}a^3_{kj}) = \sum_{k=1}^{n}\sum_{l=1}^{n}(a^1_{il}a^2_{lk})a^3_{kj} \\ &= \sum_{k=1}^{n} c_{ik}a^3_{kj} = \big(c_{ij}\big)A_3 = (A_1A_2)A_3. \end{aligned}$$

Thus, matrix multiplication is an associative operation, and $(\mathcal{M}_n(\mathbb{C}), \cdot)$ is a semigroup.

Let $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$. The matrix I_n is an element in $\mathcal{M}_n(\mathbb{C})$. For each $A = \big(a_{ij}\big) \in \mathcal{M}_n(\mathbb{C})$, the multiplication $I_nA = \big(c_{ij}\big)$, where

$$c_{ij} = \sum_{l=1}^{n} I_{il}a_{lj} = 0 + \ldots + 0 + I_{ii}a_{ij} + 0 + \ldots + 0 = 1 \cdot a_{ij} = a_{ij} \quad \forall\ 1 \le i, j \le n,$$

i.e., $I_nA = A$. Similarly, $AI_n = A$. Therefore, I_n is the identity element in $\mathcal{M}_n(\mathbb{C})$ with respect to matrix multiplication. The last statement in the proposition is a restated form of the first part of Proposition 1.6.28, i.e.,

$$\text{Inv}((\mathcal{M}_n(\mathbb{C}), \cdot)) = \{A \in \mathcal{M}_n(\mathbb{C}) : det(A) \ne 0\}.$$

Finally, let

$$A_1 = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Both A_1, A_2 are elements in $\mathcal{M}_n(\mathbb{C})$, and $A_1A_2 = A_2 \ne A_1 = A_2A_1$. Thus, matrix multiplication is not commutative. ■

Example 4.3.16 Let $G = \{A, \mathrm{B}, \mathrm{C}\} \subseteq \mathcal{M}_2(\mathbb{C})$, where

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \text{ and } C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Let $\cdot$ be matrix multiplication on $\mathcal{M}_2(\mathbb{C})$. Since

$$AX = X, BX = C, CX = C \quad \forall\, X \in G,$$

then G is closed under matrix multiplication, rendering $\cdot$ a binary operation on G (Proposition 4.1.6). The subset G inherits the associativity property from $(\mathcal{M}_2(\mathbb{C}), \cdot)$. Therefore, $(G, \cdot)$ is a semigroup. Since for each $X \in G$, $AX = X$, then A is a left identity of G. Since $BX = C \neq B$ for all $X \in G$, the semigroup G has no right identity. We do not discuss the invertible elements, as there is no identity element in G.

4.4 Idempotent Elements in Semigroups

As in the previous section, a special subset of the semigroup G, called the set of idempotents of G, is considered in this section.

Definition 4.4.1 Let $(G, *)$ be a semigroup. The element $a \in G$ is called idempotent if $a^2 = a$. The set of idempotent elements of G is denoted by $E(G)$.

Example 4.4.2

1. The identity element in any semigroup (if it exists) is idempotent.
2. Zero is the only idempotent element in $(K, +)$, where $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.
3. The integers $0, 1$ are the only idempotent elements in $(K, \cdot)$, where $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.
4. In $(M_2(\mathbb{C}), \cdot)$, the matrices $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ are examples of idempotent elements.
5. On the closed interval $I = [0, 1]$, define $x * y = \min(x, y)$, where $x, y \in I$. Clearly, $(I, *)$ is a semigroup with an identity equal to 1. For all $x \in I$,

$$x^2 = x * x = \min(x, x) = x.$$

Therefore, all elements in $(I, *)$ are idempotents.

6. Let G be any nonempty set. Define $*$ on G by $a * b = a$. Any element in G is an idempotent element, i.e., $E(G) = G$.

Proposition 4.4.3 *Let $(G, *)$ be a semigroup, and $a, b \in G$ such that $a * b = b * a$. If a, b are idempotent elements, then $a * b$ is idempotent.*

Proof If a and b are idempotent elements in G, then

$$\begin{aligned}(a*b)^2 = (a*b)*(a*b) = a*(b*a)*b = a*(a*b)*b \\ = (a*a)*(b*b) = a^2*b^2 = a*b.\end{aligned}$$

■

Corollary 4.4.4 *If $(G, *)$ is a commutative semigroup, then the set of all idempotent elements in G forms a semigroup with respect to $*$.*

Proposition 4.4.5 *Let $(G, *)$ be a monoid. The identity is an idempotent, and any other idempotent element in G is not invertible.*

Proof Let e be the identity element in G. As $e*e = e$, then e is idempotent. Assume that a is an idempotent and invertible element in G. If b is the inverse element of a, then

$$a = a*e = a*(a*b) = (a*a)*b = a*b = e.$$

Thus, there is no idempotent invertible element other than e. ■

Exercises

Solved Exercises

4.1 Let $G = \{1, 2, 3, 4, 5\}$. Determine which of the following formulas define a binary operation on G. For those that do, determine whether the operation is associative or commutative.

1. $a*b = a+b \quad \forall\, a, b \in G$
2. $a*b = 5 \quad \forall\, a, b \in G$
3. $a*b = b-1 \quad \forall\, a, b \in G$
4. $a*b = \begin{cases} 1 & if\ a, b \text{ are odd} \\ 4 & \text{if } a, b \text{ are even} \\ 5 & \text{if otherwise.} \end{cases}$

Solution:

1. As $5*4 = 5+4 = 9 \notin G$, the operation $*$ is not a binary operation on G.
2. If $a, b \in G$, then $a*b = 5$ is defined and belongs to G. Therefore, $*$ is a binary operation on G. For any $a, b, c \in G$,

$$(a*b)*c = 5*c = 5 = a*5 = a*(b*c).$$

Hence, $*$ is associative. Furthermore, for any $a, b \in G$, $a*b = 5 = b*a$, and $*$ is commutative.

3. As $2 * 1 = 1 - 1 = 0 \notin G$, the operation $*$ is not a binary operation on G.
4. Let $a, b \in G$, then $a * b$ is defined and belongs to G. Hence, $*$ defines a binary operation on G. Clearly, $*$ is commutative. Since

$$1 * (1 * 2) = 1 \neq 5 = (1 * 1) * 2,$$

then $*$ is not associative.

4.2 Let P be a set of prime numbers and B_p be the set of positive integers that can be written as a product of elements of P, i.e.,

$$B_P = \{n \in \mathbb{N} : \exists\ p_1, ..., p_s \in \mathrm{P} \ni\ n = p_1 \cdots p_s\}.$$

Show that multiplication of integers forms a binary operation on B_P. Is addition a binary operation on B_P?

Solution:

As $B_P \subseteq \mathbb{N}$, then by Proposition 4.1.6, it suffices to show that $\mathrm{B_P}$ is closed under the multiplication $\bullet$. Let $n_1 = p_1 \cdots p_s$ and $n_2 = q_1 \cdots q_r$ be the elements in $\mathrm{B_P}$, then

$$n_1 \bullet n_2 = p_1 \cdots p_s \cdot q_1 \cdots q_r$$

is a product of elements of P, i.e., $n_1 \bullet n_2 \in B_P$. For the sum operation $+$, the sum

$$n_1 + n_2 = p_1 \cdots p_s + q_1 \cdots q_r$$

is not necessarily an element of B_P. For example, if $P = \{2, 3\}$, then $2, 3 \in B_P$, but $2 + 3 = 5 \notin B_P$. Therefore, B_P is not closed under $+$. Note that, due to Theorem 2.8.7, B_P will be closed under $+$ if P is the set of all primes. Indeed, this is the only case where B_P will be closed.

4.3 On the set of complex numbers $\mathbb{C}$, define the operation $*$ by $a * b = a + b - ab$.

- Does $*$ define a binary operation on $\mathbb{C}$?
- Is $(\mathbb{C}, *)$ a semigroup? Is $(\mathbb{C}, *)$ commutative?
- Does $(\mathbb{C}, *)$ have an identity element with respect to $*$? If yes, find the invertible elements.
- Find the solutions of $7 * b = i$ and $a * a = -1$ in $(\mathbb{C}, *)$.

Solution:

- For each $a, b \in \mathbb{C}$, the image $a * b$ defines a unique element in $\mathbb{C}$. Therefore, $*$ is a binary operation on $\mathbb{C}$.
- For each $a, b, c \in \mathbb{C}$,

–

$$\begin{aligned} a*(b*c) &= a*(b+c-bc) \\ &= a+(b+c-bc)-a(b+c-bc) \\ &= a+b+c-bc-ab-ac+abc \\ &= a+b-ab+c-ac-bc+abc \\ &= (a+b-ab)+c-(a+b-ab)c \\ &= (a+b-ab)*c = (a*b)*c \end{aligned}$$

i.e., the operation $*$ is associative and $(\mathbb{C}, *)$ forms a semigroup.
For each $a, b \in \mathbb{C}$,
$a*b = a+b-ab = b+a-ba = b*a$.
Therefore, the operation $*$ is commutative and $(\mathbb{C}, *)$ is a commutative semigroup.

- To determine if an identity element exist, let $e \in \mathbb{C}$, such that

$$a*e = a \quad \forall\, a \in \mathbb{C}.$$

Since $a+e-ae = a \quad \forall\, a \in \mathbb{C}$ if and only if $e(1-a) = 0 \quad \forall\, a \in \mathbb{C}$, then e must be 0. ($1-a = 0$ does not hold for each element a in $\mathbb{C}$). We verify that 0 is an identity element as follows:

$a*0 = a+0-a\cdot 0 = a$, and $0*a = 0+a-0\cdot a = a$ for each $a \in \mathbb{C}$.

To determine the invertible elements in $\mathbb{C}$, it is enough to find the elements that have a left inverse (as $*$ is commutative). The element $a \in \mathbb{C}$ has a left inverse if and only if there exists $b \in \mathbb{C}$, such that $b*a = b+a-ba = 0$, i.e., $b = \frac{-a}{1-a}$. The element b is defined for any a in $\mathbb{C}$, such that $a \neq 1$ (verify that b is a left inverse of $a \neq 1$). If $a = 1$, then $b*1 = 1 \neq 0 \quad \forall\, b \in \mathbb{R}$. Therefore, $a = 1$ is not invertible and the invertible elements in $\mathbb{C}$ are $\mathbb{C}\backslash\{1\}$.

- If $7*b = i$, then $7+b-7b = i$, which yields $b = (7-i)/6$.
- If $a*a = -1$, then $a+a-a^2 = -1$, which implies that $a^2-2a-1 = 0$, i.e., $a = 1 \pm \sqrt{2}$.

4.4 Let $n \in \mathbb{N}$. Consider the semigroup $(\mathcal{M}_n(\mathbb{C}), \cdot)$ and let

$$G = \left\{ \left(a_{ij}\right) \in \mathcal{M}_n(\mathbb{C}) : a_{1j} = 0 \quad \forall\, 1 \leq j \leq n \right\}$$

be the subset of all matrices in $\mathcal{M}_n(\mathbb{C})$, whose first row consists of zeros.

1. Show that $(G, \cdot)$ is a semigroup.
2. Find the left (right) identity, if it exists.
3. Find the invertible elements in G, if any.

Solution:

1. If $A = \left(a_{ij}\right)$ and $B = \left(b_{ij}\right)$ are arbitrary elements in G, then $a_{1j} = b_{1j} = 0$ for all $1 \leq j \leq n$. Therefore, $AB = \left(c_{ij}\right)$ where $c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}$ and

$$c_{1j} = \sum_{l=1}^{n} a_{1l}b_{lj} = \sum_{l=1}^{n} 0 \cdot b_{lj} = 0 \quad \forall 1 \leq j \leq n.$$

Therefore, $AB \in G$ and G is closed under $\cdot$. According to Proposition 4.1.6, the operation $\cdot$ is a binary operation in G. Since $(G, \cdot)$ inherits the associativity property from $(\mathcal{M}_n(\mathbb{C}), \cdot)$, it is a semigroup.

2. Let $E_l = \left(d_{ij}.\right)$ where $d_{ij} = \begin{cases} 0 & i \neq j \\ 0 & i = j, i = 1 \\ 1 & i = j, i \neq 1 \end{cases}$ The matrix E_l is an element in G, that satisfies that for each $A = \left(a_{ij}\right)$ in G, the multiplication $E_l A = \left(c_{ij}\right)$, where

$$c_{ij} = \sum_{k=1}^{n} d_{ik}a_{kj} = 0 + \cdots + 0 + d_{ii}a_{ij} + 0 + \cdots + 0 = \begin{cases} 0 & i = 1 \\ a_{ij} & i \neq 1 \end{cases} = a_{ij}.$$

Therefore, E_l is a left identity for G. To show that the semigroup G has no right identity, let

$$A = \left(a_{ij}\right), \text{ where } a_{ij} = \begin{cases} 1 \text{ if } i = 2, j = 1 \\ 0 \text{ otherwise.} \end{cases}$$

A is an element in G. For any matrix $B = \left(b_{ij}\right)$ in G, $AB = \left(c_{ij}\right)$, where

$$c_{ij} = \sum_{l=1}^{n} a_{il}b_{lj} \underbrace{=}_{b_{1j=0}} \sum_{l=2}^{n} a_{il}b_{lj} \underbrace{=}_{a_{il}=0 \forall\ l \geq 2} 0.$$

Therefore, $AB = 0_n \neq A$, and B is not a right identity element of G.

3. Since G does not have an identity element, the notion of invertibility does not apply.

4.5 Consider the set $S = \{a, b, c\}$. Let Δ be the function defined on S by Table 4.2 (Sect. 1.5).

i. Is (S, Δ) a semigroup? Does (S, Δ) have an identity?
ii. Is (S, Δ) commuative?
iii. Does (S, Δ) have idempotent elements?

Table 4.2 The operation on S

Δ	a	b	c
a	a	a	a
b	a	b	b
c	a	b	c

iv. Find the invertible elements in S, if possible.

Solution:

i. Clearly, Δ is a binary operation on S. For each x, y, z in S, we have

$$x\Delta(y\Delta z) = (x\Delta y)\Delta z.$$

In fact, if any of x, y, z is a, the result of both side of the equation above is a. Otherwise, (x, y, z are all in $\{b, c\}$) if one of them is b, the result is b. That leaves only the case $x = y = z = c$, and the result is c in that case, and Δ is associative.

Since $a\Delta c = c\Delta a = a$, $b\Delta c = c\Delta b = b$, and $c\Delta c = c$, then c is an identity element in S. Therefore, (S, Δ) is a semigroup whose identity is c.

ii. From the table, clearly $x\Delta y = y\Delta x$ for any $x, y \in S$.
iii. As $a^2 = a$, $b^2 = b$, and $c^2 = c$, every element in S is idempotent.
iv. According to (iii) and Proposition 4.4.5, $\text{Inv}(S) = \{c\}$.

4.6 Let $(G, *)$ be a commutative semigroup, and $E(G)$ be the subset of all idempotent elements of G. Show that $E(G)$ is a semigroup. If G is a monoid, then $E(G)$ is a monoid.

Solution:

If $E(G) = \emptyset$, then it is a semigroup. Assume that $E(G)$ is not empty, and let a, b be elements in $E(G)$. As $a * b = b * a$, then by Proposition 4.4.3, $a * b \in E(G)$, i.e., $E(G)$ is closed under $*$. According to Proposition 4.1.8, $E(G)$ is a semigroup. If there exists an identity element e in G, then $e * e = e$ belongs to $E(G)$, i.e., $E(G)$ is also a monoid.

4.7 An element a in a semigroup $(G, *)$ is called cancellative if

$$a * b = a * c \Rightarrow b = c \quad \text{and} \quad b * a = c * a \Rightarrow b = c \quad \text{for all } b, c \text{ in } G.$$

The semigroup $(G, *)$ is called cancellative if every element in G is cancellative. Show that if a cancellative semigroup $(G, *)$ has an identity element e, then e is the only idempotent in G, i.e.,$E(G) = \{e\}$.

Solution:

Assume that $(G, *)$ is a cancellative semigroup and let a be an idempotent element in G. According to the definition of $E(G)$, $a^2 = a * a = a = a * e$. By the cancellative property of a, we obtain $a = e$.

Unsolved Exercises

4.8 Determine whether the operation defined on the set A is a binary operation. Explain your answer, where

1. A is the set of negative integers, and $*$ is the subtraction of integers.

2. A is the set of rational numbers $\mathbb{Q}$, and $*$ is the subtraction of rational numbers.

4.9 Let $x, y \in \mathbb{Z}$. Let $*$ be an operation defined on $\mathbb{R}$ by
$a * b = xa + yb$ for all $a, b \in \mathbb{R}$.

- Show that $*$ is associative if and only if $x, y \in \{0, 1\}$.
- Show that $*$ is commutative if and only if $x = y$.

4.10 Let $*$ be the operation defined on the complex numbers $\mathbb{C}$ as follows:

$$a * b = ab + \big(a^2 - 1\big)\big(b^2 - 1\big) \ \ \forall\, a, b \in \mathbb{C}.$$

Show that the operation $*$ is a binary operation that is not associative. Is the operation $*$ commutative? Does $\mathbb{C}$ contain an identity element? Find the invertible elements if any. Is the inverse unique in this case.

4.11 Let G be a nonempty set. Define $*$ on the elements of G by

$$a * b = b \ \ \forall\, a, b \in G.$$

Show that $*$ is a binary operation on G, any element in G is a left identity, and if G has more than one element, then G has no right identity.

4.12 Let $i = \sqrt{-1}$, and consider $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Show that the set $\mathbb{Z}[i]$ is a semigroup under multiplication and has an identity element. Find the invertible elements in $\mathbb{Z}[i]$ if any exist. This semigroup is called "Gaussian integers".

4.13 Let $n \in \mathbb{N}$. Consider the semigroup $(\mathcal{M}_n(\mathbb{C}), \cdot)$, and let $G \subseteq \mathcal{M}_n(\mathbb{C})$ be the subset of all matrices whose first column consist of zeros, i.e.,

$$G = \big\{\big(a_{ij}\big) \in \mathcal{M}_n(\mathbb{C}) : a_{i1} = 0 \ \ \forall\, 1 \le i \le n\big\}.$$

Show that $\cdot$ is a binary operation on G. Show that G has a right identity, but has no left identity.

4.14 Determine whether the given operation on G is a binary, associative, or commutative operation. Does G contain an identity element? Find the invertible elements if any exist.

- $G = \mathbb{Q}$, and $*$ is defined by $a * b = ab + 1 \ \ \forall\, a, b \in \mathbb{Q}$.
- $G = \mathbb{N}$, and $*$ is defined by $a * b = \max(a, b) \ \ \forall\, a, b \in \mathbb{N}$.
- $G = \mathbb{N}$, and $*$ is defined by $a * b = \min(a, b) \ \ \forall\, a, b \in \mathbb{N}$.

4.15 Let A be a nonempty subset of $\mathbb{R}$, and $* : A \times A \to \mathbb{R}$ be the operation defined as follows:

$$a * b = ab + a - b \quad \forall\, a, b \in A.$$

a. Let $A = \mathbb{N}$. Does $*$ define a binary operation on A? What would the answer be if A is replaced by $\mathbb{N} \cup \{0\}$, $\mathbb{Z}$, or $\mathbb{R}$?

Table 4.3 The operation on A

Δ	a	b	c
a	a	a	a
b	a	b	c
c	a	b	c

b. In any of the above cases, if $*$ is a binary operation, check whether it is associative or commutative. Does A contain an identity element? Find the invertible elements if any.

4.16 Let $n \in \mathbb{N}$. Consider the semigroup $(\mathcal{M}_n(\mathbb{C}), +)$. Let $L(\mathbb{C})$ be the subset of all lower triangular matrices in $\mathcal{M}_n(\mathbb{C})$ (Definition 1.6.3). Does $+$ define a binary operation on $L(\mathbb{C})$? Is it associative? Is $+$ commutative? Does L($\mathbb{C}$) contain an identity element? Find the invertible elements if any exist.

4.17 Repeat your answer for Question 4.16 after replacing the matrix addition by matrix multiplication.

4.18 Consider the set $A = \{a, b, c\}$ and the operation Δ defined on A, as shown in Table 4.3.

– Is (A, Δ) a monoid? Is (A, Δ) commuative?

– If A has an identity, list all invertible elements in A if there are any.
Does (A, Δ) have idempotent elements?

Chapter 5
Groups

Groups play an important role in many branches of mathematics and physics. The remainder of the book is devoted to the study of groups and their properties. This chapter contains the basic definitions and background results regarding groups. The first section presents the definition of a group, several basic results, and examples of groups. Section 5.2 is a short section devoted to the definition and examples of Cayley's tables for finite groups. Section 5.3 presents two important examples of groups, the additive and multiplicative groups of integers modulo n. The underlying set of both these groups is the integers modulo n, which was introduced in Chap. 3. Section 5.4 discusses abelian groups and defines the center of the group. A group G will be abelian if and only if it is equal to its center. The results in Sect. 5.5 are about the orders of elements of a given group and its relation to the order of the group. Section 5.6 presents a systemic method to construct a new group from given groups. However, the presented method is not the only approach and Chap. 7 also describes other methods to form a group from old ones. The section ends by defining the group exponent, which is needed in Chap. 9.

5.1 Definition and Basic Examples

In this section, we provide that basic definitions and examples that are needed for the remainder of this book.

Definition 5.1.1 A monoid in which all elements are invertible is called a group.

That is, a monoid $(G, *)$ is a group if and only if $\text{Inv}((G, *)) = G$.

When the operation $*$ is clear from context, and there is no risk of ambiguity, we say that G is a group instead of $(G, *)$. As the empty set $\emptyset$ does not contain an identity element, it cannot form a group. Let G be a nonempty set endowed with a binary operation $*$. The following statements must be verified to confirm that $(G, *)$ is a group.

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_5

1. $a * (b * c) = (a * b) * c \; \forall a, b, c \in G$.
2. There exists $e \in G$ such that $e * a = a * e = a \quad \forall\, a \in G$.
3. For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Since any group is a monoid and therefore a semigroup, all the results of semigroups and monoids (Chap. 4) is applied to groups. The following proposition restates Corollaries 4.1.16, 4.3.4, and Propositions 4.3.7, 4.3.10, and 4.4.5 for the case of groups.

Proposition 5.1.2 *Let $(G, *)$ be a group.*

1. *The identity element of G is unique.*
2. *The inverse of any element in G is unique, and*

$$(a^{-1})^{-1} = a \quad \text{for all} \;\; a \in G, \qquad (a * b)^{-1} = b^{-1} * a^{-1} \;\; \text{for all} \;\; a, b \in G.$$

3. *The identity element is the only idempotent element in G.*
4. *The left and the right cancellation laws hold in G.*

Proposition 5.1.3 *Let $(G, *)$ be a group. For any $a, b \in G$,*

1. *the equation $x * a = b$ has a unique solution in G, given by $x = b * a^{-1}$.*
2. *the equation $a * x = b$ has a unique solution in G, given by $x = a^{-1} * b$.*

Proof If $a, b \in G$ are arbitrary elements, then $b*a^{-1}$ is an element of G that satisfies

$$\left(b * a^{-1}\right) * a = b * \left(a^{-1} * a\right) = b * e = b.$$

Therefore, $b*a^{-1}$ is a solution for $x*a = b$. To show that this is the only solution, assume that y is an element in G such that $y * a = b$, then

$$y = y * e = y * \left(a * a^{-1}\right) = (y * a) * a^{-1} = b * a^{-1}.$$

The proof of the second statement is similar. ■

Example 5.1.4

1. Consider the commutative semigroups $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ (Example 4.2.5 (1)). The semigroup $(\mathbb{N}, +)$ is not a monoid. The semigroup $(\mathbb{N}, \cdot)$ is a monoid, where 1 is the only invertible element in $(\mathbb{N}, \cdot)$. Therefore, either $(\mathbb{N}, +)$ or $(\mathbb{N}, \cdot)$ forms a group.
2. Consider the monoid $(\mathbb{Z}, +)$. As $\text{Inv}((\mathbb{Z}, +)) = \mathbb{Z}$ (Example 4.3.11), $\mathbb{Z}$ is a group under addition. As $+$ is commutative, then $(\mathbb{Z}, +)$ is a commutative group. Similarly, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ form groups.
3. Consider the monoid $(\mathbb{Z}, \cdot)$ (Example 4.3.12). Since $\text{Inv}((\mathbb{Z}, \cdot)) = \{1, -1\} \neq \mathbb{Z}$, thus $\mathbb{Z}$ is not a group under multiplication. Since $\text{Inv}((\mathbb{Q}, \cdot)) = \mathbb{Q}^* \neq \mathbb{Q}$, the rational numbers do not form a group under multiplication since zero has no multiplicative inverse. Similarly, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are not groups.

4. Consider the semigroups $(\mathbb{N}, *)$ and $(\mathbb{N}, \cdot)$ defined in Example 4.2.7 as

$$a * b = \gcd(a, b),\ a \cdot b = \text{lcm}(a, b) \text{ for any } a, b \in \mathbb{N}.$$

Since the semigroup $(\mathbb{N}, *)$ has no identity element, then it is not a group. The monoid $(\mathbb{N}, \cdot)$ has an identity which equals 1. However if $a, b \in \mathbb{N}$ such that $\text{lcm}(a, b) = 1$, then $a = b = 1$, which implies that 1 is the only invertible element in $(\mathbb{N}, \cdot)$. Hence, $(\mathbb{N}, \cdot)$ is not a group.

5. Let $m, n \in \mathbb{N}$, and $\mathcal{M}_{mn}(\mathbb{C})$ be the set of all $m \times n$ matrices with complex coefficients. Consider $+$, the sum of matrices on $\mathcal{M}_{mn}(\mathbb{C})$, the monoid $(\mathcal{M}_{mn}(\mathbb{C}), +)$ is a group (Proposition 4.3.14).

6. Let $n \in \mathbb{N}$, and consider the semigroup $(\mathcal{M}_n(\mathbb{C}), \cdot)$. According to Proposition 4.3.15, $(\mathcal{M}_n(\mathbb{C}), \cdot)$ is a noncommutative monoid (semigroup with an identity element I_n). However, the zero matrix 0_n has no inverse ($0_n \cdot A = 0_n \neq I_n$ for any $A \in \mathcal{M}_n(\mathbb{C})$). Therefore, $(\mathcal{M}_n(\mathbb{C}), \cdot)$ is not a group. Another noninvertible element in $\mathcal{M}_n(\mathbb{C})$ is the matrix $E_{11} = \left(a_{ij}\right)$ with $a_{11} = 1$ and $a_{ij} = 0$ for all $i \neq 1 \vee j \neq 1$. Since the matrix $E_{11} \in \mathcal{M}_n(\mathbb{C})$ is an idempotent element different than the identity element I_n, it is not invertible (Proposition 4.4.5).

7. Let $n \in \mathbb{N}$, such that $n \geq 3$. Consider the regular n-polygon with the center at the origin and one of its vertices at $(1, 0)$. Let D_{2n} be the set of all symmetries of the regular n-polygon. As explained in Summary 1.7.11, D_{2n} consists of all the rotations by the angles $0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2(n-1)\pi}{n}$, and the reflections around the lines passing through the origin and making angles $0, \frac{\pi}{n}, \frac{2\pi}{n}, \ldots, \frac{(n-1)\pi}{n}$ with the x-axis. i.e.,

$$D_{2n} = \left\{R_0, R_{\frac{2\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}, l_o, l_{\frac{\pi}{n}}, l_{\frac{2\pi}{n}}, \ldots, l_{\frac{(n-1)\pi}{n}}\right\}.$$

The set D_{2n} is a nonempty subset that is closed under the composition (Proposition 1.7.7). The rotation by the zero angle serves as an identity element in D_{2n}. Using the results of Proposition 1.7.7, we obtain that the inverse of a rotation by angle $\frac{2k\pi}{n}$ is the rotation by angle $\frac{2(n-k)\pi}{n}$ for any $1 \leq k \leq n$, and the inverse of any reflection around a line is its own inverse (Check!). So, any element in D_{2n} has an inverse in D_{2n}. Therefore, the set D_{2n} forms a group under the composition. The group $(D_{2n}, \circ)$ of all symmetries for the regular n-polygon is called the *dihedral group*.

Example 5.1.5 Let X be any set and $G = \mathcal{P}(X)$ be the power set of X. On the elements of G, define Δ to be the symmetric difference of two sets. i.e.,

$$A \Delta B = (A \backslash B) \cup (B \backslash A) \text{ for all } A, B \in G.$$

Clearly the operation $\Delta : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ is a binary operation on G. By Proposition 1.1.11 (8), the operation Δ is an associative operation on G. For all $A \in G$, $A \Delta \emptyset = A = \emptyset \Delta A$, thus $\emptyset$ is an identity element in G with respect to Δ. For any $A \in G$, $A \Delta A = \emptyset$, and thus, every element in G is invertible and equals to its inverse. Therefore, (G, Δ) is a group. Note that by Proposition 1.1.11 (7), the operation Δ is commutative.

The following proposition provides a method to obtain a group from a given monoid.

Proposition 5.1.6 *Let* $(G, *)$ *be a monoid with identity* e. Let $f : G \to G$ *be a function such that*

1. $f(e) = e$
2. $f(f(a)) = a$ for all $a \in G$
3. $f(a * b) = f(b) * f(a)$ for all $a, b \in G$

The subset $G_f = \{a \in G : a * f(a) = f(a) * a = e\}$ *forms a group under the operation* $*$.

Proof As $e \in G$ and $e * f(e) = e = f(e) * e$, then G_f is a nonempty subset of G that is closed under the operation $*$, because for $a, b \in G_f$,

$$\begin{aligned}(a * b) * f(a * b) &= (a * b) * (f(b) * f(a)) = a * (b * f(b)) * f(a)\\ &= a * e * f(a) = a * f(a) = e.\end{aligned}$$

Using a similar argument, we obtain $f(a * b) * (a * b) = e$. Hence, $*$ is a binary operation on G_f (Proposition 4.1.6). The subset G_f inherits the associativity property from G, and e serves as an identity element for G_f. For any $a \in G_f$, let $b = f(a)$. The element $b = f(a) \in G$ and satisfies

$$\begin{aligned}&b * f(b) \underset{b=f(a)}{=} f(a) * f(f(a)) \underset{f(f(a))=a}{=} f(a) * a \underset{a \in G_f}{=} e, \text{ and}\\ &f(b) * b = f(f(a)) * f(a) = a * f(a) = e,\end{aligned}$$

which implies that $b \in G_f$. As b satisfies

$$a * b = a * f(a) = e = f(a) * a = b * a,$$

then b is the inverse of a in G_f. ■

Corollary 5.1.7 *Let* $(G, *)$ *be a monoid. The subset* $\mathrm{Inv}(G)$ *of all invertible elements in* G *forms a group under the same operation* $*$.

Proof According to Corollary 4.3.8, $\mathrm{Inv}(G) = \{a \in G : a \text{ is invertible in } G\}$ is a semigroup that contains the identity element e as e is invertible, and thus, $\mathrm{Inv}(G)$ is a monoid. The result follows by applying Proposition 5.1.6 on $\mathrm{Inv}(G)$ with f being the inverse map ($f : \mathrm{Inv}(G) \to \mathrm{Inv}(G)$ taking $a \to a^{-1}$). ■

Example 5.1.8

1. Let $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}, \cdot)$, and $(\mathbb{R}, \cdot)$ be the monoids defined in Example 4.2.5. According to the corollary above,

$$\text{Inv}(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \quad \text{Inv}(\mathbb{Z}) = \{1, -1\}, \text{ and } \text{Inv}(\mathbb{R}) = \mathbb{R}^* = \mathbb{R}\backslash\{0\}$$

   are groups under multiplication.

2. Let $n \in \mathbb{N}$, and $(\mathcal{M}_n(\mathbb{C}), \cdot)$ be the semigroup consisting of all $n \times n$ matrices with complex coefficients (Proposition 4.3.15). The set

$$\text{Inv}(\mathcal{M}_n(\mathbb{C})) = \{A \in (\mathcal{M}_n(\mathbb{C}) : \det(A) \neq 0\}$$

   forms a group under matrix multiplication, called the general linear group, denoted by $GL_n(\mathbb{C})$.

3. The set of real positive numbers $\left(\mathbb{R}^+, \cdot\right)$, endowed with the usual multiplication of real number, forms a group (Check!).

Example 5.1.9 Let $n \in \mathbb{N}$, and consider the monoid $(\mathcal{M}_n(\mathbb{R}), \cdot)$ (Proposition 4.3.15). On $\mathcal{M}_n(\mathbb{R})$, define the transpose function $\mathrm{T} : \mathcal{M}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R})$ that takes A to A^{T}, the transpose of A (Definition 1.6.13). As T satisfies the conditions of Proposition 5.1.6, the subset

$$\left\{A \in \mathcal{M}_n(\mathbb{R}) : A^{\mathrm{T}}A = AA^{\mathrm{T}} = I_n\right\}$$

forms a group under matrix multiplication, which plays a key role in many applications of group theory. This group is called the orthogonal group of order n, denoted by $O(n)$. The identity element of $O(n)$ is I_n, and the inverse of any matrix A in the group $O(n)$ is its transpose A^{T}, which can be easily computed.

Proposition 5.1.10 *Let A be a nonempty set, and $A^A = \{f : f : A \to A\}$ be the set of all functions on A. On A^A define the operation $\circ$ to be the composition of maps. i.e.,*

$$f \circ g(x) = f(g(x)) \quad \forall\, f, g \in A^A \;\wedge\; \forall\, x \in A.$$

In this case, $\left(A^A, \circ\right)$ is a noncommutative monoid. The monoid $\left(A^A, \circ\right)$ is not a group if A has more than one element.

Proof By Proposition 4.2.9, the set A^A is a noncommutative monoid under the composition of maps. If A has only one element, then A^A has only the identity map and $\left(A^A, \circ\right)$ forms a group in this case. Assume that A has more than one element and select $x_0 \in A$. Define

$$f : A \to A \text{ by } f(x) = x_0 \quad \forall\, x \in A.$$

The map f is an element of A^A. For all $g \in A^A$ and $x \neq x_0$,

$$f \circ g(x) = f(g(x)) = x_0 \neq x.$$

That is, $f \circ g \neq I_A$. Therefore, f is not invertible in A^A, and $\left(A^A, \circ\right)$ is not a group. ■

Corollary 5.1.11 *Let A be any nonempty set. The set of all bijective maps on A, denoted by $\mathfrak{S}_A$, forms a group under the composition of maps.*

Proof By Corollary 5.1.7, the subset of all invertible elements in the monoid $\left(A^A, \circ\right)$ forms a group under the operation $\circ$. The result follows since the map $f : A \to A$ is invertible if and only if it is bijective (Theorem 1.5.20). ■

The group $\mathfrak{S}_A$ is called the symmetric group of A. In the case of $A = \{1, 2, \ldots, n\}$, the symbol $\mathfrak{S}_n$ is used instead of $\mathfrak{S}_A$, and the group $(\mathfrak{S}_n, \circ)$ is called the nth symmetric group; i.e., the group $(\mathfrak{S}_n, \circ)$ consists of all bijective maps from $\{1, 2, \ldots, n\}$ to itself. We devote Chap. 6 to study the nth symmetric group.

5.2 Cayley's Tables for Finite Groups

If G is a finite set, then any binary operation $*$ on G can be represented using a table (Sect. 1.5). If G is a group, such a table is called Cayley's table of G. In such tables, the identity element and inverse of an arbitrary element can be easily identified. Moreover, one can directly determine if the operation $*$ is commutative by examining the symmetry around the diagonal of the table. The following subsequent examples illustrate the use Cayley's table to represent binary operations.

Example 5.2.1 Let $G = \{e, a, b\}$ and $*$ be the operation defined on the elements of G, as in Table 5.1. It can be easily determined that $*$ is an associative binary operation by examining all the cases. Clearly that e forms an identity element. Moreover, the inverse of any element exists in G, and $a^{-1} = b, b^{-1} = a, e^{-1} = e$. Thus, $(G, *)$ forms a group.

Example 5.2.2 (Klein group) Let $V = \{e, a, b, c\}$ and $*$ be defined on V, as in Table 5.2. It can be shown that $(V, *)$ is a group in which every element is its own inverse. Any group with four elements that satisfies this property is called the Klein 4-group, or simply, the Klein group.

Table 5.1 Cayley's table of the group G

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Table 5.2 Cayley's table of Klein group

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 5.3 Cayley's table of the symmetries of the square

$\cdot$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0	$l_{\pi/4}$	$l_{\pi/2}$	$l_{3\pi/4}$	l_0
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	$l_{\pi/2}$	$l_{3\pi/4}$	l_0	$l_{\pi/4}$
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π	$l_{3\pi/4}$	l_0	$l_{\pi/4}$	$l_{\pi/2}$
l_0	l_0	$l_{3\pi/4}$	$l_{\pi/2}$	$l_{\pi/4}$	R_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$
$l_{\pi/4}$	$l_{\pi/4}$	l_0	$l_{3\pi/4}$	$l_{\pi/2}$	$R_{\pi/2}$	R_0	$R_{3\pi/2}$	R_π
$l_{\pi/2}$	$l_{\pi/2}$	$l_{\pi/4}$	l_0	$l_{3\pi/4}$	R_π	$R_{\pi/2}$	R_0	$R_{3\pi/2}$
$l_{3\pi/4}$	$l_{3\pi/4}$	$l_{\pi/2}$	$l_{\pi/4}$	l_0	$R_{3\pi/2}$	R_π	$R_{\pi/2}$	R_0

Example 5.2.3 Let $G = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}, l_0, l_{\pi/4}, l_{\pi/2}, l_{3\pi/4}\}$, the set of all symmetries of the square illustrated in Example 1.7.9. It can be easily checked that G with matrix multiplication forms a group. Using Proposition 1.7.7, Cayley's table for such a group can be obtained as given in Table 5.3.

Example 5.2.4 Let $G = \{1, -1, i, -i, j, -j, k, -k\}$, where $1, i, j, k$ are distinct elements, and the operation $\cdot$ be the operation defined in Table 5.4. By checking all the cases, one can easily show that $\cdot$ is associative operation. Clearly that 1 is an identity element for G. The inverses of any element in G are given as follows: $1^{-1} = 1, (-1)^{-1} = -1, (x)^{-1} = -x$, for any $x \in \{\pm i, \pm j, \pm k\}$. Therefore, $(G, \cdot)$ forms a group. Note that the operation $\cdot$ is not commutative (Table 5.4).

5.3 Additive and Multiplicative Groups of Integers Modulo *n*

In this section, we briefly present two examples of finite groups defined on $\mathbb{Z}_n$, the set of integers modulo n, where $n \in \mathbb{N}$. Recall that $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ is the set of equivalence classes of the relation $\cong_n$ on $\mathbb{Z}$. The set $\mathbb{Z}_n$ forms a group under the sum operation defined on $\mathbb{Z}_n$ (Definition 3.3.1).

Proposition 5.3.1 *Let $n \in \mathbb{N}$, and $\oplus_n$ be the sum modulo n defined on $\mathbb{Z}_n$. The pair $(\mathbb{Z}_n, \oplus_n)$ forms a commutative group for each n.*

Table 5.4 Cayley's table of the group $(G, \cdot)$

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	$i1$	$-i$	i	$-j$	$-i$	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Proof According to Proposition 3.3.2, the operation $\oplus_n$ forms a binary operation on $\mathbb{Z}_n$. Let $[a], [b], [c] \in \mathbb{Z}_n$,

$$\begin{aligned}[a] \oplus_n ([b] \oplus_n [c]) &= [a] \oplus_n ([b + c]) = [a + (b + c)] \\ &= [(a + b) + c] = [a + b] \oplus_n [\mathrm{c}] = ([a] \oplus_n [b]) \oplus_n [c].\end{aligned}$$

The above equations imply that $\oplus_n$ is associative. As $[a] \oplus_n [0]{=}[a + 0] = [a]\ \forall [a] \in \mathbb{Z}_n$, the element $[0]$ is the identity element for $\mathbb{Z}_n$. For an arbitrary element $[a] \in \mathbb{Z}_n$, the element $[n - a] \in \mathbb{Z}_n$ and satisfies

$$[n - a] \oplus_n [a] = [n - a + a] = [n] = [0].$$

That is, $[n - a]$ is the inverse of $[a]$. Therefore, $\mathbb{Z}_n$ is a group under the sum modulo n. Note that we only needed to verify one direction since the operation $\oplus_n$ is commutative as $[a] \oplus_n [b] = [a + b] = [b + a] = [b] \oplus_n [a]$ for all $[a], [b] \in \mathbb{Z}_n$. ■

The tables in Example 3.4.1 are examples of Cayley's tables of the group $(\mathbb{Z}_n, \oplus_n)$ for some positive integers n.

Next, we discuss the multiplication operation $\otimes_n$ defined on $\mathbb{Z}_n$, where $n \in \mathbb{N}$. We shall see that $(\mathbb{Z}_n, \otimes_n)$ is not a group for each $n > 1$. However, using a proper subset of $(\mathbb{Z}_n, \otimes_n)$ one can construct a group under the operation $\otimes_n$. We shall prove that the subset

$$\{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

forms a group under multiplication operation $\otimes_n$. Such a group is fundamental in number theory and has many applications in factorization and cryptography. We begin our study with the set $\mathbb{Z}_1$ that contains only one element $[0]$. As $[0] \otimes_1 [0]{=}[0]$, the operation $\otimes_1$ is associative and commutative. The element $[0]$ serves as the identity element and is the inverse of itself. So,$(\mathbb{Z}_1, \otimes_1)$ forms a group. For $n > 1$, we have the following proposition.

Proposition 5.3.2 *Let $n \in \mathbb{N}\backslash\{1\}$ and $\otimes_n$ be the multiplication modulo n defined on $\mathbb{Z}_n$. The set $\mathbb{Z}_n$ is a commutative monoid, but it is not a group for any n.*

Proof According to Proposition 3.3.2, the operation $\otimes_n$ is a binary operation on $\mathbb{Z}_n$. The operation $\otimes_n$ is associative, as for each $[a], [b], [c] \in \mathbb{Z}_n$,

$$\begin{aligned}[a] \otimes_n ([b] \otimes_n [c]) &= [a] \otimes_n ([bc]) = [a(bc)] = [(ab)c] \\ &= [ab] \otimes_n [c] = ([a] \otimes_n [b]) \otimes_n [c].\end{aligned}$$

Hence, $(\mathbb{Z}_n, \otimes_n)$ is a semigroup. The element $[1] \in \mathbb{Z}_n$ satisfies

$$[1] \otimes_n [a] = [a] \otimes_n [1]=[a \times 1] = [a]$$

for each $[a] \in \mathbb{Z}_n$, and thus $[1]$ is an identity element in $(\mathbb{Z}_n, \otimes_n)$. However, for each $n > 1$ and each $[a] \in \mathbb{Z}_n$

$$[0] \otimes_n [a] = [0 \times a]=[0]\neq[1].$$

That is, $[0]$ has no inverse with respect to the operation $\otimes_n$, and $(\mathbb{Z}_n, \otimes_n)$ is not a group for each $n > 1$. The operation $\otimes_n$ is commutative, as for each $[a]$, [b] $\in \mathbb{Z}_n$,

$$[a] \otimes_n [b] = [ab] = [ba] = [b] \otimes_n [a].$$

■

As the monoid $(\mathbb{Z}_n, \otimes_n)$ is not a group for $n > 1$, in the remainder of the book, by the group $\mathbb{Z}_n$, we refer to the additive group $(\mathbb{Z}_n, \oplus_n)$.

Lemma 5.3.3 *Let $n \in \mathbb{N}\backslash\{1\}$. The invertible elements in $(\mathbb{Z}_n, \otimes_n)$ are the elements of the set*

$$\mathrm{Inv}(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

Proof Let $[a] \in \mathbb{Z}_n$. According to Definition 4.3.6, the element $[a]$ is invertible in $(\mathbb{Z}_n, \otimes_n)$ if and only if there exists $b \in \mathbb{Z}$ such that $[a] \otimes_n [b] = [1]$, which occurs if and only if $\gcd(a, n) = 1$ (Proposition 3.3.5). ■

Example 5.3.4 The following are examples of the invertible elements in $\mathbb{Z}_n$ for some positive integers n.

$$\begin{aligned}&\mathrm{Inv}(\mathbb{Z}_1) = \{[0]\}, \mathrm{Inv}(\mathbb{Z}_2) = \{[1]\}, \mathrm{Inv}(\mathbb{Z}_3) = \{[1],[2]\},\\ &\mathrm{Inv}(\mathbb{Z}_4) = \{[1], [3]\}, \mathrm{Inv}(\mathbb{Z}_5) = \{[1], [2], [3], [4]\}, \mathrm{Inv}(\mathbb{Z}_6) = \{[1], [5]\},\\ &\mathrm{Inv}(\mathbb{Z}_7) = \{[1], [2], [3], [4], [5], [6]\}, \text{and } \mathrm{Inv}(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}.\end{aligned}$$

Lemma 5.3.3 and Corollary 5.1.7 imply the following result.

Table 5.5 Cayley's tables of $(\text{Inv}(\mathbb{Z}_3), \otimes_3)$

$\otimes_3$	[1]	[2]
[1]	[1]	[2]
[2]	[2]	[1]

Table 5.6 Cayley's tables of $(\text{Inv}(\mathbb{Z}_4), \otimes_4)$

$\otimes_4$	[1]	[3]
[1]	[1]	[3]
[3]	[3]	[1]

Corollary 5.3.5

1. *For each* $n \in \mathbb{N}$, $(\text{Inv}(\mathbb{Z}_n), \otimes_n)$ *forms a group.*
2. *For a prime* p, *the set* $\text{Inv}\big(\mathbb{Z}_p\big) = \mathbb{Z}_p^* = \{[1], [2], [3], \ldots, [p-1]\}$ *forms a group under the multiplication module* p.

The group in Corollary 5.3.5 is called the multiplicative group of $\mathbb{Z}_n$. Note that $\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{[0]\}$ is not always equal to $\text{Inv}(\mathbb{Z}_n)$. For example, $\text{Inv}(\mathbb{Z}_6) = \{[1], [5]\} \neq \mathbb{Z}_6 \backslash \{[0]\}$. The set $\text{Inv}(\mathbb{Z}_n) = \mathbb{Z}_n^*$ if and only if n is prime. In fact, if n is not prime, then there exist two integers q, l such that $n = ql$ and $1 < q, l < n$. Hence, $[q] \in \mathbb{Z}_n$ and $\gcd(q, n) = q \neq 1$. i.e., $[q]$ is not invertible, and $\mathbb{Z}_n^* \neq \mathbb{Z}_n \backslash \{[0]\}$. On the other hand, for any prime p, $\gcd(k, p) = 1$ for any $0 < k < p$, which implies that $\text{Inv}\big(\mathbb{Z}_p\big) = \mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{[0]\}$.

Example 5.3.6 Cayley's tables for $(\text{Inv}(\mathbb{Z}_3), \otimes_3)$ and $(\text{Inv}(\mathbb{Z}_4), \otimes_4)$ are given in Tables 5.5 and 5.6.

Example 5.3.7 To check whether [12] is invertible in $\mathbb{Z}_{53}$, one only needs to compute $\gcd(12, 53)$. This computation can be performed using the Euclidean algorithm 2.4.1 to obtain $\gcd(12, 53) = 1$. Therefore, [12] is an invertible element in $\mathbb{Z}_{53}$. To find the inverse of [12], the backward (or forward) substitution method, as illustrated in Example 2.5.3, can be used to write 1 as a linear combination of 12 and 53, thereby obtaining $1 = 53 \times 5 - 12 \times 22$. Applying the relation mod 53 to both sides yields $12 \times (-22) \equiv 1 (\text{mod } 53)$. Since $[-22] = [31]$ in $\mathbb{Z}_{53}$, then [31] is the multiplicative inverse of [12] in $\mathbb{Z}_{53}$.

Definition 5.3.8 Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the map defined by

$$\varphi(n) = |\{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}|$$

for each positive integer n.

The map φ is known by Euler totient function. Clearly, $\varphi(p) = p - 1$ for any prime p. For any positive integer n, the number $\varphi(n)$ can be computed using the formula $\varphi(n) = n \prod\limits_{p|n} (1 - \frac{1}{p})$ (Burton, 2007).

Corollary 5.3.9 *For any $n \in \mathbb{N}$,*

$$|\mathrm{Inv}(\mathbb{Z}_n)| = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

5.4 Abelian Groups and the Center of a Group

In this short section, we define and briefly study abelian groups, which are groups with commutative binary operations. We also define the center of G and show that the center of any group forms a group. The classification of finite abelian groups will be discussed in detail in Chap. 9.

Definition 5.4.1 Let $(G, *)$ be a group, and a, b be two elements in G. We say a and b commute if $a * b = b * a$.

The operation $*$ is called commutative when every two elements in G commute. In this case, the group G is said to be abelian. The formal definition is as follows:

Definition 5.4.2 Let $(G, *)$ be a group. The group G is said to be abelian if

$$a * b = b * a \text{ for all } a, b \in G.$$

The groups in Examples 5.1.4 (2, 5) and 5.1.8 (1) are abelian. The dihedral group (Example 5.1.4 (7)) and the general linear group (Example 5.1.8 (2)) are examples of nonabelian groups. The additive and multiplicative groups of integers modulo n in Proposition 5.3.1 and Corollary 5.3.5 as well as the groups in Examples 5.2.1, 5.2.2 are finite abelian groups.

Example 5.4.3 Any group with four elements or less is an abelian group. We show this by showing the equivalent statement, any nonabelian group has at least five elements. To see this, assume that G is nonabelian. By definition of nonabelian groups, there exist two elements such that $x * y \neq y * x$.

- Since $x * y \neq y * x$, we have $x \neq y$, $x \neq e$, and $y \neq e$.
- Since $y \neq e$, we have $x \neq x * y$ and $x \neq y * x$.
- Since $x \neq e$, we have $y \neq x * y$ and $y \neq y * x$.
- Since $x * y \neq y * x$, we also have $x \neq y^{-1}$, $y \neq x^{-1}$, thus $x * y \neq e$ and $y * x \neq e$.

Thus, $e, x, y, x * y, y * x$ are distinct and the group has at least five elements.

Recall that if a is an element of $(G, *)$, then a^n denotes $\underbrace{a * a * \cdots * a}_{n \text{ times}}$, where $n \in \mathbb{N}$ (Notation 4.2.3), and if $a^2 = e$, then by the uniqueness of the inverse element, we obtain $a = a^{-1}$.

Proposition 5.4.4 *Let $(G, *)$ be a group. If $a^2 = e$ for every $a \in G$, then G is abelian.*

Proof The hypothesis is that $a^{-1} = a$ for every $a \in G$. If a, b are two elements in G, then $a * b$ is an element in G and $a * b = (a * b)^{-1}$. According to Proposition 5.1.2 (2),

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

■

Lemma 5.4.5 *Let $(G, *)$ be a group, and a, b be two elements in G. If a and b commute, then for every positive integer n,*

1. $a * b^n = b^n * a$.
2. $(a * b)^n = a^n * b^n$.

Proof We show the results by induction as follows:

1. For $n = 1$, this is the hypothesis. Suppose that $a * b^n = b^n * a$ is given, then

$$a * b^{n+1} = a * b^n * b = b^n * a * b = b^n * b * a = b^{n+1} * a.$$

So, by induction, we have $a * b = b * a \Rightarrow a * b^n = b^n * a$ for all $n \geq 1$.

2. The statement is true for $n = 1$, as $(a * b)^1 = a * b = a^1 * b^1$.

Inductive step: Assume that the statement is true for $n = k$. i.e., $(a * b)^k = a^k * b^k$.

For $n = k + 1$, by using the induction hypothesis and (1), we obtain

$$\begin{aligned}(a * b)^{k+1} &= (a * b)^k * (a * b) = \left(a^k * b^k\right) * a * b = a^k * \left(b^k * a\right) * b \\ &= a^k * \left(a * b^k\right) * b = a^{k+1} * b^{k+1}.\end{aligned}$$

Hence, the result follows by induction. ■

Note that the statements in Lemma 5.4.5 are trivial for $n = 0$. If n is a negative integer, the statements can be expressed as: If a, b commute, then $a * b^n = b^n * a$ and $(a * b)^n = b^n * a^n$. For if $n = -m$, where $m > 0$, then

$$a * b^n = a * b^{-m} = a * \left(b^{-1}\right)^m = \left(b^{-1}\right)^m * a = b^n * a$$

and

$$(a * b)^n = (a * b)^{-m} = \left((a * b)^{-1}\right)^m = \left(b^{-1} * a^{-1}\right)^m = b^{-m} * a^{-m} = b^n * a^n.$$

For a generalization of the above lemma to finite pairwise commutative elements; see Exercise 5.25.

Corollary 5.4.6 *Let $(G, *)$ be a group.*

$$(G, *) \text{ is abelian} \Leftrightarrow (a * b)^2 = a^2 * b^2 \quad \forall\, a, b \in G.$$

Proof If G is abelian, then a, b commute for all a, b in G, and Lemma 5.4.5 (2) implies the required result. For the other direction, assume that $(a * b)^2 = a^2 * b^2$ for all $a, b \in G$. This implies that

$$(a * b) * (a * b) = (a * a) * (b * b) \text{ for all } a, b \in G$$

i.e.,

$$a * (b * a) * b = a * (a * b) * b \text{ for all } a, b \in G.$$

By applying the left and right cancelation laws, we obtain $b * a = a * b$ for all $a, b \in G$ and G is abelian. ■

Note that if G is abelian, then by Lemma 5.4.5 (2), we obtain $(a * b)^n = a^n * b^n \quad \forall\, a, b \in G$ for all $n \in \mathbb{N}$. On the other hand, if $(a * b)^n = a^n * b^n \quad \forall\, a, b \in G$ and $\forall\, n \in \mathbb{N}$, then $(a * b)^2 = a^2 * b^2$ for all $a, b \in G$, which gives

$$(G, *) \text{ is abelian} \Leftrightarrow (a * b)^n = a^n * b^n \quad \forall\, a, b \in G \;\text{ and }\; \forall\, n \in \mathbb{N}.$$

Definition 5.4.7 Let $(G, *)$ be a group. The center of G, denoted by $C(G)$, is the set of elements of G that commute with every element in G. Therefore,

$$C(G) = \{a \in G : a * g = g * a \quad \forall g \in G\}.$$

As the identity element commutes with every element in the group, the center of any group is never empty.

Proposition 5.4.8 *The center of any group is a group.*

Proof Let $(G, *)$ be a group with identity e. As $e \in C(G)$, then $C(G)$ is a nonempty subset of G. For $a, b \in C(G)$ and each $g \in G$,

$$\begin{aligned}(a * b) * g = a * (b * g) = a * (g * b) &= (a * g) * b \\ &= (g * a) * b = g * (a * b)\end{aligned}$$

i.e., $a * b \in C(G)$ and $*$ is a binary operation on $C(G)$ (Proposition 4.1.6). The subset $C(G)$ inherits the associativity property from G, and e serves as an identity element in $C(G)$. For $a \in C(G)$, the inverse $a^{-1} \in G$ satisfies

$$a^{-1} * g = \left(g^{-1} * a\right)^{-1} = \left(a * g^{-1}\right)^{-1} = g * a^{-1} \quad \forall\, g \in G$$

i.e., $a^{-1} \in C(G)$. Hence, $C(G)$ forms a group. ■

Example 5.4.9

1. According to the definition of abelian groups, the group G is abelian if and only if $C(G) = G$. For example,

$$C((\mathbb{Z}, +)) = \mathbb{Z},\ C((\mathbb{C}, +)) = \mathbb{C},\ C((\mathcal{M}_{mn}(\mathbb{C}), +)) = \mathcal{M}_{mn}(\mathbb{C}).$$

2. Consider the general linear group $GL_n(\mathbb{C})$ (Example 5.1.8 (2)). The center of $GL_n(\mathbb{C})$ is

$$C(GL_n(\mathbb{C})) = \left\{\lambda I_n, \lambda \in \mathbb{C}^*\right\}.$$

For if $\lambda \in \mathbb{C}^*$ then $\lambda I_n A = \lambda A = A\lambda I_n$ for any $A \in GL_n(\mathbb{C})$, which implies that

$$\left\{\lambda I_n, \lambda \in \mathbb{C}^*\right\} \subseteq C(GL_n(\mathbb{C})).$$

For the other direction, let B be an arbitrary element in $C(GL_n(\mathbb{C}))$. We show that B is equal to λI_n for some $\lambda \in \mathbb{C}^*$. For each $1 \leq k, l \leq n$, consider the matrix E_{kl}, the matrix in $\mathcal{M}_n(\mathbb{C})$ defined by $a_{kl} = 1$ with all other entries being zero (Example 1.6.5 (3)). Let $A_{kl} = E_{kl} + I_n$. The matrix A_{kl} is an element in $GL_n(\mathbb{C})$ (Check!). Since B is an element in $C(GL_n(\mathbb{C}))$, then $BA_{kl} = A_{kl}B$, which implies that $BE_{kl} = E_{kl}B$ for each $1 \leq k, l \leq n$. i.e., B commutes with all matrices of the form E_{kl}, where $1 \leq k, l \leq n$. In particular, for each $1 \leq k, l \leq n$,

$$E_{kl}BE_{lk} = E_{kl}E_{lk}B = E_{kk}B \quad (*)$$

where the last equality is computed using the result in Example 1.6.7 (3). Since $B \in \mathcal{M}_n(\mathbb{C})$, then we have $B = \sum_{i,j=1}^{n} b_{ij}E_{ij}$ for some b_{ij} in $\mathbb{C}$ (Example 1.6.5 (3)). Substituting the expression of B in both sides of the equation $(*)$, we obtain

$$\begin{aligned} \text{L.H.S} = E_{kl}BE_{lk} &= E_{kl}\left(\sum_{i,j=1}^{n} b_{ij}E_{ij}\right)E_{lk} = \sum_{i,j=1}^{n} b_{ij}E_{kl}E_{ij}E_{lk} \\ &= \sum_{i,j=1}^{n} b_{ij}\delta_{il}\delta_{jl}E_{kk} = b_{ll}E_{kk}. \\ \text{R.H.S} = E_{kk}B &= E_{kk}\sum_{i,j=1}^{n} b_{ij}E_{ij} = \sum_{i,j=1}^{n} b_{ij}E_{kk}E_{ij} \\ &= \sum_{i,j=1}^{n} b_{ij}\delta_{ik}E_{kj} = \sum_{j=1}^{n} b_{kj}E_{kj}. \end{aligned}$$

Therefore, $b_{ll}E_{kk} = \sum_{j=1}^{n} b_{kj}E_{kj}$, which implies that $b_{kj} = 0$ for all $j \neq k$, and $b_{kk} = b_{ll}$. Namely, the matrix B is a diagonal matrix with diagonal entries equal to b_{kk}. Since $B \neq 0_n$ (B is invertible), b_{kk} cannot be zero. As k is arbitrary, there exists $\lambda \in \mathbb{C}^*$ such that $\lambda = b_{kk}$, as required.

3. As a special case of the example in (2), the center of the general linear group of order 2 is $C(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}^* \right\}$.

5.5 The Order of an Element in a Group

Recall that for an element a in a semigroup G and $n \in \mathbb{N}$, the notation a^n denotes the element of G given by $\underbrace{a * a * \cdots * a}_{n \text{ times}}$ (Notation 4.2.3). If G is a group, then the inverses of its elements are defined, and the case in which n is a negative integer or zero can be generalized as follows:

Definition 5.5.1 Let G be a group and $n \in \mathbb{Z}$. For each $a \in G$,

1. $a^n = \underbrace{a * a * \ldots * a}_{n \text{ times}}$ if $n > 0$.
2. $a^n = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{-n \text{ times}}$ if $n < 0$.
3. $a^0 = e$.

The proof of the next proposition is straightforward and left as an exercise.

Proposition 5.5.2 *Let G be a group with identity e and a be an element of G. For each $n, m \in \mathbb{Z}$,*

$$e^n = e, \ \left(a^n\right)^{-1} = \left(a^{-1}\right)^n = a^{-n}, \quad a^m a^n = a^{m+n} \quad \text{and} \quad \left(a^m\right)^n = a^{mn}.$$

Definition 5.5.3 Let $(G, *)$ be a group and a be an element in G.

1. The order of a, denoted by $\mathrm{ord}(a)$, is defined as the smallest positive integer k such that $a^k = e$. If no such number exists, we say that a has an infinite order.
2. The order of G is defined as the number of its elements (cardinality of G) if G is finite; otherwise, we say that G has infinite order.

Example 5.5.4

1. The identity element of any group G has order equal to 1, i.e., $\mathrm{ord}(e) = 1$.
2. Let $G = \{1, -1, i, -i\}$. The set G, endowed with the multiplication of the complex numbers, forms a group (Check!) whose order is 4. The identity of G is 1 and $\mathrm{ord}(1) = 1$, the element $-1 \neq 1$, while $(-1)^2 = 1$, so $\mathrm{ord}(-1) = 2$. To determine the order of i, compute a list of i^k, where k is positive integer and $k \geq 1$, as follows:

$$i^1 = i \neq 1, \quad i^2 = -1 \neq 1, \quad i^3 = -i \neq 1, \quad i^4 = 1.$$

Since $k = 4$ is the smallest positive integer satisfies that $i^k = 1$, then $\text{ord}(i) = 4$. Similarly, $\text{ord}(-i) = 4$.

3. Any element in the Klein group (Example 5.2.2) has order 2.
4. In the additive group $(\mathbb{Z}, +)$, every nonzero element has an infinite order. If $m \neq 0$, then for any positive integer k, we have $m^k = \underbrace{m + m + \cdots + m}_{k \text{ times}} = mk \neq 0$, and thus, $\text{ord}(m)$ is infinite. The order of $\mathbb{Z}$ is also infinite as the group $\mathbb{Z}$ has an infinite number of elements.
5. In the dihedral group $(D_{2n}, \circ)$ (Example 5.1.4 (7)), the order of the rotation by angle 0 is 1, the order of the rotation by $2\pi/n$ is n, and the order of any reflection in D_{2n} is 2.

Next, we study the relation between the order of a given group and the order of its elements. We shall see that if the group has a finite order, all its elements have finite orders. However, if G has infinite order, then its elements may have an infinite or a finite order. We begin with the following lemmas; the first lemma follows directly by Definition 5.5.3 (1).

Lemma 5.5.5 *Let G be a group and a be an element of G. If there exists $n \in \mathbb{N}$ such that $a^n = e$ then a has a finite order that is less than or equal to n.*

Lemma 5.5.6 *Let G be a group. Let a be an element of G, such that* $\text{ord}(a)$ *is finite. For each $n \in \mathbb{N}$,*

$$a^n = e \Leftrightarrow \text{ord}(a) | n .$$

Proof If $\text{ord}(a)|n$, then there exists $q \in \mathbb{Z}$ such that $n = q \ \text{ord}(a)$. Therefore,

$$a^n = a^{q \ \text{ord}(a)} = \left(a^{\text{ord}(a)}\right)^q = e^q = e.$$

For the other direction, assume that $n \in \mathbb{N}$ such that $a^n = e$. According to the quotient-remainder theorem (Theorem 2.1.2), applied to n and $\text{ord}(a)$, there exist $q, r \in \mathbb{Z}$ such that

$$n = q \ \text{ord}(a) + r \quad \text{where} \quad 0 \leq r < \text{ord}(a).$$

Thus,

$$a^n = e \Rightarrow a^{q \ \text{ord}(a)+r} = e \Rightarrow \left(a^{\text{ord}(a)}\right)^q * a^r = e \Rightarrow a^r = e.$$

Since $\text{ord}(a)$ is the smallest positive integer satisfying $a^{\text{ord}(a)} = e$, then r must be zero. Hence, $n = q \ \text{ord}(a)$ and $\text{ord}(a)|n$. ■

Corollary 5.5.7 *Let G be a group, and p be a prime number. Let a be an element of G such that a has a finite order.*

1. *If* $a^p = e$*, then either* $a = e$ *or* $\operatorname{ord}(a) = p$.
2. *If* $\operatorname{ord}(a) = kp$ *for some* $k \in \mathbb{N}$, *then* $\operatorname{ord}\left(a^k\right) = p$.

Proof Assume that $a^p = e$. According to Lemma 5.5.6, $\operatorname{ord}(a)$ must divide p. If $a \neq e$, then $\operatorname{ord}(a) \neq 1$, and thus, it is equal to p. For the second statement, assume that $\operatorname{ord}(a) = kp$, i.e., then kp is the smallest positive integer such that $a^{kp} = \left(a^k\right)^p = e$. As $k < kp$, then $a^k \neq e$. The result follows by (1). ■

The following corollary states that a group with a finite order must have all its elements with finite orders.

Corollary 5.5.8 *Let* $(G, *)$ *be a group.*

1. *If* G *has a finite order, then the order of any element of* G is finite and less than or equal to the order of G.
2. *If* G *contains an element with an infinite order, then the order of* G is infinite.

Proof To show the first statement, assume that G is finite and let a be any element in G. As G is closed under the operation $*$, the set $\left\{a,\ a^2,\ a^3, \ldots,\ a^s,\ \ldots\right\}$ is a subset of G. Since G is finite, the subset $\left\{a,\ a^2,\ a^3, \ldots,\ a^s,\ \ldots\right\}$ must be finite. i.e., there exist $s, t \in \mathbb{N}$ such that $a^s = a^t$. Assume (without loss of generality) that $s > t$,

$$a^s = a^t \Rightarrow a^s * a^{-t} = a^t * a^{-t} \Rightarrow a^{s-t} = a^0 = e.$$

By Lemma 5.5.5, the order of a is finite. Let $k = \operatorname{ord}(a)$, the set $\left\{e, a, a^2, a^3, \ldots, a^{k-1}\right\}$ contains distinct elements (Exercise 5.28). If k is greater than the order of G, then this set contains more elements than G, contradicting that $\left\{e, a, a^2, a^3, \ldots, a^{k-1}\right\}$ is a subset of G, and thus, the first statement holds. The second statement is the contrapositive of the first statement. ■

Note that G may have an infinite order while every element in G has a finite order. For example, consider the abelian group in Example 5.1.5. If the set X is an infinite set, then G is an example of an infinite group in which the order of every element is at most 2. For if $A \neq \emptyset$ is an element in G, then $A^2 = A \Delta A = \emptyset$.

The following proposition is a more general form of the result in Corollary 5.5.7 (2).

Proposition 5.5.9 *Let* G *be a group and* $a \in G$ *such that* $\operatorname{ord}(a) < \infty$. *For any positive integer* $k \in \mathbb{N}$.

$$\operatorname{ord}\left(a^k\right) = \frac{\operatorname{ord}(a)}{\gcd(k, \operatorname{ord}(a))}.$$

Proof Let $\operatorname{ord}(a) = n$ and k be an arbitrary element in $\mathbb{N}$. Set $\operatorname{ord}\left(a^k\right) = m$ and

$$q = \frac{n}{\gcd(k, n)}.$$

As

$$\left(a^k\right)^q = \left(a^k\right)^{\frac{n}{\gcd(k,n)}} = \left(a^n\right)^{\frac{k}{\gcd(k,n)}} = e,$$

then by Lemma 5.5.6, $m|q$, which implies that $m \le q$. On the other hand, as $a^{km} = \left(a^k\right)^m = e$, so by Lemma 5.5.6, $n|km$. Dividing both sides by $\gcd(k, n)$ yields,

$$\frac{n}{\gcd(k,n)} \text{ divides } \frac{km}{\gcd(k,n)}.$$

As $\gcd\left(\frac{n}{\gcd(k,n)}, \frac{k}{\gcd(k,n)}\right) = 1$ (Proposition 2.6.3), then by Corollary 2.5.7 (2)

$$q = \frac{n}{\gcd(k,n)} \text{ divides } m$$

which implies that $q \le m$. Therefore, $m = q$, as required. ■

Note that according to the above result,

$$\gcd(k, \operatorname{ord}(a)) = 1 \Rightarrow \operatorname{ord}\left(a^k\right) = \operatorname{ord}(a).$$

The following result states that an element a and its inverse must have the same order.

Lemma 5.5.10 *Let* $(G, *)$ *be a group. For any* a *in* G, $\operatorname{ord}(a) = \operatorname{ord}\left(a^{-1}\right)$.

Proof If $\operatorname{ord}(a) = n < \infty$, then $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e$, which implies that a^{-1} has a finite order $m \le n$ (Lemma 5.5.5). Moreover,

$$a^m = \left(\left(a^{-1}\right)^{-1}\right)^m = \left(\left(a^{-1}\right)^m\right)^{-1} = e$$

which implies that $n \le m$. Hence, $m = n$.

If $\operatorname{ord}(a) = \infty$, then from the finite cases, a finite order of a^{-1} implies a finite order for its inverse a (as $\left(a^{-1}\right)^{-1} = a$), which contradicts $\operatorname{ord}(a) = \infty$. Therefore, a^{-1} must have an infinite order. ■

Next, we study the order of $a * b$ for two elements a and b in a group G and its relation to the orders of a and b. Note that $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ do not provide any information regarding the order of $a * b$ and vice versa. For example, in $(\mathbb{Z}, +)$,

- $\operatorname{ord}(1) = \operatorname{ord}(-1) = \infty$ and $\operatorname{ord}(1 + (-1)) = \operatorname{ord}(0) = 1$.
- $\operatorname{ord}(1) = \operatorname{ord}(2) = \infty$ and $\operatorname{ord}(1 + 2) = \operatorname{ord}(3) = \infty$.
- $\operatorname{ord}(0) = 1$ and $\operatorname{ord}(0 + 0) = \operatorname{ord}(0) = 1$.

As a further example, in $GL_2(\mathbb{C})$ (Example 5.1.8), if $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}$,

$$\mathrm{ord}(a) = \mathrm{ord}(b) = 2 \ \wedge \ \mathrm{ord}(ab) = \mathrm{ord}\left(\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}\right) = \infty.$$

The next proposition shows that if a, b commute and have finite orders, then $\mathrm{ord}(a * b)$ is finite, and in certain cases the order of $a * b$ can be obtained using the orders of a and b. However, the converse is not true, as shown in the above examples. Nevertheless, in all cases, $\mathrm{ord}(a * b) = \mathrm{ord}(b * a)$ for any a, b that belong to any group G (Exercise 5.11).

Proposition 5.5.11 *Let* $(G, *)$ *be a group and* a, b *be commuting elements of* G. *If* $\mathrm{ord}(a)$ *and* $\mathrm{ord}(b)$ *are both finite, then* $\mathrm{ord}(a * b)$ *is finite and divides* $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. *Moreover, if* $\mathrm{gcd}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, then $\mathrm{ord}(a * b) = \mathrm{ord}(a)\mathrm{ord}(b)$.

Proof Let a, b be elements in G such that they commute. Let $m = \mathrm{ord}(a) < \infty$, $n = \mathrm{ord}(b) < \infty$ and $l = \mathrm{lcm}(m, n)$. By the definition of least common multiple of two integers, there exist $k_1, k_2 \in \mathbb{Z}$ such that $l = mk_1$ and $l = nk_1$. Using Lemma 5.4.5 (2),

$$(a * b)^l = a^l * b^l = a^{mk_1} * b^{nk_2} = e * e = e.$$

Therefore, $\mathrm{ord}(a * b)$ is finite (Lemma 5.5.5) and divides l (Lemma 5.5.6). If $\mathrm{gcd}(m, n) = 1$, then $l = mn$, thus $\mathrm{ord}(a * b)$ divides mn, and $\mathrm{ord}(a * b) \leq mn$. We only need to show that $mn \leq \mathrm{ord}(a * b)$. Assume that $\mathrm{ord}(a * b) = k$. As a, b commute, Lemma 5.4.5 (2) implies that

$$a^{kn} = a^{kn} * e = a^{kn} * b^{kn} = \left(a^k * b^k\right)^n = \left((a * b)^k\right)^n = e^n = e$$

and

$$b^{km} = e * b^{km} = a^{km} * b^{km} = \left(a^k * b^k\right)^m = \left((a * b)^k\right)^m = e^m = e$$

which implies that $m|kn$ and $n|km$. Since $\mathrm{gcd}(m, n) = 1$, it follows by Corollary 2.5.7 (2) that $m|k$ and $n|k$. By Corollary 2.5.7 (3), mn divides k. Hence, $mn \leq k$, and the result follows. ■

The following example shows that the condition $\mathrm{gcd}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, in Proposition 5.5.11, is essential and cannot be omitted.

Example 5.5.12 Let $G = \mathbb{Z}_{10}$ be the additive group module 10. In $(\mathbb{Z}_{10}, \oplus_{10})$,

- $\mathrm{ord}([1]) = 10$, $\mathrm{ord}([5]) = 2$, $\gcd(10, 2) = 2$, $\mathrm{ord}([1] \oplus_{10} [5]) = \mathrm{ord}([6]) = 5 \neq 20 = \mathrm{ord}([1])\mathrm{ord}([5])$.
- $\mathrm{ord}([2]) = 5$, $\mathrm{ord}([5]) = 2$, $\gcd(5, 2) = 1$, and $\mathrm{ord}([2] \oplus_{10} [5]) = \mathrm{ord}([7]) = 10 = \mathrm{ord}([2])\mathrm{ord}([5])$.

The following proposition shows that for an abelian group G, subsets such as

$$\{a^1 : a \in G\} = G,\ \{a^2 : a \in G\}, \{a^3 : a \in G\}, \ldots, \{a^{-1} : a \in G\} = G, \ldots, \{a^{-18} : a \in G\}, \ldots \text{etc},$$

and subsets such as

$$\{a \in G : a^1 = e\}, \{a \in G : a^2 = e\}, \{a \in G : a^3 = e\}, \ldots, \{a \in G : a^{-1} = e\},$$
$$\{a \in G : a^{-100} = e\}, \ldots, \{a \in G : a^{-25} = e\}, \ldots \text{etc.}$$

form groups.

Proposition 5.5.13 *Let G be an abelian group. For each $m \in \mathbb{Z}$, the sets*

$$mG = \{a^m : a \in G\} \text{ and } G[m] = \{a \in G : a^m = e\}$$

form groups.

Proof Since G is an abelian group, both sets are closed under the group operation (Check!). Therefore, both sets inherit the associativity from G. As $e^m = e$ for each m, both mG and $G[m]$ contain an identity element. Since both mG and $G[m]$ are subset of G, then every element in these sets is invertible, and we only need to verify the closure of these sets under taking the inverse.

- For each element $a^m \in mG$, its inverse $(a^m)^{-1} = \left(a^{-1}\right)^m \in mG$.
- For an element $a \in G[m]$, we have $a^m = e$, and $\left(a^{-1}\right)^m = (a^m)^{-1} = e$. Thus, a^{-1} belongs to $G[m]$.

■

Example 5.5.14

1. In the additive group $(\mathbb{Z}, +)$,

$$2\mathbb{Z} = \{a^2 : a \in \mathbb{Z}\} = \{2a : a \in \mathbb{Z}\}, \quad \mathbb{Z}[2] = \{0\}.$$

In general, for any $m \in \mathbb{Z}$,

$$m\mathbb{Z} = \{ma : a \in \mathbb{Z}\}, \quad \mathbb{Z}[m] = \{0\}.$$

2. In the additive group $(\mathbb{Z}_8, \oplus_8)$,

$$14\mathbb{Z}_8 = \{[0], [6], [4], [2]\}, \quad \mathbb{Z}_8[14] = \{[0], [4]\}.$$

3. Consider the multiplicative group $G = (\{-1, 1\}, \cdot)$. It is straightforward to verify that $2G = \{1\}$ and $5G = \{-1, 1\}$. In general,

$$m\mathrm{G} = \begin{cases} \{1\} & \text{if } m \text{ is even} \\ \{-1, 1\} & \text{if } m \text{ is odd} \end{cases}$$

4. In the multiplicative group $(\mathbb{R}^*, \cdot)$, $m\mathbb{R}^* = \{r^m : r \in \mathbb{R}^*\}$, $\mathbb{R}^*[m] = \{r \in \mathbb{R}^* : r^m = 1\}$.

   In particular,

$$2\mathbb{R}^* = \left\{r^2 : r \in \mathbb{R}^*\right\} = (0, \infty),\ \mathbb{R}^*[2] = \left\{r \in \mathbb{R}^* : r^2 = 1\right\} = \{-1, 1\},$$
$$3\mathbb{R}^* = \left\{r^3 : r \in \mathbb{R}^*\right\} = \mathbb{R}^*,\ \mathbb{R}^*[3] = \left\{r \in \mathbb{R}^* : r^3 = 1\right\} = \{1\}.$$

5. In the multiplicative group $(\mathbb{Q}^*, \cdot)$, for any integer m,

$$m\mathbb{Q}^* = \left\{r^m : r \in Q^*\right\} = \left\{p^m/q^m : p, q \in \mathbb{Z}^*\right\}, \text{ and}$$
$$\mathbb{Q}^*[m] = \left\{r \in \mathbb{Q}^* : r^m = 1\right\} = \left\{p/q : p, q \in \mathbb{Z}^* \wedge p^m = q^m\right\}.$$

   In particular,

$$2\mathbb{Q}^* = \left\{p^2/q^2 : p, q \in \mathbb{Z}^*\right\}, \mathbb{Q}^*[2] = \left\{p/q : p, q \in \mathbb{Z}^* \wedge p^2 = q^2\right\} = \{-1, 1\},$$
$$3\mathbb{Q}^* = \left\{p^3/q^3 : p, q \in \mathbb{Z}^*\right\},\ \mathbb{Q}^*[3] = \left\{p/q : p, q \in \mathbb{Z}^* \wedge p^3 = q^3\right\} = \{1\}.$$

6. Consider the dihedral group $D_6 = \left\{R_0, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, l_o, l_{\frac{\pi}{3}}, l_{\frac{2\pi}{3}}\right\}$ (Example 5.1.4 (7)). Computing $3D_6$ and $D_6[3]$, we obtain

$$3D_6 = \left\{R_0, l_o, l_{\frac{\pi}{3}}, l_{\frac{2\pi}{3}}\right\}, \quad D_6[3] = \left\{R_0, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}\right\}.$$

   Note that $3D_6$ is not a group as it is not closed under the composition (Check!), which shows that the assumption for G to be abelian in Proposition 5.5.13 is essential. Note that $D_6[3]$ in this example forms a group. Example 6.4.6 in Chap. 6 provides an example where both sets, mG and $G[m]$ are not groups.

Note that if G_1, G_2 are two groups and m is a positive integer, then $mG_1 = mG_2$ does not imply that $G_1 = G_2$. We shall provide examples supporting this remark in Chap. 7; see Example 7.3.22. We end this section by defining a property of group G, called the exponent of G.

Definition 5.5.15 Let G be a group. If there exists an integer $m \in \mathbb{N}$ such that $mG = \{e\}$, then the exponent of G is defined to be the smallest positive integer m satisfies that $mG = \{e\}$. We denote the exponent of G by $\mathrm{Exp}(G)$.

It can be easily verified that if k is a positive integer such that $kG = \{e\}$, then $\text{Exp}(G)$ divides k, as the exponent of a group G is the smallest positive integer m such that $a^m = e$ for all $a \in G$, provided that m exists.

Example 5.5.16

1. The exponent of any group G equals 1 if and only if $G = \{e\}$.
2. The exponent of Klein group is 2.
3. The groups $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$,$(\mathbb{C}, +)$ do not have exponents since for all positive integer m, and a nonzero element a in the group, we have $a^m = \underbrace{a + a + \cdots + a}_{m \text{ times}} \neq 0$.
4. If X in Example 5.1.5 is an infinite set, then $(G, \triangle)$ is an example of an infinite group whose exponent is 2.
5. For each $n \in \mathbb{N}$, the exponent of the additive group $(\mathbb{Z}_n, \oplus_n)$ equals n. For each $[a] \in \mathbb{Z}_n, [a]^n = \underbrace{[a] \oplus_n [a] \oplus_n \cdots \oplus_n [a]}_{n \text{ times}} = [\text{na}] = [0]$, and thus, $\text{Exp}(\mathbb{Z}_n) \leq n$.
   Moreover, for each positive integer $k < n$,
   $$[1]^k = \underbrace{[1] \oplus_n [1] \oplus_n \cdots \oplus_n [1]}_{k \text{ times}} = [k] \neq [0]$$
   and therefore, $\text{Exp}(\mathbb{Z}_n) = n$.
6. The group in Example 5.2.4, is a nonabelian group whose exponent is 4.

Proposition 5.5.17 *Let G be a finite group. The exponent of G exists and is equal to the least common multiple of the orders of its elements.*

Proof If $G = \{a_1, a_2, \ldots, a_n\}$ is a finite group, then the order of each element in G is finite (Corollary 5.5.8 (1)). For each $1 \leq i \leq n$, let $k_i = \text{ord}(a_i)$ and $k = \text{lcm}(k_i, k_2, \ldots, k_n)$. For each $1 \leq i \leq n$, k_i divides k, and $a_i^k = e$ (Lemma 5.5.6). Thus, $kG = \{e\}$, and the exponent of G exists. If m is a positive integer such that $mG = \{e\}$, then $a_i^m = e$ for each a_i in G. Lemma 5.5.6 implies that m is a multiple of $\text{ord}(a_i)$, $1 \leq i \leq n$. As k is the least common multiple of $\text{ord}(a_i)$, then $k \leq m$. i.e., $k = \text{Exp}(G)$. ∎

5.6 Direct Product of Groups

In this section, we present a method to construct a new group from existing ones. Starting with two groups $(G_1, *)$ and $(G_2, \cdot)$, one can construct a new group whose underlying set is the Cartesian product of G_1 and G_2, and whose binary operation is defined using $*$ and $\cdot$. We refer the reader to Definition 1.1.19 of the Cartesian product of two sets.

Definition 5.6.1 Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. The direct product of G_1 and G_2 is the set $G_1 \times G_2$ endowed with the operation $\cdot$ defined as

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \cdot b_2)$$

for any $a_1, a_2 \in G_1$ and $b_1, b_2 \in G_2$.

Theorem 5.6.2 *The direct product of two groups is a group.*

Proof Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, clearly $\cdot$ is a binary operation on $G_1 \times G_2$. To show that $\cdot$ is associative, let (a_1, b_1), (a_2, b_2), (a_3, b_3) be elements in $G_1 \times G_2$, then

$$\begin{aligned}((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 * a_2, b_1 \cdot b_2) \cdot (a_3, b_3)\\ &= ((a_1 * a_2) * a_3, (b_1 \cdot b_2) \cdot b_3)\\ &= (a_1 * (a_2 * a_3), b_1 \cdot (b_2 \cdot b_3))\\ &= (a_1, b_1) \cdot (a_2 * a_3, b_2 \cdot b_3)\\ &= (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)).\end{aligned}$$

For the identity element, let $e = (e_1, e_2) \in G_1 \times G_2$ where e_1, e_2 are the identity elements in G_1, G_2 respectively. It is straightforward to show that

$$(a, b) \cdot (e_1, e_2) = (a, b) = (e_1, e_2) \cdot (a, b)$$

for each $(a, b) \in G_1 \times G_2$. Finally, let (a, b) be any element in $G_1 \times G_2$. Since G_1, G_2 are groups, then

$$\begin{aligned}(a, b) \in G_1 \times G_2 &\Rightarrow a \in G_1 \ \wedge \ b \in G_2\\ &\Rightarrow a^{-1} \in G_1 \ \wedge \ b^{-1} \in G_2.\\ &\Rightarrow \left(a^{-1}, b^{-1}\right) \in G_1 \times G_2\end{aligned}$$

Thus, there exists an element in $G_1 \times G_2$ such that

$$(a, b) \cdot \left(a^{-1}, b^{-1}\right) = \left(a^{-1}, b^{-1}\right) \cdot (a, b) = (e_1, e_2)$$

i.e., (a, b) is an invertible element in $G_1 \times G_2$. ■

Note that

- The direct product of abelian groups is abelian. In fact, $(G_1 \times G_2, \cdot)$ is an abelian group if and only if $(G_1, *)$ and $(G_2, \cdot)$ are both abelian (Check!).
- By definition, $\text{ord}(G_1 \times G_2) = \text{ord}(G_1)\text{ord}(G_2)$.
- If $(a, b) \in G_1 \times G_2$ such that $\text{ord}(a), \text{ord}(b) < \infty$, then

$$\text{ord}((a, b)) < \infty \text{ and } \text{ord}((a, b)) = \text{lcm}(\text{ord}(a), \text{ord}(b))$$

(Exercise 5.32)

- If G_1 and G_2 are two groups having exponents, then

$$\exp(G_1 \times G_2) = \operatorname{lcm}(\exp(G_1), \exp(G_2)) \quad \text{(Exercise 5.15).}$$

Definition 5.6.1 can be easily generalized to the direct product of n groups, and one can show that the direct product of n groups is a group.

Example 5.6.3

1. Let $G_1 = G_2 = (\mathbb{R}, +)$. The direct product $G_1 \times G_2$ consists of the set $\{(a, b) : a, b \in \mathbb{R}\}$ endowed with the operation $\cdot$ defined by $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. i.e., the direct product $G_1 \times G_2$ is the plane $\mathbb{R}^2$ endowed with the sum on $\mathbb{R}^2$. This product has an infinite order and no exponent.
2. The direct product of the three groups $(\mathbb{Z}_2, \oplus_2)$, $(\mathbb{Z}_6, \oplus_6)$, and $(\mathbb{Z}_{11}, \oplus_{11})$ has its underlying set $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{11}$ with the following operation

$$([a_1],[b_1],[c_1]) \cdot ([a_2],[b_2],[c_2]) = ([a_1] \oplus_2 [a_2], [b_1] \oplus_6 [b_2], [c_1] \oplus_{11} [c_2])$$

for each $([a_1],[b_1],[c_1])$ and $([a_2],[b_2],[c_2])$ in $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{11}$. This group is finite whose order is 132. Using the results in Example 5.5.16 (5) and Exercise 5.15, one can obtain

$$\operatorname{Exp}(\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{11}) = \operatorname{lcm}(2, 6, 11) = 66.$$

3. The groups $\mathbb{Z}_n$ and $\mathbb{Z}_n \times \mathbb{Z}_n$ have the same exponent n.
4. The infinite product of the additive groups $\mathbb{Z}_3$ is an example of an infinite group, where the order of any element is finite. The exponent of the group of infinite product of $\mathbb{Z}_3$ equals 3.

If $(G_1, *)$ and $(G_2, \cdot)$ are two groups, then the direct product of G_1 and G_2 is not the only group whose underlying set is $G_1 \times G_2$. The groups in the following examples have $G_1 \times G_2$ as underlying set, but are not the direct product of G_1 and G_2.

Example 5.6.4 Consider the two groups $(\mathbb{Z}, +)$ and $(\{-1, 1\}, \cdot)$, where $+$, and$\cdot$ represent the addition and multiplication of integers, respectively. Let $G = \mathbb{Z} \times \{-1, 1\}$ and define $*$ on G by

$$(m, \alpha) * (n, \beta) = (m + \alpha\, n, \alpha\beta) \quad \forall\, m, n \in \mathbb{Z}, \quad \forall\, \alpha, \beta \in \{-1, 1\}.$$

The set G endowed with $*$ forms a group. However, it is not the direct product for the two groups $(\mathbb{Z}, +)$ and $(\{-1, 1\}, \cdot)$. We verify that G is a group as follows:

If (m, α), (n, β) are arbitrary elements in G, then $m, n \in \mathbb{Z}$ and $\alpha, \beta \in \{-1, 1\}$. Therefore, $m + \alpha\, n \in \mathbb{Z}$, $\alpha\beta \in \{-1, 1\}$, and $(m + \alpha\, n, \alpha\beta) \in G$. That is, $*$ is a binary operation on G. To show that $*$ is associative, let (m, α), (n, β), $(r, \gamma) \in G$, then

$$\begin{aligned}(m,\alpha)*((n,\beta)*(r,\gamma)) &= (m,\alpha)*(n+\beta r, \beta\gamma)\\ &= (m+\alpha(n+\beta r), \alpha(\beta\gamma))\\ &= (m+(\alpha\, n+\alpha(\beta r)), (\alpha\beta)\gamma)\\ &= ((m+\alpha\, n)+(\alpha\beta)r, (\alpha\beta)\gamma)\\ &= (m+\alpha\, n, \alpha\beta)*(r,\gamma)\\ &= ((m,\alpha)*(n,\beta))*(r,\gamma).\end{aligned}$$

To find the identity element in G, assume that (e_1, e_2) is an element in G such that

$$(m,\alpha)*(e_1,e_2) = (m+e_2e_1, \alpha\, e_2) = (m,\alpha).$$

Solving the equations $m + e_2e_1 = m, \alpha\, e_2 = \alpha$ yields $e_2 = 1 \wedge e_1 = 0$. One can easily check that $(1, 0)$ is an element in G and satisfies that $(m,\alpha)*(0,1) = (0,1)*(m,\alpha) = (m,\alpha)$ for all (m,α) in G, i.e., $(0, 1)$ is the identity element in G. Finally, let $(m,\alpha) \in G$. To find its inverse, assume that (n,β) is an element in G such that

$$(m,\alpha)*(n,\beta) = (n,\beta)*(m,\alpha) = (0,1).$$

This result implies that $m + \alpha\, n = 0 \wedge \alpha\beta = 1$. i.e., $n = -m/\alpha = -m\,\alpha, \beta = 1/\alpha = \alpha$. Clearly, $(-m\,\alpha, \alpha)$ is the inverse of (m,α) (verify!). Hence, $(G,*)$ is a group.

The direct product of $(\mathbb{Z}, +)$ and $(\{-1, 1\}, \cdot)$ has the same underlying set of G, but the operation is different. The operation in the direct product is defined by

$$(m,\alpha)\cdot(n,\beta) = (m+n, \alpha\beta) \quad \forall\, m,n \in \mathbb{Z}, \quad \forall\, \alpha,\beta \in \{-1,1\}.$$

Under this operation, the inverse of (m,α) is $(-m,\alpha)$ which is different than the inverse of (m,α) under $*$ defined above.

Example 5.6.5 Let $G_1 = G_2 = (\mathbb{R}^*, \cdot)$, $G_3 = (\mathbb{R}, +)$ and $G = \{(a,b,c) : a,b,c \in \mathbb{R} \wedge a,b \neq 0\}$. Define the operation $*$ on G by

$$(a_1,b_1,c_1)*(a_2,b_2,c_2) = (a_1a_2, b_1b_2, a_1c_2 + c_1b_2)$$

$(G,*)$ is an example of a group formed by three groups, but it is not the direct product of them. Note that the identity element in G is $e = (1,1,0)$ and the inverse of any element (a,b,c) in G is of the form $(1/a, 1/b, -c/ab)$ which is an element in G.

Exercises

Solved Exercises

5.1 Let X be a nonempty set and $G = \mathcal{P}(X)$.

a. On the elements of G, define $*$ as the intersection. i.e., $A * B = A \cap B$ for $A, B \in G$. Is $(G, *)$ a group? Is it abelian?
b. If $*$ was the union of sets, i.e., $A * B = A \cup B$ for $A, B \in G$, does the answer for (a) change? Explain.

Solution:

a. Verifying that $*$ is a commutative and associative binary operation on G is easy and left to the reader. For any $A \in G$, $A \cap X = X \cap A = A$. Hence, X is the identity element in G. However, $\emptyset \in G$ satisfies $\emptyset \cap B = \emptyset \neq X$ for all $B \in G$, so $\emptyset$ has no inverse in G. Thus, $(G, \cap)$ is not a group.
b. If $*$ in (a) is replaced by the union of sets, then $*$ is a commutative and associative binary operation on G. For any $A \in G$, $A \cup \emptyset = \emptyset \cup A = A$. Hence, $\emptyset$ is the identity element in G. However, for the set X, X is an element in G, and

$$X \cup B = X \neq \emptyset \text{ for all } B \in G,$$

thus, X has no inverse in G, and $(G, \cup)$ is not a group.

5.2 On $\mathbb{R}$, define $*$ by

$$x * y = 5 + 5x + 5y + 4xy \text{ for all } x, y \in \mathbb{R}.$$

Show that $(\mathbb{R}, *)$ is a commutative monoid. Is $(\mathbb{R}, *)$ a group? If $(\mathbb{R}, *)$ is not a group, find the invertible elements in $(\mathbb{R}, *)$.

Solution:

For all $x, y \in \mathbb{R}$, the element $x * y$ defines a unique element in $\mathbb{R}$. i.e., the operation $*$ is a binary operation on $\mathbb{R}$. The operation is associative as

$$\begin{aligned}(x * y) * z &= 5 + 5(5 + 5x + 5y + 4xy) + 5z + 4(5 + 5x + 5y + 4xy)z \\ &= 30 + 25(x + y + z) + 20(xy + xz + yz) + 16xyz\end{aligned}$$

and

$$\begin{aligned}x * (y * z) &= 5 + 5x + 5(5 + 5y + 5z + 4yz) + 4x(5 + 5y + 5z + 4yz) \\ &= 30 + 25(x + y + z) + 20(xy + xz + yz) + 16xyz.\end{aligned}$$

Thus, $(\mathbb{R}, *)$ is a semigroup. The semigroup $(\mathbb{R}, *)$ is commutative since $x * y = y * x$ for all $x, y \in \mathbb{R}$. To find a candidate identity, we need to solve the following equation for e

$$x = e * x = 5 + 5e + 5x + 4ex \text{ for all } x \in \mathbb{R}.$$

This expression is equivalent to $(1+e)(4x+5)=0$ for all $x\in\mathbb{R}$. As $4x+5=0$ does not hold for all $x\in\mathbb{R}$, $1+e$ must be zero, i.e., $e=-1$. Substituting in the definition of the operation $*$, yields

$$x*(-1)=(-1)*x=x \text{ for all } x\in\mathbb{R}.$$

Thus, -1 serves as an identity element in $(\mathbb{R},*)$. To check the invertible elements in $(\mathbb{R},*)$, consider an arbitrary element x in $\mathbb{R}$. If x is invertible, then there exists $y\in\mathbb{R}$ such that

$$x*y=y*x=-1.$$

As the operation is commutative, it is enough to search for y such that $x*y=-1$. Finding such y is equivalent to solving $5+5x+5y+4xy=-1$ for y. Now

$$5+5x+5y+4xy=-1\Leftrightarrow(5+4x)y=-5x-6\Leftrightarrow y=(-6-5x)/(5+4x)$$

which undefined when $x=-5/4$. Thus, $-5/4$ is not an invertible element in $(\mathbb{R},*)$. For all other values of x, the inverse of x is $(-6-5x)/(5+4x)\in\mathbb{R}$. Therefore, $\mathrm{Inv}((\mathbb{R},*))=\mathbb{R}\backslash\{-5/4\}$, and $(\mathbb{R},*)$ is not a group.

5.3 Consider the subset of real numbers $\mathbb{Q}\left[\sqrt{5}\right]=\left\{a+b\sqrt{5}:a,b\in\mathbb{Q}\right\}$ endowed with the usual multiplication of real numbers, i.e.,

$$\left(a+b\sqrt{5}\right)\cdot\left(c+d\sqrt{5}\right)=(ac+5bd)+(ad+bc)\sqrt{5}.$$

Show that $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$ is a commutative monoid but is not a group. Determine the invertible element in $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$.

Solution:

Note first that $(\mathbb{R},\cdot)$ is a commutative monoid (Example 4.2.5 (3)). Let $a+b\sqrt{5}$ and $c+d\sqrt{5}$ be two elements in $\mathbb{Q}\left[\sqrt{5}\right]$. Since

$$(a+b\sqrt{5})\cdot(c+d\sqrt{5})=(ac+5bd)+(ad+bc)\sqrt{5}\in\mathbb{Q}[\sqrt{5}]$$

then $\mathbb{Q}\left[\sqrt{5}\right]$ is a closed under the operation of $(\mathbb{R},\cdot)$, The subset $\mathbb{Q}\left[\sqrt{5}\right]$ inherits associativity from $\mathbb{R}$, and the integer $1=1+0\sqrt{5}$ is the identity element in $\mathbb{Q}\left[\sqrt{5}\right]$. Thus, $\mathbb{Q}\left[\sqrt{5}\right]$ is a monoid with identity 1. The monoid $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$ is commutative as the multiplication is commutative. For any element $a+b\sqrt{5}$ in $\mathbb{Q}\left[\sqrt{5}\right]$,

$$\left(a+b\sqrt{5}\right)\cdot\left(0+0\sqrt{5}\right)=0+0\sqrt{5}=0\neq 1,$$

and thus, the zero is not invertible in $\mathbb{Q}\left[\sqrt{5}\right]$, and $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$ is not a group. To determine the invertible elements in $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$, let $a+b\sqrt{5}\neq 0$ be an element in $\left(\mathbb{Q}\left[\sqrt{5}\right],\cdot\right)$. The element $a+b\sqrt{5}$ is invertible if and only if there exists $c+d\sqrt{5}$ belongs to $\mathbb{Q}\left[\sqrt{5}\right]$ such that

$$\left(a+b\sqrt{5}\right)\left(c+d\sqrt{5}\right)=1.$$

This holds if and only if

$$(ac+5bd)+(bc+ad)\sqrt{5}=1$$

i.e.,

$$ac+5bd=1\wedge bc+ad=0$$

i.e., if and only if

$$c=\frac{-a}{5b^2-a^2},\quad d=\frac{b}{5b^2-a^2}.$$

For c, d to be elements in $\mathbb{Q}$, $5b^2-a^2$ must not be zero. Since $\sqrt{5}$ is irrational, for $a, b\in\mathbb{Q}$, the equality $5b^2-a^2=0$ holds if and only if $a=b=0$. Thus, every nonzero element in $\mathbb{Q}\left[\sqrt{5}\right]$ is invertible, and $\mathrm{Inv}\left(\mathbb{Q}\left[\sqrt{5}\right]\right)=\mathbb{Q}\left[\sqrt{5}\right]\backslash\{0\}$.

5.4 Consider the subset of real numbers

$$\mathbb{Z}\left[\sqrt{5}\right]=\left\{a+b\sqrt{5}:a,b\in\mathbb{Z}\right\}$$

endowed with the usual multiplication of real numbers. Show that $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$ is a monoid. Is $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$ a group? Determine the invertible element in $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$.

Solution:

One can show that $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$ is a commutative monoid following the steps used in the solution of Exercise 5.3. To determine the invertible elements in $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$, let $a+b\sqrt{5}$ be an arbitrary element in $\left(\mathbb{Z}\left[\sqrt{5}\right],\cdot\right)$. The element $a+b\sqrt{5}$ is invertible if and only if there exists $c+d\sqrt{5}$ in $\mathbb{Z}\left[\sqrt{5}\right]$ such that $\left(a+b\sqrt{5}\right)\left(c+d\sqrt{5}\right)=1$. That is, if and only if $(ac+5bd)+(bc+ad)\sqrt{5}=1$. i.e., $ac+5bd=1\wedge bc+ad=0$.

That is, if and only if

$$c=\frac{-a}{5b^2-a^2},\quad d=\frac{b}{5b^2-a^2}.$$

For c,d to be elements in $\mathbb{Z}$, the expression $5b^2-a^2$ must not be zero and divides both a and b. i.e., $a\neq 0, b\neq 0\wedge\left(5b^2-a^2\right)$ divides $\gcd(a,b)$. Therefore,

$$\operatorname{Inv}\left(\mathbb{Z}\left[\sqrt{5}\right]\right)=\left\{a+b\sqrt{5}:a\neq 0,b\neq 0\wedge\left(5b^2-a^2\right)\mid\gcd(a,b)\right\}.$$

5.5 Let $n\in\mathbb{N}$. Show that $U(\mathbb{C})$, the set of all upper matrices in $\mathcal{M}_n(\mathbb{C})$ (Definition 1.6.3) forms a noncommutative monoid under matrix multiplication, but not a group.

Solution:

Let $A=\left(a_{ij}\right)$, $B=\left(b_{ij}\right)$ be two arbitrary matrices in $U(\mathbb{C})$. The coefficients a_{ij} and b_{ij} satisfy $a_{ij}=b_{ij}=0\quad\forall\, i>j$. If $i>j$, the entry of their product c_{ij} is

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}\underbrace{=}_{a_{ik}=0\text{ for all }i>k}\sum_{k=i}^{n}a_{ik}b_{kj}\underbrace{=}_{b_{kj}=0\text{ for all }k>jk>i>j}0.$$

That is $A\cdot B=\left(c_{ij}\right)$ with $c_{ij}=0$ for each $i>j$, and $U(\mathbb{C})$ is a closed under the operation of $(\mathcal{M}_n(\mathbb{C}),\cdot)$. The associativity is inherited from the semigroup $(\mathcal{M}_{\mathrm{n}}(\mathbb{C}),\cdot)$. Therefore, $(U(\mathbb{C}),\cdot)$ is a semigroup. This semigroup is a monoid since I_n is an upper triangular matrix and is the identity element in $U(\mathbb{C})$. As both

$$A_1=\begin{pmatrix}1&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\cdots&\vdots\\0&0&\cdots&0\end{pmatrix}\text{ and }A_2=\begin{pmatrix}0&0&\cdots&1\\0&0&\cdots&1\\\vdots&\vdots&\cdots&\vdots\\0&0&\cdots&1\end{pmatrix}$$

Table 5.7 Operation on S

Δ	a	b	c
a	c	a	a
b	a	c	b
c	a	b	c

are elements in $U(\mathbb{C})$ for each n, and

$$A_1 \cdot A_2 = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = A_2 \cdot A_1,$$

then $(U(\mathbb{C}), \cdot)$ is not commutative. The zero matrix is an upper triangular matrix that has no multiplicative inverse, and thus $(U(\mathbb{C}), \cdot)$ is not a group.

5.6 Consider the set $S = \{a, b, c\}$ and the operation Δ defined in Table 5.7

1. Is (S, Δ) a monoid? If yes, what is the identity element? Is Δ commutative?
2. Find the inverse of each element if it exists.

Solution:

1. One can easily check, using the table, that the operation Δ is binary, associative, and commutative. Therefore, (S, Δ) is a commutative semigroup. Clearly, c is an identity element of S with respect to Δ.
2. As

$$a\Delta a = b\Delta b = c\Delta c = c,$$

then

$$a = a^{-1}, \quad b = b^{-1}, \quad c = c^{-1}.$$

5.7 Let $n \geq 3$ be an integer. Consider the additive group $\mathbb{Z}_n$ and let

$$G = \{([a], [b], [c]) : [a], [b], [c] \in \mathbb{Z}_n\}.$$

On G define the operation $*$ as follows

$$([a], [b], [c]) * \left([a'], [b'], [c']\right) = \left([a + a'], [b + b'], [c + c' - ba']\right).$$

Show that G is a nonabelian group.

Solution:

Let $[a], [b], [c]$ be arbitrary elements in $\mathbb{Z}_n$. Since $\left[a+a'\right]$, $\left[b+b'\right]$ and $\left[c+c'-ba'\right]$ are elements in $\mathbb{Z}_n$, then $([a],[b],[c]) * \left(\left[a'\right],\left[b'\right],\left[c'\right]\right)$ is an element in G. To verify the well-defined property of the operation $*$, let $([a],[b],[c])$, $\left(\left[a'\right],\left[b'\right],\left[c'\right]\right)$, $([e],[f],[g])$, and $\left(\left[e'\right],\left[f'\right],\left[g'\right]\right)$ be elements in G such that

$$([a],[b],[c]) = ([e],[f],[g]) \text{ and } \left(\left[a'\right],\left[b'\right],\left[c'\right]\right) = \left(\left[e'\right],\left[f'\right],\left[g'\right]\right).$$

Since $\oplus_n$ and $\otimes_n$ are well-defined operations on $\mathbb{Z}_n$, then

$$\left[a+a'\right] = \left[e+e^{'}\right], \left[b+b'\right] = \left[f+f^{'}\right] \text{ and } \left[c+c'-ba'\right] = \left[g+g'-fe'\right].$$

Therefore,

$$\left(\left[a+a'\right],\left[b+b'\right],\left[c+c'-ba'\right]\right) = \left(\left[e+e'\right],\left[f+f'\right],\left[g+g'-fe'\right]\right)$$

which means that

$$([a],[b],[c]) * \left(\left[a'\right],\left[b'\right],\left[c'\right]\right) = ([e],[f],[g]) * \left(\left[e'\right],\left[f'\right],\left[g'\right]\right)$$

and $*$ is a binary operation on G. It is straightforward to show that $*$ is associative (left to the reader). The element $([0],[0],[0])$ is the identity element in G, as

$$([a],[b],[c]) * ([0],[0],[0]) = ([a],[b],[c]) = ([0],[0],[0]) * ([a],[b],[c]),$$

for all $([a],[b],[c])$ in G.

Let $([a],[b],[c])$ be arbitrary element in G, the triple $([n-a],[n-b],[n-c-ba])$ is an element in G that satisfies

$$\begin{aligned}([a],[b],[c]) * ([n-a],[n-b],[n-c-ba]) &= ([n],[n],[n(1-b)]) \\ &= ([0],[0],[0]).\end{aligned}$$

and

$$([n-a],[n-b],[n-c-ba]) * ([a],[b],[c]) = ([0],[0],[0]).$$

Therefore, $([a],[b],[c])$ is invertible and G is a group. The group G is not abelian as

$$\begin{aligned}([1],[1],[0]) * ([0],[1],[1]) &= ([1],[2],[1]) \\ &\neq ([1],[2],[0]) = ([0],[1],[1]) * ([1],[1],[0]).\end{aligned}$$

The group $(G, *)$ is an example of a group whose underlying set is the Cartesian product $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$, but it is not the direct product of the additive groups $(\mathbb{Z}_n, \oplus_n)$.

5.8 Let G be a group and $a, b \in G$ such that $a*b \in C(G)$. Show that $a*b = b*a$. i.e., if $a * b$ is in the center, then a, b commute.

Solution:

If a, b are elements in G such that $a * b \in C(G)$, then

$$\begin{aligned} b * a &= (a^{-1} * a) * (b * a) = a^{-1} * (a * b) * a \\ &= a^{-1} * a * (a * b) = e * (a * b) = a * b. \end{aligned}$$

5.9 Let $(G, *)$ be a group. Show that for any a, b in G and $n \in \mathbb{Z}$,

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

Solution:

The proof is done by induction on $n \geq 0$, as follows

Base step: The statement is true for $n = 0$ since

$$(a^{-1} * b * a)^0 = e = a^{-1} * a = a^{-1} * b^0 * a.$$

Inductive step: Assume that the statement is true for n, i.e.,

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

For $n + 1$,

$$\begin{aligned} (a^{-1} * b * a)^{n+1} &= (a^{-1} * b * a)^n * \left(a^{-1} * b * a\right) \\ &= \left(a^{-1} * b^n * a\right) * \left(a^{-1} * b * a\right) = a^{-1} * b^n * \left(a * a^{-1}\right) * b * a \\ &= a^{-1} * b^n * b * a = a^{-1} * b^{n+1} * a. \end{aligned}$$

Thus, by induction, the statement is true for $n \geq 0$. For a negative integer n, the integer $-n$ is positive, and thus,

$$\begin{aligned} \left(a^{-1} * b * a\right)^n &= \left(\left(a^{-1} * b * a\right)^{-1}\right)^{-n} = (a^{-1} * b^{-1} * a)^{-n} \\ &= a^{-1} * (b^{-1})^{-n} * a = a^{-1} * b^n * a. \end{aligned}$$

5.10 Let G be any group. On G, define the relation $\sim$ by

$$a \sim b \quad \text{if and only if} \quad \exists\, x \in G \ni a = x * b * x^{-1}.$$

Show that $\sim$ is an equivalence relation of G, and describe its equivalence classes.

Solution:

1. The relation $\sim$ is reflexive: Let a be an arbitrary element in G. As $e \in G$ and $a = e * a * e^{-1}$, then $a \sim a$.
2. The relation $\sim$ is symmetric: Let a, b be elements in G such that $a \sim b$. By the definition of $\sim$, there exists $x \in G$, such that $a = x * b * x^{-1}$. Let $y = x^{-1} \in G$, y satisfies $b = y * a * y^{-1}$. Therefore, $b \sim a$.
3. The relation $\sim$ is transitive: Let a, b, c be arbitrary elements in G. If $a \sim b$ and $b \sim c$, then there exist x, y in G such that

$$a = x * b * x^{-1} \text{ and } b = y * c * y^{-1}.$$

As G is a group, $x * y$ is an element in G. One can easily check that

$$a = (x * y) * c * (x * y)^{-1}$$

Thus, $a \sim c$.

Therefore, the relation $\sim$ is an equivalence relation on G. The equivalence classes of such relations divide G into disjoint subsets, each of the in the form $[a] = \left\{x * a * x^{-1} : x \in G\right\}$ where $a \in G$.

5.11 Let $(G, *)$ be a group. For any a, b in G, prove the following statements:

1. $\text{ord}(a * b)$ is finite if and only if $\text{ord}(b * a)$ is finite.
2. $\text{ord}(a * b) = \text{ord}(b * a)$.
3. $\text{ord}\left(a * b * a^{-1}\right) = \text{ord}(b)$.

Solution:

1. Assume that $\text{ord}(a * b) = n$. Using the result of Exercise 5.9, we obtain

$$(b * a)^n = (a^{-1} * (a * b) * a)^n = a^{-1} * (a * b)^n * a = e.$$

Lemma 5.5.5 implies that $b * a$ has a finite order. Similarly, one can show that the other direction holds.

2. If $\text{ord}(a * b)$ is infinite, then by (1), $\text{ord}(b * a)$ is also infinite, and the equality holds in this case. Assume that $\text{ord}(a * b) = n < \infty$, then $\text{ord}(b * a) = m < \infty$. Using the argument as in (1), we obtain $(b*a)^n = e$. Lemma 5.5.6 implies that m divides n. Similarly, one can show that $(a * b)^m = e$ and n divides m. Therefore, by Proposition 2.2.5 (3),

$$n = |n| = |m| = m.$$

3. Let $x = a * b$ and $y = a^{-1}$. By the identity in (2), $\operatorname{ord}(x * y) = \operatorname{ord}(y * x)$, which implies that

$$\begin{aligned}\operatorname{ord}\left(a * b * a^{-1}\right) &= \operatorname{ord}(x * y) = \operatorname{ord}(y * x)\\ &= \operatorname{ord}\left(a^{-1} * a * b\right) = \operatorname{ord}(b).\end{aligned}$$

5.12 Let G be a group and a, b be elements in G that commute. If $\operatorname{ord}(a) = 144$ and $\operatorname{ord}(b) = 7$, what is the order of $a * b$?

Solution:

Since $\gcd(\operatorname{ord}(a), \operatorname{ord}(b)) = \gcd(144, 7) = 1$, by Proposition 5.5.11,

$$\operatorname{ord}(a * b) = \operatorname{ord}(a)\operatorname{ord}(b) = 144 \times 7 = 1008.$$

5.13 Let $(G, *)$ be a group and k be an integer such that $k > 2$, show that the group G cannot contain exactly one element of order k.

Solution:

Let $a \in G$ and $\operatorname{ord}(a) = k > 2$. The inverse of a is an element in G, where

$$\operatorname{ord}\left(a^{-1}\right) = \operatorname{ord}(a) = k.$$

Since $a * a^{k-1} = a^k = e$, then $a^{-1} = a^{k-1} \neq a$ is another element in G whose order is k.

5.14 Let G be a group and $b \in G$. If b is the only element of order 2, then b must be in the center of G.

Solution:

Let $b \in G$ such that b is the only element of order 2. Since the order b is 2, then $b \neq e$. For any $a \in G$, $\left(a * b * a^{-1}\right)^2 = a * b^2 * a^{-1} = e$. As $b \neq e$, then $a * b * a^{-1} \neq e$ and $\operatorname{ord}\left(a * b * a^{-1}\right) = 2$. However, as b is the only element in G of order 2, then $a * b * a^{-1} = b$, which implies that result.

5.15 Let G_1 and G_2 be two groups. Show that if both G_1 and G_2 have exponents, then

$$\operatorname{Exp}(G_1 \times G_2) = \operatorname{lcm}(\operatorname{Exp}(G_1), \operatorname{Exp}(G_2)).$$

Solution:

Let $m = \operatorname{Exp}(G_1 \times G_2)$ and $k = \operatorname{lcm}(\operatorname{Exp}(G_1), \operatorname{Exp}(G_2))$. If (a_1, a_2) is an arbitrary element in $G_1 \times G_2$, then

$$(a_1, a_2)^k = \left(a_1^k, a_2^k\right) = (e_1, e_2)$$

which implies that $m \leq k$. On the other hand, as

$$(a_1, a_2)^m = \left(a_1^m, a_2^m\right) = (e_1, e_2) \text{ for each } (a_1, a_2) \text{ in } G_1 \times G_2.$$

then $a_1^m = e_1$ for each a_1 in G_1 and $a_2^m = e_2$ for each a_2 in G_2, which implies that m is a multiple of $\mathrm{Exp}(G_1)$ and $\mathrm{Exp}(G_2)$. Since k is the least common multiple of $\mathrm{Exp}(G_1)$ and $\mathrm{Exp}(G_2)$, then $k \leq m$. Therefore, $k = m$.

Unsolved Exercises

5.16 Consider the open interval of real numbers $(-1, 1)$. Let $G = ((-1, 1), *)$ where $*$ is defined as $a * b = (a + b)/(1 + ab)$. Show that G forms a group under $*$.

5.17 On the set of integers, define the operation $*$ by $a * b = 0$ for all $a, b \in \mathbb{Z}$. Does $(\mathbb{Z}, *)$ form a group? Explain.

5.18 Consider the subset of real numbers $\mathbb{Z}\left[-\sqrt{5}\right] = \left\{a - b\sqrt{5} : a, b \in \mathbb{Z}\right\}$ with the usual multiplication of real numbers. Does $\left(\mathbb{Z}\left[-\sqrt{5}\right], *\right)$ form a group? Explain your answer.

5.19 Let $i = \sqrt{-1}$. Consider the subset of real numbers $\mathbb{Q}[i] = \{a + ib : a, b \in \mathbb{Q}\}$ endowed with the usual multiplication of complex numbers. Show that $(\mathbb{Q}[i], \cdot)$ is a monoid. Explain why $(\mathbb{Q}[i], \cdot)$ is not a group and determine the set of invertible elements in $(\mathbb{Q}[i], \cdot)$.

5.20 Let $n \in \mathbb{N}$. Show that $\mathcal{U}(n) = \{A \in M_n(\mathbb{C}) : A^*A = AA^* = I_n\}$ forms a group under matrix multiplication, where A^* is the Hermitian conjugate of A (Definition 1.6.16). The group $\mathcal{U}(n)$ is called the unitary group of order n.

5.21 Let $(G, *)$ be a group, A be any set, and $f : A \to G$ be a bijection. Define on A by $a.b = f^{-1}(f(a) * f(b))$. Show that $(A, \cdot)$ is a group with identity $e_A = f^{-1}(e_G)$ and $a^{-1} = f^{-1}\left(f(a)^{-1}\right)$. If $G = (\mathbb{R}^*, \cdot)$, $A = \mathbb{R}\backslash\{-1/2\}$, and $f : A \to G$ is given by $f(a) = 4a + 2$. Show that the operation on A is given by $a \cdot b = 4ab + 2a + 2b + \frac{1}{2}$, and compute the identity and inverse of any element in A.

5.22 Write Cayley's table for each of the additive groups $(\mathbb{Z}_5, \oplus_5)$ and $(\mathbb{Z}_8, \oplus_8)$.

5.23 Find the invertible elements and their inverses in the following monoids:

$$(\mathbb{Z}_9, \otimes_9) \text{ and } (\mathbb{Z}_{13}, \otimes_{13}).$$

5.24 Let $(G, *)$ be a group. Show that the following statements are equivalent

1. $(a * b)^n = a^n * b^n \quad \forall\, a, b \in G, \ \forall\, n \in \mathbb{N}.$
2. $(a * b)^2 = a^2 * b^2 \quad \forall\, a, b \in G.$

5.25 Let $(G, *)$ be a group, and $m \in \mathbb{N}$. The elements $a_1, a_2, \ldots, a_m$ of G are said to pairwise commute if a_i, a_j commute for all $1 \leq i, j \leq m$. Show that if $a_1, a_2, \ldots, a_m$ pairwise commute elements in G, then $(a_1 * a_2 * \cdots * a_m)^n = a_1^n * a_2^n * \cdots * a_m^n$ for all positive integer n.

5.26 Let G be a group and $a \in G$ such that $\operatorname{ord}(a) = p$ for some prime p. Show that $\operatorname{ord}\left(a^k\right) = p$ for each $1 \le k < p$.

5.27 Let G be a group and $a \in G$, show that if $\operatorname{ord}(a) = k < \infty$, then the elements of the set $\left\{e, a, a^2, \ldots, a^{k-1}\right\}$ are all distinct.

5.28 Give an example (different than that in Example 5.5.16 (4)) for an infinite group that has an exponent.

5.29 Let G be any group. For any integers m_1, m_2, show that $m_1 | m_2 \Rightarrow G[m_1] = G[m_2]$ where $G[m] = \{a \in G : a^m = e\}$.

5.30 Find the direct product of the following groups:

a. $(\mathbb{Z}_9, \oplus_9)$ and $(\mathbb{Z}_{13}^*, \otimes_{13})$.
b. $(\mathbb{Z}_3, \oplus_3)$ and $(\mathbb{Z}_5, \oplus_5)$.
c. $(\mathbb{Z}_5^*, \otimes_5)$ and $(\mathbb{Z}_7^*, \otimes_7)$.
d. $(\mathbb{R}^*, \cdot)$ and $(\mathbb{R}, +)$.
e. $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$.

5.31 Let G_1, G_2 be groups. Show that if $(a, b) \in G_1 \times G_2$ such that $\operatorname{ord}(a), \operatorname{ord}(b) < \infty$, then $\operatorname{ord}((a, b)) < \infty$ and $\operatorname{ord}((a, b)) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$.

Reference

Burton, D. M. (2007). *Elementary number theory*. McGraw-Hill.

Chapter 6
The Symmetric Group "An Example of Finite Nonabelian Group"

This chapter discusses the group $\mathfrak{S}_n$ (Corollary 5.1.11), the symmetric group on n elements, which is one of the most important examples of finite groups and is widely used in applications to geometry and physics (Carter, 2009). The importance of symmetry groups in abstract algebra is due to the fact that for any finite group G, there is a symmetric group $\mathfrak{S}_n$ that contains a copy of G. For each $n \in \mathbb{N}$, the group $\mathfrak{S}_n$ consists of all the bijective maps of $\{1, 2, \ldots, n\}$ to itself, called permutations of $\{1, 2, \ldots, n\}$. These permutations are usually denoted by symbols such as ϕ and ψ. The identity permutation that corresponds to the identity map of $\{1, 2, \ldots, n\}$ is denoted by e. In this chapter, Sect. 6.1 provides a representation of the elements of $\mathfrak{S}_n$ as matrices and specifies the order of $\mathfrak{S}_n$ in terms of the integer n. Additionally, the notion of pairwise disjoint permutations is discussed, and their commutativity is verified. In Sect. 6.2, cycles, a special case of permutations, are defined and studied. The main result of this section is Proposition 6.2.9, which states that any permutation can be written as a finite product of disjoint cycles. The proof of this proposition requires a study of orbits of a permutation which discussed in Sect. 6.3 and followed by the proof of Proposition 6.2.9. The last two sections of this chapter discuss methods for determining the order of permutations and classifying permutations as odd and even.

6.1 Matrix Representation of Permutations

Let $n \in \mathbb{N}$. Each permutation ϕ of $\{1, 2, \ldots, n\}$ can be represented using a $2 \times n$ matrix. The first row of the matrix lists elements of the domain of the permutation. The images are represented in the second row with the image $\phi(i)$ placed directly under i, for each $1 \leq i \leq n$. i.e., the matrix representation of a permutation ϕ is

$$\phi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \phi(1) & \phi(2) & \phi(3) & \cdots & \phi(n) \end{pmatrix}.$$

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_6

For example, if $n = 4$, the permutation $\phi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{pmatrix}$ is the map determined by

$$\phi(1) = 3, \phi(2) = 1, \phi(3) = 4, \text{ and } \phi(4) = 2.$$

The matrix representation of the identity permutation e is

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

Remark 6.1.1 The elements in the first row in the matrix representation of ϕ can be written in any order; however, the images of the elements must be carefully arranged in the second row, ensuring that the image of any element i must be exactly below i. For example, all of the following matrices represent the same permutation:

$$\begin{pmatrix} 2\ 1\ 4\ 3 \\ 1\ 3\ 2\ 4 \end{pmatrix}, \begin{pmatrix} 1\ 3\ 2\ 4 \\ 3\ 4\ 1\ 2 \end{pmatrix}, \begin{pmatrix} 1\ 4\ 2\ 3 \\ 3\ 2\ 1\ 4 \end{pmatrix}, \begin{pmatrix} 2\ 1\ 3\ 4 \\ 1\ 3\ 4\ 2 \end{pmatrix}$$
$$\begin{pmatrix} 3\ 2\ 4\ 1 \\ 4\ 1\ 2\ 3 \end{pmatrix}, \begin{pmatrix} 3\ 1\ 4\ 2 \\ 4\ 3\ 2\ 1 \end{pmatrix}, \begin{pmatrix} 4\ 2\ 1\ 3 \\ 2\ 1\ 3\ 4 \end{pmatrix}.$$

When a matrix representation is used, the composition of two permutations (two bijective maps) ϕ and ψ is determined by the equation $\psi \circ \phi(k) = \psi(\phi(k))$. For example,

$$\text{if } \phi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 1\ 2 \end{pmatrix}, \text{ then } \psi \circ \phi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 4\ 2\ 3 \end{pmatrix}.$$

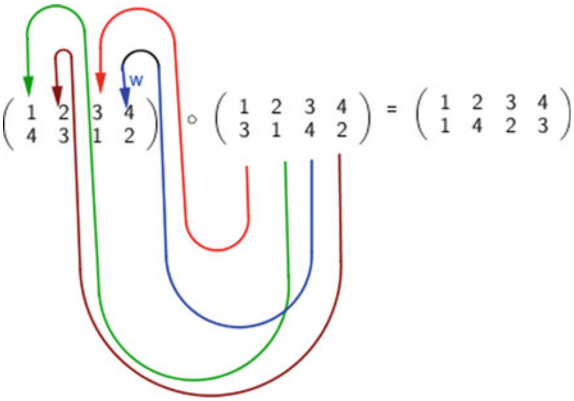
The computations can be sketched as follows:
$1 \xrightarrow{\phi} 3 \xrightarrow{\psi} 1$ gives $1 \xrightarrow{\psi\circ\phi} 1$,
$2 \xrightarrow{\phi} 1 \xrightarrow{\psi} 4$ gives $2 \xrightarrow{\psi\circ\phi} 4$,
$3 \xrightarrow{\phi} 4 \xrightarrow{\psi} 2$ gives $3 \xrightarrow{\psi\circ\phi} 2$, and
$4 \xrightarrow{\phi} 2 \xrightarrow{\psi} 3$ gives $4 \xrightarrow{\psi\circ\phi} 3$ (Fig. 6.1).

The matrix representation of ϕ^{-1} can be obtained by exchanging the two rows in the matrix ϕ. One can check that the composition of ϕ and ϕ^{-1} yields the identity map on $\{1, 2, \ldots, n\}$. For example,

$$\text{if } \phi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 1\ 2 \end{pmatrix}, \text{ then } \phi^{-1} = \begin{pmatrix} 4\ 3\ 1\ 2 \\ 1\ 2\ 3\ 4 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 2\ 1 \end{pmatrix}$$

and the composition of ϕ and ϕ^{-1} yields the identity permutation e.

Fig. 6.1 A composition of two permutations



w
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

Example 6.1.2 Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$ be two permutations on $\{1, 2, \ldots, 5\}$. One can easily check that

1. $\phi(3) = 2, \phi(5) = 4, \psi(2) = 5$, and $\psi(4) = 4$.
2. $\phi^2 = \phi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$.
3. $\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$ and $\psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$.
4. $\phi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ and $\psi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$.
5. $\phi^{-1} \circ \psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$.

The nonequality $\phi \circ \psi \neq \psi \circ \phi$ shows that $\mathfrak{S}_5$ is not abelian.

Proposition 6.1.3 *The group $\mathfrak{S}_n$ is not abelian for each $n \geq 3$.*

Proof Assume that $n \geq 3$. Consider the permutations

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \\ 2 & 1 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \end{pmatrix}, \ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots\ldots & n-1 & n \\ 3 & 2 & 1 & 4 & 5 & \ldots\ldots & n-1 & n \end{pmatrix}.$$

Both permutations are elements in $\mathfrak{S}_n$. Since $\phi \circ \psi(1) = 3 \neq 2 = \psi \circ \phi(1)$, thus $\mathfrak{S}_n$ is not abelian. ■

Example 6.1.4 The following statements describe the elements of $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{S}_3$, and $\mathfrak{S}_4$.

1. There exists only one bijection of the set $\{1\}$. Thus, $\mathfrak{S}_1$ contains only the identity map

$$\phi = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e.$$

2. For $\phi \in \mathfrak{S}_2$, a bijective map of $\{1, 2\}$, there are two choices for the image of number 1 under ϕ, namely 1 or 2. After choosing the image of 1, only one choice is left for the image of 2. Therefore, either $\phi(1) = 1$ and $\phi(2) = 2$, yielding the identity map on $\{1, 2\}$, or $\phi(1) = 2$ and $\phi(2) = 1$. These values are all the possibilities for ϕ. Hence,

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1\,2 \\ 1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix} \right\}.$$

   Note that $|\mathfrak{S}_2| = 2 \times 1 = 2!$.
3. In the case of $\mathfrak{S}_3$, the choices are branched. For a bijective map ϕ on $\{1, 2, 3\}$, there are three choices for $\phi(1)$. On choosing the image for number 1, two choices are left for $\phi(2)$, and having chosen one of these, only one choice remains for $\phi(3)$. By the multiplication rule (De Temple & Webb, 2014), there are $3 \times 2 \times 1 = 3!$ ways to form ϕ. Figure 6.2. illustrates the choices for determining an element of $\mathfrak{S}_3$.

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix} \right\}$$

4. For the group $\mathfrak{S}_4$, one can use a tree similar to that shown in (3) to find all possible permutations. Table 6.1 lists all possible choices for $\phi(i)$, $1 \leq i \leq 4$.

   Each column, from the second on, represents an element of $\mathfrak{S}_4$. For example, the second column represents the identity permutation, and the third column represents the permutation $\begin{pmatrix} 1\;2\;\;3\;4 \\ 1\;2\;\;4\;3 \end{pmatrix}$. Clearly, there exist $24 = 4!$ permutations in $\mathfrak{S}_4$.

The same method used to solve this example can be used to prove the following theorem.

Theorem 6.1.5 *Let $n \in \mathbb{N}$. There exist $n!$ permutations in $\mathfrak{S}_n$.*

Proof The number of elements in $\mathfrak{S}_n$ is equal to the number of all possibilities of ϕ. To construct ϕ, the process is initiated by choosing an element for $\phi(1)$ from $\{1, 2, \ldots, n\}$. There are n choices for $\phi(1)$. Once $\phi(1)$ is chosen, $n-1$ choices remain for $\phi(2)$, namely $\{1, 2, \ldots, n\} \backslash \{\phi(1)\}$. After $\phi(1)$ and $\phi(2)$ have been selected, $n-2$ choices remain for $\phi(3)$, and so on. Continuing such selections, eventually, only one choice remains for $\phi(n)$. By the multiplication rule, the number of ways to form ϕ is

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!.$$

Therefore, there are $n!$ possibilities for ϕ. ■

Fig. 6.2 Elements of $\mathfrak{S}_3$

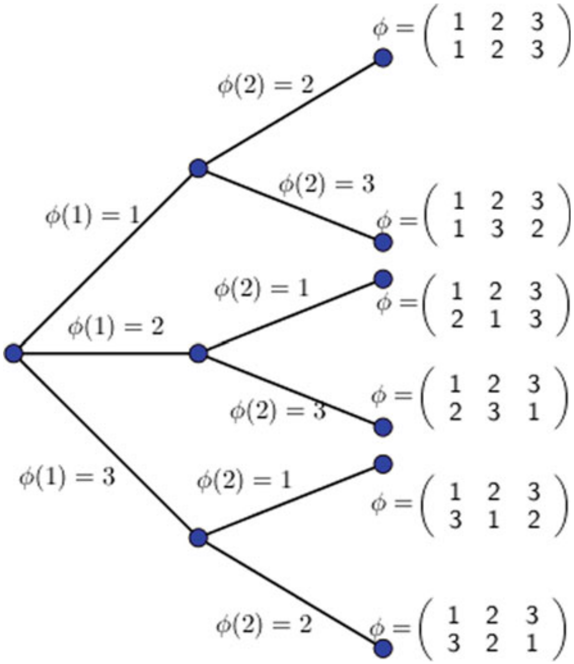

$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\phi(2) = 2$
$\phi(2) = 3$
$\phi(1) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$\phi(2) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
$\phi(1) = 2$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
$\phi(2) = 3$
$\phi(1) = 3$
$\phi(2) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$\phi(2) = 2$
$\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Table 6.1 Elements of $\mathfrak{S}_4$

$\phi(1)$	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	3	3	4	4	4	4	4	4
$\phi(2)$	2	2	3	3	4	4	1	1	3	3	4	4	1	1	2	2	4	4	1	1	2	2	3	3
$\phi(3)$	3	4	2	4	2	3	3	4	1	4	1	3	2	4	1	4	1	2	2	3	1	3	1	2
$\phi(4)$	4	3	4	2	3	2	4	3	4	1	3	1	4	2	4	1	2	1	3	2	3	1	2	1

Definition 6.1.6 Let $n \in \mathbb{N}$, ϕ be a permutation on $\{1, 2, \ldots, n\}$, and k be an element of $\{1, 2, \ldots, n\}$. We say ϕ fixes k if $\phi(k) = k$; otherwise, we say ϕ moves k. The subset of all elements in $\{1, 2, \ldots, n\}$ that are moved by ϕ is denoted by $\text{Move}(\phi)$. The subset of all permutations in $\mathfrak{S}_n$ that fix k is denoted by $(\mathfrak{S}_n)_k$. i.e.,

$$\text{Move}(\phi) = \{k : \phi(k) \neq k\} \text{ and } (\mathfrak{S}_n)_k = \{\phi \in \mathfrak{S}_n : \phi(k) = k\}.$$

For example, in $\mathfrak{S}_3$,

$$\text{Move}\left(\begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}\right) = \{2, 3\}, \ \text{Move}\left(\begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}\right) = \emptyset,$$

$$(\mathfrak{S}_3)_2 = \left\{\begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}\right\}, \ (\mathfrak{S}_3)_1 = \left\{\begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}\right\}.$$

Remark 6.1.7 The element $k \in \text{Move}(\phi)$ if and only if $\phi(k) \in \text{Move}(\phi)$. This result follows directly by the injectivity of ϕ.

Definition 6.1.8 Let $n \in \mathbb{N}$ and ϕ, ψ be two distinct permutations on $\{1, 2, \ldots, n\}$. The permutations ϕ and ψ are said to be disjoint if $\text{Move}(\phi) \cap \text{Move}(\psi) = \emptyset$. Let $\phi_1, \ldots, \phi_m$ be distinct permutations on $\{1, 2, \ldots, n\}$. The permutations $\phi_1, \ldots, \phi_m$ are called pairwise disjoint if ϕ_i, ϕ_j are disjoint for all $i \neq j$, where $1 \leq i, j \leq m$.

Having two disjoint permutations on $\{1, 2, \ldots, n\}$ means that if one of them moves an element k then the other one fixes k. For any integer n, the identity permutation on $\{1, 2, \ldots, n\}$ does not move any element. Therefore, $\text{Move}(e) = \emptyset$, and it is disjoint from other permutations.

Example 6.1.9 The permutations

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \ \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

are disjoint permutations in $\mathfrak{S}_5$. Similarly,

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix} \text{ and}$$
$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

are pairwise disjoint permutations in $\mathfrak{S}_6$. The permutations

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

are in $\mathfrak{S}_3$ and are not disjoint as $\text{Move}(\phi_1) \cap \text{Move}(\phi_2) = \{1, 2\} \neq \emptyset$.

Proposition 6.1.10 *Let $n \in \mathbb{N}$, and let ϕ, ψ be permutations on $\{1, 2, \ldots, n\}$. If ϕ, ψ are disjoint, then $\phi \circ \psi = \psi \circ \phi$ (any two disjoint permutations commute).*

Proof Assume that ϕ, ψ are disjoint. Let k be an element in $\{1, 2, \ldots, n\}$. Since $\text{Move}(\phi) \cap \text{Move}(\psi) = \emptyset$, only one of the following three cases holds:

1. $k \in \text{Mov}(\phi) \wedge k \notin \text{Mo}v(\psi)$.
2. $k \in \text{Mov}(\psi) \wedge k \notin \text{Mov}(\phi)$.
3. $k \notin \text{Mov}(\phi) \cup \text{Mov}(\psi)$.

If the first case holds, then Remark 6.1.7 implies that $\phi(k) \in \text{Mov}(\phi)$. Thus, $\phi(k) \notin \text{Mov}(\psi)$ and

$$\phi \circ \psi(k) = \phi(\psi(k)) = \phi(k) = \psi(\phi(k)) = \psi \circ \phi(k).$$

Similarly, the second case follows by exchanging the role of ϕ and ψ. For the last case, $\phi(k) = k = \psi(k)$, which implies that

$$\phi \circ \psi(k) = \phi(\psi(k)) = \phi(k) = k = \psi(k) = \psi(\phi(k)).$$

■

According to Lemma 5.4.5 (2),

Corollary 6.1.11 *Let $n \in \mathbb{N}$. If ϕ and ψ are two disjoint permutations on $\{1, 2, \ldots, n\}$, then*

$$(\phi\psi)^k = \phi^k\psi^k \text{ for all } k \in \mathbb{N}.$$

Using Exercises 5.25 and 6.2.7, one can easily show the following corollary.

Corollary 6.1.12 *Let $m \in \mathbb{N}$ and $\phi_1, \phi_2, \ldots, \phi_m$ be a set of pairwise disjoint permutations. If $(\phi_1\phi_2 \ldots \phi_m)^k = e$ for some $k \in \mathbb{N}$, then $\phi_i^k = e$ for each $1 \le i \le m$.*

The following example shows that the converse of Proposition 6.1.10 is not true.

Example 6.1.13 On $\{1, 2, 3, 4\}$, consider the permutations

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

As $\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \psi \circ \phi$, the two permutations commute, but they are not disjoint since $\text{Move}(\phi) \cap \text{Move}(\psi) = \{1, 2\} \neq \emptyset$. In general, for any permutation ϕ not equal to the identity, ϕ commutes with itself, but $\text{Move}(\phi) \cap \text{Move}(\phi) = \text{Move}(\phi) \neq \emptyset$, and thus, ϕ and ϕ are not disjoint.

6.2 Cycles on $\{1, 2, \ldots, n\}$

Although the matrix representation gives a complete description of a permutation, there are other representations that are often useful. One such representation based on the notion of cycles.

Definition 6.2.1 Let $n, k \in \mathbb{N}$ and $i_1, i_2, \ldots, i_k$ be distinct elements in $\{1, 2, \ldots, n\}$. A cycle (or a cyclic permutation) $\psi = (i_1 i_2 \ldots i_k)$ on $\{1, 2, \ldots, n\}$ means the function defined on $\{1, 2, \ldots, n\}$ by

$$\psi(j) = \begin{cases} i_{s+1} & j = i_s \wedge 1 \leq s < k \\ i_1 & j = i_k \\ j & j \notin \{i_1, \ldots, i_k\} \end{cases}$$

for any $j \in \{1, 2, \ldots, n\}$. The number k is called the length of the cycle. A cycle of length k is called a k-cycle, and a 2-cycle is called a transposition. The trivial cycle is a cycle of length 1. Let a be an element in $\{1, 2, \ldots, n\}$. We say that a appears in the cycle $(i_1 i_2 \ldots i_k)$, denoted by $a \in (i_1 i_2 \ldots i_k)$, if $a = i_s$ for some $1 \leq s \leq k$.

Intuitively, a cycle $(i_1 i_2 \ldots i_k)$ is the function on $\{1, 2, \ldots, n\}$ that takes i_s to the following element in the line, takes the last element to the first element, and fixes all elements that do not appear in the cycle, i.e., $(i_1 i_2 \ldots i_k)(i_s) = \begin{cases} i_{s+1} & 1 \leq s < k \\ i_1 & s = k \end{cases}$. For example, the cycle $(3\ 2\ 6\ 4)$ on $\{1, 2, 3, 4, 5, 6\}$ is the function that takes $3 \to 2, 2 \to 6, 6 \to 4, 4 \to 3$ and fixes all other elements in $\{1, 2, 3, 4, 5, 6\}$. The length of $(3\ 2\ 6\ 4)$ is 4. The cycle $(1\ 4)$ is the function on $\{1, 2, 3, 4, 5, 6\}$ that takes $1 \to 4$, $4 \to 1$ and fixes all other elements in $\{1, 2, 3, 4, 5, 6\}$. The length of $(1\ 4)$ is 2. The cycle $(1\ 4)$ represents a transposition. The map $\mathcal{R}_{s,t}$ in Example 1.5.17 is the transposition $(s\ t)$ on $\{1, 2, \ldots, n\}$. Using Definition 6.2.1, one can easily verify that for any k such that $1 \leq k \leq n$,

$$(i_2 \ldots i_k i_1) = (i_1 i_2 \ldots i_k) = (i_k i_1 i_2 \ldots i_{k-1})$$

as all of these cycles represent the following function

$$i_1 \to i_2, i_2 \to i_3, \ldots, i_{k-1} \to i_k, i_k \to i_1 \wedge j \to j \quad \forall j \notin \{i_1, \ldots, i_k\}.$$

For example, on $\{1, 2, \ldots, 8\}$, the cycles

$$(3\ 1\ 5\ 2), (2\ 3\ 1\ 5), (5\ 2\ 3\ 1), \text{ and } (1\ 5\ 2\ 3)$$

represent the same cycle of length 4. The transposition $(3\ 5)$ exchanges 5 and 3. The cycles $(3\ 1\ 5\ 2)$ and $(3\ 5)$ are visualized as in Fig. 6.3.

Definition 6.2.2 (*Product of cycles*) Let $n, k, r \in \mathbb{N}$, and let $(i_1 i_2 \ldots i_k)$ and $(j_1 j_2 \ldots j_r)$ be two cycles on $\{1, 2, \ldots, n\}$. The product of $(i_1 i_2 \ldots i_k)$ and

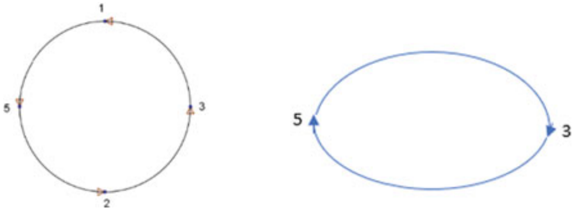


Fig. 6.3 Cycles (3 1 5 2) and (3 5)

$(j_1 j_2 \ldots j_r)$ is defined as their composition $(i_1 i_2 \ldots i_k) \circ (j_1 j_2 \ldots j_r)$, obtained by applying $(j_1 j_2 \ldots j_r)$ then $(i_1 i_2 \ldots i_k)$. i.e.,

$$(i_1 i_2 \ldots i_k) \circ (j_1 j_2 \ldots j_r)(j) = (i_1 i_2 \ldots i_k)((j_1 j_2 \ldots j_r)(j)).$$

The product of $(i_1 i_2 \ldots i_k)$ and $(j_1 j_2 \ldots j_r)$ is denoted by $(i_1 i_2 \ldots i_k)\ (j_1 j_2 \ldots j_r)$.

Remark 6.2.3 Let $n \in \mathbb{N}$.

1. For each $i \in \{1, 2, \ldots, n\}$, the trivial cycle (i) on $\{1, 2, \ldots, n\}$ maps i to itself and fixes all other elements. Hence,

$$(1) = (2) = \cdots = (i) = \cdots = (n)$$

all of which represent the identity function on $\{1, 2, \ldots, n\}$.
2. For $i, j \in \{1, 2, \ldots, n\}$ such that $i \neq j$, $(ij)^2 = (ij)(ij) = e$.
3. No representation exists for the identity function as a transposition.

Example 6.2.4

1. On $\{1, 2, 3, 4, 5\}$, consider the two cycles $(2\ 4\ 1)$ and $(3\ 5\ 4)$. The product of the two cycles can computed as $(2\ 4\ 1)(3\ 5\ 4) = (3\ 5\ 1\ 2\ 4)$ or $(3\ 5\ 4)(2\ 4\ 1) = (2\ 3\ 5\ 4\ 1)$. Cleary that the product of cycles need not be commutative.
2. Consider the set $\{1, 2, 3, 4, \ldots, 8\}$. If $\rho = (1\ 4\ 3\ 8)(2\ 6\ 3)(4\ 2)$ (a product of three cycles), then

$$\rho(1) = 4, \rho(2) = 3, \rho(3) = 2, \rho(4) = 6,$$
$$\rho(5) = 5, \rho(6) = 8, \rho(7) = 7, \rho(8) = 1.$$

The product ρ can be written as a product of the two cycles $(1\ 4\ 6\ 8)(2\ 3)$. However, ρ has no representation as one cycle.
3. On $\{1, 2, 3, 4, \ldots, 10\}$, consider $\sigma = (2\ 5)(2\ 7)(2\ 4)(2\ 1)$. This permutation can be written as one cycle $\sigma = (2\ 1\ 4\ 7\ 5)$.
4. On $\{1, 2, 3, 4, \ldots, 9\}$, $(2\ 3\ 6\ 7\ 9)(3) = (2\ 3\ 6\ 7\ 9)(8) = (2\ 3\ 6\ 7\ 9)(7) = (2\ 3\ 6\ 7\ 9)$.
5. On $\{1, 2, 3, 4, \ldots, 8\}$, $(2\ 5\ 6\ 1\ 7)(4\ 5\ 3\ 2\ 6\ 1) = (4\ 6\ 7\ 2\ 1)(5\ 3)$

$$(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 2) = (2\ 5\ 7\ 4\ 6)$$
$$(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 1) = (1\ 5)(2\ 7\ 4\ 6).$$

6. The product of two cycles is not necessarily a cycle. For example, on $\{1, 2, 3, 4, \ldots, 11\}$, consider $(2\ 5\ 6\ 1\ 7)(4\ 5\ 3\ 2\ 6\ 1)$ and $(2\ 7\ 4\ 3)(4\ 6\ 3)(5\ 1)$. Both products are product of cycles but cannot be written as one cycle.

The following lemma is needed later and can be easily proved using Definition 6.2.1 and induction on r.

Lemma 6.2.5 *Let $n \in \mathbb{N}$, and let $(i_1 i_2 \dots i_k)$ be a cycle on $\{1, 2, \dots, n\}$. For any positive integer r and any $1 \le s \le k$,*

$$((i_1 i_2 \cdots i_k))^r (i_s) = i_{f(s,r)}$$

where $f(s,r) = \begin{cases} r+s \bmod k & \text{if } r+s \neq qk \text{ for all } q \in \mathbb{N} \\ k & \text{if } r+s = qk \text{ for some } q \in \mathbb{N} \end{cases}.$

As the product (composition) of the two cycles $(i_1 i_2 \dots i_k)$ and $(i_k i_{k-1} \dots i_1)$ is the identity, both cycles are bijective maps on $\{1, 2, \dots, n\}$. This result is stated in the following proposition.

Proposition 6.2.6 *Let $n, k \in \mathbb{N}$, and let $i_1, i_2, \dots, i_k$ be distinct elements in $\{1, 2, \dots, n\}$. The cycle $(i_1 i_2 \dots i_k)$ is a permutation on $\{1, 2, \dots, n\}$, whose inverse is the cycle $(i_k i_{k-1} \dots i_1)$.*

As an example for applying Proposition 6.2.6, consider the group $\mathfrak{S}_7$ and the permutation $\phi = (2\ 3\ 1\ 4\ 7\ 5)$. The inverse permutation is $\phi^{-1} = (5\ 7\ 4\ 1\ 3\ 2)$. The reader should notice that although the inverse of a cycle is a cycle, the set of all cycles in $\mathfrak{S}_n$ is not closed under the product of cycles (composition in $\mathfrak{S}_n$), as shown in items (2) and (6) in Example 6.2.4. Hence, the subset of all cycles in $\mathfrak{S}_n$ does not form a group under the composition (the product of cycles).

If $(i_1 i_2 \dots i_k)$ is a cycle on $\{1, 2, \dots, n\}$, then by renaming the elements in $\{1, 2, \dots, n\} \backslash \{i_1, i_2, \dots, i_k\}$ to be $i_{k+1}, i_{k+2}, \dots, i_n$, the following corollary can be easily proved:

Corollary 6.2.7 *Let $n, k \in \mathbb{N}$ such that $k \le n$. Any cycle $(i_1 i_2 \dots i_k)$ on $\{1, 2, \dots, n\}$ has a matrix representation as*

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k & i_{k+1} & i_{k+2} & \dots & i_n \\ i_2 & i_3 & \dots & i_k & i_1 & i_{k+1} & i_{k+2} & \dots & i_n \end{pmatrix}.$$

Example 6.2.8

1. The cycle $(2\ 3\ 1\ 5)$ on $\{1, 2, 3, 4, 5\}$ can be represented as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$.
2. Let

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 1 & 7 & 5 & 3 & 6 & 8 & 9 \end{pmatrix}.$$

   The permutation ϕ is the matrix representation for the cycle $(1\ 4\ 7\ 6\ 3)$.
3. Let

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

The permutation ϕ is a matrix representation for the transposition $(1\ 3)$.

4. Let

$$\psi = \begin{pmatrix} 1\,2\,3 & 4\,5\,6 & 7\,8\,9 \\ 4\,5\,1 & 7\,9\,3 & 6\,8\,2 \end{pmatrix}.$$

The permutation ψ cannot be written as a cycle on $\{1, 2, 3, \ldots, 9\}$. However, it can be written as a product of cycles as: $(1\ 4\ 7\ 6\ 3)(2\ 5\ 9)$.

5. Let

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

The permutation ψ cannot be written as a cycle on $\{1, 2, 3, \ldots, 6\}$. However, it can be written as a product of cycles as: $(1\ 6\ 4)(2\ 3\ 5)$.

6. Consider the group $\mathfrak{S}_7$. If $\phi = (2\ 3\ 1)(4\ 7\ 5)$, then

$$\phi^{-1} = ((2\ 3\ 1)(4\ 7\ 5))^{-1} = (4\ 7\ 5)^{-1}(2\ 3\ 1)^{-1} = (5\ 7\ 4)(1\ 3\ 2).$$

As seen in the above example that certain permutations cannot be written as cycles but can be written as a product of two or more cycles. In general, we have the following proposition.

Proposition 6.2.9 *Let $n \in \mathbb{N}$. Any permutation on $\{1, 2, \ldots, n\}$ can be written as a finite product of disjoint cycles.*

The importance of the decomposition in Proposition 6.2.9 is due to the fact that disjoint cycles commute (Proposition 6.1.10). Therefore, one can write any permutation as a product of commuting cycles. We postpone the proof of the proposition to the subsequent sections. We end this section by recalling the notion of disjoint cycles and presenting several observations. As any cycle is a permutation (Proposition 6.2.6), thus all definitions and universal results for permutations apply to cycles. For example, Definition 6.1.8 still holds for cycles. Proposition 6.1.10 implies that any disjoint cycles on $\{1, 2, \ldots, n\}$ commute, and if ϕ and ψ are two disjoint cycles on $\{1, 2, \ldots, n\}$, then by Corollary 6.1.11,

$$(\phi\psi)^k = \phi^k\psi^k \text{ for all } k \in \mathbb{N}.$$

Lemma 6.2.10 *Let $n \in \mathbb{N}$. If $(i_1 i_2 \ldots i_k)$ is a cycle on $\{1, 2, \ldots, n\}$, then*

$$\text{Move}((i_1 i_2, \ldots, i_k)) = \{i_1, i_2, \ldots, i_k\}.$$

Proof Assume that $\phi = (i_1 i_2 \ldots i_k)$. As $i_1 \xrightarrow{\phi} i_2, i_2 \xrightarrow{\phi} i_3, \ldots, i_{k-1} \xrightarrow{\phi} i_k, i_k \xrightarrow{\phi} i_1$ and all i_s s are distinct, then $\phi(i_s) \neq i_s$ for each $1 \leq s \leq k$. Hence, $\{i_1, i_2, \ldots, i_k\} \subseteq \text{Move}(\phi)$. For the other inclusion, if $j \notin \text{Move}(\phi)$, then by definition of a cycle, $\phi(j) = j$, which implies that $j \notin \{i_1, i_2, \ldots, i_k\}$. ■

The above lemma and Definition 6.1.8 imply the following results:

Corollary 6.2.11 *Let $n, k, r \in \mathbb{N}$. The cycles $(i_1 i_2 \dots i_k)$ and $(j_1 j_2 \dots j_r)$ on $\{1, 2, \dots, n\}$ are disjoint if and only if $i_s \neq j_t$ for all s, t such that $1 \leq s \leq k$, $1 \leq t \leq r$.*

This corollary can be used to decide if two cycles are disjoint. For example, one can directly say that the cycles $(1\ 5)$ and $(2\ 7\ 4\ 6)$ on $\{1, 2, 3, 4, 5, 6, 7\}$ are disjoint while $(2\ 7\ 4\ 3)$ and $(4\ 6\ 3)$ are not.

6.3 Orbits of a Permutation

In this section, we use the elements of $\mathfrak{S}_n$ to define equivalence relations on the set $\{1, 2, \dots, n\}$ where $n \in \mathbb{N}$. Each $\phi \in \mathfrak{S}_n$ defines an equivalence relation on $\{1, 2, \dots, n\}$, dividing the set $\{1, 2, \dots, n\}$ into disjoint sets (equivalence classes) called orbits of ϕ. More information regarding equivalence relations can be found in Sect. 1.4.

Definition 6.3.1 Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. On $\{1, 2, \dots, n\}$ define the relation $\cong_\phi$ by

$$i \cong_\phi j \Leftrightarrow \exists\, m \in \mathbb{Z} \ni j = \phi^m(i), \quad \text{where } i, j \in \{1, 2, \dots, n\}.$$

Lemma 6.3.2 *Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. The relation $\cong_\phi$ in* Definition 6.3.1 *is an equivalence relation.*

Proof For each $i \in \{1, 2, \dots, n\}, i = \phi^0(i)$, thus $i \cong_\phi i$ and $\cong_\phi$ is reflexive. Assume that $i \cong_\phi j$. i.e., there exists $m \in \mathbb{Z} \ni j = \phi^m(i)$. Applying the function ϕ^{-m} on both sides yields $i = \phi^{-m}(j)$. Therefore, $\exists\, l = -m \in \mathbb{Z}$ such that $i = \phi^l(j)$, i.e., $j \cong_\phi i$, and $\cong_\phi$ is symmetric. Finally, let $i \cong_\phi j$ and $j \cong_\phi k$. According to the definition of $\cong_\phi$, there exist $m, l \in \mathbb{Z}$ such that $j = \phi^m(i)$ and $k = \phi^l(j)$. Set $s = l + m \in \mathbb{Z}$, then

$$\phi^s(i) = \phi^{l+m}(i) = \phi^l\big(\phi^m(i)\big) = \phi^l(j) = k.$$

i.e., $i \cong_\phi k$ and $\cong_\phi$ is transitive. By Definition 1.4.1, the relation $\cong_\phi$ is an equivalence relation. ■

The equivalence classes generated by the relation $\cong_\phi$ form a partition of the set $\{1, 2, \dots, n\}$ (Theorem 1.4.10). These equivalence classes are called the orbits of ϕ.

Definition 6.3.3 Let $n \in \mathbb{N}$ and $\phi \in \mathfrak{S}_n$. For each $0 \leq i \leq n$, the equivalence class of $\cong_\phi$ that contains i, denoted by $\mathcal{O}r_\phi(i)$, is called the orbit of i under ϕ. The sets $\mathcal{O}r_\phi(i), i \in \{1, 2, \dots, n\}$ are called the orbits of ϕ.

Any two orbits of $\phi \in \mathfrak{S}_n$ (by their construction) are either identical or disjoint, and the union of the orbits of ϕ is the set $\{1, 2, \ldots, n\}$. One also has that for each $i \in \{1, 2, \ldots, n\}$,

$$\mathcal{O}r_\phi(i) = \left\{j \in \{1, 2, \ldots, n\} : i \cong_\phi j\right\} = \left\{j \in \{1, 2, \ldots, n\} : \exists\, m \in \mathbb{Z} \ni j = \phi^m(i)\right\}$$
$$= \left\{\phi^m(i) : m \in \mathbb{Z}\right\}.$$

Proposition 6.3.4 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \ldots, n\}$. The orbit of i under ϕ is a nonempty finite set given by*

$$\mathcal{O}r_\phi(i) = \left\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\right\}$$

where *k is the smallest nonnegative integer satisfying $\phi^k(i) = i$.*

Proof Let $i \in \{1, 2, \ldots, n\}$. As $i = \phi^0(i) \in \{\phi^m(i) : m \in \mathbb{Z}\} = \mathcal{O}r_\phi(i) \subseteq \{1, 2, \ldots, n\}$, then $\mathcal{O}r_\phi(i)$ is a nonempty finite set. Hence, there exist $m_1, m_2 \in \mathbb{Z}$ such that

$$m_1 < m_2 \text{ and } \phi^{m_1}(i) = \phi^{m_2}(i).$$

Applying the function ϕ^{-m_1} on both sides yields $\phi^{m_2 - m_1}(i) = i$; i.e., there exists a nonnegative integer $s = m_2 - m_1$ such that $\phi^s(i) = i$. Let k be the smallest nonnegative integer satisfying $\phi^k(i) = i$ and $B = \left\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\right\}$, we show that $B = \mathcal{O}r_\phi(i)$. Since

$$B = \left\{i, \phi(i), \phi^2(i), \ldots, \phi^{k-1}(i)\right\} \subseteq \left\{\phi^m(i) : m \in \mathbb{Z}\right\} = \mathcal{O}r_\phi(i),$$

then $B \subseteq \mathcal{O}r_\phi(i)$. For the other inclusion, let $\phi^m(i)$ be any element of $\mathcal{O}r_\phi(i)$ where $m \in \mathbb{Z}$. Applying the Euclidean Algorithm 2.4.1 on m, k, gives that there exist two integers $q, r \in \mathbb{Z}$ such that

$$m = qk + r, \quad 0 \le r < k.$$

That is,

$$\phi^m(i) = \phi^{r+qk}(i) = \phi^r\left(\phi^{qk}(i)\right) = \phi^r\left(\left(\phi^k\right)^q(i)\right)$$

$$= \begin{cases} \phi^r\left(\underbrace{\phi^k \circ \phi^k \circ \cdots \circ \phi^k(i)}_{q \text{ times}}\right) = \phi^r(i) & q \ge 0 \\ \phi^r\left(\underbrace{\phi^{-k} \circ \phi^{-k} \circ \cdots \circ \phi^{-k}(i)}_{-q \text{ times}}\right) = \phi^r(i)\ q < 0 \end{cases}$$

i.e., $\phi^m(i) = \phi^r(i) \in B$, which implies that $\mathcal{O}r_\phi(i) \subseteq B$. ■

The last proposition provides a practical method for determining the orbits of a permutation ϕ in $\mathfrak{S}_n$, as follows:

- Begin by choosing an integer $i \in \{1, 2, \ldots, n\}$, and compute $\phi(i), \phi^2(i), \ldots$ until i is reached.
- The set $\left\{\phi(i), \phi^2(i), \ldots, i\right\}$ forms $\mathcal{O}r_\phi(i)$, the first orbit.
- Choose an integer from the set $\{1, 2, \ldots, n\}\backslash\mathcal{O}r_\phi(i)$ and compute its orbit in the same way as the first orbit.
- Repeat the same process until the obtained orbits contains all the elements in $\{1, 2, \ldots, n\}$.

Example 6.3.5 Let

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$$

be a permutation on $\{1, 2, \ldots, 11\}$. The orbits of ϕ can be obtained as follows:

- By choosing a number in $\{1, 2, \ldots, 11\}$, say $i = 2$, one can compute
$$\phi(2) = 6, \phi^2(2) = \phi(6) = 5, \phi^3(2) = \phi(5) = 2$$
to obtain $\mathcal{O}r_\phi(2) = \{2, 5, 6\}$.
- Select a number in the set $\{1, 2, \ldots, 11\}\backslash\{2, 5, 6\}$, say $i = 1$. Compute
$$\phi(1) = 9, \phi(9) = 3, \phi(3) = 8, \phi(8) = 1$$
to obtain $\mathcal{O}r_\phi(1) = \{1, 3, 8, 9\}$.
- Choose a number in $\{1, 2, \ldots, 11\}\backslash\{2, 5, 6, 1, 3, 8, 9\}$, say $i = 4$. Compute $\phi(4) = 10, \phi(10) = 4$ to obtain $\mathcal{O}r_\phi(4) = \{4, 10\}$.
- Choose a number in $\{1, 2, \ldots, 11\}\backslash\{2, 5, 6, 1, 3, 8, 9, 4, 10\}$, say $i = 7$. Compute $\phi(7) = 7$ to obtain $\mathcal{O}r_\phi(7) = \{7\}$.
- Only one element remains in the set $\{1, 2, \ldots, 11\}\backslash\{2, 5, 6, 1, 3, 8, 9, 4, 10, 7\}$, which is 11. Compute $\phi(11) = 11$, which yields$\mathcal{O}r_\phi(11) = \{11\}$.
- Terminate the process as there are no elements remain in $\{1, 2, \ldots, 11\}$.

Thus, all the distinct orbits of ϕ are $\{2, 6, 5\}, \{1, 9, 3, 8\}, \{4, 10\}, \{7\}, \{11\}$. Note that since the orbits of a permutation are equivalence classes (either identical or disjoint), then $\mathcal{O}r_\phi(5) = \mathcal{O}r_\phi(6) = \{2, 5, 6\}$, $\mathcal{O}r_\phi(9) = \mathcal{O}r_\phi(3) = \mathcal{O}r_\phi(8) = \{1, 3, 8, 9\}$, and $\mathcal{O}r_\phi(10) = \{4, 10\}$.

The following definition restates Definition 1.5.3 using the notation of this chapter. We remind the reader that any permutation $\phi \in \mathfrak{S}_n$ is a bijective function from $\{1, 2, \ldots, n\}$ to itself.

Definition 6.3.6 Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $A \subseteq \{1, 2, \dots, n\}$. The restriction of ϕ on the subset A, denoted by $\phi_{|A}$ is the function on A that satisfies $\phi_{|A}(x) = \phi(x)\ \forall\, x \in A$.

The next proposition shows that the restriction of a permutation on one of its orbits is a cycle that is formed by the elements of such an orbit.

Proposition 6.3.7 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \dots, n\}$. The restriction of ϕ on $\mathcal{O}r_{\phi}(i)$ is the cycle $\big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)$ on $\{1, 2, \dots, n\}$. i.e.,*

$$\phi_{|\mathcal{O}r_{\phi}(i)} = \big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)$$

where kis the smallest nonnegative integer satisfying $\phi^k(i) = i$.

Proof Assume that $i \in \{1, 2, \dots, n\}$. We show that

$$\phi_{|\mathcal{O}r_{\phi}(i)}(j) = \big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)(j) \quad \forall\ j \in \mathcal{O}r_{\phi}(i).$$

Let $j \in \mathcal{O}r_{\phi}(i)$. Since $\mathcal{O}r_{\phi}(i) = \big\{i, \phi(i), \phi^2(i), \dots, \phi^{k-1}(i)\big\}$, there exists an integer s such that $0 \leq s \leq k-1$ and $j = \phi^s(i)$. Using Definition 6.2.1, we obtain

$$\begin{aligned}
\big(i\ \phi(i)\ \phi^2(i) \dots \phi^{k-1}(i)\big)(j) &= \big(i\ \phi(i)\phi^2(i) \dots \phi^{k-1}(i)\big)\big(\phi^s(i)\big) \\
&= \begin{cases} \phi^{s+1}(i) & 0 \leq s < k-1 \\ i & s = k-1 \end{cases} \\
&= \begin{cases} \phi^{s+1}(i) & 0 \leq s < k-1 \\ \phi^k(i) & s = k-1 \end{cases} \\
&= \phi^{s+1}(i) = \phi\big(\phi^s(i)\big) = \phi(j) = \phi_{|\mathcal{O}r_{\phi}(i)}(j).
\end{aligned}$$

$\blacksquare$

Intuitively, the pervious proposition indicates that if ϕ is a permutation on $\{1, 2, \dots, n\}$, then for each $i \in \{1, 2, \dots, n\}$, the restriction $\phi_{|\mathcal{O}r_{\phi}(i)}$ is the cycle obtained by inserting i as the first element in the cycle and continuously applying ϕ on the element to obtain the next one. This process is repeated until all the elements in the orbit have been considered.

Example 6.3.8

1. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$.
   The orbits of ϕ are

   $$\{1, 3, 8, 9\}, \{2, 5, 6\}, \{4, 10\}, \{7\}, \{11\} \text{ (Example 6.3.5).}$$

   Therefore, according to the results of the last proposition,

$$\phi_{|\{1,3,8,9\}} = (1\ 9\ 3\ 8), \phi_{|\{7\}} = (7), \phi_{|\{2,5,6\}} = (2\ 6\ 5), \phi_{|\{4,10\}} = (4\ 10),\ \phi_{|\{11\}} = (11).$$

2. The orbits of $\phi = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 2\ 4 \end{pmatrix}$ as a permutation in $\mathfrak{S}_4$ are

$$\mathcal{O}r_\phi(1) = \{1, 2, 3\} = \mathcal{O}r_\phi(2) = \mathcal{O}r_\phi(3),\ \mathcal{O}r_\phi(4) = \{4\}.$$

The permutation ϕ has only one orbit that contains more than one element. Therefore, ϕ is a cycle.

Corollary 6.3.9 *Let $n \in \mathbb{N}$, and $\phi \in \mathfrak{S}_n$. For each $i \in \{1, \dots, n\}$* not fixed by ϕ,

$$\mathrm{Move}\Big(\phi_{|\mathcal{O}r_\phi(i)}\Big) = \mathcal{O}r_\phi(i).$$

Proof Let $i \in \{1, 2, \dots, n\}$. The results of Lemma 6.2.10, Propositions 6.3.4, and 6.3.7 can be used to obtain

$$\begin{aligned}\mathrm{Move}\Big(\phi_{|\mathcal{O}r_\phi(i)}\Big) &= \mathrm{Move}\big((i\ \phi(i)\phi^2(i)\dots\phi^{k-1}(i))\big) \\ &= \big\{i, \phi(i), \phi^2(i), \dots, \phi^{k-1}(i)\big\} = \mathcal{O}r_\phi(i).\end{aligned}$$

■

As the orbits of ϕ (by construction) are disjoint, the following direct result can be obtained.

Corollary 6.3.10 *Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $i \in \{1, 2, \dots, n\}$. The cycles obtained by the restriction of ϕ on its orbits are disjoint cycles.*

Next, we prove Proposition 6.2.9 by showing that any permutation ϕ is a product of the cycles obtained by the restrictions of ϕ on its orbits.

Proof of Proposition 6.2.9

Let $n \in \mathbb{N}$, $\phi \in \mathfrak{S}_n$, and $A_1, \dots, A_m$ be the distinct orbits of ϕ. For each $1 \le j \le m$, let ψ_j be the cycle obtained by the restriction of ϕ on A_j. We show that

$$\phi(i) = \psi_m \circ \psi_{m-1} \circ \cdots \circ \psi_2 \circ \psi_1(i) \text{ for each } i \in \{1, 2, \dots, n\}.$$

Assume $i \in \{1, 2, \dots, n\}$. As the orbits of ϕ form a partition for $\{1, 2, \dots, n\}$, there exists l, $1 \le l \le m$ such that $i \in A_l$ and $i \notin A_j$ for all $j \ne l$. Therefore, $i \in \mathrm{Move}(\psi_l)$ and $i \notin \mathrm{Move}\big(\psi_j\big)$ for all $j \ne l$ (Corollary 6.3.9). Therefore,

- $\psi_j(i) = i$ for each $1 \le j < l$
- $\psi_l(i) = \phi(i)$ (Proposition 6.3.7)
- $\psi_j(\phi(i)) = \phi(i)$ for each $l < j \le m$

where the last line follows by Remark 6.1.7. That is,

$$\psi_{l-1} \circ \cdots \circ \psi_1(i) = i, \; \psi_l(i) = \phi(i), \quad \psi_m \circ \cdots \circ \psi_{l+1}(\phi(i)) = \phi(i)$$

which implies

$$\psi_m \circ \cdots \circ \psi_1(i) = \psi_m \circ \cdots \circ \psi_{l+1}(\psi_l(\psi_{l-1} \circ \cdots \circ \psi_1(i))) = \phi(i).$$

According to Corollary 6.3.10, the cycles ψ_j are disjoint. ■

Example 6.3.11

1. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}$ be a permutation in $\mathfrak{S}_{11}$. The distinct orbits of ϕ are $\{1, 9, 3, 8\}$, $\{2, 6, 5\}$, $\{4, 10\}$, $\{7\}$, $\{11\}$, and the corresponding cycles are

$$(1\ 9\ 3\ 8), (2\ 6\ 5), (4\ 10), (7), (11).$$

Hence, ϕ can be written as the following product of disjoint cycles

$$\phi = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10)(7)(11) = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10).$$

2. Let $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 2 & 7 & 4 \end{pmatrix}$ be a permutation in $\mathfrak{S}_7$. Similar to (1), the permutation ϕ can be written as a product of disjoint cycles as follows:

$$\phi = (1\ 3)(2\ 5)(4\ 6\ 7).$$

The reader may notice that

- For a permutation $\phi \in \mathfrak{S}_n$, the number of disjoint cycles (with a length greater than one) form ϕ is less than $n/2$. This occurs because of the simple fact that if the set $\{1, 2, \ldots, n\}$ was divided into disjoint subsets where each subset contains at least two elements, then the number of such subsets must be less than or equal to half of the original set.
- The set of distinct orbits (equivalence classes) of the permutation ϕ is unique (Corollary 1.4.14). Therefore, if all the cycles (length one included) are considered in writing the permutation as a product of disjoint cycles, this product will be unique up to cycle rearrangements.

Proposition 6.3.12 *Let $n \in \mathbb{N}$. If all cycles of length one are considered, then any permutation on $\{1, 2, \ldots, n\}$ can be uniquely (up to rearrangement) written as a finite product of disjoint cycles.*

Example 6.3.13 Using the results of Example 6.1.4, one can easily verify that the group $\mathfrak{S}_1$ consists of only 1-cycle (identity permutation). For $n = 2$, the symmetric group $\mathfrak{S}_2 = \{(1), (12)\}$ consists of two cycles: 1-cycle and 2-cycle (a transposition). The group $\mathfrak{S}_3$ consists of six cycles: one 1-cycle, two 2-cycles, and three 3-cycles. The group $\mathfrak{S}_4$ contains cycles and permutations that cannot be written as one cycle. The elements of $\mathfrak{S}_4$ consist of one 1-cycle, six 2-cycles, eight 3-cycles, six 4-cycles, and three permutations written as a product of two cycles. Similarly, one can continue to analyze the structure of $\mathfrak{S}_n$ using the multiplication rule, as in Example 6.1.4.

6.4 Order of a Permutation

For any $n \in \mathbb{N}$, the orders of the permutations in $\mathfrak{S}_n$ can be investigated. We start with an example of which computing ϕ^k for different permutation ϕ in $\mathfrak{S}_n$ for some chosen k and n.

Example 6.4.1

1. In $(\mathfrak{S}_5, \circ)$, if $\phi = (1\ 2\ 3\ 4)$, then

$$\begin{aligned}\phi^2 &= (1\ 2\ 3\ 4)^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (13)(24)\\ \phi^3 &= (1\ 2\ 3\ 4)^3 = (1\ 2\ 3\ 4)(13)(24) = (1\ 4\ 3\ 2)\\ \phi^4 &= \phi^2\phi^2 = (13)(24)(13)(24) = (13)(13)(24)(24) = (1)(2) = e.\end{aligned}$$

2. In $(\mathfrak{S}_3, \circ)$, if $\phi = (1\ 2)$, then

$$\begin{aligned}\phi^2 &= (1\ 2)^2 = (1) = e.\\ \phi^3 &= (1\ 2)^3 = (1\ 2)(1\ 2)^2 = (1\ 2)e = (1\ 2).\end{aligned}$$

   In general, $\phi^{2k+1} = (1\ 2)$, and $\phi^{2k} = e$ for any integer k.

3. In $(\mathfrak{S}_7, \circ)$, if $\phi = (1\ 2\ 3)(2\ 7\ 1\ 6)$, then $\phi = (1\ 6\ 3)(2\ 7)$ and

$$\begin{aligned}\phi^2 &= ((1\ 6\ 3)(2\ 7))^2 = (1\ 6\ 3)(2\ 7)(1\ 6\ 3)(2\ 7)\\ &= (1\ 6\ 3)(1\ 6\ 3)(2\ 7)(2\ 7) = ((1\ 6\ 3))^2 = (1\ 3\ 6)\\ \phi^3 &= \phi^2\phi = (1\ 3\ 6)(1\ 6\ 3)(2\ 7) = (2\ 7)\\ \phi^4 &= \phi^3\phi = (2\ 7)(1\ 6\ 3)(2\ 7) = (2\ 7)(2\ 7)(1\ 6\ 3) = (1\ 6\ 3)\\ \phi^5 &= \phi^4\phi = (1\ 6\ 3)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(2\ 7)\\ \phi^6 &= \phi^5\phi = (1\ 3\ 6)(2\ 7)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(1\ 6\ 3)(2\ 7)(2\ 7) = e.\end{aligned}$$

4. In $(\mathfrak{S}_6, \circ)$, if $\phi = (2\ 5\ 4)(6\ 3\ 1)(4\ 3)$, then

$$\begin{aligned}
\phi &= (1\ 6\ 3\ 2\ 5\ 4)\\
\phi^2 &= (1\ 3\ 5)(2\ 4\ 6)\\
\phi^3 &= \phi^2\phi = (1\ 2)(3\ 4\ )(5\ 6)\\
\phi^4 &= \phi^2\phi^2 = (1\ 5\ 3)(2\ 6\ 4)\\
\phi^5 &= \phi^4\phi = (1\ 4\ 5\ 2\ 3\ 6)\\
\phi^6 &= \phi^5\phi = (1\ 4\ 5\ 2\ 3\ 6)(1\ 6\ 3\ 2\ 5\ 4) = e.
\end{aligned}$$

The reader may note that computing ϕ^k becomes increasingly complicated as k and n become bigger, and some of the above computations were cumbersome. The computations of the exponent can be simplified using Propositions 6.2.9, and 6.2.6 and the results presented in this section. The following lemma computes the order of a cycle. Recall the order of an element in a group defined in Sect. 5.5.

Lemma 6.4.2 *Let $n \in \mathbb{N}$. The order of a cycle in $\mathfrak{S}_n$ is equal to its length, i.e.,*

$$\operatorname{ord}((i_1 i_2 \dots i_k)) = k$$

where $i_1, i_2, \dots, i_k$ are elements in $\{1, 2, \dots, n\}$. In particular, the order of a transposition is 2.

Proof We show that k is the smallest positive integer such that $(i_1 i_2 \dots i_k)^k = e$. Let $1 \le s \le k$. By Lemma 6.2.5,

$$(i_1 i_2 \dots i_k)^k (i_s) = i_{f(s,k)}$$

where

$$\begin{aligned}
f(s,k) &= \begin{cases} k+s \mod k & \text{if } k+s \neq qk \text{ for all } q \in \mathbb{N} \\ k & \text{if } k+s = qk \text{ for some } q \in \mathbb{N} \end{cases}\\
&= \begin{cases} s \mod k & \text{if } k+s \neq qk \text{ for all } q \in \mathbb{N} \\ k & \text{if } k+s = qk \text{ for some } q \in \mathbb{N} \end{cases}
\end{aligned}$$

Since $1 \le s \le k$, then $k+1 \le s+k \le 2k$, which implies that the only possibility for $s+k$ to be a multiple of k is $2k$, i.e.,

$$\begin{aligned}
f(s,k) &= \begin{cases} s \mod k & k+s \neq 2k \\ k & k+s = 2k \end{cases}\\
&= \begin{cases} s \mod k & s \neq k \\ k & s = k \end{cases}\\
&= s.
\end{aligned}$$

i.e., $(i_1 i_2 \dots i_k)^k (i_s) = i_s$ for each $1 \le s \le k$, and $(i_1 i_2 \dots i_k)^k = e$. Let r be a positive integer such that $r < k$. We compute $(i_1 i_2 \dots i_k)^r (i_1)$ as follows:

$$(i_1 i_2 \dots i_k)^r(i_1) = i_{f(1,r)}$$

where

$$f(1,r) = \begin{cases} r+1 \bmod k & \text{if } r+1 \neq qk \text{ for all } q \in \mathbb{N} \\ k & \text{if } r+1 = qk \text{ for some } q \in \mathbb{N}. \end{cases}$$

Since $r < k$, we have $r+1 < k+1 \leq 2k$, which implies that the only possibility for $r+1$ to be a multiple of k is k. i.e.,

$$f(1,r) = \begin{cases} r+1 \bmod k & \text{if } r+1 \neq k \\ k & \text{if } r+1 = k. \end{cases}$$

In both cases $f(1,r) = r+1 \neq 1$. i.e., $(i_1 i_2 \dots i_k)^r(i_1) \neq i_1$. Therefore $((i_1 i_2 \dots i_k))^r \neq e$. ■

Since every permutation in $\mathfrak{S}_n$ is a finite product of disjoint commuting cycles, one can calculate the order of a permutation using the orders (lengths) of its factor cycles using the following lemma.

Proposition 6.4.3 *Let $n \in \mathbb{N}$. The order of a permutation is the least common multiple of the orders of its factor disjoint cycles. i.e., if $\psi_1, \psi_2, \dots, \psi_s$ are a set of pairwise disjoint cycles such that length ψ_i equals k_i, where $1 \leq i \leq s$, then*

$$\operatorname{ord}(\psi_1\psi_2 \cdots \psi_s) = \operatorname{lcm}(k_1, k_2, \dots, k_s).$$

Proof Let $l = \operatorname{lcm}(k_1, k_2, \dots, k_s)$. For each $1 \leq i \leq s$, there exists an integer m_i such that $l = k_i m_i$. As $\psi_1, \psi_2, \dots, \psi_s$ are pairwise disjoint cycles, they commute, which implies that

$$\begin{aligned}(\psi_1\psi_2 \cdots \psi_s)^l &= (\psi_1)^l(\psi_2)^l \cdots (\psi_s)^l = (\psi_1)^{k_1 m_1}(\psi_2)^{k_2 m_2} \cdots (\psi_s)^{k_s m_s} \\ &= e \cdot e \cdots e = e.\end{aligned}$$

By Lemma 5.5.6, $\operatorname{ord}(\psi_1\psi_2 \cdots \psi_s)$ divides l. On another hand, since

$$(\psi_1\psi_2 \dots \psi_s)^{\operatorname{ord}(\psi_1\psi_2 \dots \psi_s)} = e$$

and the cycles $\psi_1, \psi_2, \dots, \psi_s$ are disjoint, by Corollary 6.1.12, $\psi_i^{\operatorname{ord}(\psi_1\psi_2 \dots \psi_s)} = e$ for each $1 \leq i \leq s$, which implies that k_i divides $\operatorname{ord}(\psi_1\psi_2 \dots \psi_s)$ for each $1 \leq i \leq s$. Therefore, the least common multiple $l = \operatorname{lcm}(k_1, k_2, \dots, k_s)$ divides $\operatorname{ord}(\psi_1\psi_2 \dots \psi_s)$. Proposition 2.2.5 (3) implies the result. ■

Considering the above results, we compute some of the permutations in Example 6.4.1, leaving the others as an exercise:

- In $(\mathfrak{S}_5, \circ)$, if $\phi = (1\ 2\ 3\ 4)$, then $\operatorname{ord}(\phi) = 4$, and

$$\begin{aligned}\phi^2 &= (1\ 2\ 3\ 4)^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4)\\ \phi^3 &= (1\ 2\ 3\ 4)^3 = (1\ 2\ 3\ 4)(1\ 3)(2\ 4) = (1\ 4\ 3\ 2)\\ \phi^4 &= ((1\ 2\ 3\ 4))^4 = e.\end{aligned}$$

- In $(\mathfrak{S}_7, \circ)$, let $\phi = (1\ 2\ 3)(2\ 7\ 1\ 6)$. The permutation ϕ is not a cycle but can be written as a product of disjoint cycles $\phi = (1\ 6\ 3)(2\ 7)$. Thus, $\text{ord}(\phi) = \text{lcm}(3, 2) = 6$, and

$$\begin{aligned}\phi^2 &= ((1\ 6\ 3)(2\ 7))^2 = ((1\ 6\ 3))^2 = (1\ 3\ 6)\\ \phi^3 &= \phi^2\phi = (1\ 3\ 6)(1\ 6\ 3)(2\ 7) = e(2\ 7) = (2\ 7)\\ \phi^4 &= ((1\ 3\ 6))^2 = (1\ 6\ 3)\\ \phi^5 &= \phi^4\phi = (1\ 6\ 3)(1\ 6\ 3)(2\ 7) = (1\ 3\ 6)(2\ 7)\\ \phi^6 &= e.\end{aligned}$$

- In $(\mathfrak{S}_6, \circ)$, let $\phi = (2\ 5\ 4)(6\ 3\ 1)(4\ 3)$. This permutation is a product of cycles that are not disjoint. By rewriting ϕ as a product of disjoint cycles, we obtain $\phi = (1\ 6\ 3\ 2\ 5\ 4)$, a 1-cycle of length 6. Therefore, $\text{ord}(\phi) = 6$.

Example 6.4.4 Consider the permutation $\phi = (2\ 4)(1\ 3\ 6)$ in $\mathfrak{S}_7$. To find ϕ^{100}, one first computes the order of ϕ. As ϕ is a product of disjoint cycles, $\text{ord}(\phi) = \text{lcm}(2, 3) = 6$. i.e., $\phi^6 = e$. Applying the division algorithm on 6 and 100 yields $100 = 16 \times 6 + 4$. Thus,

$$\begin{aligned}\phi^{100} &= \phi^{4+16\times 6} = \phi^4\left(\phi^6\right)^{16}\\ &= \phi^4(e)^{16} = \phi^4.\end{aligned}$$

The cycles $(2\ 4)$ and $(1\ 3\ 6)$ are disjoint, and thus, they commute. Consequently,

$$\phi^4 = ((2\ 4)(1\ 3\ 6))^4 = (2\ 4)^4(1\ 3\ 6)^4.$$

Since $(2\ 4)^4 = \left((2\ 4)^2\right)^2 = e^2 = e$ and $(1\ 3\ 6)^4 = (1\ 3\ 6)^3(1\ 3\ 6)^1 = e(1\ 3\ 6) = (1\ 3\ 6)$, then $\phi^4 = (1\ 3\ 6)$.

The next example shows that both conditions $a * b = b * a$ and $\gcd(\text{ord}(a), \text{ord}(b)) = 1$ in Proposition 5.5.11 cannot be eliminated.

Example 6.4.5 The cycles $(1\ 2)$, $(1\ 3)$, and $(3\ 4)$ are elements in the group $\mathfrak{S}_4$. Each of these cycles is a cycle of order 2, and

$$\begin{aligned}\text{ord}((1\ 2)(1\ 3)) &= \text{Ord}((1\ 3\ 2)) = 3 \neq 4 = \text{ord}((1\ 2)) \cdot \text{ord}((1\ 3))\\ \text{ord}((1\ 2)(1\ 3\ 4)) &= \text{Ord}((1\ 3\ 4\ 2)) = 4 \neq 6 = \text{ord}((1\ 2)) \cdot \text{ord}((1\ 3\ 4))\\ \text{ord}((1\ 2)(3\ 4)) &= 2 \neq 4 = \text{ord}((1\ 2)) \cdot \text{ord}((3\ 4)).\end{aligned}$$

The next example shows that the assumption for a group G to be abelian in Proposition 5.5.13 is essential. Recall that for any $m \in \mathbb{Z}$, $mG = \{a^m : a \in G\}$ and $G[m] = \{a \in G : a^m = e\}$.

Example 6.4.6 Consider the symmetric group $\mathfrak{S}_4$. As shown in Example 6.3.13, the group $\mathfrak{S}_4$ consists of one 1-cycle, six 2-cycles, eight 3-cycles, six 4-cycles, and three products of 2-cycles. Each of these permutations, except the 3-cycles, has an order that divides 4. Therefore,

1. The set $4\mathfrak{S}_4$ contains only the identity and the 3-cycles. Since $(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$ is not an element in $4\mathfrak{S}_4$, the set $4\mathfrak{S}_4$ is not closed under the product of cycles, so it is not a group.
2. The set $\mathfrak{S}_4[4]$ contains all the permutations, except the 3-cycles. Since $(1\ 2)(2\ 4) = (1\ 2\ 4)$ is not an element of $\mathfrak{S}_4[4]$, the set $\mathfrak{S}_4[4]$ is not closed under the product of cycles, so it is not a group.

6.5 Odd and Even Permutations

In this section, each permutation in $\mathfrak{S}_n$ for $n \in \mathbb{N}$ is classified as an even or odd permutation. For $n > 1$, this determination is based on expressing a permutation ϕ as a finite product of transpositions. Expressing ϕ as a product of transpositions can be performed by expressing the permutation as a product of cycles, then writing each cycle as a product of transpositions. In the case where $n = 1$, the group $\mathfrak{S}_1$ has only one cycle of length 1. Hence, no transposition in $\mathfrak{S}_1$. Recall that a cycle $(i_1 i_2 \dots i_k)$ in $\mathfrak{S}_n$, where $2 \le k \le n$, is

$$(i_1 i_2 \dots i_k)(i_s) = \begin{cases} i_{s+1} & 1 \le s < k \\ i_1 & s = k \end{cases} \quad \text{for } 1 \le s \le k.$$

Proposition 6.5.1 *Let $n \in \mathbb{N}$ such that $n > 1$. Any cycle in $\mathfrak{S}_n$ can be written as a product of transpositions. Namely, $e = (i_1 i_2)(i_1 i_2)$ for any $i_1 \ne i_2$ and*

$$(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2) \quad \text{for any } 2 \le k \le n.$$

Proof The statement for the identity element is clear. Let $n \ge 2$ and assume that $(i_1 i_2 \dots i_k)$ is a cycle in $\mathfrak{S}_n$. It suffices to show that $(i_1 i_2 \dots i_k)(i_s) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)(i_s)$ for any $1 \le s \le k$.

- If $s = 1$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)$ on i_1 is given by the steps

$$i_1 \xrightarrow{(i_1 i_2)} i_2 \xrightarrow{(i_1 i_3)} i_2 \cdots i_2 \xrightarrow{(i_1 i_{k-1})} i_2 \xrightarrow{(i_1 i_k)} i_2$$

  and yields i_2, which is $(i_1 i_2 \dots i_k)(i_1)$.

- If $1 < s < k$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)$ on i_s is given by the steps

$$i_s \xrightarrow{(i_1 i_2)} i_s \xrightarrow{(i_1 i_3)} i_s \cdots \xrightarrow{(i_1 i_{s-1})} i_s \xrightarrow{(i_1 i_s)} i_1 \xrightarrow{(i_1 i_{s+1})} i_{s+1} \xrightarrow{(i_1 i_{s+2})} i_{s+1} \cdots i_{s+1} \xrightarrow{(i_1 i_k)} i_{s+1}$$

Thus, $i_{s+1} = (i_1 i_2 \dots i_k)(i_s)$.

- If $s = k$, then applying the product $(i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_3)(i_1 i_2)$ to i_k is given by the steps

$$i_k \xrightarrow{(i_1 i_2)} i_k \xrightarrow{(i_1 i_3)} i_k \cdots i_k \xrightarrow{(i_1 i_{k-1})} i_k \xrightarrow{(i_1 i_k)} i_1$$

and yields $i_1 = (i_1 i_2 \dots i_k)(i_k)$.

Hence, the equality is satisfied for all $1 \leq s \leq k$. ■

Remark 6.5.2

1. According to the previous proposition, any cycle of length k, where $k > 1$, can be written as a product of $k - 1$ transpositions.
2. For any $n \in \mathbb{N}$, and for any $i, j \in \{1, 2, \dots, n\}$ such that $i \neq j$, the transposition (ij) can be written as $(ij) = (aj)(ai)(aj)$, where $a \in \{1, 2, \dots, n\} \backslash \{i, j\}$.

Corollary 6.5.3 *Let $n \in \mathbb{N}$ such that $n > 1$.*

1. *Any permutation in $\mathfrak{S}_n$ can be written as a product of a finite number of transpositions.*
2. *Any permutation in $\mathfrak{S}_n$ can be written as a product of a finite number of transpositions of the form (ak_i) for fixed $a \in \{1, 2, \dots, n\}$ with $k_i \in \{1, 2, \dots, n\} \backslash \{a\}$.*

Example 6.5.4 Consider the group $(\mathfrak{S}_9, \circ)$

$$\begin{aligned}
e &= (5\ 8)(5\ 8),\ e = (1\ 2\ 3)(3\ 2\ 1) = (1\ 3)(1\ 2)(3\ 1)(3\ 2),\\
&= (1\ 3)(1\ 2)(1\ 3)(1\ 3)(1\ 2)(1\ 3).\\
\phi &= (3\ 6\ 4\ 2)(5\ 8\ 7) = (3\ 2)(3\ 4)(3\ 6)(5\ 7)(5\ 8)\\
&= (3\ 2)(3\ 4)(3\ 6)(3\ 7)(3\ 5)(3\ 7)(3\ 8)(3\ 5)(3\ 8).\\
\psi &= (4\ 3\ 5\ 1) = (4\ 1)(4\ 5)(4\ 3).
\end{aligned}$$

Using Corollary 6.5.3, one can classify the permutations into odd and even permutations, as follows

Definition 6.5.5 Let $n \in \mathbb{N}$ such that $n > 1$, and $\phi \in \mathfrak{S}_n$. We say that ϕ is an odd permutation if it can be written as a product of an odd number of transpositions. We say that ϕ is an even permutation if ϕ can be written as a product of an even number of transpositions.

Example 6.5.6

1. The identity permutation is an even permutation.
2. Let

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 6 & 8 & 10 & 2 & 5 & 7 & 1 & 3 & 4 & 11 \end{pmatrix}.$$

   As $\phi = (1\ 9\ 3\ 8)(2\ 6\ 5)(4\ 10) = (1\ 8)(1\ 3)(1\ 9)(2\ 5)(2\ 6)(4\ 10)$, then ϕ is even.
3. Let

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

   The permutation $\phi = (1\ 3\ 5\ 2\ 4\ 6)$ is a cycle of length 6, and thus, it is an odd permutation.

Writing a permutation as a product of transpositions is not unique. For example, if $\phi = \tau_m \dots \tau_2\tau_1$, where $\tau_1, \tau_2, \dots, \tau_m$ are transpositions, then

$$\tau_m \dots \tau_2\tau_1(1\ 3)(1\ 2)(3\ 1)(3\ 2) \text{ and } \tau_m \dots \tau_2\tau_1(5\ 8)(5\ 8)$$

are equal to ϕ. However, if ϕ is represented as a product of an odd (resp. even) number of transpositions, then the number of transpositions in any other such representation of ϕ must be odd (resp. even). In the remainder of this section, we prove that any permutation ϕ cannot be simultaneously even and odd. We show the result for the identity permutation, and then for the general case. The following technical lemmas are needed.

Lemma 6.5.7 *Let $n \in \mathbb{N}$ such that $n > 1$. If σ and (ij) are different transpositions in $\mathfrak{S}_n$, then there exists a transposition τ in $\mathfrak{S}_n$ and $l \in \{1, 2, \dots, n\}$ such that $i \notin \tau$ and $\sigma(ij) = (il)\tau$.*

Proof If σ and (ij) are disjoint cycles, they commute, and the result follows by putting $\tau = \sigma$ and $l = j$. If σ and (ij) are not disjoint, then $\sigma = (is)$ or $\sigma = (sj)$ for some $s \in \{1, 2, \dots, n\}\backslash\{i, j\}$.

- If $\sigma = (is)$, then

$$\sigma(ij) = (is)(ij) = (ijs) = (jsi) = (ji)(js) = (ij)(js).$$

  and the result follows by putting $\tau = (js)$ and $l = j$.
- If $\sigma = (sj)$, then

$$\sigma(ij) = (sj)(ij) = (jis) = (sji) = (si)(sj) = (is)(js)$$

  and the result follows by putting $\tau = (js)$ and $l = s$. ■

Lemma 6.5.8 *Let $n \in \mathbb{N}$, $n > 1$, and $\phi \in \mathfrak{S}_n$. Let $\phi = \tau_k\tau_{k-1}\cdots\tau_1, k \geq 2$ be a representation of ϕ as a product of transpositions. Let $s \in \tau_1$ for some $s \in \{1, 2, \dots, n\}$. If ϕ cannot be expressed as a product of $k - 2$ transpositions, then for each i such that $1 \leq i \leq k$, there is a representation of ϕ as a product of transpositions*

$$\alpha_k\alpha_{k-1}\cdots\alpha_i\cdots\alpha_1$$

such that α_i is the first transposition that moves s.

Proof The proof is done by induction on i. Assume that ϕ cannot be written as a product of $k - 2$ transpositions.

- If $i = 1$, let $\alpha_t = \tau_t$ for all $1 \leq t \leq k$, then $\alpha_k\alpha_{k-1}\cdots\alpha_1$ is a representation of ϕ as a product of transpositions such that α_1 is the first transposition that moves s; i.e., the statement is true at $i = 1$.
- Assume that the statement is true for i. That is, there exists $\sigma_k\sigma_{k-1}\cdots\sigma_1$, a representation of ϕ as a product of transpositions such that σ_i is the first transposition that moves s.
- To prove the statement for $i + 1$, we need to find a representation of ϕ as a product of transpositions $\alpha_k\alpha_{k-1}\cdots\alpha_1$, such that the first transposition that moves s is α_{i+1}.

  By the induction hypothesis $\phi = \sigma_k\sigma_{k-1}\cdots\sigma_1$ such that σ_i is the first transposition that moves s. If $\sigma_{i+1} = \sigma_i$, then $\sigma_{i+1}\sigma_i = e$, and ϕ can be written as a product of $k - 2$ transpositions, which contradicts the assumption. Thus, $\sigma_{i+1} \neq \sigma_i$. By Lemma 6.5.7, there exists a transposition τ and $l \in \{1, 2, \dots, n\}$, such that $s \notin \tau$ and $\sigma_{i+1}\sigma_i = (sl)\tau$. By defining the following set of transpositions

$$\alpha_j = \begin{cases} (sl) & j = i + 1 \\ \tau & j = i \\ \sigma_j & j \notin \{i, i + 1\} \end{cases}$$

  the product

$$\begin{aligned} \alpha_k\alpha_{k-1}\cdots\alpha_{i+2}\alpha_{i+1}\alpha_i\alpha_{i-1}\cdots\alpha_1 &= \sigma_k\sigma_{k-1}\cdots\sigma_{i+2}(sl)\tau\sigma_{i-1}\cdots\sigma_1 \\ &= \sigma_k\sigma_{k-1}\cdots\sigma_{i+2}\sigma_{i+1}\sigma_i\sigma_{i-1}\cdots\sigma_1 = \phi \end{aligned}$$

  is an expression for ϕ as a product of transpositions such that α_{i+1} is the first transposition that moves s. Thus, by induction, the statement is true for all i where $1 \leq i \leq k$. ■

Lemma 6.5.9 *Let $n \in \mathbb{N}$, $n > 1$, and $e \in \mathfrak{S}_n$. If e is written as a product of k transpositions, then it can be written as a product of $k - 2$ transpositions.*

Proof Assume that $e = \tau_k\tau_{k-1}\cdots\tau_1$ for some $k \geq 2$ and $s \in \tau_1$ where $s \in \{1, 2, \dots, n\}$. If e cannot be written as a product of $k - 2$ transpositions, then by Lemma 6.5.8, there exists an expression for e as a product of transpositions $\alpha_k\alpha_{k-1}\cdots\alpha_1$, where α_k is the first transposition that moves s. Hence, $\alpha_k(s) \neq s$. However, $s = e(s) = \alpha_k\alpha_{k-1}\cdots\alpha_1(s) = \alpha_k(s)$, which is a contradiction. ■

The identity permutation is an even permutation as $e = (ij)(ij)$ for any $i \neq j$. The following result shows that e cannot be odd.

Corollary 6.5.10 *Let $n \in \mathbb{N}$. The identity permutation $e \in \mathfrak{S}_n$ is not an odd permutation.*

Proof Assume that e can be written as a product of k transpositions where k is odd, i.e., $k = 2q + 1$ for some integer q. Repeatedly applying Lemma 6.5.9, e can be written as a product of $k - 2$ transpositions then as $k - 4$ transpositions, and finally after q repetitions, e can be written as a product of $k - 2q$ transpositions. Since $k-2q = 1$, then e is a transposition, which contradicts that e is the identity map. ■

Corollary 6.5.11 *Let $n \in \mathbb{N}$, $n > 1$, and $\phi \in \mathfrak{S}_n$. The permutation ϕ is either even or odd and cannot be both.*

Proof Let $\phi = \tau_k\cdots\tau_1$ and $\phi = \alpha_s\cdots\alpha_1$ be two expressions for ϕ as product of transpositions. Using the second expression, we obtain $\phi^{-1} = \alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_s^{-1}$ which implies that

$$e = \phi^{-1}\phi = \alpha_1^{-1}\alpha_2^{-1}\cdots\alpha_s^{-1}\cdot\tau_k\cdots\tau_1 = \alpha_1\cdots\alpha_s\cdot\tau_k\cdots\tau_1$$

Thus, e is a product of $k + s$ transpositions. As e cannot be an odd permutation, then $k + s$ must be an even integer. Therefore, k and s must be either both even, or both odd. ■

Using the last corollary and Remark 6.5.2 (1), one obtains the following result.

Corollary 6.5.12 *Let $n, k \in \mathbb{N}$, $n > 1$, $k \leq n$, and ϕ is a cycle of length k. The cycle ϕ is an odd permutation if and only if k is even, and vice versa.*

For each $n \in \mathbb{N}$, the set of even permutations in $\mathfrak{S}_n$ is denoted by $\mathcal{A}_n$, while $\mathcal{B}_n$ denotes the set of all odd permutation of $\mathfrak{S}_n$. Since e is an even permutation, $\mathcal{A}_n$ is never empty. The last corollary shows that the two sets do not intersect.

$$\mathcal{A}_n = \{\phi \in \mathfrak{S}_n : \phi \text{ is even}\}, \mathcal{B}_n = \{\phi \in \mathfrak{S}_n : \phi \text{ is odd}\}.$$

If $n = 1$, then $\mathfrak{S}_1 = \mathcal{A}_1 = \{e\}$ and $\mathcal{B}_1 = \emptyset$.
If $n = 2$, then $\mathfrak{S}_2 = \{e, (1\ 2)\}$, $\mathcal{A}_2 = \{e\}$, and $\mathcal{B}_2 = \{(1\ 2)\}$.

Example 6.5.13 To list all the elements in $\mathcal{A}_3$ and $\mathcal{B}_3$, list all the elements of $\mathfrak{S}_3$

$$\mathfrak{S}_3 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 3), (1\ 2), (2\ 3)\}.$$

As all the permutations $\mathfrak{S}_3$ are cycles, by using Corollary 6.5.12, we obtain

$$\mathcal{A}_3 = \{(1\ 2)(1\ 2), (1\ 3)(1\ 2), (1\ 2)(1\ 3)\}, \mathcal{B}_3 = \{(1\ 3), (1\ 2), (2\ 3)\}.$$

Another way to determine if a permutation is odd or even is by defining a function on $\mathfrak{S}_n$, called the sign function.

Definition 6.5.14 Let $n \in \mathbb{N}$, and ϕ in $\mathfrak{S}_n$. The sign of ϕ, denoted by $\mathrm{sgn}(\phi)$, is defined as $(-1)^k$, where k is the number of transpositions in any expression for ϕ as a product of transpositions.

Corollary 6.5.15 *Let $n \in \mathbb{N}$. The map* $\mathrm{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ *satisfies*

$$\mathrm{sgn}(\phi) = \begin{cases} 1 & \text{if } \phi \text{ is even} \\ -1 & \text{if } \phi \text{ is odd} \end{cases}$$

for any $\phi \in \mathfrak{S}_n$.

The following proposition provides a computationally convenient way to determine the sign of a permutation without the need of writing it as a product of transpositions.

Proposition 6.5.16 *Let $n \in \mathbb{N}$, and ϕ in $\mathfrak{S}_n$. The sign of ϕ is computed using the following equation*

$$\mathrm{sgn}(\phi) = \prod_{1 \le i < j \le n} \frac{\phi(j) - \phi(i)}{j - i}.$$

Example 6.5.17: Let $\phi = (1\ 2) \in \mathfrak{S}_3$. As the permutation ϕ is odd, then $\mathrm{sgn}(\phi)$ is -1. Using the formula in Proposition 6.5.16,

$$\begin{aligned} \mathrm{sgn}(\phi) &= \frac{\phi(3) - \phi(2)}{3 - 2} \frac{\phi(3) - \phi(1)}{3 - 1} \frac{\phi(2) - \phi(1)}{2 - 1} \\ &= \frac{3 - 1}{1} \cdot \frac{3 - 2}{2} \cdot \frac{1 - 2}{1} = (2)\left(\frac{1}{2}\right)(-1) = -1, \end{aligned}$$

as expected.

Our next goal is to show that $\mathcal{A}_n$ is always a group, and $\mathcal{B}_n$ is not a group for any n. We begin with the following proposition.

Proposition 6.5.18 Let $n \in \mathbb{N}$, and $\phi, \psi \in \mathfrak{S}_n$.

1. If ϕ, ψ have the same parity, then $\phi \circ \psi$ is even.
2. If ϕ, ψ have opposite parity, then $\phi \circ \psi$ is odd.
3. The product of two even (odd) permutations is an even permutation.

4. The product of a finite number of even permutations is an even permutation.
5. ϕ^{-1} is even (odd) if and only if ϕ is even (odd).
6. The cycle $(i_1 \dots i_k)$ is even (odd) if and only if k is odd (even).

Proof Let $\phi = \tau_k \cdots \tau_1$ and $\psi = \beta_s \cdots \beta_1$ be expressions of ϕ, ψ as products of transpositions. The composition $\phi \circ \psi = \tau_k \cdots \tau_1 \cdot \beta_s \cdots \beta_1$ is a product of $k + s$ transpositions.

1. If k and s have the same parity (either both even or both odd), then $k + s$ is even, and $\phi \circ \psi$ is even.
2. If k and s have the opposite parity (one is even and the other is odd), then $k + s$ is odd, so $\phi \circ \psi$ is odd.
3. The statement (3) follows form (1).
4. The statement of (4) follows from (3) by induction on the number of permutations.
5. The result of (5) follows as $\phi^{-1} = \tau_1^{-1} \cdots \tau_k^{-1} = \tau_1 \cdots \tau_k$ can be expressed using the same number of transpositions forming ϕ.
6. The result in (6) follows by Remark 6.5.2 which states that any cycle of length k where $k > 1$, can be written as a product of $k - 1$ transpositions. ■

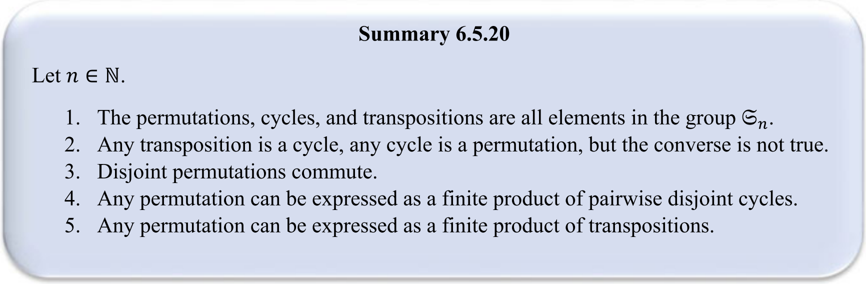
Note that since the product of two odd permutations is even, $\mathcal{B}_n$ is never closed and thus is never a group under the composition of maps.

Corollary 6.5.19 *Let* $n \in \mathbb{N}$, $n > 1$. *The set* $\mathcal{A}_n$ *of all even permutations on* $\{1, 2, \dots, n\}$ *forms a group under composition.*

Proof As $e \in \mathcal{A}_n$, the set $\mathcal{A}_n$ is a nonempty subset of $\mathfrak{S}_n$. As the composition of two even permutations is even, $\mathcal{A}_n$ is closed under composition, which implies that $\circ$ forms a binary operation on $\mathcal{A}_n$ (Proposition 4.1.6). The associativity property is inherited from $\mathfrak{S}_n$, and e serves as an identity element in $\mathcal{A}_n$. As the inverse of an even permutation is even (Proposition 6.5.18 (5)), $\mathcal{A}_n$ is closed undertaking the inverse, and thus, it is a group. ■

Definition 6.5.20 Let $n \in \mathbb{N}$, $n > 1$. The group $\mathcal{A}_n$ is called the alternating group of degree n.

Figure 6.4 summarized the main results about permutation that are shown in this chapter.



Summary 6.5.20

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

1. The permutations, cycles, and transpositions are all elements in the group $\mathfrak{S}_n$.
2. Any transposition is a cycle, any cycle is a permutation, but the converse is not true.
3. Disjoint permutations commute.
4. Any permutation can be expressed as a finite product of pairwise disjoint cycles.
5. Any permutation can be expressed as a finite product of transpositions.

Fig. 6.4 Summary

Exercises

Solved Exercises

6.1 Consider the following permutations.

$$\alpha = (2\ 5\ 6)(3\ 4) \in \mathfrak{S}_7$$

$$\beta = (2\ 5\ 3)(8\ 9\ 1\ 1)(7\ 1\ 4) \in \mathfrak{S}_{11}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 1 & 6 & 4 & 7 \end{pmatrix} \in \mathfrak{S}_7$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 2 & 3 & 10 & 6 & 4 & 7 & 9 & 8 & 1 \end{pmatrix} \in \mathfrak{S}_{10}.$$

(a) Write the matrix representation of the permutations α and β.
(b) Write the permutations γ and δ as a product of disjoint cycles.
(c) Find the order of all the above permutations.
(d) For each of the permutations determine whether it is odd or even.
(e) Find Move(α), Move(γ).
(f) Find γ^{39} and δ^{121}.
(g) Are the permutations α and γ disjoint? Explain.

Solution:

(a) Using the result in Corollary 6.2.7, we have

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

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 5 & 2 & 7 & 3 & 6 & 1 & 9 & 11 & 10 & 8 \end{pmatrix}.$$

(b) Applying the method in the proof of Proposition 6.2.9 yields

$$\gamma = (1\ 5\ 6\ 4) \text{ and } \delta = (1\ 5\ 6\ 4\ 10)(8\ 9).$$

(c) By Proposition 6.4.3,

$$\operatorname{ord}(\alpha) = \operatorname{lcm}(3, 2) = 6, \text{ and } \operatorname{ord}(\beta) = \operatorname{lcm}(3, 3, 3) = 3.$$

As $\gamma = (1\ 5\ 6\ 4)$ is a cycle of length 4, then $\operatorname{ord}(\gamma) = 4$. Finally, $\operatorname{ord}(\delta) = \operatorname{lcm}(5, 2) = 10$.

(d) Using the results in Proposition 6.5.18, one can obtain

- $\alpha = (2\ 5\ 6)(3\ 4)$ is a product of an even cycle and an odd cycle, and thus an odd permutation.
- $\beta = (2\ 5\ 3)(8\ 9\ 11)(7\ 1\ 4)$ is a product of three even cycles, and thus, it is an even permutation.
- $\gamma = (1\ 5\ 6\ 4)$ is a 4-cycle, and thus, it is an odd permutation.
- $\delta = (1\ 5\ 6\ 4\ 10)(8\ 9)$ is a product of even and odd permutations, and thus, it is an odd permutation.

(e) Using Definition 6.1.6, we obtain

$$\text{Move}(\alpha) = \{2, 3, 4, 5, 6\} \text{ and } \text{Move}(\gamma) = \{1, 4, 5, 6\}.$$

(f) Several methods can be used to compute γ^{39}, we present two methods both of which use the fact that $\text{ord}(\gamma) = 4$. The first method applies the quotient-remainder theorem on 39 and 4 to obtain

$$\gamma^{39} = \gamma^{9\times4+3} = \left(\gamma^4\right)^9\gamma^3 = \gamma^3 = (4\ 6\ 5\ 1).$$

An alternative method that uses fewer computations starts by noting that $\gamma\ \gamma^{39} = \gamma^{40} = (\gamma^4)^{10} = e$, thus $\gamma^{39} = \gamma^{-1} = (1\ 5\ 6\ 4)^{-1} = (4\ 6\ 5\ 1)$.

The two methods are applied to compute δ^{121} using the fact that $\text{ord}(\delta) = 10$, as follows:

$$\delta^{121} = \delta^{12\times10+1} = (\delta^{10})^{12}\delta = e\delta = \delta.$$

and

$$\delta^{-1}\delta^{121} = \delta^{120} = (\delta^{10})^{12} = e,\ \text{which implies that } \delta^{120} = \delta.$$

(g) No. The permutations α and γ are not disjoint since $\text{Move}(\alpha) \cap \text{Move}(\gamma) \neq \emptyset$.

6.2. Let $\alpha = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 4\ 3 \end{pmatrix}$, and $\beta = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 1\ 3\ 4 \end{pmatrix}$. Do α and β commute? Find $(\alpha\beta)^4$.

Solution:

Expressing α and β as a product of cycles yields

$$\alpha = (3\ 4) \text{ and } \beta = (1\ 2).$$

Since α and β are disjoint, by Proposition 6.1.10, $\alpha\beta = \beta\alpha$. Using the result of Corollary 6.1.11, we obtain

$$(\alpha\beta)^4 = \alpha^4\beta^4 = \left((34)^2\right)^2\left((12)^2\right)^2 = e.$$

6.3. Let $\alpha = (2\ 5\ 6)(3\ 2\ 4\ 1) \in \mathfrak{S}_7$. Find $\alpha^{-1}(2)$ and $\alpha(5)$.

Solution:

Since α takes 5 to 6 then $\alpha(5) = 6$. To compute $\alpha^{-1}(2)$, we must compute α^{-1} using one of the following methods:

- $\alpha = (256)(3241) = (135624)$, which implies that $\alpha^{-1} = (426531)$.
- $\alpha^{-1} = (3241)^{-1}(256)^{-1} = (1423)(652)$.

In both cases, $\alpha^{-1}(2) = 6$.

6.4. Let A be any nonempty set. Consider the symmetric group of A (Corollary 5.1.11). For each element f in $\mathfrak{S}_A$, define the relation $\cong_f$ on A as follows:

$$i \cong_f j \Leftrightarrow \exists\, m \in \mathbb{Z} \ni j = f^m(i).$$

The relation $\cong_f$ is an equivalence relation on the set A (Check!). The equivalence classes of such relation are called the orbits of f and given for each $i \in A$ as

$$\mathcal{O}r_f(i) = \left\{f^k(i) : k \in \mathbb{Z}\right\}.$$

Consider the additive group $(\mathbb{Z}, +)$. Let $f : \mathbb{Z} \to \mathbb{Z}$ be the map defined by $f(n) = n + 2$. As f is a bijective map on $\mathbb{Z}$, then f belongs to $\mathfrak{S}_{\mathbb{Z}}$, the symmetric group on $\mathbb{Z}$. Find all the distinct orbits of f.

Solution:

Let $i \in \mathbb{Z}$ be an arbitrary element.

$$\mathcal{O}r_f(i) = \left\{f^k(i) : k \in \mathbb{Z}\right\}.$$

One can show by induction on k that $f^k(i) = i + 2k$. Therefore, for any $i \in \mathbb{Z}$

$$\mathcal{O}r_f(i) = \{i + 2k : k \in \mathbb{Z}\} = i + 2\mathbb{Z}.$$

By applying the quotient-remainder theorem (Theorem 2.1.2) on i and 2, one obtain that there exist $q, r \in \mathbb{Z}$ such that $i = 2q + r$, where $0 \leq r < 2$, i.e.,

$$\mathcal{O}r_f(i) = i + 2\mathbb{Z} = r + 2q + 2\mathbb{Z} = r + 2\mathbb{Z}, \text{ where } r = 0, 1.$$

Hence, only two orbits of f exist, namely $2\mathbb{Z}$ (at $r = 0$) and $1 + 2\mathbb{Z}$ at $(r = 1)$.

6.5. Consider the symmetric group $\mathfrak{S}_9$. Find two elements α, β in $\mathfrak{S}_9$ such that

$$\operatorname{ord}(\alpha) = \operatorname{ord}(\beta) = 5 \text{ and } \operatorname{ord}(\alpha\beta) = 9.$$

Solution:

Let $\alpha = (1\ 2\ 3\ 4\ 5), \beta = (1\ 6\ 7\ 8\ 9) \in \mathfrak{S}_9$. As the order of any cycle is equal to its length, then $\text{ord}(\alpha) = 5 = \text{ord}(\beta)$. The product

$$\alpha\beta = (1\ 2\ 3\ 4\ 5)(1\ 6\ 7\ 8\ 9) = (1\ 6\ 7\ 8\ 9\ 2\ 3\ 4\ 5).$$

Therefore, $\text{ord}(\alpha\beta) = 9$.

6.6. Prove that $\alpha = (4\ 5\ 7\ 2\ 1\ 8) \in \mathfrak{S}_8$ is not a product of 3-cycles.

Solution:

Assume that α is a product of only 3-cycles. As any 3-cycle is an even permutation, thus by Proposition 6.5.18 (4), α is an even permutation, which contradicts the fact that

$$\alpha = (4\ 8)(4\ 1)(4\ 2)(4\ 7)(4\ 5)$$

is a product of five transpositions. Therefore, α cannot be a product of only 3-cycles.

6.7. Let $n \in \mathbb{N}$ such that $n > 1$. Prove that in $\mathfrak{S}_n$, the number of even permutations equals the number of odd permutations. Namely,

$$|\mathcal{A}_n| = |\mathcal{B}_n| = \frac{n!}{2}.$$

Solution:

Since $n > 1$, then $(1\ 2) \in \mathfrak{S}_n$. Define

$$\begin{aligned} f : \mathcal{A}_n &\to \mathcal{B}_n \\ \phi &\mapsto (12)\phi. \end{aligned}$$

The permutation $(1\ 2)$ is an odd permutation. Therefore, by Proposition 6.5.18 (2), the permutation $(1\ 2)\phi$ is odd for each $\phi \in \mathcal{A}_n$. Hence, f defines a function from $\mathcal{A}_n$ to $\mathcal{B}_n$. The map f is injective since

$$\begin{aligned} f(\phi_1) = f(\phi_2) &\Rightarrow (1\ 2)\phi_1 = (1\ 2)\phi_2 \\ &\Rightarrow (1\ 2)(1\ 2)\phi_1 = (1\ 2)(1\ 2)\phi_2 \\ &\Rightarrow \phi_1 = \phi_2. \end{aligned}$$

Since for any $\psi \in \mathcal{B}_n$, the permutation $(1\ 2)\psi \in \mathcal{A}_n$ and satisfies $f((1\ 2)\psi) = \psi$, then f is also surjective. Thus, f is a bijective map, and $|\mathcal{A}_n| = |\mathcal{B}_n|$. Since $\{\mathcal{A}_n, \mathcal{B}_n\}$ form a partition of the set $\mathfrak{S}_n$, then $n! = |\mathfrak{S}_n| = |\mathcal{A}_n| + |\mathcal{B}_n| = 2|\mathcal{A}_n|$, which implies the result.

6.8. Let $n \in \mathbb{N}$. Show that $\mathcal{A}_n = \mathfrak{S}_n$ if and only if $n = 1$.

Solution:

If $n = 1$, then $\mathfrak{S}_1 = \{e\}$. Since $\mathcal{A}_1$ is a group, it cannot be empty, and $\mathcal{A}_1$ is a nonempty subset of $\{e\}$. Thus, $\mathfrak{S}_1 = \mathcal{A}_1$. For the other direction, assume that $n > 1$, then $\alpha = (1\ 2)$ belongs to $\mathfrak{S}_n$. As the permutation α is odd permutation then α does not belong to $\mathcal{A}_n$. Therefore, $\mathfrak{S}_n \neq \mathcal{A}_n$.

6.9. Let $n \in \mathbb{N}$ and α be a cycle in $\mathfrak{S}_n$. Show that

$$\text{ord}(\alpha) \ \text{ is odd if and only if } \ \alpha \ \text{ is an even permutation.}$$

Solution:

Assume that $\alpha = (i_1 i_2 \ldots i_k)$ is a cycle in $\mathfrak{S}_n$. According to Lemma 6.4.2, we obtain $\text{ord}(\alpha) = k$. Proposition 6.5.18 (6) now implies the result.

6.10. Let $n \in \mathbb{N}$, where $n \geq 3$. Show that no nontrivial cycle belongs to the center of $\mathfrak{S}_n$. i.e., $C(\mathfrak{S}_n) = \{e\}$ for all $n \geq 3$.

Solution:

Let $\alpha = (i_1 i_2 \ldots i_k)$ be any cycle in $\mathfrak{S}_n$ such that $k \geq 2$.

- If $k = 2$, then $\alpha = (i_1 i_2)$. By choosing $i_3 \in \{1, 2, \ldots, n\} \backslash \{i_1, i_2\}$ $(n \geq k)$, and direct computations yield,

$$\alpha(i_1 i_3) = (i_1 i_3 i_2) \neq (i_1 i_2 i_3) = (i_1 i_3)\alpha,$$

  and α is not in the center.
- If $k > 2$, then $(i_1 i_2 \ldots i_k)(i_1 i_k)(i_k) = i_2 \neq i_k = (i_1 i_k)(i_1 i_2 \ldots i_k)(i_k)$. i.e.,

$$\alpha(i_1 i_k)(i_k) \neq (i_1 i_k)\alpha(i_k)$$

  and α is not in the center.

Unsolved Exercises

6.11. Let $\phi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,1\,5\,2 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,4\,5 \end{pmatrix}$ be permutations in $\mathfrak{S}_6$.
Express both ϕ and ψ as a product of disjoint cycles. Find $\phi \circ \psi$ and $\psi \circ \phi$.

6.12. In $\mathfrak{S}_4$, find α^{6431}, where $\alpha = (1\ 2\ 3\ 4)$.

6.13. Consider the group $\mathfrak{S}_6$ and the permutations

$$\phi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,5\,2\,1\,6\,4 \end{pmatrix}, \psi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,5\,3\,1\,6 \end{pmatrix}, \varphi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,5\,6\,5\,4 \end{pmatrix}$$

Find the order of these permutations. Find the permutation $\psi \circ \phi \circ \varphi$ and its inverse.

6.14. Find the order of the given permutations:

$$\alpha = (2\ 4\ 1\ 7)(3\ 5\ 6) \text{ as an element in } \mathfrak{S}_7$$
$$\beta = (1\ 4\ 2)(8\ 6)(3\ 5\ 6\ 7) \text{ as an element in } \mathfrak{S}_8$$

6.15. Consider the group $\mathfrak{S}_7$. Write the following permutations as a product of transpositions.

- $(1\ 2\ 3)(4\ 3\ 6\ 5)$.
- $(1\ 2\ 3\ 4\ 5)$.
- $(5\ 7)(3\ 2\ 4)(1\ 6)$.
- $(1\ 2\ 3)(4\ 5\ 6)$.
- $(3\ 4\ 2\ 6)(3\ 4\ 2\ 6)$.

6.16. Consider the group $\mathfrak{S}_8$. Let $\phi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 5\,4\,6\,2\,3\,8\,1\,7 \end{pmatrix}$, and $\psi = (1\ 5\ 3\ 4)$

i. Find the permutations

$$\phi^3\psi^{-2}\phi,\quad \psi^2\phi\psi,\quad \phi^2\psi^2,\quad \phi\psi\phi,\quad \psi\phi,\quad \phi\psi,\quad \psi^{-1}, \phi^{-1}.$$

ii. Find the parity of ϕ, ψ, and all permutations in (i).

iii. Find $\mathrm{ord}(\phi)$, $\mathrm{ord}(\psi)$, $\mathrm{ord}\big(\phi^2\big)$, and $\mathrm{ord}\big(\psi^4\big)$.

iv. Find the orbits of ϕ and ψ and the orbits of all permutations in (i).

v. Compute ϕ^7, ψ^6, ϕ^{22}.

6.17. Consider the permutations $\phi = (1\ 3\ 5)(1\ 2)$ and $\psi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 5\,2\,1\,7\,3\,6\,4 \end{pmatrix}$ as elements in $\mathfrak{S}_7$. Determine if these permutations are even or odd.

6.18. Let $\alpha = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,4\,3\,1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix}$ be elements in $\mathfrak{S}_4$.

a. Express α, β as products of transpositions.

b. Determine if α, β are even or odd permutations.

c. Find $\alpha \circ \beta$ and $\beta \circ \alpha$ and determine their parity.

d. Find the orders of $\alpha \circ \beta$, $\beta \circ \alpha$, β, α.

e. Does $\alpha(2) \in \mathrm{Move}(\alpha)$? Find $\mathrm{Move}(\alpha) \cap \mathrm{Move}(\beta)$.

f. Find all the distinct orbits of α and β.

6.19. Repeat all the questions in Exercise 6.18 given that $\beta = (2\ 4\ 3\ 5)$ and $\alpha = (1\ 2\ 3\ 6)$ as elements in $\mathfrak{S}_6$.

6.20. Consider the permutations $\phi = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,2\,4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$ as elements in $\mathfrak{S}_4$. Find $(\psi\phi)^5$ and its order as an element of $\mathfrak{S}_4$.

6.21. Give an example of $n \in \mathbb{N}$, and elements α and β in $\mathfrak{S}_n$ such that $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$and $\mathrm{ord}(\alpha\beta) = 4$.

6.22. Give an example of $n \in \mathbb{N}$, and elements α and β in $\mathfrak{S}_n$ such that $\mathrm{ord}(\alpha) = 3$, $\mathrm{ord}(\beta) = 4$. and $\mathrm{ord}(\alpha\beta) \neq \mathrm{lcm}(3, 4)$

6.23. List all possible orders of an element of $\mathcal{A}_6$.

Table 6.2 Table of the group $(A, *)$

$*$	x	y	z	g	h	k
x	x	y	z	g	h	k
y	y	x	k	h	g	z
z	z	h	x	k	y	g
g	g	k	h	x	z	y
h	h	z	g	y	k	x
k	k	g	y	z	x	h

6.24. Show that $C(\mathfrak{S}_n) = \{e\}$, for each $n \geq 3$.

6.25. How many cycles of order 3 are in $\mathfrak{S}_5$? How many cycles of order 3 are in $\mathfrak{S}_6$?

6.26. How many permutations in $\mathfrak{S}_5$ are of the form of a product of two transpositions?

6.27. Let $n \in \mathbb{N}$, and consider the group $\mathfrak{S}_n$. Let ϕ and ψ be two disjoint permutations in $\mathfrak{S}_n$. Show that if $\phi\psi = e$, then $\phi = \psi = e$.

6.28. Let $G = (\mathfrak{S}_3, \circ)$, $A = \{x, y, z, g, h, k\}$, and $f : A \to G$ be the bijective map given by $f(x) = e$, $f(y) = (1\ 2)$, $f(z) = (1\ 3)$, $f(g) = (2\ 3)$, $f(h) = (1\ 2\ 3)$, $f(k) = (1\ 3\ 2)$. Let $(A, *)$ be the group defined in Exercise 5.21. Show that the group structure on A is given by Table 6.2.

References

Carter, N. C. (2009). *Visual group theory.* Mathematical Association of America.

De Temple, D., & Webb, W. (2014). *Combinatorial reasoning, an introduction to the art of counting.* John Wiley & Sons, Inc.

Chapter 7
Subgroups

The present chapter focuses on subgroups, which are subsets of a group G that form groups under the operation inherited from G. For any group, the subset that contains only the identity element forms a subgroup, known as the trivial subgroup. Another subgroup of a group G is the whole set G. A subgroup that is not the trivial or not the whole group is called a proper subgroup. The first section of this chapter presents the definitions and basic examples of subgroups needed for the following sections. Section 7.2 examines the operation on subgroups such as intersection, union, and product of subgroups. Section 7.3 focuses on the study of the subgroups generated by subsets and presents important results regrading them. The most content heavy section in this chapter is Sect. 7.4, which introduces the notion of the cosets of a subgroup and presents the statement and proof of Lagrange's theorem. Normal subgroups are defined and studied in Sect. 7.5. In Sect. 7.6, the internal direct product of subgroups is described. We shall see in Chap 8 that the internal direct product of two subgroups can be identified with their direct product defined in Sect. 5.6 (Exercise 8.6). We end the chapter with an important notion in group theory known as quotient groups.

7.1 Definitions and Basic Examples

In this section, we present the basic definitions needed to study subgroups, and many examples to illustrate the associated notions.

Definition 7.1.1 Let $(G, *)$ be a group, and H be a nonempty subset of G. If H is a group under the operation $*$, then H is said to be a subgroup of G and denoted by $H < G$.

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_7

Example 7.1.2

1. For a group G, the subsets $H = \{e\}$ and $H = G$ are always subgroups of G. The subgroup $H = \{e\}$ is called the trivial subgroup of G. A proper subgroup of G is any nontrivial subgroup that is not equal to G.
2. The groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are subgroups of $(\mathbb{C}, +)$.
3. The group $\left(\mathbb{R}^+, \cdot\right)$ is subgroup of the multiplicative group $(\mathbb{R}^*, \cdot)$.
4. For each $n \in \mathbb{N}$, the set $\mathcal{A}_n$ consisting of all even permutations on $\{1, 2, \ldots, n\}$ forms a group under composition (Corollary 6.5.19), therefore $\mathcal{A}_n$ is a subgroup of $\mathfrak{S}_n$.
5. Let $n \in \mathbb{N}$, $n \geq 3$. As the product of two cycles of $\mathfrak{S}_n$ is not necessarily a cycle, the subset of $\mathfrak{S}_n$ that consists of all cycles on $\{1, 2, \ldots, n\}$ is not a subgroup.
6. For each $n \in \mathbb{N}$, the group $O(n)$, the orthogonal group of order n (Example 5.1.9), forms a subgroup of the general linear group $GL_n(\mathbb{R})$.

According to the uniqueness of the identity and inverse element (Corollaries 4.1.16 and 4.3.4), we obtain the following result.

Lemma 7.1.3 *Let G be a group and H be a subgroup of G. The identity elements in H and G coincide. For each $h \in H$, the inverse of h in H coincides with the inverse of h as an element in G.*

Note that the above lemma is not necessarily true in case of G is not a group. For example, let $G = \mathbb{R}^3$ endowed with the operation $*$, where $(x_1, x_2, x_3)*(y_1, y_2, y_3) = (x_1y_1, x_2y_2, x_3y_3)$. Let $H = \{(x_1, x_2, 0) : x_1, x_2 \in \mathbb{R}^*\}$. It is easy to verify that G is a monoid with identity $e_G = (1, 1, 1)$, and G is not a group since $(0, 0, 0)$ is not invertible in G. However, the subset H of G is a group under $*$ with an identity $e_H = (1, 1, 0)$ (Check!).

According to Definition 7.1.1, to show that a nonempty subset H is a subgroup of G, one must verify that H is closed under the operation $*$ and satisfies the three conditions that follow Definition 5.1.1. The following proposition shortens the processes used to verify that H is a subgroup of G.

Proposition 7.1.4 *Let $(G, *)$ be a group and H be a nonempty subset of G. The following statements are equivalent:*

1. *H is a subgroup of G.*
2. *H is closed under the operation $*$ and under taking the inverse, i.e.,*

$$a * b \in H \quad \forall\, a, b \in H \quad \wedge \quad a^{-1} \in H \quad \forall\, a \in H.$$

3. *$a * b^{-1} \in H$ for each $a, b \in H$.*

Proof We show that $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$, as follows.

If (1) holds, then H is a group under the operation $*$. Hence, H is closed under $*$ and by Lemma 7.1.3, it is close under taking the inverse. If (2) holds, let a, b be any arbitrary elements in H. Since $b \in H$, then by assumption b^{-1} is also an element of H. Since H is also closed under $*$, then $a * b^{-1} \in H$, as required. Assume that (3) holds. As H is a nonempty set, there exists a in H such that $a * a^{-1} \in H$. Thus, $e \in H$, and H contains the identity element of G. If $a \in H$, then $a^{-1} = e * a^{-1} \in H$. Thus, H contains the inverses of its elements. For any $a, b \in H$, as $b^{-1} \in H$, then $a * b = a * \left(b^{-1}\right)^{-1} \in H$. That is, H is closed under the operation $*$. Finally, H inherits the associativity property of $*$ as H is a subset of G. Consequently, H is a subgroup of G. ■

Example 7.1.5

1. The set of even integers, $2\mathbb{Z} = \{2q : q \in \mathbb{Z}\}$ forms a subgroup of $(\mathbb{Z}, +)$, while the odd integers do not. Note that the zero element belongs to $2\mathbb{Z}$, and thus, $2\mathbb{Z}$ is a nonempty subset of $\mathbb{Z}$ that satisfies $2q_1 - 2q_2 = 2(q_1 - q_2) \in 2\mathbb{Z}$ for all $q_1, q_2 \in \mathbb{Z}$. By Proposition 7.1.4, $2\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. The set of odd integers does not contain an identity element with respect to $+$. Moreover, it is not closed under the addition operation since the sum of two odd integers is always even.
2. Similar to $2\mathbb{Z}$, one can show that

$$n\mathbb{Z} = \{nq : q \in \mathbb{Z}\} \text{ is a subgroup of } (\mathbb{Z}, +) \text{ for any } n \in \mathbb{N}.$$

In fact, $n\mathbb{Z}$, $n \in \mathbb{N}$ are the only nontrivial subgroups of $(\mathbb{Z}, +)$ (Exercise 7.23).

3. Let G be an abelian group. For each integer m, the sets

$$mG = \left\{a^m : a \in G\right\} \text{ and } G[m] = \left\{a \in G : a^m = e\right\}$$

form subgroups of G (Proposition 5.5.13). For example, if G is the additive group $\mathbb{Z}_{30}$ then

$$5\mathbb{Z}_{30} = \{[0], [5], [10], [15], [20], [25]\} \text{ and } \mathbb{Z}_{30}[5] = \{[0], [6], [12], [18], [24]\}$$

are examples of subgroups of $\mathbb{Z}_{30}$. If G is not an abelian group, then the sets mG and $G[m]$ are not necessarily subgroups of G. For example, consider the symmetric group $\mathfrak{S}_3$. The subset

$$3\mathfrak{S}_3 = \{e, (12), (13), (23)\} = \mathfrak{S}_3[2]$$

is not a subgroup of $\mathfrak{S}_3$ (Check!). See also Example 6.4.6.

If H is a finite subset of a given group G, then the required conditions for H to be a subgroup can be weakened from those in Proposition 7.1.4. The following proposition demonstrates that one needs only to show that $*$ is a binary operation on H.

Proposition 7.1.6 *Let* $(G, *)$ *be a group and* H *be a finite nonempty subset of* G. *The subset* H *is a subgroup of* G *if and only if* H *is closed under the operation* $*$, *i.e.,*

$$H < G \Leftrightarrow a * b \in H \quad \forall \quad a, b \in H$$

Proof Assume that H is a finite nonempty subset of G. If H is a subgroup of G, then $(H, *)$ is a group, and therefore, H is closed under $*$. For the other direction, assume that H is closed under $*$. It suffices to show that the inverse of any element of H belongs to H (Proposition 7.1.4 (2)). Let a be any element of H. Since H is closed under $*$, then for each $n \in \mathbb{N}$, $a^n = \underbrace{a * \cdots * a}_{n \text{ times}}$ belongs to H. Therefore, $\{a, a^2, a^3, \ldots\} \subseteq H$. Since H is finite, there exist $m, n \in \mathbb{N}$ such that $a^m = a^n$. Without loss of generality, assume $m > n$, multiplying both sides of the equality by a^{-n} yields

$$\begin{aligned} a^m = a^n &\Rightarrow a^m * a^{-n} = a^n * a^{-n} \Rightarrow a^{m-n} = e \\ &\Rightarrow a * a^{m-n-1} = a^{m-n-1} * a = e. \end{aligned}$$

Since $m > n \geq 1$, then $m - n \geq 1$, and thus,

$$a^{-1} = a^{m-n-1} \in H.$$

■

Note that if $[a]$ is an arbitrary element in $\mathbb{Z}_n$, for any $q \in \mathbb{Z}$,

$$[aq] = \underbrace{[a] \oplus_n [a] \oplus_n \cdots \oplus_n [a]}_{q \text{ times}} \in \mathbb{Z}_n.$$

i.e., the set $[a]\mathbb{Z} = \{[aq] : q \in \mathbb{Z}\}$ forms a subset of $\mathbb{Z}_n$. The next example shows that $[a]\mathbb{Z}$ is a subgroup of the additive group $(\mathbb{Z}_n, \oplus_n)$ for any $a \in \mathbb{Z}$.

Example 7.1.7 Let $n \in \mathbb{N}$ and consider the additive group $(\mathbb{Z}_n, \oplus_n)$. For each $[a] \in \mathbb{Z}_n$, the subset $[a]\mathbb{Z} = \{[aq] : q \in \mathbb{Z}\}$ is nonempty as the zero element $[0] = [a0] \in [a]\mathbb{Z}$. If $[aq_1], [aq_2] \in [a]\mathbb{Z}$ for some $q_1, q_2 \in \mathbb{Z}$, then

$$[aq_1] \oplus_n [-aq_2] = [a(q_1 - q_2)] \in [a]\mathbb{Z}, \quad \text{where } q_1 - q_2 \in \mathbb{Z}.$$

By Proposition 7.1.6, $[a]\mathbb{Z}$ is a subgroup of $\mathbb{Z}_n$. In fact, these subgroups are the only subgroups of $\mathbb{Z}_n$ (Exercise 7.24).

For instance, if $n = 12$, then $[1]\mathbb{Z} = \{[q] : q \in \mathbb{Z}\} = \mathbb{Z}_{12}$, $[2]\mathbb{Z} = \{[0],[2],[4],[6],[8],[10]\}$, $[3]\mathbb{Z} = \{[0],[3],[6],[9]\}$, $[4]\mathbb{Z} = \{[0],[4],[8]\}$, $[5]\mathbb{Z} = \mathbb{Z}_{12}$, $[6]\mathbb{Z} = \{[0],[6]\}$, $[7]\mathbb{Z} = \mathbb{Z}_{12}$, $[8]\mathbb{Z} = \{[0],[8],[4]\}$, $[9]\mathbb{Z} = \{[0],[9],[6],[3]\}$, $[10]\mathbb{Z} = \{[0],[10],[8],[6],[4],[2]\}$, and $[11]\mathbb{Z} = \mathbb{Z}_{12}$ are all subgroups of $\mathbb{Z}_{12}$.

Example 7.1.8

1. Consider the group $(\mathbb{C}^*, \cdot)$, where $\cdot$ is the multiplication of complex numbers. Let $H(4) = \left\{z \in \mathbb{C}^* : z^4 = 1\right\} = \{\pm 1, \pm i\}$. The subset $H(4)$ is a subgroup of $(\mathbb{C}^*, \cdot)$. In general, for each $n \in \mathbb{N}$, one can show that

$$H(n) = \left\{z \in \mathbb{C}^* : z^n = 1\right\}$$

is a subgroup of $(\mathbb{C}^*, \cdot)$ using Proposition 7.1.4 (3), as follows: Assume that $n \in \mathbb{N}$, since $1 \in H(n)$, then $H(n)$ is a nonempty subset of $\mathbb{C}^*$. If z_1, z_2 are two elements in $H(n)$, then

$$\left(z_1 z_2^{-1}\right)^n = (z_1)^n \left(z_2^{-1}\right)^n = (z_1)^n \left(z_2^n\right)^{-1} = 1$$

i.e., $z_1 z_2^{-1} \in H(n)$. The subgroup $H(n)$ is called the group of the nth roots of unity.

With basic knowledge of complex analysis (Exercise 7.1), one can see that the subgroup $H(n)$ is finite. Namely,

$$H(n) = \left\{e^{\frac{2\pi i k}{n}} : 0 \leq k < n\right\}$$

where $e^{i\theta} = \cos\theta + i \sin\theta$.

2. Consider the group $(\mathbb{C}^*, \cdot)$, where $\cdot$ is the multiplication on complex numbers. Let T be the unit circle, i.e., $T = \{z \in \mathbb{C}^* : |z| = 1\}$. The unit circle T is a nonempty subset of $\mathbb{C}^*$ that forms a subgroup of $(\mathbb{C}^*, \cdot)$ (Check!). Note that the circle $\{z \in \mathbb{C}^* : |z| = 4\}$, whose center is at $(0, 0)$ and whose radius is 2, is a nonempty subset of $\mathbb{C}^*$ that is not a subgroup of $(\mathbb{C}^*, \cdot)$ since it is not closed under multiplication.

Example 7.1.9

1. Consider the group $(\mathfrak{S}_n, \circ)$ where $n \geq 3$, and let $H = \{e, (123), (132)\}$. The set H is a nonempty subset of $\mathfrak{S}_n$ that is closed under composition and taking the inverse since $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are inverse of each other. Therefore, H is a subgroup of the symmetric group $(\mathfrak{S}_n, \circ)$. If $n = 3$, then $H = \mathcal{A}_3$, which we have already shown to be a subgroup of $(\mathfrak{S}_3, \circ)$ (Corollary 6.5.19). Similarly, one can prove that $\mathcal{A}_k < \mathfrak{S}_n$ for all $n \geq k$.
2. Consider the group $(\mathfrak{S}_7, \circ)$. Let A be the subset of $\mathfrak{S}_7$ that consists of all permutations that permute only $\{2,\ 3,\ 5\}$ and fix any other elements in $\{1, 2, \ldots, 7\}$.

The subset A contains the identity and the product of two permutations of A is an element in A. Thus, A is a nonempty finite subset of $\mathfrak{S}_7$ that is closed under the product of permutations. Therefore, A is a subgroup of $\mathfrak{S}_7$ (Proposition 7.1.6). Note that A consists of permutations that only permute three elements, so A can be considered as a permutation group on three elements.

3. We generalize the above example as follows. Let $n \in \mathbb{N}$. Consider the group $(\mathfrak{S}_n, \circ)$, choose k such that $1 < k \leq n$, and let F_k be a subset of k element of $\{1, 2, \ldots, n\}$. Let A be the subset of $\mathfrak{S}_n$ that consists of all permutations that permute the elements of F_k and fix all other elements in $\{1, 2, \ldots, n\}$. As the product of two permutations of A is an element in A, then A is a nonempty finite subset of $\mathfrak{S}_n$ that is closed under the product of permutations. Therefore, A is a subgroup of $\mathfrak{S}_n$ (Proposition 7.1.6). Since A consists of permutations that only permute k elements, then A is considered as a permutation group on k elements.

Example 7.1.10 The center of any group G is a subgroup of G. This result directly follows by Proposition 5.4.8. For example, consider $GL_2(\mathbb{R})$, the group of invertible 2×2 matrices with real coefficients under the matrix multiplication. The subset $\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}^*\right\}$ is a subgroup of $GL_2(\mathbb{R})$ since it is the center of $GL_2(\mathbb{R})$ (Example 5.4.9 (3)).

Proposition 7.1.11 *Let $(G, *)$ be an abelian group and $T = \{a \in G : \mathrm{ord}(a) < \infty\}$. The subset T forms a subgroup of G. The subgroup T is called the torsion subgroup of G.*

Proof Since $\mathrm{ord}(e) = 1$, then T is a nonempty subset of G. Let x, y be any elements in T such that $\mathrm{ord}(x) = n < \infty$, $\mathrm{ord}(y) = m < \infty$. Since G is abelian, it follows by Lemma 5.4.5 (2) that

$$\left(x * y^{-1}\right)^{nm} = x^{nm} * \left(y^{-1}\right)^{nm}.$$

Hence,

$$\left(x * y^{-1}\right)^{nm} = x^{nm} * \left(y^{-1}\right)^{nm} = \left(x^n\right)^m * \left(y^m\right)^{-n} = e$$

i.e., By Lemma 5.5.5, $\mathrm{ord}\left(x * y^{-1}\right) \leq nm < \infty$, and T is a subgroup of G. ■

The requirement in the last proposition that G is abelian is necessary. For example, in the group $(GL_2(\mathbb{R}), \cdot)$, the elements $A = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ have finite orders $(\mathrm{ord}(A) = \mathrm{ord}(B) = 2)$. However, one can show by induction that $(AB)^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \neq I_2$ for each positive integer n. Therefore, T is not a subgroup of $GL_2(\mathbb{R})$.

Let G be a group. According to Corollary 5.1.11, the set of all bijective maps on G, denoted by $\mathfrak{S}_G$, forms a group under the composition of maps. Our next goal is to present examples of subgroups of the group $\mathfrak{S}_G$, the subgroup of left and right multiplications. We begin with the following definition.

Definition 7.1.12 Let $(G, *)$ be a group. For $a \in G$, the map $f_a : G \to G$ defined by $x \mapsto a * x$ for all $x \in G$, is called the left multiplication by a.

Proposition 7.1.13 *Let G be a group. For $a \in G$, the left multiplication by a is a bijective map on G and $f_a^{-1} = f_{a^{-1}}$.*

Proof The injectivity of the map f_a follows by cancelation law. To show that f_a is surjective, let y be an arbitrary element in G. As G is a group, $x = a^{-1}y$ is an element in G and satisfies $f_a(x) = y$. Since

$$\begin{aligned} f_{a^{-1}} f_a(x) &= a^{-1} * (a * x) = x, \quad \text{and} \\ f_a f_{a^{-1}}(x) &= a * (a^{-1} * x) = x, \end{aligned}$$

then $f_a^{-1} = f_{a^{-1}}$. ■

The set of all left multiplication maps of G is denoted by $Lm(G)$. Similarly, one can define the right multiplication on G. The set of all right multiplication maps of G is denoted by $Rm(G)$.

Proposition 7.1.14 *Let G be a group. The set $Lm(G)$ forms a subgroup of $\mathfrak{S}_G$, such that $f_a \circ f_b = f_{a*b}$ for all $a, b \in G$.*

Proof By Proposition 7.1.13, $Lm(G)$ is a subset of $\mathfrak{S}_G$. This subset is nonempty, as $f_e \in Lm(G)$. For each $f_a, f_b \in Lm(G)$,

$$f_a f_b^{-1}(x) = a * \left(b^{-1} * x\right) = \left(a * b^{-1}\right) * x = f_{a*b^{-1}}(x) \quad \text{for all } x \in G$$

i.e., $f_a f_b^{-1} = f_{a*b^{-1}} \in Lm(G)$. Therefore, $Lm(G)$ is a subgroup of $\mathfrak{S}_G$.

For each $a, b \in G$,

$$f_a \circ f_b(x) = a * (b * x) = (a * b) * x = f_{a*b}(x) \quad \text{for all } x \in G.$$

■

7.2 Operations on Subgroups

In this section, we study set's operations on subgroups, such as intersections and union of subgroups. We also define the product of subgroups. We defer the study of the quotient of groups to Sect. 7.7, as several results must be developed before the quotient can be defined.

Proposition 7.2.1 *Let $(G, *)$ be a group. The intersection of any family of subgroups of G is a subgroup of G. i.e., if $\{H_i : i \in I \subseteq \mathbb{N}\}$ is a set of subgroups of G, then $\bigcap_{i \in I} H_i < G$.*

Proof Since $e \in H_i \subseteq G$ for each $i \in I$, then $e \in \bigcap_{i \in I} H_i \subseteq G$, and thus, $\bigcap_{i \in I} H_i$ is a nonempty subset of G. Let a, b be elements in $\bigcap_{i \in I} H_i$. Both elements $a, b \in H_i$ for each $i \in I$. Since H_i is a subgroup of G, then $a * b^{-1} \in H_i$ for each $i \in I$. Therefore $a * b^{-1} \in \bigcap_{i \in I} H_i$. Proposition 7.1.4 (3) implies the result. ■

Example 7.2.2 Consider the additive group $(\mathbb{Z}, +)$ and its subgroups $H = 2\mathbb{Z}$, $K = 5\mathbb{Z}$. According to Proposition 7.2.1, the intersection $H \cap K = 10\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. However, their union is not closed under the addition operation $+$, since $2 \in H$ and $5 \in K$, but $2 + 5 = 7 \notin H \cup K$.

This example shows that the union of subgroups of G does not need to form a subgroup of G. The following proposition determines the conditions on H and K under which the union $H \cup K$ forms a subgroup of G.

Proposition 7.2.3 *Let G be a group. If H, K are subgroups of G, then*

$$H \cup K < G \Leftrightarrow H \subseteq K \quad \vee \quad K \subseteq H.$$

Proof If $H \subseteq K \vee K \subseteq H$, then $H \cup K = K \vee H \cup K = H$. In both cases, $H \cup K$ is a subgroup of G. For the other direction, assume that $H, K,$ and $H \cup K$ are subgroups of G. If $H \nsubseteq K$, we show that $K \subseteq H$, as follows. Let y be an arbitrary element of K. Since $H \nsubseteq K$, there exists $x_0 \in H$ such that $x_0 \notin K$. Both elements x_0 and y belong to $H \cup K$ Since $H \cup K$ is a subgroup of G, we have that $x_0 * y^{-1} \in H \cup K$. If $x_0 * y^{-1} \in K$, then $x_0 = x_0 * y^{-1} * y \in K$, which leads to a contradiction. Hence, $x_0 * y^{-1}$ must be an element of H. Since H is a group, we get

$$y^{-1} = x_0^{-1} * x_0 * y^{-1} \in H.$$

Thus, $y \in H$. Consequently, $K \subseteq H$. If $K \nsubseteq H$ by similar argument we can show that $H \subseteq K$. ■

Definition 7.2.4 Let $(G, *)$ be a group and let H, K be subsets of G. The product of H and K is defined as the subset.

$$HK = \{h * k : h \in H, k \in K\}.$$

If H has only one element h, we write hK for HK. Similarly, we write Hk for HK if K contains only one element k. It is easy to show that if H, K and F are subgroups of a group G, then their product satisfies the following:

- $(HK)F = H(KF)$.
- $H \subseteq HK$ and $H \subseteq KH$.
- If the operation $*$ is abelian, then $HK = KH$.
- If $H \subseteq K$, then both HK and KH are equal to K. In particular,

$$\{e\}H = H, \;\; H\{e\} = H, \;\text{ and } GH = G, \;\; HG = G.$$

Definition 7.2.4 can be generalized to a product of n subgroups of G, as follows:

Definition 7.2.5 Let $(G, *)$ be a group, and let $H_1, \dots, H_n$ be subgroups of G. The subset

$$\{h_1 * h_2 * \cdots * h_n : h_i \in H_i, 1 \le i \le n\}$$

is called the product of the subgroups $H_1, \dots, H_n$ and denoted by $H_1 H_2 \cdots H_n$.

Example 7.2.6

1. Consider the additive group $(\mathbb{Z}, +)$. Let $H = 5\mathbb{Z}$ and $K = 8\mathbb{Z}$. Both H and K are subgroups of $(\mathbb{Z}, +)$. The product of H and K is

$$5\mathbb{Z} + 8\mathbb{Z} = \{5n + 8m : m, n \in \mathbb{Z}\}$$

Note that

$$\begin{aligned} 5\mathbb{Z} + 8\mathbb{Z} &= \{5n + 8m : m, n \in \mathbb{Z}\} = \{5(n + m) + 3m : m, n \in \mathbb{Z}\} \\ &= \{5k + 3m : m, k \in \mathbb{Z}\} = \{2k + 3k + 3m : m, k \in \mathbb{Z}\} \\ &= \{2k + 3(k + m) : m, k \in \mathbb{Z}\} = \{2k + 3s : s, k \in \mathbb{Z}\} \\ &= \{2k + 2s + s : s, k \in \mathbb{Z}\} = \{2(k + s) + s : s, k \in \mathbb{Z}\} \\ &= \{2t + s : s, t \in \mathbb{Z}\} = \{z : z \in \mathbb{Z}\} = \mathbb{Z}. \end{aligned}$$

This equality can be obtained in one step using Exercise 7.12.

2. Consider the additive group $(\mathbb{Z}_{12}, \oplus_{12})$ and the subgroups

$H_{[2]} = [2]\mathbb{Z} = \{[0], [2], [4], [6], [8], [10]\}$, $H_{[3]} = [3]\mathbb{Z} = \{[0], [3], [6], [9]\}$, and $H_{[4]} = [4]\mathbb{Z} = \{[0], [4], [8]\}$.

The product of $H_{[2]}$ and $H_{[4]}$ is

$$H_{[2]}H_{[4]} = H_{[2]} \oplus_{12} H_{[4]} = \{[0], [4], [8], [2], [6], [10]\} = H_{[2]}.$$

The product of $H_{[2]}$ and $H_{[3]}$ is

$$\begin{aligned} H_{[2]}H_{[3]} &= H_{[2]} \oplus_{12} H_{[3]} \\ &= \{[0], [3], [6], [9], [2], [5], [8], [11], [4], [7], [10], [1]\} = \mathbb{Z}_{12}. \end{aligned}$$

The product of $H_{[3]}$ and $H_{[4]}$ is

$$H_{[3]} \oplus_{12} H_{[4]} = \{[0], [4], [8], [3], [7], [11], [6], [10], [2], [9], [1], [5]\} = \mathbb{Z}_{12}.$$

The product of $H_{[2]}$, $H_{[3]}$, and $H_{[4]}$ is

$$\begin{aligned} H_{[2]}H_{[3]}H_{[4]} &= H_{[2]} \oplus_{12} H_{[3]} \oplus_{12} H_{[4]} \\ &= \mathbb{Z}_{12} \oplus_{12} H_{[4]} = \mathbb{Z}_{12}. \end{aligned}$$

3. Consider the group $(\mathbb{C}^*, \cdot)$ defined in Example 7.1.8 and its subgroups

$$H(n) = \left\{z \in \mathbb{C}^* : z^n = 1\right\}.$$

To compute the product of $H(2)$ and $H(5)$, we list all the elements of both subgroups and multiply them, as follows:

$$\begin{aligned} H(2) &= \left\{e^{i0}, e^{\pi i}\right\} = \{1, -1\} \\ H(5) &= \left\{e^{i0}, e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}\right\}. \end{aligned}$$

Therefore,

$$\begin{aligned} H(2)H(5) &= \left\{z_1 z_2 \in \mathbb{C}^* : z_1^2 = 1 \wedge z_2^5 = 1\right\} \\ &= \left\{e^{i0}, e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}, -e^{i0}, -e^{\frac{2\pi i}{5}}, -e^{\frac{4\pi i}{5}}, -e^{\frac{6\pi i}{5}}, -e^{\frac{8\pi i}{5}}\right\}. \end{aligned}$$

Example 7.2.7 Let $G = \mathfrak{S}_3$ endowed with composition of functions, $H = \{e, (1\ 2)\}$ and $K = \{e, (1\ 3)\}$. The sets H and K are subgroups of G (verify!), and their product HK is

$$\begin{aligned} HK &= \{e, (1\ 3), (1\ 2), (1\ 2)(1\ 3)\} \\ &= \{e, (1\ 2), (1\ 3), (1\ 3\ 2)\} \end{aligned}$$

and

$$\begin{aligned} KH &= \{e, (1\ 2), (1\ 3), (1\ 3)(1\ 2)\} \\ &= \{e, (1\ 2), (1\ 3), (1\ 2\ 3)\} \neq HK. \end{aligned}$$

Since $(1\ 3)(1\ 2) = (1\ 2\ 3) \notin HK$ and $(1\ 2)(1\ 3) = (1\ 3\ 2) \notin KH$, neither HK nor KH is a group. This result shows that when both H and K are subgroups of G, their product HK is not necessarily a subgroup of G. The following proposition determines the conditions needed to guarantee that HK becomes a group.

Proposition 7.2.8 *If $(G, *)$ is a group and H, K are subgroups of G, then*

$$HK < G \Leftrightarrow HK = KH.$$

Proof Assume that HK is a subgroup of G. We show that $KH \subseteq HK$ and $HK \subseteq KH$ as follows. If $y \in KH$, there exist $h \in H, k \in K \ni y = k * h$. As H and K are groups, $h^{-1} \in H$ and $k^{-1} \in K$, and $h^{-1} * k^{-1} \in HK$. Since HK is a group,

$$y = k * h = \left(h^{-1} * k^{-1}\right)^{-1} \in HK$$

i.e., $KH \subseteq HK$. For the other inclusion, if $y \in HK$, then there exist $h \in H, k \in K \ni y = h * k$. Since HK is a subgroup, then $y^{-1} = (h * k)^{-1} \in HK$, i.e., $(h * k)^{-1} = h_1 * k_1$ for some $h_1 \in H$ and $k_1 \in K$. Consequently, $y = h * k = (h_1 * k_1)^{-1} = k_1^{-1} * h_1^{-1} \in KH$ and $HK \subseteq KH$. To show the other direction of the biconditional statement, assume that $HK = KH$. Since $e = e * e \in HK$, then HK is a nonempty subset of G. Let x, y be any elements in HK, then there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $x = h_1 * k_1$, $y = h_2 * k_2$. Hence,

$$x * y^{-1} = h_1 * k_1 * (h_2 * k_2)^{-1} = h_1 * k_1 * k_2^{-1} * h_2^{-1} = h_1 * k_3 * h_2^{-1}$$

where $k_3 \in K$. Since $k_3 * h_2^{-1}$ is an element in KH, and $HK = KH$, then there exist $h \in H, k \in K$ such that $k_3 * h_2^{-1} = h * k$. Therefore, $x * y^{-1} = h_1 * h * k \in HK$. According to Proposition 7.1.4 (3), HK forms a subgroup of G. ■

According to Proposition 7.2.8, all the product groups in Example 7.2.6 are groups.

Corollary 7.2.9 *Let G be an abelian group. If H and K are subgroups of G, then HK is a subgroup of G.*

Note that $HK = KH$ does not mean that any pair of elements in H and K commute. For example, in the symmetric group $\mathfrak{S}_3$, if $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ and $K = \{e, (1\ 2)\}$, then $HK = KH = \mathfrak{S}_3$, but $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$. The reader should note that if G is a finite group and H, K are subgroups of G, then HK and KH can be easily obtained using tables. For example, the elements of HK and KH in Example 7.2.7 are in Tables 7.1 and 7.2.

Proposition 7.2.10 *Let G be a group and let H, K be subgroups of G such that $H \cap K = \{e\}$. Every element in the product HK can be written in a unique form of $h * k$, where $h \in H$ and $k \in K$.*

Proof Assume that $h_1 * k_1 = h_2 * k_2$ are two representations of an element in HK, then

$$k_1 * k_2^{-1} = h_1^{-1} * (h_1 * k_1) * k_2^{-1} = h_1^{-1} * (h_2 * k_2) * k_2^{-1} = h_1^{-1} * h_2.$$

Table 7.1 HK in Example 7.2.7

$\circ$	e	(1 3)
e	e	(1 3)
(1 2)	(1 2)	(1 3 2)

Table 7.2 KH in Example 7.2.7

$\circ$	e	(1 2)
e	e	(1 2)
(1 3)	(1 3)	(1 2 3)

Hence, $k_1 * k_2^{-1} = h_1^{-1} * h_2$ belongs to both H and K, so to their intersection $\{e\}$. That is, $k_1 * k_2^{-1} = e = h_1^{-1} * h_2$, which implies that $h_1 = h_2, k_1 = k_2$. ■

The generalization of Proposition 7.2.10 to n subgroups is not possible unless we introduce certain conditions for the subgroups. These conditions are introduced after studying normal subgroups in Sect. 7.5 (Proposition 7.5.16).

7.3 Subgroups Generated by a Set and Finitely Generated Subgroups

Let G be a group and S be a subset of G. Let $H_i, i \in I \subseteq \mathbb{N}$ be all subgroups of G that contain S. According to Proposition 7.2.1, the intersection of the subgroups $H_i, i \in I$, forms a subgroup of the whole group G. This subgroup still contains the subset S and is called the subgroup generated by S.

Definition 7.3.1 Let G be a group and S be a subset of G. The subgroup of G generated by S, denoted by $\langle S \rangle$, is the intersection of all subgroups of G that contain S. i.e.,

$$\langle S \rangle = \cap\{H_i : \quad S \subseteq H_i, \quad H_i < G\}.$$

It follows directly from the definition of $\langle S \rangle$ that if H is a subgroup containing S, it will contain $\langle S \rangle$. If $S = \{a_1, a_2, \ldots, a_n\}$ is a finite set, then $\langle S \rangle$ is said to be finitely generated, and the notation $\langle a_1, a_2, \ldots, a_n \rangle$ is used instead of $\langle \{a_1, a_2, \ldots, a_n\} \rangle$.

Definition 7.3.2 Let G be a group and $S \subseteq G$. If $G = \langle S \rangle$, then G is said to be generated by S (or S generates G). If S is a finite set, then G is said to be a finitely generated group.

Lemma 7.3.3 *Let G be a group and S be a subset of G. The subgroup generated by S is the smallest subgroup of G that contains S.*

Proof Since $\langle S \rangle$ is an intersection of subgroups of G, then by Proposition 7.2.1, $\langle S \rangle$ is a subgroup of G that contains S. Assume that H is a subgroup of G that contains S. The subgroup H belongs to the set $\{H_i : S \subseteq H_i, H_i < G\}$. i.e., $\langle S \rangle = \cap\{H_i : S \subseteq H_i, \quad H_i < G\} \subseteq H$. Therefore, $\langle S \rangle$ is the smallest subgroup of G that contains S. ■

Corollary 7.3.4 *Let $(G, *)$ be a group and T, S be subsets of G. If $T \subseteq S$, then $\langle T \rangle \subseteq \langle S \rangle$. In particular, if $x \in S$, then $\langle x \rangle \subseteq \langle S \rangle$.*

Proof Assume that T, S are subsets of G such that $T \subseteq S$. Since $T \subseteq S \subseteq \langle S \rangle$, then $\langle S \rangle$ is a subgroup of G that contains T. Therefore, $\langle S \rangle$ contains the intersection of all subgroups of G that contain T, i.e., $\langle S \rangle$ contains $\langle T \rangle$. If $x \in S$, then $\{x\} \subseteq S$, which implies that $\langle x \rangle = \langle \{x\} \rangle \subseteq \langle S \rangle$. ■

The empty set $\emptyset$ is a subset of the trivial subgroup $\{e\}$, and the only subgroup of G that contains G is G itself, which implies that

$$\langle\emptyset\rangle = \langle e\rangle = \{e\} \ \text{ and } \ \langle G\rangle = G.$$

For a subset S different from $\emptyset$, $\{e\}$, and G, one must have practical tools to compute $\langle S\rangle$ since it is not always possible to find all the subgroups containing a given subset S. To obtain a useable formula to compute $\langle S\rangle$, we provide several necessary lemmas and propositions.

Lemma 7.3.5 *Let $(G, *)$ be a group and S be a nonempty subset of G. The subset*

$$H = \left\{a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} : a_i \in S, r_i \in \mathbb{Z}, \quad 1 \le i \le n, \quad n \in \mathbb{N}\right\}$$

is a subgroup of G that contains S.

Proof Since S is not empty, and for each $a \in S$, $a = a^1 \in H$, thus H is a nonempty subset of G that contains S. Let $x, y \in H$. According to the definition of H,

$x = a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}$, and $y = b_1^{t_1} * b_2^{t_2} * \cdots * b_m^{t_m}$ for some $n, m \in \mathbb{Z}$, $a_i, b_j \in S$, and $r_i, t_j \in \mathbb{Z}$.

where $1 \le i \le n$, $1 \le j \le m$. Hence,

$$\begin{aligned} x * y^{-1} &= \left(a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}\right) * \left(b_1^{t_1} * b_2^{t_2} * \cdots * b_m^{t_m}\right)^{-1} \\ &= a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} * b_m^{-t_m} * \cdots * b_2^{-t_2} * b_1^{-t_1} \in H \end{aligned}$$

i.e., $H < G$ (Proposition 7.1.4). ■

Proposition 7.3.6 *Let G be a group and $\emptyset \neq S \subseteq G$. The subgroup generated by S can be expressed as*

$$\langle S\rangle = \left\{a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} : a_i \in S, r_i \in \mathbb{Z}, \quad 1 \le i \le n, \quad n \in \mathbb{N}\right\}.$$

If S consists of one element a, then $\langle a\rangle = \langle\{a\}\rangle = \{a^n : n \in \mathbb{Z}\}$.

Proof Let $H = \left\{a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} : a_i \in S, r_i \in \mathbb{Z}, \quad 1 \le i \le n, \quad n \in \mathbb{N}\right\}$. By Lemma 7.3.5, H is a subgroup of G that contains S. Hence, $\langle S\rangle \subseteq \langle H\rangle = H$ (Corollary 7.3.4). For the other direction, if $x \in H$, then $x = a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}$ for some $r_i \in \mathbb{Z}$, where $1 \le i \le n$ and $a_1, a_2, \ldots, a_n \in S$. Therefore, $a_1, a_2, \ldots, a_n \in \langle S\rangle$. Since $\langle S\rangle$ is a subgroup of G, then $x = a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} \in \langle S\rangle$. Consequently, $H \subseteq \langle S\rangle$. ■

Note that the elements $a_i \in S$ in the expression $a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}$ may not be different. For example, if a_1 and a_2 are elements in S, then

$$a_1 * a_2^3 * a_1^2 * a_2 * a_1 * a_2^{11}$$

is an element in $\langle S\rangle$.

Corollary 7.3.7 *If G is a group, and a is an element in G, then $\langle a\rangle = \left\langle a^{-1}\right\rangle$.*

Example 7.3.8 In $(\mathbb{Z}, +)$, one can easily check that

1. $\langle -1\rangle = \langle 1\rangle = \{k, k \in \mathbb{Z}\} = \mathbb{Z}$, $\langle -2\rangle = \langle 2\rangle = \{2k,\ \ k \in \mathbb{Z}\} = 2\mathbb{Z}$.

   In general, for any $a \in \mathbb{Z}$, the subgroup generated by a is

   $$\langle a\rangle = \{ak : k \in \mathbb{Z}\} = a\mathbb{Z},$$

   where ka is the additive notation of a^k.

2. For any $a, b \in \mathbb{Z}$, $b|a$ if and only if there exists $q \in \mathbb{Z}$ such that $a = qb$, this is if and only if $\langle a\rangle \subseteq \langle b\rangle$, i.e.,

   $$\langle a\rangle \subseteq \langle b\rangle \text{ if any only if } b|a.$$

3. To compute $\langle\{2, 3\}\rangle$, the situation is slightly more complicated than the examples in (1). Using the additive term notation, we obtain

   $$\begin{aligned}\langle\{2, 3\}\rangle &= \{2n + 3m : n, m \in \mathbb{Z}\}\\ &= \{2n : n \in \mathbb{Z}\} + \{3m : m \in \mathbb{Z}\}\\ &= 2\mathbb{Z} + 3\mathbb{Z}.\end{aligned}$$

4. Similarly, one can check that in $(\mathbb{Z}, +)$, the subgroup generated by $\{a_1, a_2, \ldots, a_r\}$ is

   $$a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_r\mathbb{Z}.$$

Example 7.3.9

1. Consider the additive $(\mathbb{Z}_n, \oplus_n)$. It can be easily observed that

   $$\langle[1]\rangle = \left\{[1]^n, n \in \mathbb{Z}\right\} = \{n[1], n \in \mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\} = \mathbb{Z}_n.$$

   Since $[n-1]$ is the additive inverse of $[1]$ in $(\mathbb{Z}_n, \oplus_n)$, then $\langle[n-1]\rangle = \mathbb{Z}_n$.

2. Consider the group $(\mathbb{Z}_{12}, \oplus_{12})$ and its subgroup $H = \langle[3]\rangle$. By examining the order of $[3]$, we obtain $\text{ord}([3]) = 4$, and

   $$H = \left\{[3]^k : k \in \mathbb{Z}\right\} = \left\{[3]^0, [3]^1, [3]^2, [3]^3\right\} = \{[0], [3], [6], [9]\}.$$

Note that $[3]^k = \underbrace{[3] \oplus_{12} [3] \oplus_{12} \cdots \oplus_{12} [3]}_{k \text{ times}}$. We compute all generated subgroups of H, as follows:

The subgroups of H generated by one element are $\langle [0] \rangle = \{[0]\}$, $\langle [6] \rangle = \{[0], [6]\}$, and $\langle [3] \rangle = \langle [9] \rangle = H$.

The subgroups of H generated by two elements are $\langle [0], [3] \rangle = \langle [0], [9] \rangle = \langle [3], [9] \rangle = \langle [3], [6] \rangle = \langle [6], [9] \rangle = H$, and $\langle [0], [6] \rangle = \{[0], [6]\} = \langle [6] \rangle$. There is only one subgroup of H generated by three elements which is $\langle [0], [3], [6] \rangle = \langle [0], [3], [9] \rangle = \langle [0], [6], [9] \rangle = \langle [3], [6], [9] \rangle = H$. Finally, there is one subgroup of H generated by four element which H itself, as $\langle H \rangle = H$. Thus, all distinct generated subgroups of H are $\{[0]\}$, $\{[0], [6]\}$, and H itself. All of these subgroups are generated by one element.

Examples 7.3.8 and 7.3.9 show that a generating set of a subgroup is not unique. In particular, if a subgroup H is generated by $\{a_1, a_2, \ldots, a_n, \ldots\}$, then H is also generated by $\left\{a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}, \ldots\right\}$.

Example 7.3.10 Consider the symmetric group $(\mathfrak{S}_5, \circ)$. The following are finitely generated subgroups of $\mathfrak{S}_5$.

1. $H = \langle (1\ 2) \rangle = \{e, (1\ 2)\}$.
2. $K = \langle (1\ 5\ 3) \rangle = \{e, (1\ 5\ 3), (1\ 3\ 5)\}$.
3. $S = \left\langle (2\ 4\ 5\ 3)^5 \right\rangle = \langle (2\ 3\ 5\ 4) \rangle = \{e, (2\ 4\ 5\ 3), (2\ 5)(3\ 4), (2\ 3\ 5\ 4)\}$.
4. $V = \langle (1\ 3)(2\ 5) \rangle = \{e, (1\ 3)(2\ 5)\}$.
5. $W = \langle (1\ 3), (2\ 5) \rangle = \{e, (1\ 3), (2\ 5), (1\ 3)(2\ 5)\}$.
6. $R = \langle (1\ 3), (2\ 5\ 3) \rangle$.

It is difficult to use the definition to list all elements in the subgroup R as

$$R = \left\{a_1^{r_1} * \cdots * a_k^{r_k} : a_i \in \{(2\ 5\ 3), (1\ 3)\}, r_i \in \mathbb{Z}, k \in \mathbb{N}\right\}.$$

Since no permutation in R moves 4, any permutation in R must be a permutation on $\{1, 2, 3, 5\}$. Let H be the subgroup of $\mathfrak{S}_5$ that permutes $\{1, 2, 3, 5\}$ (Example 7.1.9 (3)). We show that $R = H$. Clearly, $R \subseteq H$. For the other inclusion, let ϕ be a permutation on $\{1, 2, 3, 5\}$. According to Corollary 6.5.3 (2), the permutation ϕ can be written as a finite product of transpositions of the forms $(1\ j)$, where $j \in \{2, 3, 5\}$. Since $(1\ 3) \in R$, $(1\ 5) = (2\ 5\ 3)^2(1\ 3)(2\ 5\ 3) \in R$, and $(1\ 2) = (253)(13)(2\ 3\ 5) \in$ R, then R contains all the transpositions $(1\ j)$, where $j \in \{2, 3, 5\}$, and hence contains any product of them, in particular, $\phi \in R$. Therefore, $H \subseteq R$. Note that the case with the subgroup W in (5) is easier since the cycles (13) and (25) commute. These cycles can be rearranged to ease the problem, which cannot be realized in the case of the subgroup R.

Example 7.3.11 Let $n \in \mathbb{N}$ such that $n \geq 3$. Consider the dihedral group $(D_{2n}, \circ)$ that consists of all symmetries for the regular n-polygon. The group D_{2n} is an example of a finitely generated group that is generated by two elements. Namely, $D_{2n} = \left\langle R_{\frac{2\pi}{n}}, l_o \right\rangle$. To show this equality, the equations in Proposition 1.7.7 can be used to obtain

$$\text{ord}\left(R_{\frac{2\pi}{n}}\right) = n, ord(l_o) = 2, \quad \text{and} \quad \left(R_{\frac{2\pi}{n}} l_o\right)^2 = \left(l_o R_{\frac{2\pi}{n}}\right)^2 = R_0.$$

Therefore, by Exercise 7.30, $l_o\left(R_{\frac{2\pi}{n}}\right)^k = \left(R_{\frac{2\pi}{n}}\right)^{n-k} l_o$ for any $0 \le k \le n-1$, and

$$\left\langle R_{\frac{2\pi}{n}}, l_o\right\rangle = \left\{R_0, R_{\frac{2\pi}{n}}, R_{\frac{4\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}, l_o, l_{\frac{\pi}{n}}, \ldots, l_{\frac{(n-1)\pi}{n}}\right\} = D_{2n}.$$

Moreover,

- The subgroup of D_{2n} that is generated by R_0 is $\langle R_0\rangle = R_0$.
- The subgroup of D_{2n} that is generated by $R_{\frac{2\pi}{n}}$ is

$$\left\langle R_{\frac{2\pi}{n}}\right\rangle = \left\{\left(R_{\frac{2\pi}{n}}\right)^k : 0 \le k \le n-1\right\} = \left\{R_0, R_{\frac{2\pi}{n}}, \ldots., R_{\frac{2(n-1)\pi}{n}}\right\}$$

which is the subgroup of all rotations of the regular n-polygon.

- For any $0 \le k \le n-1$, the subgroup generated by $l_{\frac{k\pi}{n}}$ is $\left\langle l_{\frac{k\pi}{n}}\right\rangle = \left\{R_0, l_{\frac{k\pi}{n}}\right\}$ (Check!).

Example 7.3.12 Consider the two matrices

$$r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Both matrices are elements of the group $O(2)$, the orthogonal group of order 2 (Example 5.1.9). One can easily verify that $\text{ord}(r) = 4$, $\text{ord}(s) = 2$ and $(rs)^2 = (sr)^2 = I_2$. Hence, by Exercise 7.30, $sr^k = r^{4-k}s$, $1 \le k \le 3$, and the subgroup of $O(2)$ generated by $\{r, s\}$ is

$$\langle r, s\rangle = \left\{r^n s^m : 0 \le n < 4, \quad 0 \le m < 2\right\} = \left\{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\right\}.$$

Table 7.3 shows Cayley's table of $\langle r, s\rangle$. The reader may verify, using the table, that the following are subgroups of $\langle r, s\rangle$.

- $\langle r\rangle = \left\langle r^3\right\rangle = \left\{e, r, r^2, r^3\right\}$.
- $\left\langle r^2\right\rangle = \left\{e, r^2\right\}$.
- $\left\langle r^i s\right\rangle = \left\{e, r^i s\right\}, \quad \forall\, 0 \le i \le 3$.

Note that if one considers a square with the center at the origin and vertices at $(1, 0)$, $(0, 1)$, $(-1, 0)$ and $(0, -1)$ (Fig. 7.1), then the matrices r and s represent the rotation of the square by $\frac{\pi}{2}$ around $(0, 0)$, and the reflection around the x-axis (Propositions 1.7.3 and 1.7.6). Therefore, the subgroup $\langle r, s\rangle$ can be identified with

Table 7.3 Cayley's table of $\langle r, s\rangle$

$\cdot$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
rs	rs	s	r^3s	r^2s	r	e	r^3	r^2
r^2s	r^2s	rs	s	r^3s	r^2	r	e	r^3
r^3s	r^3s	r^2s	rs	s	r^3	r^2	r	e

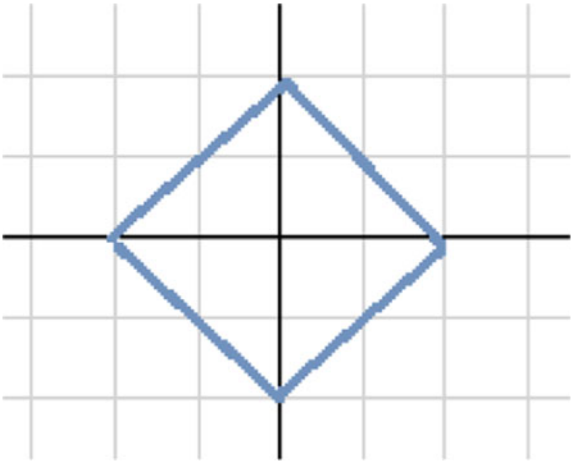
the group D_8, which is the group of the symmetries of the square. The reader may compare Table 7.3 with that obtained in Example 1.7.9.

Example 7.3.13 Consider the group $\mathfrak{S}_4$ and its two elements, the permutation $\alpha = (1\ 2\ 3\ 4)$ and transposition $\tau = (2\ 4)$. It is straightforward to check that $\operatorname{ord}(\alpha) = 4$, $\operatorname{ord}(\tau) = 2$, and $(\alpha\tau)^2 = (\tau\alpha)^2 = e$. According to the result in Exercise 7.30, $\tau\alpha^k = \alpha^{4-k}\tau$ for each $1 \leq k \leq 3$. Let K be the subgroup of $\mathfrak{S}_4$ that is generated by $\{\alpha, \tau\}$, the elements of K can be listed as follows:

$$K = \langle \alpha, \tau\rangle = \left\{\tau^s\alpha^k : 0 \leq s \leq 1, 0 \leq k \leq 3\right\} = \left\{e, \alpha, \alpha^2, \alpha^3, \tau, \tau\alpha, \tau\alpha^2, \tau\alpha^3\right\}.$$

Note that if one considers a square centered at the origin and with vertices numbered from 1 to 4 (Fig. 7.2), then the rotation of the square by $\frac{\pi}{2}$ permutes the vertices and can be represented by the permutation $\alpha = (1\ 2\ 3\ 4)$. The reflection around the x-axis is achieved by permutating the vertices 2 and 4 and fixing all

Fig. 7.1 Regular 4-polygon



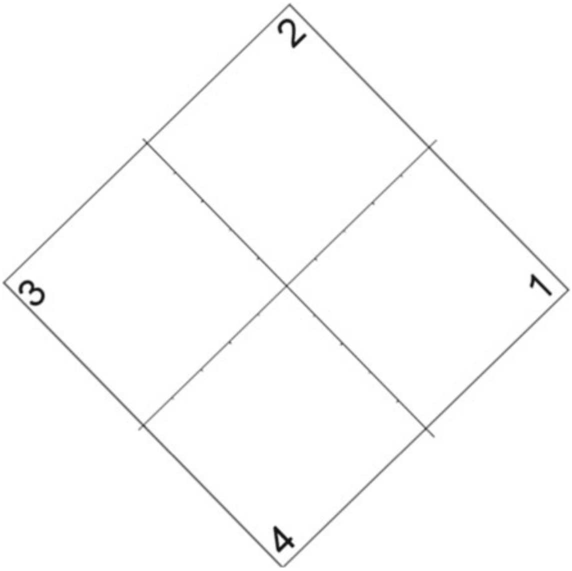


Fig. 7.2 A square centered at the origin and with vertices numbered from 1 to 4

other elements. This permutation can be represented by the transposition $\tau = (24)$. Therefore, the subgroup $\langle \alpha, \tau \rangle$ can be identified with the group D_8, the group of all symmetries of the square.

The generalizations of Examples 7.3.12 and 7.3.13 for an arbitrary positive integer $n \geq 3$ can be obtained following the same steps as in the above examples (Exercises 7.5 and 7.6). For now, the reader should compare the last two examples with Example 7.3.11 for the case of $n = 4$.

Example 7.3.14 Let $n \in \mathbb{N}$ such that $n \geq 3$. The group $\mathfrak{S}_n$ is generated by two elements, namely

$$\mathfrak{S}_n = \langle (1\ 2), (2\ 3\ 4 \ldots n) \rangle$$

To show this, one shows the following expression by induction on s:

$$(2\ 3\ 4 \ldots n)^s (1\ 2)(2\ 3\ 4 \ldots n)^{-s} = (1(2+s)) \text{ for each } 0 \leq s \leq n-2$$

which implies that $\langle (1\ 2), (2\ 3\ 4 \ldots n) \rangle$ contains all the transpositions of the form $(1\ k)$ for $2 \leq k \leq n$. The result follows by Exercise 7.3.

Next, we investigate the subgroups generated by the intersection and the union of two subgroups. Let G be a group and H, K be subgroups of G. As the intersection of any subgroups is a group, $\langle H \cap K \rangle = H \cap K$. However, this is not the case for the union as $H \cup K$ is not always group (verify!). According to Proposition 3.7.6,

$$\langle H \cup K \rangle = \left\{ a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n} : a_i \in H \cup K, r_i \in \mathbb{Z}, 1 \leq i \leq n, n \in \mathbb{N} \right\}$$

which is not easy to describe. The following proposition states that if $HK = KH$, then $\langle H \cup K\rangle$ can be easily described.

Proposition 7.3.15 *Let G be a group. If H, K are subgroups of G, then*

$$KH = HK \Leftrightarrow \langle H \cup K\rangle = HK.$$

In particular, if G is abelian, then $\langle H \cup K\rangle = HK$.

Proof According to Proposition 7.2.8, $KH = HK$ if and only if HK is a subgroup of G. Therefore, we demonstrate this result by showing that $KH < G \Leftrightarrow \langle H \cup K\rangle = HK$. If $\langle H \cup K\rangle = HK$, then HK is a group and one direction trivially follows. For the other direction, assume that HK is a subgroup of G. We show that $\langle H \cup K\rangle = HK$, as follows. As HK contains both H and K, then $H \cup K \subseteq HK$, which yields that $\langle H \cup K\rangle \subseteq \langle HK\rangle = HK$. On the other hand, let h, k be arbitrary elements in H and K, respectively. As $h, k \in H \cup K \subseteq \langle H \cup K\rangle$ and $\langle H \cup K\rangle$ is a group, then $hk = h * k \in \langle H \cup K\rangle$, which implies that $HK \subseteq \langle H \cup K\rangle$. ■

Proposition 7.3.16 *Let G be a group and let $H_1, \ldots, H_n$ be subgroups of G. For each $1 \le j \le n$,*

$$\text{if } K = \left\langle \bigcup_{\substack{i=1\\ i\neq j}}^{n} H_i \right\rangle, \text{then } \left\langle H_j \cup K\right\rangle = \left\langle \bigcup_{i=1}^{n} H_i \right\rangle.$$

Proof Assume that $K = \left\langle \bigcup_{\substack{i=1\\ i\neq j}}^{n} H_i \right\rangle$. Since $\bigcup_{i=1}^{n} H_i = H_j \cup \left(\bigcup_{\substack{i=1\\ i\neq j}}^{n} H_i \right)$ is contained in $H_j \cup K$, then $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle \subseteq \left\langle H_j \cup K\right\rangle$ (Corollary 7.3.4). For the other direction, since $\bigcup_{\substack{i=1\\ i\neq j}}^{n} H_i \subseteq \bigcup_{i=1}^{n} H_i$, then by Corollary 7.3.4, $K = \left\langle \bigcup_{\substack{i=1\\ i\neq j}}^{n} H_i \right\rangle \subseteq \left\langle \bigcup_{i=1}^{n} H_i \right\rangle$. As $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle$ contains H_j, it contains $H_j \cup K$, and hence the smallest subgroup generated by $H_j \cup K$. i.e., $\left\langle H_j \cup K\right\rangle \subseteq \left\langle \bigcup_{i=1}^{n} H_i \right\rangle$. ■

We will focus on groups generated by one element. Such groups are said to be cyclic and are discussed in Sect. 9.1. The following results pertain to subgroups generated by one element.

Proposition 7.3.17 *Let G be a group. For any $a \in G$, if $\mathrm{ord}(a) = n < \infty$, then*

$$\langle a\rangle = \left\{e, a, a^2, \ldots, a^{n-1}\right\}.$$

If a has an infinite order, then $\langle a\rangle$ has an infinitely many elements.

Proof Let $x \in \langle a\rangle$. By Proposition 7.3.6, $x = a^m$ for some $m \in \mathbb{Z}$. Applying the quotient-remainder theorem (Theorem 2.1.2) to m and n yields that there exist $q, r \in \mathbb{Z}$ such that $m = qn + r$, $0 \le r < n$. Therefore,

$$x = a^{qn+r} = a^{qn}a^r = ea^r = a^r, \quad 0 \le r < n.$$

i.e., $x \in \left\{e, a, a^2, \ldots, a^{n-1}\right\}$ and $\langle a \rangle \subseteq \left\{e, a, a^2, \ldots, a^{n-1}\right\}$. The other inclusion is trivial. The last statement follows by definition of $\operatorname{ord}(a)$. ■

Corollary 7.3.18 *Let G be a group and $a \in G$. The order of the subgroup generated by a is equal to* $\operatorname{ord}(a)$*, i.e.,* $\operatorname{ord}(a) = |\langle a \rangle|$.

Proposition 7.3.19 *Let G be a group and $a \in G$ such that* $\operatorname{ord}(a) = n < \infty$. *For each $k \in \mathbb{N}$,*

$$\left\langle a^k \right\rangle = \left\langle a^{\gcd(k,n)} \right\rangle.$$

Moreover, $\left|\left\langle a^k \right\rangle\right| = \frac{n}{\gcd(k,n)}$.

Proof Let $k \in \mathbb{N}$. Since $\gcd(k, n)|k$, there exists $q \in \mathbb{Z}$ such that $k = q \cdot \gcd(k, n)$, which implies that

$$a^k = a^{q \gcd(k,n)} = \left(a^{\gcd(k,n)}\right)^q \in \left\langle a^{\gcd(k,n)} \right\rangle.$$

Therefore, by Corollary 7.3.4, $\left\langle a^k \right\rangle \subseteq \left\langle a^{\gcd(k,n)} \right\rangle$. For the other direction, using Bézout's lemma (Theorem 2.5.1), there exist $x, y \in \mathbb{Z}$ such that $\gcd(k, n) = xk + yn$. Therefore,

$$a^{\gcd(k,n)} = a^{xk+yn} = a^{xk}a^{yn} \underset{a^{yn}=(a^n)^y=e^y=e}{=} a^{xk} = \left(a^k\right)^x \in \left\langle a^k \right\rangle.$$

The result in Corollary 7.3.4 implies that $\left\langle a^{\gcd(k,n)} \right\rangle \subseteq \left\langle a^k \right\rangle$.
i.e.,
$\left\langle a^k \right\rangle = \left\langle a^{\gcd(k,n)} \right\rangle$.
By Proposition 5.5.9, one obtains $\left|\left\langle a^k \right\rangle\right| = \operatorname{ord}\left(a^k\right) = \frac{\operatorname{ord}(a)}{\gcd(k,n)}$. ■

Example 7.3.20 Let $n \in \mathbb{N}$. Consider the additive group $(\mathbb{Z}_n, \oplus_n)$. For each $k \in \mathbb{Z}$, we have $\langle [k] \rangle = \mathbb{Z}_n$ if and only if $\gcd(k, n) = 1$. To show this result, note the additive group $\mathbb{Z}_n = \langle [1] \rangle$ (Example 7.3.9), which implies that $\operatorname{ord}([1]) = n$. Therefore, by Proposition 7.3.19, for each $k \in \mathbb{Z}$,

$$|\langle [k] \rangle| = \left|\left\langle [1]^k \right\rangle\right| = \frac{n}{\gcd(k, n)} = n \Leftrightarrow \gcd(k, n) = 1.$$

The result follows as $\langle [k] \rangle$ is a subgroup of $\mathbb{Z}_n$ and the order of $\mathbb{Z}_n$ is n.
Example 7.3.20 provides a list of elements such that $\langle [k] \rangle = \mathbb{Z}_n$, which is

$$\{[k] \in \mathbb{Z}_n : \gcd(k, n) = 1\}.$$

This set, denoted by $\operatorname{Inv}(\mathbb{Z}_n)$, contains all the generators of the additive group $\mathbb{Z}_n$. Note that this set forms a multiplicative group under the operation $\otimes_n$ (Lemma 5.3.3 and Corollary 5.3.5). The following proposition shows that if p is a prime number, then there is $[a] \in \text{Inv}\big(\mathbb{Z}_p\big)$ such that $[a]$ generates this group. However, finding the number $[a]$ is a problem in number theory and is thus beyond the scope of this book. For reference, see (Burton, 2007). If $p = 7$ for example, then one can easily check that [3] is a generator of the multiplicative group $\text{Inv}(\mathbb{Z}_7)$.

Proposition 7.3.21 *Let p be a prime number and consider the group $\big(\text{Inv}\big(\mathbb{Z}_p\big), \otimes_p\big)$. There exists an element $[a] \in \text{Inv}\big(\mathbb{Z}_p\big)$ such that $\langle [a] \rangle = \text{Inv}\big(\mathbb{Z}_p\big)$.*

We end the section with the following example that will be needed in Chap 9. For the definition of mG, see Proposition 5.5.13.

Example 7.3.22

1. Let $G = \mathbb{Z}_9 \times \mathbb{Z}_3$ and $a = ([1], [0])$. The subgroup generated by a is

$$\langle a \rangle = \langle ([1], [0]) \rangle = \big\{([1], [0])^k : k \in \mathbb{Z}\big\} = \{([k], [0]) : k \in \mathbb{Z}\} = \mathbb{Z}_9 \times \{[0]\}.$$

The reader must note that although $3G = \{[0], [3], [6]\} \times \{[0]\} = 3(\mathbb{Z}_9 \times \{[0]\}) = 3\langle a \rangle$, the group G is not equal to $\langle a \rangle$.

2. Consider the group $\mathfrak{S}_7$ and let $H = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$ and $K = \{e, (4\ 5\ 6), (4\ 6\ 5)\}$. Clearly, H and K are subgroups of $\mathfrak{S}_7$ that satisfy $3H = \{e\} = 3K$, but $H \neq K$.

7.4 Cosets of Subgroups and Lagrange's Theorem

Let G be a group and H be a subgroup of G. For an element $a \in G$, one can form new subsets of G using H by considering the product of a and H, i.e.,

$$aH = \{a * h : h \in H\} \text{ and } Ha = \{h * a : h \in H\}.$$

Such subsets are not necessarily subgroups of G. For example, in the symmetric group $\mathfrak{S}_3$, the set $H = \{e, (12)\}$ is a subgroup of $\mathfrak{S}_3$, but $(13)H = \{(13), (13)(12)\}$ is not. In fact, for any $a \notin H$, the set aH does not contain the identity element, hence, in not a group. The subsets aH, $a \in G$ are called cosets of H.

Definition 7.4.1 Let G be a group and H be a subgroup of G. A left coset of H is a subset of G of the form $aH = \{a * h : h \in H\}$, where $a \in G$. A right coset of H is $Ha = \{h * a : h \in H\}$, where $a \in G$.

If G is an abelian group, then a left coset of H is also a right coset of H. In this case, a coset of H means either cosets. Clearly, $eH = H = He$, which means that H is a left and a right coset of itself. Hence, the set of all cosets of a given subgroup H is never empty. If the left and right cosets of H are equal, we denote the set of all cosets of H by G/H.

Example 7.4.2 Consider the group $(\mathbb{Z}, +)$ and its subgroup $5\mathbb{Z}$. The left cosets of $5\mathbb{Z}$ are of the form $m + 5\mathbb{Z}$, where $m \in \mathbb{Z}$. According to the quotient-remainder theorem (Theorem 2.1.2), there exist $q, r \in \mathbb{Z}$ such that $m = 5q + r$ and $0 \leq r < 5$. Hence,

$$m + 5\mathbb{Z} = (5q + r) + 5\mathbb{Z} = r + 5\mathbb{Z} \text{ such that } 0 \leq r < 5.$$

Consequently, there exist only five different left cosets of $5\mathbb{Z}$, which are

$$5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}.$$

As $(\mathbb{Z}, +)$ is an abelian group, the left cosets are also right cosets, i.e.,

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}.$$

A generalization of the preceding example shows that the list of all cosets of $n\mathbb{Z}$ in $(\mathbb{Z}, +)$ is

$$\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} : 0 \leq r < n\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Example 7.4.3 Consider the group $(\mathfrak{S}_3, \circ)$ and its subgroup $H = \langle e, (2\ 3)\rangle = \{e, (2\ 3)\}$. The left cosets of H are

$$\begin{aligned} H &= (2\ 3)H = \{e, (2\ 3)\} \\ (1\ 2)H &= (1\ 2\ 3)H = \{(1\ 2), (1\ 2\ 3)\} \\ (1\ 3)H &= (1\ 3\ 2)H = \{(1\ 3), (1\ 3\ 2)\} \end{aligned}$$

Thus, the set $\{H, (1\ 2)H, (1\ 3)H\}$ constitutes all the left cosets of H. The group $\mathfrak{S}_3$ is not abelian, and thus, we cannot directly deduce the right cosets. Computing the right cosets of H, one finds

$$\begin{aligned} H &= H(2\ 3) = \{e, (2\ 3)\} \\ H(1\ 2) &= H(1\ 3\ 2) = \{(1\ 2), (1\ 3\ 2)\} \\ H(1\ 3) &= H(1\ 2\ 3) = \{(1\ 3), (1\ 2\ 3)\} \end{aligned}$$

The set of the right cosets is $\{H, H(1\ 2), H(1\ 3)\}$, which are different from the left cosets.

Note that any point (u, w) in the plane $\mathbb{R}^2$ can be represented as a vector $ui + wj$ in the plane with $u, w \in \mathbb{R}$ and i, j are the unit vectors in the direction of x-axis and y-axis respectively. The following example uses the definition of vectors and sum of vectors in linear algebra. For reference see (Boyd & Vandenberghe, 2018).

Example 7.4.4 Let $G = \{ui + wj : u, w \in \mathbb{R}\}$, the set of all vectors in the plane $\mathbb{R}^2$. The set G forms a group under the sum of vectors $+$, where the zero vector serves

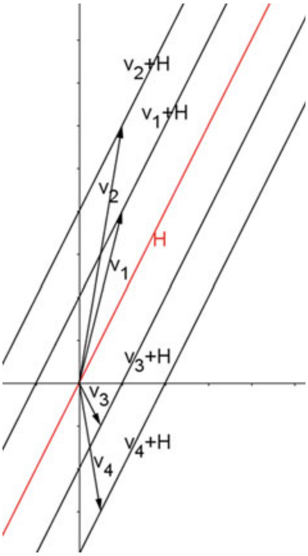


Fig. 7.3 Set of all parallel lines to H

as an identity element, and the inverse of any vector v is $-v$. Let H be a line passing the origin in $\mathbb{R}^2$. As $v_1 - v_2 \in H$ for any $v_1, v_2 \in H$, then H is a subgroup of $(G, +)$. For $v = ui + wj \in G$, the left coset $v\ H$ is a line parallel to H and passes the point $v = (u, w)$. As the sum of the vectors is abelian, then $vH = Hv$ is also a right coset of H, i.e.,

$$G/H = \{vH : v \in G\}$$

is the set of all parallel lines to H (Fig. 7.3).

Proposition 7.4.5 *Let G be a group and H be a subgroup of G. For all $a \in G$, the following statements hold:*

1. $a \in aH$ and $a \in Ha$.
2. $Ha = H \Leftrightarrow a \in H \Leftrightarrow aH = H$.
3. $|Ha| = |H| = |aH|$.

Proof

1. If H is a subgroup of G, then $a = a * e \in aH$ and $a = e * a \in Ha$.
2. We only show $Ha = H \Leftrightarrow a \in H$ as the other equivalence is similar.

If $Ha = H$, then $a = e * a \in Ha = H \Rightarrow a \in H$. For the other direction, assume that $a \in H$. We show that $Ha = H$, as follows:

- For each $h \in H$, $h * a \in H$, and thus, $Ha = \{h * a : h \in H\} \subseteq H$.
- For each $h \in H$, $h * a^{-1} \in H$, which implies that

$$h = h * e = h * \left(a^{-1} * a\right) = \left(h * a^{-1}\right) * a = h_1 * a \in Ha \Rightarrow H \subseteq Ha.$$

3. Define the maps $f : H \to Ha$ and $g : H \to aH$ such that $f(h) = h * a$ and $g(h) = a * h$. The result in (3) follows as f and g are bijective maps. ■

Proposition 7.4.6 *Let G be a group, H be a subgroup of G, and a, b be elements in G. The following statements are equivalent*

1. $Ha = Hb.$
2. $b \in Ha.$
3. $a \in Hb.$
4. $a * b^{-1} \in H.$

Proof We show that 1 ⇒ 2 ⇒ 3 ⇒ 4 ⇒ 1.

(1 ⇒ 2) $Ha = Hb \Rightarrow b = e * b \in Hb = Ha \Rightarrow b \in Ha.$

(2 ⇒ 3) $b \in Ha \Rightarrow \exists\, h \in H \ni b = h{*}a \Rightarrow \exists\, h \in H \ni a = h^{-1}{*}b \Rightarrow a \in Hb.$

(3 ⇒ 4) $a \in Hb \Rightarrow \exists\, h \in H \ni a = h * b \Rightarrow \exists\, h \in H \ni h = a * b^{-1} \Rightarrow a * b^{-1} \in H.$

(4 ⇒ 1) Assume that $a * b^{-1} \in H$. As H is a group,

$$\begin{aligned}\forall\, h \in H, h * a &= h * a * \left(b^{-1} * b\right)\\ &= h * \left(a * b^{-1}\right) * b \in Hb \Rightarrow Ha = \{h * a, h \in H\} \subseteq Hb\end{aligned}$$

and

$$\begin{aligned}\forall\, h \in H, h * b &= h * b * \left(a^{-1} * a\right)\\ &= h * \left(a * b^{-1}\right)^{-1} * a \in Ha \Rightarrow Hb = \{h * b, h \in H\} \subseteq Ha,\end{aligned}$$

i.e., $Ha = Hb$. ■

Note that Proposition 7.4.6 shows that the representation of a right coset of H in the form Ha is not unique, in the sense that Ha might equal to Hb without a being equal to b. One can prove similar statements for the left cosets of H.

Proposition 7.4.7 *Let G be a group, H be a subgroup of G, and a, b be elements in G. The following statements are equivalent*

1. $aH = bH.$
2. $b \in aH.$
3. $a \in bH.$
4. $b^{-1} * a \in H.$

The next proposition shows that a certain flexibility exists in dealing with the cosets of a given subgroup. The results in the proposition guarantee a translation by an element's inverse (free movement between the two sides of the equation through multiplication by the inverse of the element).

Proposition 7.4.8 *Let G be a group, H be a subgroup of G, and a, b be elements in G. The following statements hold:*

1. $Ha = Hb \Leftrightarrow H = H\big(b * a^{-1}\big) \Leftrightarrow H = H\big(a * b^{-1}\big)$.
2. $aH = bH \Leftrightarrow H = \big(b^{-1} * a\big)H \Leftrightarrow H = \big(a^{-1} * b\big)H$.
3. $aH = Hb \Leftrightarrow H = a^{-1}Hb \Leftrightarrow H = aHb^{-1}$.

Proof We only prove that $aH = Hb \Leftrightarrow H = aHb^{-1}$. The proofs of other statements are similar and left as easy exercises. If $aH = Hb$, then

$$\begin{aligned} aHb^{-1} &= \big\{a * h * b^{-1} : h \in H\big\} = \big\{x * b^{-1} : x \in aH\big\} \\ &= \big\{x * b^{-1} : x \in Hb\big\} = \big\{h_1 * b * b^{-1} : h_1 \in H\big\} = H. \end{aligned}$$

For the other direction, assume that $H = aHb^{-1} = \big\{a * h * b^{-1} : h \in H\big\}$, then

$$\begin{aligned} Hb &= \{h * b : h \in H\} = \big\{\big(a * h_1 * b^{-1}\big) * b : h_1 \in H\big\} \\ &= \{a * h_1 : h_1 \in H\} = aH. \end{aligned}$$

■

The relations in the previous proposition hold if one replaces the equality sign by inclusion with a small modification. We leave it to the reader to verify the statement of the following proposition.

Proposition 7.4.9 *Let G be a group, H be a subgroup of G, and a, b be elements in G. The following statements hold:*

1. $Ha \subseteq Hb \Leftrightarrow H \subseteq H\big(b * a^{-1}\big) \Leftrightarrow H\big(a * b^{-1}\big) \subseteq H$.
2. $aH \subseteq bH \Leftrightarrow H \subseteq \big(a^{-1} * b\big)H \Leftrightarrow \big(b^{-1} * a\big)H \subseteq H$.
3. $aH \subseteq Hb \Leftrightarrow H \subseteq a^{-1}Hb \Leftrightarrow aHb^{-1} \subseteq H$.

Proposition 7.4.10 *Let G be a group and H be a subgroup of G. The numbers of left and right cosets of H are equal.*

Proof Let $\mathfrak{L}$ and $\mathfrak{R}$ be the left and right cosets of H, respectively. Define $f : \mathfrak{L} \to \mathfrak{R}$ as the map that takes aH to Ha^{-1} for all $aH \in \mathfrak{L}$. To verify that f is well-defined, assume that aH, bH are two left cosets of H such that $aH = bH$. By Proposition 7.4.7, $b^{-1} * \big(a^{-1}\big)^{-1} = b^{-1} * a \in H$. Thus, by Proposition 7.4.6, $f(bH) = Hb^{-1} = Ha^{-1} = f(aH)$. The map f is injective, since if

$$Ha^{-1} = f(aH) = f(bH) = Hb^{-1} \text{ for some } a, b \in G,$$

then by Proposition 7.4.6, $\big(a^{-1} * b\big) \in H$. Therefore, $b^{-1} * a = \big(a^{-1} * b\big)^{-1} \in H$, which implies that $aH = bH$ (Proposition 7.4.7). To show that f is surjective, assume that Ha is an element in $\mathfrak{R}$. Clearly $a^{-1}H$ is an element in $\mathfrak{L}$ that satisfies

$$f\big(a^{-1}H\big) = H\big(a^{-1}\big)^{-1} = Ha.$$

The map f is bijective, and therefore $|\mathfrak{T}| = |\mathfrak{R}|$. ■

Definition 7.4.11 Let G be a group and H be a subgroup of G. The number of the left (right) cosets of H is called the index of H and denoted by $[G : H]$.

Clearly, if G is finite, then the index of any subgroup of G is finite. However, if G is infinite, then the index of a subgroup of G could be either finite or infinite; see Examples 7.4.2 and 7.4.4. For any group G, we have $[G : \{e\}] = |G|$.

Example 7.4.12

1. Consider the additive $(\mathbb{Z}, +)$. Using the results of Example 7.4.2, the index of the subgroup $n\mathbb{Z}$ is $[\mathbb{Z}, n\mathbb{Z}] = n$.
2. In the group $(\text{Inv}(\mathbb{Z}_7), \otimes_7)$, let $H = \langle[2]\rangle = \{[1], [2], [4]\}$. To compute the index of H, we compute the right cosets of H, as follows.

Since $[1]$ is the identity element of the group, $H = H \otimes_7 [1] = \{[1], [2], [4]\}$. Using Proposition 7.4.6, we obtain

$$H \otimes_7 [1] = H \otimes_7 [2] = H \otimes_7 [4].$$

Next, we compute $H \otimes_7 [3] = \{[5], [6], [3]\}$. By Proposition 7.4.6, we have

$$H \otimes_7 [3] = H \otimes_7 [5] = H \otimes_7 [6].$$

Therefore, the different right cosets of H are only H and $H \otimes_7 [3]$, and $[\text{Inv}(\mathbb{Z}_7) : H] = 2$.

Next, we state and prove Lagrange's theorem. To this end, several lemmas are needed. For now, using a fixed subgroup H of a group G, we define an equivalence relation on G whose equivalence classes are the left (right) cosets of H.

Lemma 7.4.13 *Let G be a group and H be a subgroup of G. Define the following relation on G,*

$$\text{for } a, b \in G, \quad a \cong b \Leftrightarrow \left(a^{-1} * b\right) \in H.$$

The relation $\cong$ is an equivalence relation on G, with the equivalence class of $a \in G$ being aH.

Proof For any $a \in G, a^{-1}*a = e \in H$, which implies that $a \cong a$, and $\cong$ is reflexive. If $a \cong b$, then $a^{-1} * b \in H$. Since H is a group, $b^{-1} * a = \left(a^{-1} * b\right)^{-1} \in H$, which implies that $b \cong a$. Therefore, $\cong$ is symmetric. To show that $\cong$ is transitive, assume that $a \cong b$ and $b \cong c$. According to the definition of $\cong$, $a^{-1} * b \in H \wedge b^{-1} * c \in H$. Therefore,

$$a^{-1} * c = a^{-1} * \left(b * b^{-1}\right) * c = \left(a^{-1} * b\right) * \left(b^{-1} * c\right) \in H$$

i.e., $a \cong c$. The relation $\cong$ is reflexive, symmetric, and transitive, and is thus, an equivalence relation (Definition 1.4.1). For any $a \in G$, the equivalence class of a is

$$\begin{aligned}[][a] &= \{b \in G : a \cong b\} = \left\{b \in G : \left(a^{-1} * b\right) \in H\right\} \\ &= \left\{b \in G : \exists\, h \in H \ni h = a^{-1} * b\right\} \\ &= \{b \in G : \exists\, h \in H \ni b = a * h\} = aH.\end{aligned}$$

■

Similarly, one can show that $a \cong b \Leftrightarrow \left(a * b^{-1}\right) \in H$ defines an equivalence relation on G such that the equivalence class of any element $a \in G$ is Ha. As the set of equivalence classes forms a partition of the set under consideration, the following corollary follows.

Corollary 7.4.14 *Let G be a group and H be a subgroup of G. There exist two partitions of the group G obtained from the left and right cosets of H. Namely, the sets $\{aH, a \in G\}$ and $\{Ha : a \in G\}$ satisfy the following statements:*

1. $Ha \neq Hb \Rightarrow Ha \cap Hb = \emptyset \quad \wedge \quad aH \neq bH \Rightarrow aH \cap bH = \emptyset.$
2. $\bigcup_{a \in G} Ha = G = \bigcup_{a \in G} aH.$

Since aH is an equivalence class, by Proposition 1.4.9 (2), it can be represented by any element in aH. By Proposition 7.4.5, $|aH| = |H|$, which implies that there exist $|H|$ representatives of aH. As $b \in aH \Leftrightarrow bH = aH$ (Proposition 7.4.6), then one can define a representative of the coset of a given subgroup, as follows.

Definition 7.4.15 Let G be a group, $a \in G$, and H be a subgroup of G. A representative of aH is any element $b \in G$ such that $aH = bH$.

Lemma 7.4.16 *Let G be a group. If H, K are subgroups of G such that $K \subseteq H$, then*

$$[G : K] = [G : H][H : K].$$

If any two of the three indices are infinite, the third index is also infinite.

Proof Let $\{a_i H : i \in I\}$ be all distinct left cosets of H, and let $\left\{b_j K : j \in J\right\}$ be all distinct left cosets of K as a subgroup of H. Thus, $|I| = [G : H]$ and $|J| = [H : K]$. According to Corollary 7.4.14,

$$G = \bigcup\nolimits_{i \in I} a_i H \text{ and } H = \bigcup\nolimits_{j \in J} b_j K.$$

Therefore,

$$G = \bigcup\nolimits_{i \in I} a_i \left(\bigcup\nolimits_{j \in J} b_j K\right) = \bigcup\nolimits_{(i,j) \in I \times J} (a_i * b_j) K$$

i.e., the set $\{(a_i * b_j)K : i \in I, j \in J\}$ contains all the left cosets of K in G. To show that these cosets are distinct, assume that $(a_i * b_j)K = (a_r * b_s)K$ for some $i, r \in I$ and $j, s \in J$. Proposition 7.4.7 implies that $a_i * b_j \in (a_r * b_s)K$, i.e., $a_i * b_j = a_r * b_s * k$ for some $k \in K$. Hence,

$$a_i H \underset{b_j \in H}{=} a_i * b_j H = (a_r * b_s * k)H \underset{b_s, k \in H}{=} a_r H.$$

As the cosets $a_i H$ are mutually disjoint, $i = r$ and $b_j = b_s * k$. Thus,

$$b_j K = (b_s * k)K \underset{k \in K}{=} b_s K.$$

As the cosets $b_j K$ are mutually disjoint, $j = s$. Therefore, $i =$ r and $j =$ s. That is, the set $\{(a_i * b_j)K : i \in I, j \in J\}$ is the set of all distinct left cosets of K in G. Therefore,

$$\begin{aligned}[G : K] &= \left|\{(a_i * b_j)K : i \in I, j \in J\}\right| = |I \times J| = |I| \times |J| \\ &= [G : H] \times [H : K].\end{aligned}$$

The last statement is clear. ■

Applying Lemma 7.4.16 with $K = \{e\}$, we obtain the following important theorem in algebra.

Theorem 7.4.17 (Lagrange's Theorem)
Let G be a group. If H is a subgroup of G, then

$$|G| = [G : H] \cdot |H|.$$

In particular, if G is finite, then $|H|$ divides $|G|$.

Exercise 7.10 provides an alternative proof of Lagrange's theorem for the case where G is finite. The following example shows that not all possible divisors of the order of a group are orders of some subgroups. The group $\mathcal{A}_4$ has 12 elements, and 6 divides 12, while $\mathcal{A}_4$ has no subgroup of order 6.

Example 7.4.18 The group $\mathcal{A}_4$ has no subgroup of order 6. To show this result, assume that $\mathcal{A}_4$ has a subgroup H of order 6. By Lagrange's theorem, there are only two cosets of H in $\mathcal{A}_4$. As the group $\mathcal{A}_4$ contains eight 3-cycles and H has only six elements, there exists a 3-cycle, say ψ, which is not in H. Since $\psi^2 = \psi^{-1}$ and ψ^{-1} is not in H, then ψ^2 is also not in H. As there exist only two cosets of H, we have

$$\psi^2 H = \psi H = \mathcal{A}_4 \backslash H.$$

Multiplying both sides by ψ^{-1} yields $\psi H = H$, which contradicts that ψ is not in H. Therefore, $\mathcal{A}_4$ has no subgroup H of order 6.

The following corollary follows by Lagrange's theorem, Corollary 7.3.18, Proposition 5.5.17, and Exercise 2.24.

Corollary 7.4.19 *Let G be a finite group.*

1. *For any $a \in G$, $\operatorname{ord}(a)$ divides the order of G and $a^{|G|} = e$.*
2. *The exponent of G divides $|G|$.*

Using that $a^{|G|} = e$ for any a in G, yields the special case; for any element $[a] \in \mathbb{Z}_p^*$, and any prime p, $\left[a^{p-1}\right] = [a]^{p-1} = [a]^{|\mathbb{Z}_p^*|} = [1]$, which implies that $a^{p-1} \cong 1 \ mod \ p$.

Another corollary of Lagrange's theorem is the following:

Corollary 7.4.20 *Let G be a group and let H, K be finite subgroups of G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{e\}$. In particular, any two subgroups of distinct prime orders have a trivial intersection.*

Proof As $H \cap K$ is a subgroup of both H and K, then by Lagrange's theorem, $|H \cap K|$ divides both $|H|$ and $|K|$, and thus their greatest common divisor (Corollary 2.5.7). As the only positive divisor of 1 is 1 itself, then $|H \cap K| = 1$ and $H \cap K = \{e\}$. If H and K are two distinct subgroups of prime orders, then $\gcd(|H|, |K|) = 1$, and the second statement follows. ■

Note that the second statement in the above corollary can be generalized to include distinct subgroups with prime orders as follows: any two distinct subgroups of prime orders have a trivial intersection (Exercise 7.42).

Proposition 7.4.21 *Let G be a group and let $a \in G$ such that $\operatorname{ord}(a) < \infty$. For any m, r divisors of $\operatorname{ord}(a)$,*

$$\left\langle a^r \right\rangle \subseteq \left\langle a^m \right\rangle \Leftrightarrow m|r.$$

Proof Let $\operatorname{ord}(a) = n$, and let m, r be divisors of n. If $\langle a^r \rangle \subseteq \langle a^m \rangle$, then by Lagrange's theorem and Proposition 5.5.9,

$$\left|\left\langle a^r \right\rangle\right| = n/r \ \text{ divides } \ \left|\left\langle a^m \right\rangle\right| = n/m.$$

Rearranging this statement, we get that m divides r (Check!). On the other hand, if $m|r$, then $r = ms$ for some $s \in \mathbb{Z}$, and

$$a^r = \left(a^m\right)^s \in \left\langle a^m \right\rangle.$$

By Corollary 7.3.4, $\langle a^r \rangle \subseteq \langle a^m \rangle$. ■

Corollary 7.4.22 *Let G be a group and $a \in G$ such that $ord(a) = n < \infty$. For each $m, r \in \mathbb{N}$,*

$$\left\langle a^r \right\rangle = \left\langle a^m \right\rangle \Leftrightarrow \gcd(r, n) = \gcd(m, n).$$

Proof Assume that $\langle a^r \rangle = \langle a^m \rangle$. By Propositions 7.3.19, we have $\left\langle a^{\gcd(r,n)} \right\rangle = \left\langle a^{\gcd(m,n)} \right\rangle$ Since both exponents are divisors of n, it follows from Proposition 7.4.21 that $\gcd(r,n) | \gcd(m,n)$ and $\gcd(r,m) | \gcd(r,n)$, the equality follows from Proposition 2.2.5 (3). For the other direction, assume $\gcd(r,n) = \gcd(m,n)$, by Proposition 7.3.19,

$$\left\langle a^r \right\rangle = \left\langle a^{\gcd(r,n)} \right\rangle = \left\langle a^{\gcd(m,n)} \right\rangle = \left\langle a^m \right\rangle.$$

■

Next, we consider a group G having two subgroups H and K. We investigate the relation of the cosets of the intersection $H \cap K$ with the cosets of both H and K. The following proposition states that a coset of the intersection of two groups is the intersection of their cosets containing the same representative. The representative of the coset of a subgroup in defined in Definition 7.4.15.

Proposition 7.4.23 *Let $(G, *)$ be a group and let H, K be subgroups of G. For each $a \in G$,*

1. $a(H \cap K) = (aH) \cap (aK)$.
2. $(H \cap K)a = (Ha) \cap (Ka)$.

Proof Let a be any element in G. If $y \in a(H \cap K)$, then $y = a * b$ for some $b \in H \cap K$, i.e.,

$$y = a * b \in aH \quad \text{and} \quad y = a * b \in aK.$$

Therefore, $y \in (aH) \cap (aK)$, and $a(H \cap K) \subseteq (aH) \cap (aK)$. For the other inclusion, if $y \in (aH) \cap (aK)$, then $y = a * h$ for some $h \in H$, and $y = a * k$ for some $k \in K$. As the element a is invertible, and $a * h = y = a * k$, then $h = k \in H \cap K$. Therefore, $y \in a(H \cap K)$, and $(aH) \cap (aK) \subseteq a(H \cap K)$. The proof of the second statement is similar. ■

The following lemma generalizes the last proposition to the case involving cosets of two subgroups with different representatives.

Lemma 7.4.24 *Let G be a group and H, K be subgroups of G. For each $a, b \in G$,*

1. $(aH) \cap (bK) = \emptyset$ *or* $\exists\, c \in G \ni (aH) \cap (aK) = c(H \cap K)$.
2. $(Ha) \cap (Kb) = \emptyset$ *or* $\exists\, c \in G \ni (Ha) \cap (Kb) = (H \cap K)c$.

Proof If $(aH) \cap (bK) \neq \emptyset$, then there exists $c \in G$ such that

$$c = a * h, h \in H \quad \text{and} \quad c = b * k, \; k \in K.$$

Since $h \in H$ and $k \in K$, then

$$c\,H = (a * h)H = a * (hH) = aH$$

and

$$c\ K = (b * k)K = b * (kK) = bK.$$

By Proposition 7.4.23,

$$(aH) \cap (bK) = (cH) \cap (cK) = c(H \cap K).$$

The second statement is similar. ■

Corollary 7.4.26 demonstrates the relation between the index of the intersection of subgroups and the indices of the subgroups. The following lemma is required to prove Corollary 7.4.26.

Lemma 7.4.25 *Let G be a group. If H and K are subgroups of G, then*

$$[H : H \cap K] \leq [G : K].$$

If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = HK$.

Proof Define

$$f : \{h(H \cap K) : h \in H\} \to \{aK : a \in G\}$$

$$h(H \cap K) \mapsto hK.$$

We show that f is a well-defined injective map as follows:

If $h_1(H \cap K) = h_2(H \cap K)$, then $h_1^{-1} * h_2 \in H \cap K \subseteq K$, thus $h_1 K = h_2 K$. i.e., f is well-defined. The map f is injective, for if $f(h_1(H \cap K)) = f(h_2(H \cap K))$, then $h_1 K = h_2 K$, which implies that $h_1^{-1} * h_2 \in K$. As $h_1, h_2 \in H$, then $h_1^{-1} * h_2 \in H \cap K$, and $h_1(H \cap K) = h_2(H \cap K)$. Therefore,

$$[H : H \cap K] = |\{h(H \cap K) : h \in H\}| \leq |\{aK : a \in G\}| = [G : K].$$

For the second statement, assume that $[G : K]$ is finite. We show that

$$[H : H \cap K] = [G : K] \Longleftrightarrow f \text{ is surjective} \Longleftrightarrow G = HK$$

as follows.

If $[H : H \cap K] = [G : K]$, then f is an injective map of finite sets of equal cardinalities which implies that f is surjective (Exercise 1.6). Clearly, if f is surjective, then $[H : H \cap K] = [G : K]$. i.e., the first equivalence is true. For the second equivalence, assume that f is surjective and $a \in G$ is an arbitrary element. Since f is surjective, there exists $h \in H$ such that

$$aK = f(h(H \cap K)) = hK,$$

which implies that $h^{-1} * a \in K$. i.e., $h^{-1} * a = k$ for some $k \in K$. Therefore, $a = h * k \in HK$ and $G \subseteq HK$. As HK is a subset of G, then $G = HK$. For the other direction, let $G = HK$, and let aK be an arbitrary element in $\{aK : a \in G\}$. As $a \in G = HK$ then $a = h*k$ for some $h \in H$ and $k \in K$. Therefore, $a*k^{-1} = h \in H$ and

$$f(h(H \cap K)) = f\big((a * k^{-1})(H \cap K)\big) = \big(a * k^{-1}\big)K = aK.$$

Therefore, f is subjective. ■

Using the lemma above, Lemma 7.4.16, and the inclusion $H \cap K \subseteq H \subseteq G$, the following corollary can be obtained.

Corollary 7.4.26 *Let G be a group and let H, K be subgroups of G. If the indices of H and K are finite, then*

1. $[G : H \cap K] \leq [G : H] \cdot [G : K]$.
2. $[G : H \cap K] = [G : H] \cdot [G : K]$ *if and only if* $G = HK$.

7.5 Normal Subgroups of a Group

In Sect. 7.2, we defined and studied operations on subgroups, including the intersection, union, and product of two groups. In this section, we introduce a notion that enables us to define a group structure on the set of cosets, called quotient group. We will introduce the notion of normal subgroups, which will be used to define the quotient of groups in Sect. 7.7. Recall that for a subgroup H of G, the coset aH is not always equal to Ha.

Definition 7.5.1 Let G be a group and H be a subgroup of G. The subgroup H is said to be normal, denoted by $H \trianglelefteq G$, if $aH = Ha \quad \forall\, a \in G$.

If G is a group, then for any $a \in G$,

$$a\{e\} = \{a\} = \{e\}a \text{ and } aG = G = Ga.$$

Therefore, both $\{e\}$ and G are always normal subgroups of G. Note that for a normal subgroup, the left and the right cosets are identical.

Proposition 7.5.2 *Let G be a group and H be a subgroup of G. The following statements are equivalent:*

1. *H is a normal subgroup of G.*
2. *$aHa^{-1} = H$ for all $a \in G$.*
3. *$aHa^{-1} \subseteq H$ for all $a \in G$.*
4. *$aH \subseteq Ha$ for all $a \in G$.*

Proof We prove the equivalence by showing that $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$.

- Assume that H is a normal subgroup of G. By the definition of normality, $aH = Ha$ for each a in G. By Proposition 7.4.8 (3), $aHa^{-1} = H$ for all $a \in G$.
- If (2) holds, then the statement in (3) is automatically satisfied.
- Assuming (3), Proposition 7.4.9 (3) directly implies (4).
- Assume (4) holds. Let a be an arbitrary element in G, since $a^{-1} \in G$, then $a^{-1}H \subseteq Ha^{-1}$. By applying Proposition 7.4.9 (3) twice, we obtain

$$a\big(a^{-1}H\big)a \subseteq a\big(Ha^{-1}\big)a$$

which implies that $Ha \subseteq aH$, and hence, $Ha = aH$. ■

Note that

1. Any subgroup of an abelian group is normal (Check!).
2. Having the equivalence $1 \Leftrightarrow 4$ in the proposition above reduces the work required to show that a subgroup is normal. By this equivalence, it is sufficient to show that for each $a \in G$, and for each $h \in H$, $a * h \in Ha$.
3. The equivalence $1 \Leftrightarrow 3$ also drastically reduces the computations. Using this equivalence, it suffices to show that for each $h \in H$ and for all $a \in G, a*h*a^{-1} \in H$.
4. Notably, H being a normal subgroup of G does not mean that the elements of H commute with the elements of G. The statement $aH = Ha$ only means that for any $h \in H$, there exists $k \in H$ such that $a * h = k * a$. However, normal subgroups provide a certain mobility. For example, if H_1, H_2, and H_3 are three normal subgroups of G, then for any $a \in G$,

$$a * h_1 * h_2 * h_3 = k_1 * a * h_2 * h_3 = k_1 * k_2 * a * h_3 = k_1 * k_2 * k_3 * a$$

where $h_i, k_i \in H_i$. Therefore, although the elements do not commute, the elements of a group G can be moved among those of the normal subgroup. In general, the following proposition can be proved by induction.

Proposition 7.5.3 *Let G be a group and let $H_1, \ldots, H_n$ be normal subgroups of G. Let $h_i \in H_i$, $1 \leq i \leq n$. For any $a \in G$ and $1 \leq i < n$, there exist elements $k_s \in H_s$, $1 \leq s \leq i$ such that*

$$a * h_1 * h_2 * \cdots * h_i * h_{i+1} * \cdots * h_n = k_1 * k_2 * \cdots k_i * a * h_{i+1} \cdots * h_n$$

and there exist $k_s \in H_s$, $1 \leq s \leq n$ such that

$$a * h_1 * h_2 * \cdots * \cdots * h_n = k_1 * k_2 * \cdots k_n * a.$$

The direct examples of normal subgroups are subgroups of abelian groups. For example, $n\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$ for all $n \in \mathbb{N}$, the circle is a normal subgroup of $(\mathbb{C}^*, \cdot)$, and all the subgroups in Example 7.1.8 are normal subgroups of $(\mathbb{C}^*, \cdot)$. The following example is for a normal subgroup of nonabelian group.

Example 7.5.4 Let $n \in \mathbb{N}$. The set $SL_n(\mathbb{R})$, of all $n \times n$ invertible matrices whose determinant is 1 (Notation 1.6.25), forms a normal subgroup of the group of $n \times n$ invertible matrices on the real numbers. i.e.,

$$SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R}) \quad \text{for all } n \in \mathbb{N}.$$

As $\det(I_n) = 1$, then $SL_n(\mathbb{R})$ is a nonempty subset of $GL_n(\mathbb{R})$. Using the results of Proposition 1.6.23 and Exercise 1.9, for any $A, B \in SL_n(\mathbb{R})$,

$$det\big(AB^{-1}\big) = det(A)det\big(B^{-1}\big) = det(A)\frac{1}{det(B)} = 1 \cdot 1 = 1.$$

Hence, $AB^{-1} \in SL_n(\mathbb{R})$ for all $A, B \in SL_n(\mathbb{R})$. Therefore, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$ (Proposition 7.1.4 (3)). Moreover, if $A \in GL_n(\mathbb{R})$ and $B \in SL_n(\mathbb{R})$, then

$$det\big(ABA^{-1}\big) = det(A)det(B)det\big(A^{-1}\big) = det(A) \cdot 1 \cdot \frac{1}{det(A)} = 1$$

i.e., $ABA^{-1} \in SL_n(\mathbb{R})$. Therefore, $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$ (Proposition 7.5.2 (3)).

Example 7.5.5

1. Let $n \in \mathbb{N}$, such that $n \geq 3$. Consider the nonabelian group $(\mathfrak{S}_n, \circ)$ and its subgroup $\mathcal{A}_n$. One can use the results from Proposition 6.5.18 to show that for any $\phi \in \mathfrak{S}_n$ and $\psi \in \mathcal{A}_n$, the product $\varphi\ \psi\ \phi^{-1}$ is always an even permutation. Therefore, $\mathcal{A}_n$ is a normal subgroup.
2. The subgroup $\langle(12)\rangle = \{e, (12)\}$ is an example of a non-normal subgroup of $(\mathfrak{S}_n, \circ)$, $n \geq 3$, as

$$(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin \langle(12)\rangle.$$

The result in Example 7.5.5 (1) can be deduced as a corollary of more general results, as follows:

Proposition 7.5.6 *Let G be a group and H be a subgroup of H. If $[G : H] = 2$, then H is a normal subgroup of G.*

Proof Assume that $a \in G$ is an arbitrary element. Since $[G : H] = 2$, then there exist only two right and two left cosets of H.

- If $a \in H$, then by Proposition 7.4.5 (2), we have $Ha = H = aH$.
- If $a \notin H$, then $H \neq Ha$. As H and Ha are the only right cosets of H, then the set $\{H, Ha\}$ forms a partition of G. i.e., $Ha = G\backslash H$. Similarly, using the left cosets of H, one shows that $aH = G\backslash H$. Hence, $Ha = aH$.

As a is an arbitrary element in G, the subgroup H is normal. ■

For any $n \in \mathbb{N}$, where $n \geq 2$, the group $\mathcal{A}_n$ contains half the elements of $\mathfrak{S}_n$. Hence, one directly obtains $[\mathfrak{S}_n : \mathcal{A}_n] = 2$ and the following corollary.

Corollary 7.5.7 $\mathcal{A}_n \trianglelefteq \mathfrak{S}_n$ *for all* $n \in \mathbb{N}$.

Let G be any group. Recall that the center of G is $C(G) = \{g \in G : g * a = a * g \;\; \forall\, a \in G\}$.

Proposition 7.5.8 *The center of a group is a normal subgroup.*

Proof Let G be a group. According to Proposition 5.4.8, the center $C(G)$ is a subgroup of G. For all $a \in G$ and all $c \in C(G)$,

$$a * c * a^{-1} = c * a * a^{-1} = c \in C(G).$$

Hence, $a \;\; C(G) \;\; a^{-1} \subseteq C(G)$. Proposition 7.5.2 (3) implies that $C(G)$ is normal. ■

For the remainder of this section, we consider a group G and discuss the notion of normality in the presence of several subgroups of G. We begin with the next result that automatically follows.

Proposition 7.5.9 *Let G be a group and H be a normal subgroup of G. The normality of H in G implies its normality in any other subgroup of G containing H. i.e., if $H < K < G$, then*

$$H \trianglelefteq G \Rightarrow H \trianglelefteq K.$$

Note that

- The converse of the proposition above is not always true. If $H < K < G$ and H is normal in K, the group H is not necessarily normal in G. For example, let

  $$H = \langle(1\ 2)(3\ 4)\rangle = \{e, (1\ 2)(3\ 4)\} \text{ and } K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\}.$$

  Both H and K are subgroups of $\mathfrak{S}_4$ (Check!). The group K is an abelian subgroup (Klein group) that contains H.Therefore, H is a normal subgroup of K, but H is not normal in $\mathfrak{S}_4$ as $(2\ 3)H \neq H(2\ 3)$.
- The normality is not a transitive relation. i.e.,

  $$H \trianglelefteq K,\ K \trianglelefteq G \not\Rightarrow H \trianglelefteq G.$$

This result can be shown using the above example, as $H = \langle (1\ 2)(3\ 4)\ \rangle \trianglelefteq K$ and $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\} \trianglelefteq \mathfrak{S}_4$ (Check!), but H is not normal in $\mathfrak{S}_4$.

The following results explain the relation of normal subgroups with the normality of their intersection.

Proposition 7.5.10 *Let G be a group. If H_1, H_2, K_1, and K_2 are subgroups of G, then*

$$H_1 \trianglelefteq K_1,\ H_2 \trianglelefteq K_2 \Longrightarrow H_1 \cap H_2 \trianglelefteq K_1 \cap K_2.$$

Proof Assume that $H_1 \trianglelefteq K_1$ and $H_2 \trianglelefteq K_2$. As $K_1 \cap K_2$ contains $H_1 \cap H_2$ and the intersection of two subgroups of G is a subgroup of G, then both $H_1 \cap H_2$ and $K_1 \cap K_2$ are subgroups of G, and

$$H_1 \cap H_2 < K_1 \cap K_2.$$

If $k \in K_1 \cap K_2$ and $h \in H_1 \cap H_2$, then.

- $k \in K_1, h \in H_1$ and $H_1 \trianglelefteq K_1$ implies that $k * h * k^{-1} \in H_1$
- $k \in K_2, h \in H_2$ and $H_2 \trianglelefteq K_2$, implies that $k * h * k^{-1} \in H_2$

The two statements imply that $k * h * k^{-1} \in H_1 \cap H_2$. By Proposition 7.5.2(3), $H_1 \cap H_2$ is a normal subgroup of $K_1 \cap K_2$. ■

Corollary 7.5.11 *Let G be a group. Let H, K be subgroups of G such that $H \trianglelefteq G$.*

1. *The intersection of H with any subgroup K of G is a normal subgroup of K, i.e.,*

$$H \trianglelefteq G \ \wedge\ K < G \Longrightarrow H \cap K \trianglelefteq K.$$

2. *If K is a normal subgroup of G, then $H \cap K$ is a normal subgroup of G, i.e.,*

$$\text{if } H \trianglelefteq G \text{ and } K \trianglelefteq G, \text{ then } H \cap K \trianglelefteq G.$$

Proof Since any group is a normal subgroup of itself, then Proposition 7.5.10 can be applied with $H_1 = H$, $K_1 = G$, and $H_2 = K_2 = K$, to directly obtain the first statement. The second statement can be also obtained by applying Proposition 7.5.10 with $H_1 = H$, $H_2 = K$, $K_1 = K_2 = G$. ■

Note that if H is a normal subgroup of G, then the intersection of H with any subgroup K of G is not necessarily normal in H, i.e., $H \trianglelefteq G \wedge K < G \nRightarrow H \cap K \trianglelefteq H$. For example, consider any non-normal subgroup K of G, and let $H = G$. In this case, H is a normal subgroup of G, but $H \cap K = K$ is not normal in H.

Next, we examine the product of a normal subgroup with any other subgroup. One of the nice properties of a normal subgroup is that its product with any other subgroup will be always a group, as shown in the following proposition.

Proposition 7.5.12 *Let G be a group and H, K be subgroups of G.*

1. *If H is a normal subgroup of G, then HK is a subgroup of G. Namely, $HK = \langle H \cup K \rangle$. Moreover, $H \trianglelefteq HK$.*
2. *If both H and K are normal subgroups of G, then HK is a normal of G, i.e.,*

$$\text{if } H \trianglelefteq G \text{ and } K \trianglelefteq G, \text{ then } HK \trianglelefteq G.$$

Proof Assume that $H \trianglelefteq G$. For any $h \in H, k \in K$,

$$h * k = k * k^{-1} * h * k = k * \left(k^{-1} * h * k\right) \in KH$$

which implies that $HK \subseteq KH$. Note that $k^{-1} * h * k \in H$, by the normality of H.

Similarly,

$$k * h = k * h * k^{-1} * k = \left(k * h * k^{-1}\right) * k \in HK$$

i.e., $KH \subseteq HK$. Therefore, $HK = KH$, and Proposition 7.2.8 implies that HK is a subgroup of G. According to Proposition 7.3.15, $HK = \langle H \cup K \rangle$. Since $H < HK < G$ and $H \trianglelefteq G$, then $H \trianglelefteq HK$ (Proposition 7.5.9). For the second statement, assume that both H and K are normal. Let $g \in G$, and let $h * k \in HK$ be arbitrary elements. Since

$$g * h * g^{-1} \in H, g * k * g^{-1} \in K,$$

then

$$\begin{aligned} g * (h * k) * g^{-1} &= g * \left(h * \left(g^{-1} * g\right) * k\right) * g^{-1} \\ &= \left(g * h * g^{-1}\right) * \left(g * k * g^{-1}\right) \in HK. \end{aligned}$$

Since g, h, k are arbitrary, then by Proposition 7.5.2 (3), $HK \trianglelefteq G$. ■

To generalize these results to n subgroups, we recall the definition of the product of n subgroups (Definition 7.2.5).

Proposition 7.5.13 *Let G be a group, $n \in \mathbb{N}$, and let $H_1, \ldots, H_n$ be normal subgroups of G. The product $H_1 \cdots H_n$ is the subgroup of G generated by $\bigcup_{i=1}^{n} H_i$ and it is a normal subgroup of G. i.e.,*

$$\left\langle \bigcup_{i=1}^{n} H_i \right\rangle = H_1 \cdots H_n \trianglelefteq G.$$

Proof The proof is performed by induction on n, as follows:

- If $n = 1$, then the statement is true, as $H_1 = \langle H_1 \rangle$ and H_1 is a normal subgroup of G.

- Assume that the statement is true at n. i.e., $H_1 H_2 \cdots H_n = \left\langle \bigcup_{i=1}^{n} H_i \right\rangle$ and $H_1 \cdots H_n$ is a normal subgroup of G.
- At $n+1$, let $H_1, \ldots, H_n, H_{n+1}$ be normal subgroups of G and $K = H_1 \cdots H_n$. By Proposition 7.5.12 (2) and the induction hypothesis, one obtains that $K H_{n+1} = \langle K \cup H_{n+1} \rangle$, and $K H_{n+1}$ is a normal subgroup of G. By Proposition 7.3.16,

$$\langle K \cup H_{n+1} \rangle = \left\langle \bigcup_{i=1}^{n+1} H_i \right\rangle.$$

By the steps above and the principle of mathematical induction, the statement is true for any $n \in \mathbb{N}$. ■

As $H_1 \cup H_2 \cup \cdots \cup H_n = H_{\alpha(1)} \cup H_{\alpha(2)} \cup \cdots \cup H_{\alpha(n)}$ for any permutation α on $\{1, 2, 3, \ldots., n\}$, the last proposition implies the following corollary.

Corollary 7.5.14 *Let G be a group, $n \in \mathbb{N}$, and let $H_1, \ldots, H_n$ be normal subgroups of G. For any $\alpha \in \mathfrak{S}_n$,*

$$H_1 H_2 \cdots H_n = H_{\alpha(1)} H_{\alpha(2)} \cdots H_{\alpha(n)}.$$

We end the section by proving several results that are needed for Chap 9. We begin with the following lemma, which states that the elements of two normal subgroups with trivial intersection commute.

Lemma 7.5.15 *Let G be a group and H, K be normal subgroups of G. If $H \cap K = \{e\}$, then any $h \in H$ and $k \in K$ commute. i.e., $h * k = k * h$ for each $h \in H$ and $k \in K$.*

Proof Assume that H, K are normal subgroups of G and $H \cap K = \{e\}$. Let $h \in H$ and $k \in K$ be arbitrary elements. By Proposition 7.5.2,

$$k * h^{-1} * k^{-1} \in H \quad \text{and} \quad h * k * h^{-1} \in K$$

which implies that $h * \left(k * h^{-1} * k^{-1}\right) \in H$ and $\left(h * k * h^{-1}\right) * k^{-1} \in K$. Thus, the element $h * k * h^{-1} * k^{-1} \in H \cap K = \{e\}$. Therefore, $h * k = k * h$. ■

Proposition 7.5.16 *Let G be a group and let $H_1, \ldots, H_n$ be normal subgroups of G such that for each $1 \leq i \leq n$, $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$.*

1. For each $1 \leq i \leq n$,

$$\text{if } h \in H_i \text{ and } k \in \left\langle \bigcup_{j \neq i} H_j \right\rangle, \text{ then } h * k = k * h.$$

2. Every element in $H_1 \cdots H_n$ can be uniquely written in the form $h_1 * h_2 * \cdots * h_n$, where $h_i \in H_i$.

Proof

1. Let $K = \left\langle \bigcup_{j \neq i} H_j \right\rangle$. According to Proposition 7.5.13, K is a normal subgroup of G. As H_i is also a normal subgroup and $K \cap H_i = \{e\}$, then the result follows by Lemma 7.5.15.
2. By induction on n: If $n = 2$, then this is the statement of Proposition 7.2.10. Assume that the result is true for n. For $n + 1$, let $H_1, \ldots, H_{n+1}$ be normal subgroups. Assume that

   $$h_1 * h_2 * \cdots * h_n * h_{n+1} \text{ and } k_1 * k_2 * \cdots * k_n * k_{n+1}$$

   are two representations of an element in $H_1 \cdots H_{n+1}$. i.e.,

   $$h_1 * h_2 * \cdots * h_n * h_{n+1} = k_1 * k_2 * \cdots * k_n * k_{n+1}.$$

   As $H_1, \ldots, H_n$ are normal subgroups, by Proposition 7.5.13, the product $H_1 \cdots H_n = \left\langle \bigcup_{i=1}^{n} H_i \right\rangle$ forms a subgroup of G. Therefore,

   $$(h_1 * h_2 * \cdots * h_n) * h_{n+1} \text{ and } (k_1 * k_2 * \cdots * k_n) * k_{n+1}$$

   are two representations of the same element in the product $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle H_{n+1}$. By applying Proposition 7.2.10 to the subgroups $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle$ and H_{n+1}, we get

   $$h_1 * h_2 * \cdots * h_n = k_1 * k_2 * \cdots * k_n \text{ and } h_{n+1} = k_{n+1}.$$

   By the induction hypothesis, we obtain that $h_1 = k_1, h_2 = k_2, \ldots, h_n = k_n$.

Therefore $h_1 = k_1, h_2 = k_2, \ldots, h_n = k_n, h_{n+1} = k_{n+1}$ and the representations are equal.

By the principle of mathematical induction, the statement is true for all $n \in \mathbb{N}$. ■

Remark 7.5.17 The statement in Proposition 7.5.16 (2) does not require H_i to be normal if $n = 2$ (Proposition 7.2.10); however, this requirement cannot be omitted for $n > 2$, as it is required for the proof to show that the product $H_1 \cdots H_n$ forms a subgroup.

Proposition 7.5.18 *Let G be a group. If $H_1, \ldots, H_n$ are normal subgroups of G, then the following statements are equivalent.*

1. $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$ *for all* $1 \leq i \leq n$.
2. *For each* $h_i \in H_i$, $1 \leq i \leq n$

   $$h_1 * \cdots * h_n = e \Rightarrow h_1 = h_2 = \cdots = h_n = e.$$

Proof Assume that (1) holds. We show by induction on n that

$$h_1 * \cdots * h_n = e \Rightarrow h_1 = h_2 = \cdots = h_n = e.$$

The result is trivial for $n = 1$. If $n = 2$, the result easily follows (Exercise 7.8). Assume that the result is true for n, and $h_1 * \cdots * h_{n+1} = e$. Let $k = h_1 * \cdots * h_n$. The element $k \in \left\langle \bigcup_{j \neq n+1} H_j \right\rangle$, and $k * h_{n+1} = e$. By the case of $n = 2$, we obtain $k = e = h_{n+1}$. Using the induction hypothesis, as $k = h_1 * \cdots * h_n$, one also gets $h_1 = \cdots = h_n = e$.

For the other direction, assume that (2) holds. Let $h \in H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle$. Since $\left\langle \bigcup_{j \neq i} H_j \right\rangle = H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$ (Proposition 7.5.13), then $h = h_1 * \cdots * h_{i-1} * h_{i+1} * \cdots * h_n$, where $h_j \in H_j$, $1 \leq j \leq n$, $j \neq i$. i.e.,

$$h^{-1} * h_1 * \cdots * h_{i-1} * h_{i+1} * \cdots * h_n = e.$$

By Proposition 7.5.3,

$$k_1 * \cdots * k_{i-1} * h^{-1} * h_{i+1} * \cdots * h_n = e$$

where $k_t \in H_t$, $1 \leq t \leq i - 1$. Since $h \in H_i$, then by the hypothesis assumption

$$k_1 = \cdots = k_{i-1} = h^{-1} = h_{i+1} = h_n = e.$$

As $h^{-1} = e$, then $h = e$, and $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle$ is trivial. ■

The requirement of H_i to be normal in Proposition 7.5.18 can be omitted if $n = 2$ (Exercise 7.8).

Proposition 7.5.19 *Let G be a group, and let $H_1, \ldots, H_n$ be normal subgroups of G such that $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$ for all $1 \leq i \leq n$. Let $m \in \mathbb{N}$, where $m \leq n$, for each $h_i, k_i \in H_i$, $1 \leq i \leq m$.*

$$(h_1 * h_2 * \cdots * h_m) * (k_1 * k_2 * \cdots * k_m) = (h_1 * k_1) * (h_2 * k_2) * \cdots * (h_m * k_m).$$

Proof We show the statement by induction on m, where $1 \leq m \leq n$.

- If $m = 1$, then $(h_1) * (k_1) = (h_1 * k_1)$, and thus, the statement is true.
- Assume that the statement is true for m.
- For $m + 1$, one must show that

$$(h_1 * \cdots * h_{m+1}) * (k_1 * \cdots * k_{m+1}) = (h_1 * k_1) * \cdots * (h_{m+1} * k_{m+1})$$

  where $h_i, k_i \in H_i$.

  – As $k_1 \in H_1$, $h_2 * h_3 * \cdots * h_{m+1} \in \left\langle \bigcup_{j=2}^{m+1} H_j \right\rangle$, and $H_1 \cap \left\langle \bigcup_{j=2}^{m+1} H_j \right\rangle = \{e\}$, then by Lemma 7.5.15,

$$(h_2 * \cdots * h_{m+1}) * k_1 = k_1 * (h_2 * \cdots * h_{m+1})$$

– By the induction hypothesis,

$$(h_2 * \cdots * h_{m+1}) * (k_2 * \cdots * k_{m+1}) = (h_2 * k_2) * \cdots * (h_{m+1} * k_{m+1})$$

Thus,

$$\begin{aligned}(h_1 * h_2 * \cdots * h_{m+1}) * (k_1 * k_2 * \cdots * k_{m+1}) &= h_1 * (h_2 * \cdots * h_{m+1} * k_1) * k_2 * \cdots * k_{m+1}\\ &= h_1 * (k_1 * h_2 * \cdots * h_{m+1}) * k_2 * \cdots * k_{m+1}\\ &= (h_1 * k_1) * (h_2 * \cdots * h_{m+1}) * (k_2 \cdots k_{m+1})\\ &= (h_1 * k_1) * (h_2 * k_2) * \cdots * (h_{m+1} * k_{m+1}).\end{aligned}$$

■

7.6 Internal Direct Product of Subgroups

In this section, we examine what it means for a group G to be the internal direct product of subgroup. We begin by defining the notion using only two subgroups, and then extend the definition to n subgroups. The nomenclature *internal* is justified in Exercise 8.6. Recall that if G is a group and H, K are two normal subgroups of G, then their product $HK = \{h * k : h \in H, k \in K\}$ is a subgroup of G.

Definition 7.6.1 Let G be a group and let H, K be normal subgroups of G. The group G is called the internal direct product of H and K if the following conditions are satisfied:

$$H \cap K = \{e\} \ \text{ and } \ G = HK.$$

The condition $H \cap K = \{e\}$ has a key role in defining the notion of internal direct product. The condition ensures that every element in the product HK is written in a unique form of $h * k$ (Proposition 7.2.10).

Example 7.6.2

1. Consider the additive group $(\mathbb{Z}_6, \oplus_6)$. Let

$$H = \langle[2]\rangle = \{[0], [2], [4]\} \text{ and } K = \langle[3]\rangle = \{[0], [3]\}.$$

It is straightforward to check that the conditions in Definition 7.6.1 are satisfied. Therefore, $\mathbb{Z}_6$ is the internal direct product of $\langle[2]\rangle$ and $\langle[3]\rangle$.

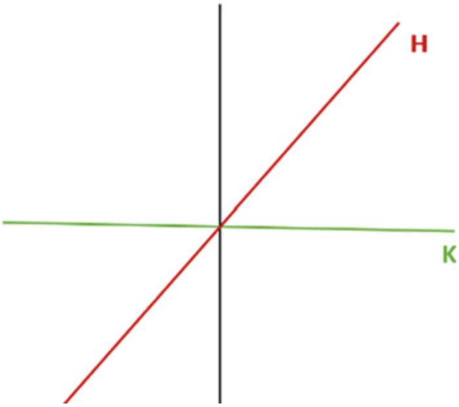


Fig. 7.4 The subgroup H and K

2. Consider the abelian group $(\mathbb{Z} \times \mathbb{Z}, +)$. Let $H = \{(x, 0) : x \in \mathbb{Z}\}$ and $K = \{(0, y) : y \in \mathbb{Z}\}$. Both subsets H and K are normal subgroups of $\mathbb{Z} \times \mathbb{Z}$, where $H + K = \mathbb{Z} \times \mathbb{Z}$ (verify!). The intersection of H and K is $\{(0, 0)\}$, which is the identity element in $\mathbb{Z} \times \mathbb{Z}$. Therefore, $\mathbb{Z} \times \mathbb{Z}$ is the internal direct product of H and K.
3. The groups $H = \{(a, a) : a \in \mathbb{R}\}$ and $K = \{(b, 0) : b \in \mathbb{R}\}$ are subgroups of $(\mathbb{R} \times \mathbb{R}, +)$ (Fig. 7.4). It can be easily verified that $(\mathbb{R} \times \mathbb{R}, +)$ is the internal direct product of H and K.
4. Consider the additive group $(\mathbb{Z}, +)$. Let $H = 2\mathbb{Z}$ and $K = 4\mathbb{Z}$. The product of H and K is $2\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z} \neq \mathbb{Z}$. Therefore, $\mathbb{Z}$ is not an internal direct product of H and K.
5. Consider the additive group $(\mathbb{Z}, +)$. Let $H = 2\mathbb{Z}$ and $K = 3\mathbb{Z}$. The product of H and K is $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$. However, $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z} \neq \{0\}$. Therefore, $\mathbb{Z}$ is not an internal direct product of H and K.

Example 7.6.3 Let $G = \{([x_1], [x_2], [x_3]) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 : x_1 + x_2 + x_3 \equiv 0 \mod 3\}$. Define $\oplus$ on the elements of G by

$$([x_1], [x_2], [x_3]) \oplus ([y_1], [y_2], [y_3]) = ([x_1] \oplus_3 [y_1], [x_2] \oplus_3 [y_2], [x_3] \oplus_3 [y_3])$$

for any $([x_1], [x_2], [x_3])$, $([y_1], [y_2], [y_3])$ in G. It is straightforward to show that G is an abelian group (verify!). In fact, G is a subgroup of the additive group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Let

$$\begin{aligned} H &= \{([x_1], [x_2], [x_3]) \in G : x_1 + x_2 + x_3 \equiv 0 \mod 3, \quad x_2 \equiv 0 \mod 3\} \\ \text{and} \quad K &= \{([x_1], [x_2], [x_3]) \in G : x_1 + x_2 + x_3 \equiv 0 \mod 3, \quad x_1 \equiv 0 \mod 3\}. \end{aligned}$$

As both H and K are closed under the addition and taking the additive inverse, so H and K are subgroups of G. We show that G is the internal direct product of H and K. Both subgroups H, K are normal, as G is abelian. Any element $([x_1], [x_2], [x_3])$

in $H \cap K$ must satisfy

$$x_1 + x_2 + x_3 \equiv 0 \mod 3, \; x_1 \equiv 0 \mod 3, \quad \text{and} \; x_2 \equiv 0 \mod 3.$$

Hence,

$$x_3 \equiv 0 + 0 + x_3 \equiv x_1 + x_2 + x_3 \equiv 0 \mod 3$$

which yields $([x_1], [x_2], [x_3]) = ([0], [0], [0])$. Thus, $H \cap K = \{0_G\}$.

According to Definition 7.6.1, we need to show that $G = HK$. As the group G contains both H and K, it contains their product $HK = \langle H \cup K \rangle$. To check the other inclusion, let $([x_1], [x_2], [x_3])$ be an arbitrary element in G. By the definition of G,

$$x_3 \equiv -x_1 - x_2 \;\; mod \; 3.$$

Therefore, $([x_1], [x_2], [x_3]) = ([x_1], [x_2], -[x_1] - [x_2])$. Hence,

$$([x_1], [x_2], [x_3]) = ([x_1], [0], [-x_1]) \oplus ([0], [x_2], [-x_2]) \in HK.$$

Example 7.6.4 Consider the group G consisting of $\mathbb{R}^3$ endowed with the vector addition. Let

$$H_1 = \{(x_1, x_2, x_3) \in G : x_1 + x_2 + x_3 = 0\} \;\text{ and }\; H_2 = \{(x, x, x) \in G : x \in \mathbb{R}\}.$$

It can be easily checked that H_1 and H_2 are subgroups of G. Both subgroups are normal, as G is abelian. Any element in $H_1 \cap H_2$ has the form (x, x, x), where $x + x + x = 0$, which implies that $x = 0$, i.e., $H_1 \cap H_2 = \{(0, 0, 0)\}$. Any element $(x_1, x_2, x_3) \in G$ can be expressed as

$$(x_1, x_2, x_3) = (x_1 - z, x_2 - z, x_3 - z) + (z, z, z) \in H_1 + H_2$$

where $z = (x_1 + x_2 + x_3)/3$. Therefore, $H_1 + H_2 = G$ is the internal direct product of H_1 and H_2.

Next, we generalize the notion of the internal direct product to arbitrary finite number of subgroups.

Definition 7.6.5 Let G be a group and let $H_1, \ldots, H_n$ be normal subgroups of G. If

1. $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$ for all $1 \leq i \leq n$.
2. $G = H_1 \cdots H_n$.

then G is called the internal direct product of the subgroups $H_1, \ldots, H_n$.

Note that $H_i \cap \left\langle \bigcup_{i \neq j} H_j \right\rangle = \{e\}$ implies that $H_i \cap H_j = \{e\}$ for each $i \neq j$, but the converse is not true (Exercise 7.6).

Example 7.6.6 Let G be the additive group $\mathbb{Z}^4 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, and

$$H_1 = \{(x, 0, 0, x) : x \in \mathbb{Z}\}, \quad H_2 = \{(0, x, 0, 3x) : x \in \mathbb{Z}\},$$
$$H_3 = \{(0, 0, x, -x) : x \in \mathbb{Z}\}, \quad H_4 = \{(0, 0, 0, x) : x \in \mathbb{Z}\}.$$

The group G is abelian, and thus, all the subgroups H_i are normal subgroups. We show that G is the internal direct product of $H_1, \ldots, H_4$.

- Any element in $\langle H_2 \cup H_3 \cup H_4 \rangle$ has 0 in the first coordinate. Therefore, any element in $H_1 \cap \langle H_2 \cup H_3 \cup H_4 \rangle$ has 0 in the first coordinate and must be of the form $(x, 0, 0, x)$, which implies that this element must be $(0, 0, 0, 0)$.
- Any element in $\langle H_1 \cup H_3 \cup H_4 \rangle$ has 0 in the second coordinate. Therefore, any element in $H_2 \cap \langle H_1 \cup H_3 \cup H_4 \rangle$ has 0 in the second coordinate and must be of the form $(0, x, 0, 3x)$, which implies that this element must be $(0, 0, 0, 0)$.
- Similarly, one can show that $H_3 \cap \langle H_1 \cup H_2 \cup H_4 \rangle$ contains only $(0, 0, 0, 0)$.
- Since the group $\mathbb{Z}^4$ is abelian, any element in $\langle H_1 \cup H_2 \cup H_3 \rangle$ has the form $(x_1, x_2, x_3, x_1 + 3x_2 - x_3)$, where $x_1, x_2, x_3 \in \mathbb{Z}$. For this elements to be in H_4, the first three elements must be zeros. Therefore, the only element in $H_4 \cap \langle H_1 \cup H_2 \cup H_3 \rangle$ is $(0, 0, 0, 0)$.

Hence the subgroups H_1, H_2, H_3, and H_4 satisfy $H_j \cap \left\langle \bigcup_{i \neq j} H_i \right\rangle = \{e\}$ for all $1 \leq j \leq 4$. Since H_1, H_2, H_3, H_4 are normal subgroups of G, then by Proposition 7.5.13, their product $H_1 H_2 H_3 H_4$ forms a subgroup of G. To show that G is contained in $H_1 H_2 H_3 H_4$, assume that (x_1, x_2, x_3, x_4) is an arbitrary element in G. As

$$\begin{aligned}(x_1, x_2, x_3, x_4) = (x_1, 0, 0, x_1) + (0, x_2, 0, 3x_2) + (0, 0, x_3, -x_3)\\ +(0, 0, 0, -x_1 - 3x_2 + x_3 + x_4)\end{aligned}$$

belongs to$H_1 H_2 H_3 H_4$, then $G = H_1 H_2 H_3 H_4$, i.e., G is the internal direct product of $H_1, \ldots, H_4$.

Example 7.6.7 Consider the additive group $(\mathbb{Z} \times \mathbb{Z}, +)$. Let

$$H_1 = \mathbb{Z} \times \{0\}, H_2 = \{0\} \times \mathbb{Z}, \quad \text{and} \quad H_3 = \{(n, n) : n \in \mathbb{Z}\}.$$

The subgroups H_i, with $i = 1, 2, 3$, are normal subgroups of $\mathbb{Z} \times \mathbb{Z}$. As $H_3 \cap \langle H_1 \cup H_2 \rangle = H_3 \neq \{(0, 0)\}$, then $\mathbb{Z} \times \mathbb{Z}$ is not an internal direct product of H_1, H_2, and H_3.

7.7 The Quotient Groups

Let G be a group and H be a subgroup of G. If H is a normal subgroup of G, then the right and left cosets of H coincide, and G/H will denote the set of all cosets of H without distinguishing between the right and left cosets, i.e., $G/H = \{aH : a \in G\}$.

In what follows, we define an operation $\cdot_{G/H}$ on the set G/H. This operation is well-defined if and only if H is a normal subgroup, in which case, G/H forms a group known as the quotient group of G by H.

Definition 7.7.1 Let G be a group and H be a subgroup of G. Define the operation $\cdot_{G/H}$ on G/H as

$$(aH) \cdot_{G/H} (bH) = (a * b)H \qquad \forall a, b \in G.$$

Lemma 7.7.2 *Let $(G, *)$ be a group and H be a subgroup of G. The group H is a normal subgroup of G if and only if $\cdot_{G/H}$ is well-defined, i.e., if and only if for all $a, b, a', b' \in G$,*

$$aH = a'H \ \wedge \ bH = b'H \Rightarrow (a * b)H = \big(a' * b'\big)H$$

Proof Assume that H is a normal subgroup of G, and let a, b, a', and b' be elements in G such that $aH = a'H$ and $bH = b'H$. To show that $(a * b)H = \big(a' * b'\big)H$, it suffices (by Proposition 7.4.7) to show that $(a * b) \in \big(a' * b'\big)H$ by the following steps:

- Here, $b \in bH = b'H \Rightarrow \exists\, h_1 \in H \ni b = b' * h_1 \Rightarrow \exists\, h_1 \in H \ni a * b = a * b' * h_1$.
- Since H is a normal subgroup of G, then $b'H = Hb'$. Hence, there exists $h_2 \in H$ such that $b' * h_1 = h_2 * b'$, i.e., $\exists\, h_2 \in H \ni a * b = a * h_2 * b'$.
- As $aH = a'H$, there exists $h_3 \in H$ such that $a * h_2 = a' * h_3$. Hence, $\exists\, h_3 \in H \ni a * b = a' * h_3 * b'$.
- Again, as H is a normal subgroup of G, then $Hb' = b'H$, and there exists $h_4 \in H$ such that $h_3 * b' = b' * h_4$. i.e., $\exists\, h_4 \in H \ni a * b = a' * b' * h_4$.

One can summarize these steps as follows:

$$a * b \underset{bH = b'H}{=} a * b' * h_1 \underset{b'H = Hb'}{=} a * h_2 * b' \underset{aH = a'H}{=} a' * h_3 * b' \underset{b'H = Hb'}{=} a' * b' * h_4.$$

Therefore, $(a * b) \in \big(a' * b'\big)H$.

For the other direction, assume that

$$aH = a'H \ \wedge \ bH = b'H \Rightarrow (a * b)H = \big(a' * b'\big)H$$

holds for any $a, b, a', b' \in G$. Let $g \in G$ and $h \in H$. As $eH = hH$ and $gH = gH$, then by the assumption,

$$gH = (e * g)H = (h * g)H.$$

Hence, Proposition 7.4.7 implies that $(h * g) \in gH$. As this is true for all $h \in H$, then $Hg \subseteq gH$ and H is normal (Proposition 7.5.2). ■

Proposition 7.7.3 *Let $(G, *)$ be a group and H be a normal subgroup of G. The operation $\cdot_{G/H}$ defined on G/H by*

$$(aH) \cdot_{G/H} (bH) = (a * b)H \quad \forall\, a, b \in G$$

is a binary operation on G/H that turns it into a group.

Proof For any $aH, bH \in G/H$, the coset $(a * b)H$ is an element in G/H, i.e., G/H is closed under $\cdot_{G/H}$. Since H is normal, Lemma 7.7.2 implies that the operation $\cdot_{G/H}$ is a well- defined binary operation on G/H. To show the associative property of $\cdot_{G/H}$, let aH, bH, and cH be arbitrary elements in G/H, then

$$\begin{aligned}\big((aH) \cdot_{G/H} (bH)\big) \cdot_{G/H} (cH) &= ((a * b)H) \cdot_{G/H} (cH) = ((a * b) * c)H \\ &= (a * (b * c))H = (aH) \cdot_{G/H} ((b * c)H) \\ &= (aH) \cdot_{G/H} \big((bH) \cdot_{G/H} (cH)\big).\end{aligned}$$

As $H = eH \in G/H$ and satisfies $(eH) \cdot_{G/H} (aH) = aH = (aH) \cdot_{G/H} (eH)$ for each $a \in G$, then H is an identity element of G/H with respect to the operation $\cdot_{G/H}$. Finally, if aH is an element in G/H, then $a^{-1}H$ is also an element in G/H satisfying

$$(aH) \cdot_{G/H} \left(a^{-1}H\right) = H = \left(a^{-1}H\right) \cdot_{G/H} (aH)$$

i.e., aH is invertible in G/H, where $(aH)^{-1} = a^{-1}H$. ■

Definition 7.7.4 (Quotient group) Let G be a group and H be a normal subgroup of G. The group $\left(G/H, \cdot_{G/H}\right)$ defined in Proposition 7.7.3 is called the quotient group of G by H.

For an abelian group G, since any subgroup of G is normal, the quotient group G/H is always defined for any subgroup H of G. The following example pertain to a quotient group constructed from a nonabelian group.

Example 7.7.5 Consider the nonabelian group $\mathfrak{S}_4$ and its subgroup.

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

There are $[\mathfrak{S}_4 : H] = 6$ left (right) cosets of H that can be directly computed to obtain

$$\begin{aligned}eH &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = He \\ (1\ 2)H &= \{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\} = H(1\ 2) \\ (1\ 3)H &= \{(1\ 3), (1\ 2\ 3\ 4), (2\ 4), (1\ 4\ 3\ 2)\} = H(1\ 3) \\ (2\ 3)H &= \{(2\ 3), (1\ 3\ 4\ 2), (1\ 2\ 4\ 3), (1\ 4)\} = H(2\ 3)\end{aligned}$$

Table 7.4 Cayley's table of $\left(\mathfrak{S}_4/H, \cdot_{\mathfrak{S}_4/H}\right)$

$\cdot_{\mathfrak{S}_4/H}$	H	$(1\ 2)H$	$(1\ 3)H$	$(2\ 3)H$	$(1\ 2\ 3)H$	$(1\ 3\ 2)H$
H	H	$(1\ 2)H$	$(1\ 3)H$	$(2\ 3)H$	$(1\ 2\ 3)H$	$(1\ 3\ 2)H$
$(1\ 2)H$	$(1\ 2)H$	H	$(1\ 3\ 2)H$	$(1\ 2\ 3)H$	$(2\ 3)H$	$(1\ 3)H$
$(1\ 3)H$	$(1\ 3)H$	$(1\ 2\ 3)H$	H	$(1\ 3\ 2)H$	$(1\ 2)H$	$(2\ 3)H$
$(2\ 3)H$	$(2\ 3)H$	$(1\ 3\ 2)H$	$(1\ 2\ 3)H$	H	$(1\ 3)H$	$(1\ 2)H$
$(1\ 2\ 3)H$	$(1\ 2\ 3)H$	$(1\ 3)H$	$(2\ 3)H$	$(1\ 2)H$	$(1\ 3\ 2)H$	H
$(1\ 3\ 2)H$	$(1\ 3\ 2)H$	$(2\ 3)H$	$(1\ 2)H$	$(1\ 3)H$	H	$(1\ 2\ 3)H$

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\} = H(1\ 2\ 3)$$
$$(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\} = H(1\ 3\ 2)$$

As these six cosets are different, then these are all the left (right) cosets of H. The subgroup H is normal as $\phi H = H\phi$ for all ϕ in $\mathfrak{S}_4$. Therefore, $\mathfrak{S}_4/H$ forms a group under the operation $\cdot_{\mathfrak{S}_4/H}$. To obtain Cayley's table for $\left(\mathfrak{S}_4/H, \cdot_{\mathfrak{S}_4/H}\right)$ (Table 7.4), consider

$$\mathfrak{S}_4/H = \{H, (1\ 2)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H\}.$$

Therefore,

Recall that the elements of G/H are equivalent classes of an equivalence relation (Lemma 7.4.13). Each class can be represented by any element in that class. For example,

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3\ 4), (2\ 4), (1\ 4\ 3\ 2)\}$$

is equal to $(1\ 2\ 3\ 4)H$, $(2\ 4)H$, and $(1\ 4\ 3\ 2)H$. All these subsets are representations of the same coset of H (Proposition 7.4.7). These different representations for aH lead to different but equivalent representations of G/H, for example

$$\begin{aligned}\mathfrak{S}_4/H &= \{H, (1\ 2)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H\}\\ &= \{H, (1\ 2)H, (1\ 2\ 3\ 4)H, (2\ 3)H, (1\ 4\ 2)H, (1\ 3\ 2)H\}\\ &= \{H, (1\ 2)H, (2\ 4)H, (2\ 3)H, (1\ 3\ 4)H, (1\ 3\ 2)H\}.\end{aligned}$$

All of sets are equivalent representations for $\mathfrak{S}_4/H$, in the last example (Check!). Therefore, the following fact must be considered:

If $\{eH, a_1H, \dots, a_mH\}$ represents G/H, then in computing $(a_iH) \cdot_{G/H} \left(a_jH\right) = \left(a_i * a_j\right)H$, the element $a_i * a_j$ may not belong to the set $\{e, a_1, \dots, a_m\}$, but there must be an element $a_k \in G$ such that $\left(a_i * a_j\right)H = a_kH$. For example, if one chooses the representation

$$\mathfrak{S}_4/H = \{H, (1\ 3\ 2\ 4)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H\}$$

then in finding the product

$$(1\ 3\ 2\ 4)H \cdot_{\mathfrak{S}_4/H} (1\ 3)H = (1\ 3\ 2\ 4)(1\ 3)H = (1\ 2\ 4)H,$$

the coset $(1\ 2\ 4)H$ does not appear in the representation of $\mathfrak{S}_4/H$, Nevertheless, $(1\ 2\ 4)H = (1\ 3\ 2)H$, which belongs to the current representation of $\mathfrak{S}_4/H$.

Let G be a group and H, K be normal subgroups of G. If H is normal and contained in K, then it is straightforward to show that K/H forms a subgroup of G/H. The next proposition shows that any subgroup of G/H must be in the form of a quotient group.

Proposition 7.7.6 *Let G be a group and H be a normal subgroup of G. Any subgroup of G/H is of the form K/H, where K is a subgroup of G containing H.*

Proof Let $\mathcal{K}$ be a subgroup of G/H. Let $K = \{a \in G : aH \in \mathcal{K}\}$. We show that K is a subgroup of G containing H and that $\mathcal{K} = K/H$, as follows:

K is a nonempty subgroup of G, as $eH = H \in \mathcal{K}$. Thus, $e \in K$. If a, b are any elements in K, then aH and bH are elements in $\mathcal{K}$. Since $\mathcal{K}$ is a subgroup of G/H,

$$\left(a * b^{-1}\right)H = aH \cdot_{G/H} b^{-1}H = aH \cdot_{G/H} (bH)^{-1} \in \mathcal{K}.$$

Therefore, $a * b^{-1} \in K$. According to Proposition 7.1.4 (3), K is a subgroup of G. Let h be an arbitrary element in H, then $hH = H \in \mathcal{K}$, which implies that $h \in K$. Hence, $H \subseteq K$. As H is a normal subgroup of the whole group G, then it is normal in the subgroup K. Finally

$$K/H = \{aH : a \in K\} = \{aH : a \in G \ \wedge \ aH \in \mathcal{K}\} = \{aH : aH \in \mathcal{K}\} = \mathcal{K}.$$

■

Proposition 7.7.6 has another proof that uses the notion of homomorphism studied in Chap 8. The other proof is given in Exercise 8.7.

Proposition 7.7.7 *Let G be a group and H be a normal subgroup of G. If G is abelian, then G/H is abelian. If G is finite, then G/H is finite.*

Proof Assume that G is an abelian group. The quotient group G/H is abelian as.

$$(aH) \cdot_{G/H} (bH) = (a * b)H = (b * a)H = (bH) \cdot_{G/H} (aH)$$

for all elements $aH, bH \in G/H$. If G is finite, then H is also finite. By Lagrange's theorem 7.4.17,

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

i.e., G/H is also finite. ■

Remark 7.7.8 The converse of the two statements in Proposition 7.7.7, is not always true. For example, the group $\mathfrak{S}_n$ is not abelian, while its quotient $\mathfrak{S}_n/\mathcal{A}_n$, which only has two elements, is an abelian group. For the converse of the second statement, if G/H is finite, then G is finite if and only if H is finite. If G is an infinite group, then G/H can be either finite or infinite as shown in the following example.

Example 7.7.9

1. Consider the abelian group $(\mathbb{Z}, +)$. For each $n \in \mathbb{N}$, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. The set $\mathbb{Z}/n\mathbb{Z}$ consists of all elements of the form $a + n\mathbb{Z}$, where $a \in \mathbb{Z}$. By Example 7.4.2,

$$\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} : 0 \leq r < n\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

The operation

$$(a + \mathbb{Z}) +_{\mathbb{Z}/n\mathbb{Z}} (b + \mathbb{Z}) = (a + b) + \mathbb{Z}$$

turns $\mathbb{Z}/n\mathbb{Z}$ into a group, i.e., $\mathbb{Z}/n\mathbb{Z}$ is an example of a finite quotient group formed by infinite groups.

2. Let $n \in \mathbb{N}$ such that $n \geq 2$. Consider the group $\mathfrak{S}_n$ and its subgroup $\mathcal{A}_n$. By Corollary 7.5.7, the group $\mathcal{A}_n$ is a normal subgroup of $\mathfrak{S}_n$. As $[\mathfrak{S}_n : \mathcal{A}_n] = 2$, then $(\mathfrak{S}_n/\mathcal{A}_n, \circ_{\mathfrak{S}_n/\mathcal{A}_n})$ is a finite group formed by a quotient of two finite groups. As (12) is a permutation that belongs to $\mathfrak{S}_n$ for all $n \geq 2$, but not to $\mathcal{A}_n$, then for any $n \geq 2$, $(1\ 2)\mathcal{A}_n \neq \mathcal{A}_n$, i.e.,

$$\mathfrak{S}_n/\mathcal{A}_n = \{\mathcal{A}_n,\ (1\ 2)\mathcal{A}_n\}.$$

The following Cayley's table (Table 7.5) pertains to the quotient group $\mathfrak{S}_n/\mathcal{A}_n$.

3. Consider the group $(\mathbb{C}, +)$. The group $(\mathbb{R}, +)$ is a normal subgroup of $(\mathbb{C}, +)$, as $(\mathbb{C}, +)$ is abelian. The quotient $\mathbb{C}/\mathbb{R}$ can be described as

$$\begin{aligned}\mathbb{C}/\mathbb{R} &= \{z + \mathbb{R} : z \in \mathbb{C}\}\\ &= \{(x + iy) + \mathbb{R} : x, y \in \mathbb{R}\}\\ &= \{(iy + x) + \mathbb{R} : x, y \in \mathbb{R}\}\\ &= \{iy + \mathbb{R} : y \in \mathbb{R}\}.\end{aligned}$$

$\mathbb{C}/\mathbb{R}$ is an example of an infinite quotient group under the operation

Table 7.5 Cayley's table of $(\mathfrak{S}_n/\mathcal{A}_n, \circ_{\mathfrak{S}_n/\mathcal{A}_n})$

$\circ_{\mathfrak{S}_n/n}$	$\mathcal{A}_n$	$(1\ 2)\mathcal{A}_n$
$\mathcal{A}_n$	$\mathcal{A}_n$	$(1\ 2)\mathcal{A}_n$
$(1\ 2)\mathcal{A}_n$	$(1\ 2)\mathcal{A}_n$	$\mathcal{A}_n$

$$(iy_1 + \mathbb{R}) +_{\mathbb{C}/\mathbb{R}} (iy_2 + \mathbb{R}) = i(y_1 + y_2) + \mathbb{R}.$$

$\mathbb{C}/\mathbb{R}$ is a quotient group of two infinite groups.

We end the section with the proof of an important theorem in group theory called Cauchy's theorem. We provide the proof for the abelian case. A generalization to the nonabelian case also exists; see Theorem 5.2 in (Hungerford, 2003). The proof for the nonabelian case requires subjects that are beyond the scope of this book.

Lemma 7.7.10 *Let* $(G, *)$ *be a group,* H *be a normal subgroup of* G*, and* $a \in G$*. If* $\text{ord}(a)$ *is finite, then* $\text{ord}(a * \text{H})$ *is finite and divides* $\text{ord}(a)$.

Proof Let $k = \text{ord}(a)$. As

$$(aH)^k = \underbrace{(aH) * (aH) * \cdots * (aH)}_{k\ times} = a^k H = H = e_{G/H}$$

then by Lemma 5.5.6, $\text{ord}(aH)$ divides k. ■

Proposition 7.7.11 (Cauchy's theorem, the abelian case)
Let G *be a finite abelian group, and* p *be a prime number. If* p *divides* $|G|$, *then there exists an element* $a \in G$ *such that* $\text{ord}(a) = |\langle a\rangle| = p$.

Proof We show the result by strong induction on $|G|$. As p divides $|G|$, then $|G| \geq p > 1$. Therefore, we begin the base step at p.

Base step: If $|G| = p > 1$, then there exists $a \in G\backslash\{e\}$. Consider the subgroup of G generated by the element a. By Lagrange's theorem (Theorem 7.4.17), $|\langle a\rangle|$ divides p. As $a \neq e$, then $|\langle a\rangle| > 1$ and $\text{ord}(a) = |\langle a\rangle| = p$.

Inductive step: Assume that $|G| > p$ and the statement is true for all groups whose orders are less than $|G|$. Select $a \in G$ such that $a \in G\backslash\{e\}$. Since G is an abelian group, then $\langle a\rangle$ is a normal subgroup of G, which implies that $G/\langle a\rangle$ is a group whose order is less than $|G|$.

- If $p||\langle a\rangle|$, then $|\langle a\rangle| = kp$ for some $k \in \mathbb{N}$. By Corollary 5.5.7, $\left|\langle a^k\rangle\right| = p$ and a^k is the required element in G.
- Assume that $p \nmid |\langle a\rangle|$. As p divides $|G| = |G/\langle a\rangle| \cdot |\langle a\rangle|$ and $p \nmid |\langle a\rangle|$, then p divides $|G/\langle a\rangle|$. By the induction hypothesis, there exists an element $g\langle a\rangle \in G/\langle a\rangle$ such that $\text{ord}(g\langle a\rangle) = p$. According to Lemma 7.7.10, $\text{ord}(g\langle a\rangle)$ divides $\text{ord}(g)$, which implies that $\text{ord}(g) = kp$ for some $k \in \mathbb{N}$. By Corollary 5.5.7, $\text{ord}\left(g^k\right) = p$, and g^k is the required element in G. ■

Theorem 7.7.12 (Cauchy's theorem) Let G be a finite group, and p be a prime number. If p divides $|G|$, then there exists an element $a \in G$ such that $|\langle a\rangle| = p$.

Note that Cauchy's theorem provides a converse of Lagrange's theorem in the case in which G is finite and the divisor is prime. Using both results, the following corollary can be established.

Corollary 7.7.13 *Let G be a finite group. A prime p divides $|G|$ if and only if there exists a subgroup H of G such that $|H| = p$.*

Example 7.4.18 shows that Corollary 7.7.13 is not true if p is not prime.

Exercises

Solved Exercises

7.1 Any complex number $z \in \mathbb{C}$ can be written as $z = |z|e^{i\theta}$, where $e^{i\theta} = \cos\theta + i \sin\theta$ for some angle θ. Show that if $n \in \mathbb{N}$, then the distinct complex solutions for the equation $z^n = 1$ are

$$e^{\frac{2\pi ik}{n}}, \quad \text{where} \quad k = 0, 1, \dots, n-1.$$

Solution: As $\left(e^{\frac{2\pi ik}{n}}\right)^n = e^{2\pi ik} = \cos 2\pi k + i \sin 2\pi k = 1$, for any integer k, the complex number $e^{\frac{2\pi ik}{n}}$ is a solution for the equation $z^n = 1$. Clearly, $e^{\frac{2\pi ik}{n}}$ gives different solution for $k = 0, 1, \dots, n-1$, which implies that these are all of the possible solutions. Note that an equation in $\mathbb{C}$ of degree n has at most n solutions.

7.2 Let $n \in \mathbb{N}$, and let $U(\mathbb{C})$ be the upper triangular matrices in $\mathcal{M}_n(\mathbb{C})$ (Definition 1.6.3). i.e.,

$$U(\mathbb{C}) = \left\{\left(a_{ij}\right) \in \mathcal{M}_n(\mathbb{C}) : a_{ij} = 0 \quad \forall\, i > j\right\}.$$

Show that $U(\mathbb{C})$ forms an abelian subgroup of $(\mathcal{M}_n(\mathbb{C}), +)$.

Solution:

As the zero matrix is an upper triangular matrix, $U(\mathbb{C})$ is a nonempty subset of $(\mathcal{M}_n(\mathbb{C}), +)$. Let $A = \left(a_{ij}\right)$, $B = \left(b_{ij}\right)$ be two arbitrary matrices in $U(\mathbb{C})$. i.e., the coefficients a_{ij} and b_{ij} satisfy $a_{ij} = b_{ij} = 0 \quad \forall\, i > j$. Since

$$A + (-B) = \left(a_{ij} - b_{ij}\right)$$

where $a_{ij} - b_{ij} = 0 \quad \forall\, i > j$, then $A - B = A + (-B)$ belongs to subset $U(\mathbb{C})$. By Proposition 7.1.4 (3), $(U(\mathbb{C}), +)$ is a subgroup of $(\mathcal{M}_n(\mathbb{C}), +)$. The commutativity is inherited from the group $\mathcal{M}_n(\mathbb{C})$.

7.3 Let $n \in \mathbb{N}$ and $a \in \{1, 2, \dots, n\}$. Prove that the only subgroup of $\mathfrak{S}_n$ that contains all the transpositions $(a\ k)$ for all $1 \leq k \leq n, k \neq a$ is $\mathfrak{S}_n$. In particular, the only subgroup of $\mathfrak{S}_n$ that contains the transpositions $(1\ k)$ for all $2 \leq k \leq n$ is $\mathfrak{S}_n$.

Solution:

Let A be a subgroup of $\mathfrak{S}_n$ such that A contains all the transpositions $(a\ k)$ for all $1 \leq k \leq n, k \neq a$. According to Remark 6.5.2 (2), for any $i, j \in \{1, 2, \dots, n\}$ such that $i \neq j$,

- if $i = a$, then $(i\ \ j) = (a\ \ j) \in A$,

- if $j = a$, then $(i\ j) = (i\ a) = (a\ i) \in A$.
- if $i \neq a$, and $j \neq a$, then $(i\ j) = (a\ j)(a\ i)(a\ j) \in A$.

Therefore, A contains all transpositions $(i\ j)$. Since any permutation in $\mathfrak{S}_n$ is a finite product of transpositions (Corollary 6.5.3 (1)) and A is closed under composition, then any permutation in $\mathfrak{S}_n$ lies in A, which implies the results.

7.4 Consider the additive group $(\mathbb{Z}_{12}, \oplus_{12})$ and its subgroups $H_1 = \{[0], [6]\}$, $H_2 = \{[0], [4], [8]\}$, and $H_3 = \{[0], [3], [6], [9]\}$. For which collection of subgroups H_i does the union of H_i form a subgroup of $\mathbb{Z}_{12}$?

Solution:

One way to solve the question is to compute the unions of each two of the subgroups, and the union of all the subgroup to obtain four subsets of $\mathbb{Z}_{12}$. Next, examine every subset obtained for being a subgroup. The alternative and faster way to solve the question is to use Proposition 7.2.3, as follows:

- As $H_1 \subsetneq H_2$ and $H_2 \subsetneq H_1$, then $H_1 \cup H_2$ is not a subgroup of $\mathbb{Z}_{12}$.
- As $H_1 \subseteq H_3$, then $H_1 \cup H_3$ is a subgroup of $\mathbb{Z}_{12}$.
- As $H_2 \subsetneq H_3$ and $H_3 \subsetneq H_2$, then $H_2 \cup H_3$ is not a subgroup of $\mathbb{Z}_{12}$.
- For the union of the three subgroups, we apply Proposition 7.2.3 to the subgroups $H_1 \cup H_3$ and H_2. As none of the subgroups is contained within the other, then their union $H_1 \cup H_2 \cup H_3$ is not a subgroup.

Therefore, only the union of H_1 and H_3 forms a subgroup of $\mathbb{Z}_{12}$.

7.5 Let $n \in \mathbb{N}$ such that $n \geq 3$. Consider the two matrices

$$r = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \text{ and } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Show that the matrices r and s belong to $O(2)$ (the group of orthogonal matrices of order 2). Show that $r^n = s^2 = e$, $(sr)^2 = (rs)^2 = e$, and find the subgroup of $O(2)$ generated by r and s.

Solution:

Using matrix multiplication, it can be verified that

$$r\, r^T = r^T r = I_2 \text{ and } s\, s^T = s^T s = I_2.$$

Therefore, both matrices are elements of the group $O(2)$. The matrices r and s represent the rotation around the origin with the angle $\frac{2\pi}{n}$ and the reflection over the x-axis, respectively (Sect. 1.7). Clearly $\text{ord}(s) = 2$, and by Proposition 1.7.7, one can easily show that $\text{ord}(r) = n$ and $(sr)^2 = (rs)^2 = e$. By Exercise 7.30, $sr^k = r^{n-k}s$ for each $0 \leq k \leq n-1$ and

$$\begin{aligned}\langle r, s\rangle &= \left\{r^k s^m : 0 \leq k < n, \quad 0 \leq m < 2\right\} \\ &= \left\{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1} s\right\}.\end{aligned}$$

7.6 Let $n \in \mathbb{N}$ such that $n \geq 3$. Consider $\mathfrak{S}_n$, the group of all permutations on $\{1, 2, \dots, n\}$. Let $K = \langle \alpha, \tau \rangle$ be the subgroup generated by $\{\alpha, \tau\}$ where $\alpha = (1\ 2 \cdots n)$ and

$$\tau = (2\ \ n)(3\ \ n-1)(4\ \ n-2)\dots(k\ \ \ n-k+2)\dots\left(\left\lceil\frac{n}{2}\right\rceil\ \ n-\left\lceil\frac{n}{2}\right\rceil+2\right)$$

here $f(x) = \lceil x \rceil$ is the ceiling function defined by $\lceil x \rceil = \min\{k \in \mathbb{Z} : k \geq x\}$.

(e.g., in $\mathfrak{S}_4$, $\alpha = (1\ 2\ 3\ 4)$ and $\tau = (2\ 4)$. In $\mathfrak{S}_5$, $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\tau = (2\ 5)(3\ 4)$ and so on). Show that $\mathrm{ord}(\alpha) = n, \mathrm{ord}(\tau) = 2$, and the permutations α, τ satisfy $(\tau\alpha)^2 = e$ and $\tau\alpha^k = \alpha^{n-k}\tau$ for each $0 \leq k \leq n-1$. Therefore,

$$K = \langle \alpha, \tau \rangle = \left\{\alpha^k \tau^s : 0 \leq s \leq 1, \quad 0 \leq k \leq n-1\right\}.$$

Solution:

The permutation α is a cycle of length n, and thus, by Lemma 6.4.2, $\mathrm{ord}(\alpha) = n$. The permutation τ is a product of disjoint (commuting) transpositions, each of which is of order 2. Therefore, the result in Exercise 5.25 implies that $\mathrm{ord}(\tau) = 2$. To show that $(\tau\alpha)^2 = e$, it suffices to show that $\tau\alpha\tau(k) = \alpha^{-1}(k)$ for all $k \in \{1, 2, \dots, n\}$ as follows:

i If $k = 1$, then $\tau\alpha\tau(1) = \tau\alpha(1) = \tau(2) = n = \alpha^{-1}(1)$.
ii If $k = 2$, then $\tau\alpha\tau(2) = \tau\alpha(n) = \tau(1) = 1 = \alpha^{-1}(2)$.
iii For k such that $2 < k \leq n$, we have $2 < n-k+2 < n$, and

$$\tau\alpha\tau(k) = \tau\alpha(n-k+2) = \tau(n-k+3) = k-1 = \alpha^{-1}(k).$$

Therefore, $\tau\alpha\tau(k) = \alpha^{-1}(k)$ for all $k \in \{1, 2, \dots, n\}$. i.e., $\tau\alpha\tau = \alpha^{-1}$ and $(\tau\alpha)^2 = e$. By Exercise 7.30, $\tau\alpha^k = \alpha^{n-k}\tau$ for all $1 \leq k \leq n$ and

$$\begin{aligned} K = \langle \alpha, \tau \rangle &= \left\{\alpha^k \tau^s : s, k \in \mathbb{Z}\right\} \\ &= \left\{\alpha^k \tau^s : 0 \leq s \leq 1, \quad 0 \leq k \leq n-1\right\}. \\ &= \left\{\alpha, \alpha^2, \dots, \alpha^{n-1}, \tau, \alpha\tau, \alpha^2\tau, \dots, \alpha^{n-1}\tau\right\}. \end{aligned}$$

7.7 Let G be a group and $H_i, 1 \leq i \leq n$ be subgroups of G. Show that $H_i \cap \left\langle \bigcup_{i \neq j} H_j \right\rangle = \{e\}$ implies that $H_i \cap H_j = \{e\}$ for all $1 \leq i \neq j \leq n$, but the converse is not true.

Solution:

Assume that $H_i \cap \left\langle \bigcup_{i \neq j} H_j \right\rangle = \{e\}$. For any $i, j \in \{1, 2, \dots, n\}$ such that $i \neq j$, we have

$$H_i \cap H_j \subseteq H_i \cap \left\langle \bigcup_{i \neq j} H_j \right\rangle = \{e\}.$$

Therefore, $H_i \cap H_j = \{e\}$. To show that the converse is not true, consider the additive group $(\mathbb{Z} \times \mathbb{Z}, +)$. Let $H_1 = \mathbb{Z} \times \{0\}$, $H_2 = \{0\} \times \mathbb{Z}$, and $H_3 = \{(n, n) : n \in \mathbb{Z}\}$.

For each $i \neq j$, the intersection $H_i \cap H_j = \{(0, 0)\}$ but $H_3 \cap \langle H_1 \cup H_2 \rangle = H_3 \neq \{(0, 0)\}$.

7.8 Let G be a group and H, K be subgroups of G. Show that

$$H \cap K = \{e\} \Leftrightarrow \text{for each } h \in H \text{ and } k \in K, h * k = e \Rightarrow h = k = e.$$

Solution

Assume that $H \cap K = \{e\}$ and let $h \in H$, $k \in K$ be arbitrary elements such that $h * k = e$. As K is a group, then $h = (h * k) * k^{-1} = e * k^{-1} \in K$, which implies that $h \in H \cap K$. Therefore, $h = e$ and $k = e * k = h * k = e$. For the other direction, assume that for each $h \in H$ and $k \in K$, $h * k = e \Rightarrow h = k = e$, and let d be an arbitrary element in $H \cap K$. As $d \in K$ and K is a group, $d^{-1} \in K$. As $d \in H$, and $d * d^{-1} = e$, thus by the assumption, $d = d^{-1} = e$.

Remark To generalize the result in this exercise, the subgroups under consideration must be normal subgroups, and this condition cannot be omitted (Proposition 7.5.18). A more general form of Proposition 7.5.18 is demonstrated in Exercise 7.9.

7.9 Let G be a group, and $H_1, \ldots, H_n$ be normal subgroups of G. The following statements are equivalent:

1. $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$ for all $1 \leq i \leq n$.
2. For all $m \in \mathbb{N}$, where $m \leq n$ and $h_i \in H_i$, $1 \leq i \leq m$,

$$h_1 * \cdots * h_m = e \Rightarrow h_1 = h_2 = \cdots = h_m = e.$$

Solution:

Assume that $H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\}$ for all $1 \leq i \leq n$. If $h_1 * \cdots * h_m = e$, then

$$e = h_1 * \cdots * h_m * e * e * \cdots * e = h_1 * \cdots * h_m * h_{m+1} * \cdots * h_n$$

where $h_{m+1} = \cdots = h_n = e$. By Proposition 7.5.18,

$$h_1 = h_2 = \cdots = h_m = h_{m+1} = \cdots = h_n = e.$$

Thus equalities $h_1 = h_2 = \cdots = h_m = e$ holds. For the other direction,

$$h_1 * \cdots * h_m = e \Rightarrow h_1 = h_2 = \cdots = h_m = e$$

holds for all $m \leq n$, in particular, for $m = n$. Hence, by Preposition 7.5.18,

$$H_i \cap \left\langle \bigcup_{j \neq i} H_j \right\rangle = \{e\} \text{ for all } 1 \leq i \leq n.$$

7.10 Let G be a finite group and H be a subgroup of G. Without using Lagrange's theorem, show that

$$|H| \text{ divides } |G| \text{ and } [G : H] = |G|/|H|.$$

Solution:

Let $a_1H, a_2H, \ldots, a_kH$ be all distinct left cosets of H. According to Proposition 7.4.5,

$$|a_iH| = |H|, \quad \forall\, 1 \leq i \leq k.$$

By this and Corollary 7.4.14,

$$|G| = \sum_{i=1}^{k} |a_iH| = \sum_{i=1}^{k} |H| = k|H|,$$

where k is the number of left (right) cosets of H. Consequently,

$$|H| \text{ divides } |G| \text{ and } [G : H] = |G|/|H|.$$

7.11 Let $(G, *)$ be a group and a, b be elements of G whose orders are finite. Show that if

$$a * b = b * a \text{ and } \langle a\rangle \cap \langle b\rangle = \{e\}, \text{ then } \mathrm{ord}(a * b) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)).$$

Solution:

Let a, b be elements in G such that $a*b = b*a$. Since the orders of a and b are finite, $\mathrm{ord}(a * b)$ is finite (Proposition 5.5.11). Let $l = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. According to Lemma 5.4.5 (2), $(a * b)^l = a^l * b^l = e$. Therefore, Lemma 5.5.6 implies that $\mathrm{ord}(a * b)$ divides l, i.e., $\mathrm{ord}(a * b) \leq l$. On the other hand, let $k = \mathrm{ord}(a * b)$, by Lemma 5.4.5 (2),

$$(a * b)^k = a^k * b^k = e,$$

which implies that $a^k = b^{-k} \in \langle b\rangle$. As $a^k \in \langle a\rangle$, then $a^k \in \langle a\rangle \cap \langle b\rangle = \{e\}$ and $a^k = e$ which implies that $\mathrm{ord}(a)$ divides k (Lemma 5.5.6). Similarly, one can show that $\mathrm{ord}(b)$ divides k, i.e., k is a positive multiple of both $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$. As l is the least common multiple, then $l \leq k$. Therefore, $k = l$.

7.12 Consider the additive group $(\mathbb{Z}, +)$. Show that for any $a, b \in \mathbb{Z}$ such that $a \neq 0$ or $b \neq 0$, the following identities hold:

- $\langle a\rangle\langle b\rangle = \langle \gcd(a, b)\rangle$ ($\langle a\rangle\langle b\rangle$ is also denoted by $\langle a\rangle + \langle b\rangle$)

- $\langle a\rangle \cap \langle b\rangle = \langle \mathrm{lcm}(a, b)\rangle$

Solution:

- Since $\gcd(a, b)$ divides both a and b, then as shown Example 7.3.8 (2), $\langle a\rangle \subseteq \langle \gcd(a, b)\rangle$ and $\langle b\rangle \subseteq \langle \gcd(a, b)\rangle$. Therefore, $\langle a\rangle\langle b\rangle \subseteq \langle \gcd(a, b)\rangle$. On the other hand, by Bézout's lemma, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$. Therefore,

$$\gcd(a, b) = xa + yb \in \langle a\rangle\langle b\rangle.$$

  As $\langle a\rangle\langle b\rangle$ is a group (Proposition 7.2.8), then by Corollary 7.3.4, $\langle \gcd(a, b)\rangle \subseteq \langle a\rangle\langle b\rangle$.
- As $\mathrm{lcm}(a, b) \in \langle a\rangle \cap \langle b\rangle$, and $\langle a\rangle \cap \langle b\rangle$ is a group, then $\langle \mathrm{lcm}(a, b)\rangle \subseteq \langle a\rangle\cap\langle b\rangle$. On the other hand, any element x in $\langle a\rangle\cap\langle b\rangle$ is a multiple of a and b. By Exercise 2.24, $\mathrm{lcm}(a, b)$ divides x, which implies that $x \in \langle \mathrm{lcm}(a, b)\rangle$. i.e., $\langle a\rangle \cap \langle b\rangle \subseteq \langle \mathrm{lcm}(a, b)\rangle$.

7.13 Let G be a group. For each $a \in G$, let $C_a = \{x \in G : x * a = a * x\}$. Show that

i C_a is a subgroup of G that is equal to G if and only if $a \in C(G)$.

ii $[G : C_a] = |[a]|$, where $[a]$ is the equivalence class of a for the conjugacy relation defined on G in Exercise 5.10.

iii If G is a finite group, then

$$|G| = |C(G)| + \sum_{C_a \neq G} [G : C_a].$$

Solution:

i Let a be an arbitrary element in G. As $e \in C_a$, then C_a is a nonempty subset of G. Let $x, y \in C_a$. As $y^{-1} * a = y^{-1} * a$, then it can be easily verified that

$$\left(x * y^{-1}\right) * a = a * \left(x * y^{-1}\right)$$

which implies that $x * y^{-1} \in C_a$, and C_a is a subgroup of G. Any element $a \in C(G)$ if and only if $a * x = x * a$ for all $x \in G$. This is, if and only if $C_a = G$.

ii Let a be an arbitrary element in G, and let $\{xC_a : x \in G\}$ be the left cosets of C_a. Define

$$\begin{aligned} f :&\{xC_a : x \in G\} \to [a] \\ &xC_a \mapsto x * a * x^{-1}. \end{aligned}$$

The result follows by showing that f is a bijective map. To show that f is well-defined, let xC_a, yC_a be any elements in $\{xC_a : x \in G\}$ such that $xC_a = yC_a$, then by Proposition 7.4.7, $y^{-1} * x \in C_a$, which yields $x = y * c$ for some $c \in C_a$. Therefore,

$$\begin{aligned} x * a * x^{-1} &= y * c * a * (y * c)^{-1} = y * c * a * c^{-1} * y^{-1} \\ &= y * a * c * c^{-1} * y^{-1} = y * a * y^{-1}. \end{aligned}$$

To show that f is injective, let xC_a, yC_a be two elements in $\{xC_a : x \in G\}$.

$$\begin{aligned} f(xC_a) = f(yC_a) &\Rightarrow x * a * x^{-1} = y * a * y^{-1} \\ &\Rightarrow y^{-1} * x * a = a * y^{-1} * x \\ &\Rightarrow y^{-1} * x \in C_a \Rightarrow xC_a = yC_a. \end{aligned}$$

Finally, assume that $b \in [a]$, i.e., $b = x * a * x^{-1}$ for some $x \in G$, then $f(xC_a) = x * a * x^{-1} = b$, and f is surjective.

iii Assume that G is a finite group. Let $[a_1], [a_2], \ldots, [a_k]$ be all distinct equivalence classes of the conjugacy equivalence relation $\sim$ defined on G, as in Exercise 5.10. As the equivalence classes of $\sim$ form a partition of G,

$$|G| = \sum_{a_i \in G} |[a_i]|.$$

By (ii),

$$|G| = \sum_{a_i \in G} [G : C_{a_i}].$$

Since for any $a \in G$, $a \in C(G)$ if and only if $[G : C_a] = 1$ ($C_a = G$),

$$\begin{aligned} |G| &= \underbrace{1 + 1 + \cdots + 1}_{|C(G)| \text{ times}} + \sum_{C_a \neq G} [G : C_{a_i}] \\ &= |C(G)| + \sum_{C_a \neq G} [G : C_{a_i}]. \end{aligned}$$

This equation is a well-known important equation in group theory, known as the conjugacy class equation.

7.14 Let $(G, *)$ be a group and H be a subgroup of G. Show that for any $a \in G$, $a^{-1} * H * a$ is a subgroup of G.

Solution:

Let a be an arbitrary element in G. As $e = a^{-1} * e * a \in a^{-1} * H * a$, thus $a^{-1} * H * a$ is a nonempty subset of G. If x, y are two elements in $a^{-1} * H * a$, then $x = a^{-1} * h_1 * a$ and $y = a^{-1} * h_2 * a$ for some $h_1, h_2 \in H$. Therefore,

$$\begin{aligned} x * y^{-1} &= a^{-1} * h_1 * a * \left(a^{-1} * h_2 * a\right)^{-1} = a^{-1} * h_1 * a * a^{-1} * h_2^{-1} * a \\ &= a^{-1} * h_1 * h_2^{-1} * a = a^{-1} * h * a \in a^{-1} * H * a \end{aligned}$$

where $h = h_1 * h_2^{-1} \in H$. By Proposition 7.1.4 (3), $a^{-1} * H * a$ is a subgroup of G.

7.15 Let G be a group. Show that any normal subgroup of G that consists of two elements must be in the center of G, i.e., $H \trianglelefteq G,\ |H| = 2 \ \Rightarrow\ H \subseteq C(G)$.

Solution:

Assume that H is a subgroup of G, where $H = \{e, h\}$ and $h \neq e$. As $e \in C(G)$, we only need to show that h belongs to $C(G)$. As H is a normal subgroup of G, then by Proposition 7.5.2, for each $a \in G$, $a*h*a^{-1} \in H$. i.e., $a*h*a^{-1}$ is either equal to e or h. If $a*h*a^{-1} = e$, then $h = e$ contradicting that H has two elements. Therefore, $a * h * a^{-1} = h$, i.e., $a * h = h * a$ for all $a \in G$, and h is at the center of G.

7.16 Let G be a finite group and H be a normal subgroup of G. Show that for each element $aH \in G/H$, where $\operatorname{ord}(a) < \infty$, there exists an element $b \in G$ such that $\operatorname{ord}(b) = \operatorname{ord}(aH)$.

Solution:

Let aH be an arbitrary element in G/H. According to Lemma 7.7.10, $\operatorname{ord}(aH)$ divides $\operatorname{ord}(a)$. Therefore, there exists $k \in \mathbb{Z}$ such that $\operatorname{ord}(a) = k \operatorname{ord}(aH)$. Let $b = a^k \in G$. By Proposition 5.5.9, we obtain

$$\operatorname{ord}(b) = \operatorname{ord}\left(a^k\right) = \frac{\operatorname{ord}(a)}{\gcd(k, \operatorname{ord}(a))} = \frac{\operatorname{ord}(a)}{\gcd(k, k \operatorname{ord}(aH))} = \frac{\operatorname{ord}(a)}{k} = \operatorname{ord}(aH).$$

7.17 Let G be a group, H be a finite normal subgroup of G, and $a \in G$. Show that if $\operatorname{ord}(aH)$ is finite, then $\operatorname{ord}(a)$ is finite.

Solution:

Since H is a normal subgroup of G, then aH is an element in the group G/H. Let k be equal to $\operatorname{ord}(aH)$. As $H = (aH)^k = a^k H$, by Proposition 7.4.5 (2), $a^k \in H$. As H is finite, Corollary 5.5.8 implies that $\operatorname{ord}\left(a^k\right)$ is finite; i.e., there exists $m \in \mathbb{N}$ such that $\left(a^k\right)^m = e$. Lemma 5.5.5 implies that $\operatorname{ord}(a)$ is finite.

7.18 Let $(G, *)$ be a group, H be a normal subgroup of G, and $a \in G$. If $\operatorname{ord}(aH) = 7$ and $|H| = 3$, find all possible orders of a.

Solution:

As $(a * H)^7 = a^7 * H = H$, then $a^7 \in H$. Hence, there exists $h \in H$ such that $a^7 = h$. Since $e = h^3 = a^{21}$, the order a is finite. By Lemma 5.5.6, $\text{ord}(a)$ divides 21. Since $\text{ord}(a * H)$ must divide $\text{ord}(a)$ (Lemma 7.7.10), $\text{ord}(a)$ must be a multiple of 7. Therefore, the possible orders of a are only 7 and 21.

Unsolved Exercises

7.19 Let V_4 be the set

$$\left\{\begin{pmatrix} 1\,2\,3\,\;4 \\ 1\,2\,3\,\;4 \end{pmatrix}, \begin{pmatrix} 1\,2\,3\,\;4 \\ 2\,1\,4\,\;3 \end{pmatrix}, \begin{pmatrix} 1\,2\,3\,\;4 \\ 3\,4\,1\,\;2 \end{pmatrix}, \begin{pmatrix} 1\,2\,3\,\;4 \\ 4\,3\,2\,\;1 \end{pmatrix}\right\}$$

Show that V_4 is an abelian subgroup of $\mathfrak{S}_4$ under the composition.

7.20 Let $n \in \mathbb{N}$, and let $L(\mathbb{C})$ be the lower triangular matrices in $\mathcal{M}_n(\mathbb{C})$. i.e.,

$$L(\mathbb{C}) = \left\{(a_{ij}) \in \mathcal{M}_n(\mathbb{C}) : a_{ij} = 0 \quad \forall\, j > i, \quad 1 \le i, j \le n\right\}.$$

Show that $L(\mathbb{C})$ forms a subgroup of $\mathcal{M}_n(\mathbb{C})$ under the matrix addition.

7.21 Determine if the following statements are true or false. Explain your answer.

i. $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.
ii. $\mathbb{Q}^*$ is a subgroup of $(\mathbb{C}^*, \cdot)$.
iii. $\mathbb{Z}[i]$ is a subgroup of $(\mathbb{R}, +)$.

7.22 Let G be an abelian group and $k \in \mathbb{Z}$. Show that $H(k) = \left\{a \in G : a^k = a\right\}$ is a subgroup of G.

7.23 Show that any subgroup of the additive group $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

7.24 Let $n \in \mathbb{N}$. Show that any subgroup of the additive group $(\mathbb{Z}_n, \oplus_n)$ is of the form $[k]\mathbb{Z}$ for some $k \in \{0, 1, \ldots, n-1\}$.

7.25 Give an example (different than Example 7.2.7) of a group G that has subgroups H, K, for which the product HK is not a subgroup of G.

7.26 Consider the additive group $(\mathbb{Z}, +)$, and let $H = 2\mathbb{Z}$ and $K = 6\mathbb{Z}$. Find HK and $H \cap K$.

7.27 Consider the additive group $(\mathbb{Z}, +)$. Without using the result of Exercise 7.12, show that for any $a, b \in \mathbb{Z}$

$$\langle a\rangle\langle b\rangle = \mathbb{Z} \Leftrightarrow \gcd(a, b) = 1.$$

7.28 Let G be a group, H be a subgroup of G, and $a \in G$ be an element of finite order. Show that

$$a^k \in H \;\wedge\; \gcd(\text{ord}(a), k) = 1 \Rightarrow a \in H.$$

7.29 Find the following subgroups:

a. $\langle\{3,\ 12\}\rangle$ as a subgroup of $(\mathbb{Z}, +)$.
b. $\langle -1\rangle$ as a subgroup of $(\mathbb{Z}, +)$.
c. $\left\langle (3\ 4\ 2)^7 \right\rangle$ as a subgroup of $(\mathfrak{S}_6, \circ)$.
d. $\langle (2\ 4\ 5\ 1)\rangle$ as a subgroup of $(\mathfrak{S}_6, \circ)$.

7.30 Let G be a group and a, b be two elements of G such that $\operatorname{ord}(a) = n$, $\operatorname{ord}(b) = 2$. Show that if $(a * b)^2 = e$, then $b * a^k = a^{n-k} * b$ for all $k \in \{0, 1, 2, \dots, n-1\}$ and

$$\langle a, b\rangle = \left\{e, a, a^2, \dots, a^{n-1}, b, a * b, a^2 * b, \dots, a^{n-1} * b\right\}.$$

7.31 Let G be a group and H, K be subgroups of G. If $|H| = 13$ and $|K| = 44$, find the order of $H \cap K$.

7.32 Find all the left and right cosets of $5\mathbb{Z}$ as a subgroup of $(\mathbb{Z}, +)$.

7.33 Find all the normal subgroups of $\mathfrak{S}_3$.

7.34 Let G_1, G_2 be groups and let H_1, H_2 be subgroups of G_1 and G_2, respectively. Show that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$. Show that if H_1, H_2 are normal subgroups, then $H_1 \times H_2$ is a normal subgroup of $G_1 \times G_2$. In particular, show that $G_1 \times \left\{e_{G_2}\right\}$ and $\left\{e_{G_1}\right\} \times G_1$ are normal subgroups of the product $G_1 \times G_2$.

7.35 Let G_1 and G_2 be groups. Give an example of a subgroup of $G_1 \times G_2$ such that it is not a product of a subgroup of $G_1 \times G_2$. (Hint: take $G \neq \{e\}$ and $H = \{(a, a) : a \in G\}$ is a subgroup of $G \times G$ but is not a direct product of subgroups of G).

7.36 Let G be a finite group and H be a normal subgroup of G. Show that

$$\gcd(|H|, [G : H]) = 1 \Rightarrow H = \left\{a \in G : a^{|H|} = e\right\}.$$

7.37 Let G be a finite group. Show that if there exists an integer m such that

$$(a * b)^m = a^m * b^m \text{ for all } a, b \in G$$

then

$$mG = \left\{a^m : a \in G\right\} \text{ and } G[m] = \left\{a \in G : a^m = e\right\}$$

form normal subgroups of G such that $|mG| = [G : G[m]]$.

Remark If $m = 1$, then G is abelian, $mG = G$ and $G[m] = \{e\}$ are normal subgroups of G, and $|mG| = |G| = [G : \{e\}] = [G : G[m]]$.

7.38 Let G be a group and let $H_1, \dots, H_n$ be normal subgroups of G. Show that the group G is the internal direct product of the subgroup $H_1, \dots, H_n$ if and only if the following conditions hold:

i $G = H_1 H_2 \cdots H_n$.
ii $h_1 * h_2 * \cdots * h_n = e \Rightarrow h_i = e$ for all $h_i \in H_i$, $1 \leq i \leq n$.

7.39 Let G be a group, H be a normal subgroup of G, and $a \in G$. Assuming that $\mathrm{ord}(aH) = 8$ and $|H| = 5$, find all possible orders of a.

7.40 Consider the additive group $(\mathbb{Z}_8, \oplus_8)$ and its subgroup $H = \{[0], [4]\}$. List all cosets of H, and find Cayley's table for $\left(\mathbb{Z}_8/H, \oplus_{\mathbb{Z}_8/H}\right)$.

7.41 Give an example of an infinite group G that has no element of finite order and a normal subgroup H such that G/H contains an element of finite order.

7.42 Let G be a group. Show that any two distinct subgroups of G of prime orders have a trivial intersection.

References

Boyd, S., & Vandenberghe, L. (2018). *Introduction to applied linear algebra vectors, matrices, and least squares.* Cambridge University Press.

Burton, D. M. (2007). *Elementary number theory.* MacGraw-Hill.

Hungerford, T. (2003). *Graduate texts in mathematics algebra.* Springer.

Chapter 8
Group Homomorphisms and Isomorphic Groups

In this chapter, maps between two groups called homomorphisms are presented and discussed. The bijective versions of these maps, isomorphisms, are studied. Isomorphisms respect all group structures, such as the cardinality of the group, order of the group elements, commutativity, and structures of all its subgroups. We begin by studying homomorphisms, stating their definition and proving some basic results in Sect. 8.1. Section 8.2 discusses isomorphisms by introducing the notions of the kernel and image of homomorphisms. In Sect. 8.3, we define what it means for the two groups to be isomorphic and state Cayley's theorem, an important theorem in group theory that enables us to see any group G as a subgroup of its symmetric group $\mathfrak{S}_G$. Section 8.4 presents and discusses the three fundamental theorems of homomorphisms. The chapter ends with Sect. 8.5, by defining the group action and explaining the relationship between group actions and group homomorphisms.

8.1 Group Homomorphisms, Definitions, and Basic Examples

The present section introduces group homomorphisms which are maps between two groups that preserve the group operation (i.e., the image of the product of two elements in the domain is equal to the product of their images in the codomain group).

Definition 8.1.1 Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. The map $f : G_1 \to G_2$ is said to be a group homomorphism (or simply, homomorphism) if

$$f(a * b) = f(a) \cdot f(b) \quad \forall\, a, b \in G_1.$$

A group homomorphism f is said to be

- a monomorphism if f is injective (one-to-one).
- an epimorphism if f is surjective (onto).

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_8

- an isomorphism if f is bijective.

The set of all group homomorphisms from G_1 to G_2 is denoted by $\mathrm{Hom}(G_1, G_2)$. We use $\mathrm{Hom}(G)$ to denote $\mathrm{Hom}(G, G)$. An isomorphism from G to itself is called an automorphism, and the set of all automorphisms of G is denoted $\mathrm{Aut}(G)$. We postpone the detailed study of isomorphisms and automorphisms to subsequent sections. This section is devoted to presenting the main definitions, examples, and basic results. For more information, refer to (Adkins & Weintraub, 1992).

Proposition 8.1.2 *The composition of two group homomorphisms (isomorphism) is a group homomorphism (isomorphism).*

Proof Let $(G_1, *)$, $(G_2, \cdot)$ and $(G_3, \bullet)$ be groups. Let $f : G_1 \to G_2$, and $g : G_2 \to G_3$ be group homomorphisms. The composition $g \circ f : G_1 \to G_3$ satisfies that

$$\begin{aligned} g \circ f(a * b) &= g(f(a * b)) = g(f(a) \cdot f(b)) \\ &= g(f(a)) \bullet g(f(b)) \\ &= g \circ f(a) \bullet g \circ f(b) \quad \text{for all } a, b \in G_1. \end{aligned}$$

Therefore, $g \circ f$ is a homomorphism. If both functions f and G are bijections, then $g \circ f$ is a bijection (Exercise 1.21). ■

Example 8.1.3

1. For two groups $(G_1, *)$ and $(G_2, \cdot)$, the function

$$\begin{aligned} f :&G_1 \to G_2 \\ &a \mapsto e_2 \qquad \text{for all } \ a \in G_1 \end{aligned}$$

is a group homomorphism as

$$f(a * b) = e_2 = e_2 \cdot e_2 = f(a) \cdot f(b) \text{ for all } a, b \in G_1.$$

This homomorphism is called the trivial homomorphism from G_1 into G_2.

2. For any group $(G, *)$,

   a. If H is a subgroup of G, then the inclusion map $\iota : H \to G$ defined by $\iota(h) = h$ is a monomorphism. The map ι is a one to one map that satisfies

$$\iota(h * k) = h * k = \iota(h) * \iota(k) \quad \forall\, h, k \in H.$$

   If $H = G$, then the identity map $\iota : G \to G$ is an automorphism.

b. If G is abelian, then the map $f : G \to G$ defined by $f(a) = a^{-1}$ is an automorphism. For if $a, b \in G$, then

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

The map f is one to one as $f(a) = f(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow a = b$. The map f is onto as for each $b \in G$, there exist $a = b^{-1} \in G$ and

$$f(a) = f\big(b^{-1}\big) = (b^{-1})^{-1} = b.$$

c. Let H be a normal subgroup of G. Define

$$\begin{aligned} \pi : G &\to G/H \\ a &\mapsto aH. \end{aligned}$$

The map π is an onto, as for each $aH \in G/H$, there exists $a \in G$ such that $\pi(a) = aH$. Moreover, π satisfies

$$\pi(a)\pi(b) = (aH)(bH) = (ab)H = \pi(ab),$$

and thus, π is an epimorphism. The map π is known as the quotient map of G into G/H.

d. For $a \in G$, the left multiplication by a,
$f_a : G \to G$ defined by $x \mapsto a * x \quad \forall\, x \in G$
is not a homomorphism for $a \neq e$. (Check!). In fact,
The map f_a is a homomorphism

$$\begin{aligned} &\text{if and only if } f_a(x * y) = f_a(x) * f_a(y) \ \text{ for all } x, y \in G \\ &\text{if and only if } \ a * x * y = a * x * a * y \ \text{ for all } x, y \in G \\ &\text{if and only if } a = e. \text{ i.e., } \ f_a \text{ is the identity map on } G \end{aligned}$$

3. Consider the additive group $(\mathbb{Z}, +)$. Define the map $f : \mathbb{Z} \to \mathbb{Z}$ by $f(a) = 3a$. The map f is a group homomorphism as

$$f(m + n) = 3(m + n) = 3m + 3n = f(m) + f(n) \ \text{ for all } \ m, n \in \mathbb{Z}.$$

The map f is a one to one map, but it is not onto since $f(\mathbb{Z}) = 3\mathbb{Z} \neq \mathbb{Z}$. Therefore, f is not an isomorphism.

4. Let m be any nonzero integer. It is straightforward to show that the map
$g : \mathbb{Z} \to m\mathbb{Z}$ given by $g(a) = ma$ is an isomorphism.
5. Consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, \oplus_n)$. Define

$$f : \mathbb{Z} \to \mathbb{Z}_n \text{ by } f(a) = [a], \quad \text{for all } \ a \in \mathbb{Z}.$$

For all $a, b \in \mathbb{Z}$, $f(a+b) = [a+b] = [a] \oplus_n [b] = f(a) \oplus_n f(b)$.

Hence, the map f is a homomorphism. However, The map f is not an isomorphism since it is not one to one, for example $f(n) = [n] = [0] = f(0)$ but $n \neq 0$. One can easily show that f is an epimorphism.

6. Consider the two groups $(\mathbb{Z}_{12}, \oplus_{12})$ and $(\mathbb{Z}_{30}, \oplus_{30})$. Let

$$\begin{aligned} f : \mathbb{Z}_{12} &\to \mathbb{Z}_{30} \\ [x]_{12} &\mapsto [5x]_{30} \end{aligned}$$

where $[x]_k$ denotes the equivalence class of x in $\mathbb{Z}_k$. According to Example 3.2.4, the map f is well-defined. The map f is a homomorphism as

$$\begin{aligned} f\big([x]_{12} \oplus_{12} [y]_{12}\big) &= f\big([x+y]_{12}\big) = [5(x+y)]_{30} \\ &= [5x]_{30} \oplus_{30} [5y]_{30} = f([x]_{12}) \oplus_{30} f\big([y]_{12}\big) \end{aligned}$$

for each $[x]_{12}, [y]_{12}$ in $\mathbb{Z}_{12}$. Since $\mathbb{Z}_{12}$ and $\mathbb{Z}_{30}$ have different cardinalities, no bijective maps exist between the two sets, so f is not an isomorphism.

7. Consider the groups $(\mathbb{R}, +)$ and $\big(\mathbb{R}^+, \cdot\big)$. Define $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = e^x \ \ \forall\, x \in \mathbb{R}$, where e is Euler number ($e \simeq 2.7$). The map f is an isomorphism. To show that f is a homomorphism, assume $x, y \in \mathbb{R}$, then

$$f(x+y) = e^{x+y} = e^x e^y = f(x) \cdot f(y).$$

The map f is a one to one function as

$$f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow \ln\big(e^x\big) = \ln\big(e^y\big) \Rightarrow x = y.$$

The map f is onto, for if $y \in \mathbb{R}^+$, then by putting $x = \ln y$,

$$f(x) = f(\ln(y)) = e^{ln(y)} = y.$$

Note that the map $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ defined by $f(x) = e^x \quad \forall\, x \in \mathbb{R}$ is still a homomorphism, but it is not an isomorphism as it is not surjective (Check!).

8. Let $n \in \mathbb{N}$. On $\mathfrak{S}_n$, consider the map sgn given in Corollary 6.5.15, i.e.,

$$\operatorname{sgn} : \mathfrak{S}_n \to \{1, -1\}, \text{ where } \operatorname{sgn}(\phi) = \begin{cases} 1 & \text{if} \quad \phi \quad \text{even} \\ -1 & \text{if} \quad \phi \quad \text{odd} \end{cases} \text{ for all } \phi \in \mathfrak{S}_n.$$

The set $\{1, -1\}$ forms a group under the multiplication (Check!). The map sgn is a homomorphism. Assume that ϕ, ψ are in $\mathfrak{S}_n$.

- If ϕ, ψ have the same parity, then by Proposition 6.4.15, $\phi \circ \psi$ is even and $\operatorname{sgn}(\phi \circ \psi) = 1 = \operatorname{sgn}(\phi)\operatorname{sgn}(\psi)$
- If ϕ, ψ have opposite parities, then by Proposition 6.4.15, $\phi \circ \psi$ is odd and

$$\operatorname{sgn}(\phi \circ \psi) = -1 = \operatorname{sgn}(\phi)\operatorname{sgn}(\psi).$$

In both cases,

$\text{sgn}(\phi \circ \psi) = \text{sgn}(\phi)\text{sgn}(\psi)$.

Therefore, sgn is a homomorphism. Since $\text{sgn}(e) = 1$, $\text{sgn}((12)) = -1$, the map sgn is surjective for each $n > 1$. Therefore, the map sgn is an epimorphism for any $n > 1$

9. Consider the group $(\mathbb{Q}^*)$. Define $f : \mathbb{Q}^* \to \mathbb{Q}^*$ by $f(x) = 3x$. Then

$$f(x \cdot y) = 3(x \cdot y) = 3xy,$$

$$f(x) \cdot f(y) = 3x \cdot 3y = 9xy.$$

Hence, f is not a homomorphism.

Next, we state and prove several basic results of homomorphisms.

Proposition 8.1.4 *Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. Let e_1, e_2 be the groups' identities in G_1 and G_2, respectively, and $f : G_1 \to G_2$ be a group homomorphism. The following statements hold:*

1. $f(e_1) = e_2$(any homomorphism takes the identity to the identity).
2. $f(a^{-1}) = f(a)^{-1}$ for all $a \in G_1$ (any homomorphism takes the inverse of any element to the inverse of its image).
3. $f(a^n) = (f(a))^n$ for all $a \in G_1$ and $n \in \mathbb{Z}$.

Proof

1. The image $f(e_1)$ defines an element in G_2 that satisfies the following equation

$$e_2 = f(e_1)^{-1} \cdot f(e_1) = f(e_1)^{-1} \cdot f(e_1 * e_1) = f(e_1)^{-1} \cdot f(e_1) \cdot f(e_1) = f(e_1).$$

2. For all $a \in G_1$,

$$f(a) \cdot f(a^{-1}) = f(a * a^{-1}) = f(e_1) = e_2,$$
$$f(a^{-1}) \cdot f(a) = f(a^{-1} * a) = f(e_1) = e_2.$$

Thus, $f(a^{-1})$ is the inverse of $f(a)$.

3. If n is an integer such that $n \geq 0$, we show the result by induction on n as follows:

For $n = 0$,

$f(a^n) = f(a^0) = f(e_1) = e_2 = f(a)^0 = f(a)^n$ for all $a \in G_1$. ■

Assume that the statement is true for n, i.e., $f(a^n) = f(a)^n$ for all $a \in G_1$.

For $n + 1$, using the hypothesis, one obtains.

$f(a^{n+1}) = f(a^n * a) = f(a^n) \cdot f(a) = f(a)^n \cdot f(a) = f(a)^{n+1}$ for all $a \in G_1$.

Hence, by induction, the statement is true for all integers $n \geq 0$. For the case in which $n < 0$, set $n = -k$ where $k > 0$. This yields the following equalities

$f(a^n) = f\left(\left(a^k\right)^{-1}\right) = f\left(a^k\right)^{-1} \underset{k \geq 0}{=} \left(f(a)^k\right)^{-1} = f(a)^n$ for all $a \in G_1$.

Proposition 8.1.5 *Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and $G_1 = \langle S \rangle$ for some $S \subseteq G_1$. Let $f : G_1 \to G_2$ be a group homomorphism. The map f is determined by its values on the generating set S.*

Proof Let $a \in G_1$ be an arbitrary element. According to Proposition 7.3.6, there exists $n \in \mathbb{N}$, $r_i \in \mathbb{Z}$, and $a_i \in S$, $1 \leq i \leq n$ such that $a = a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}$. As f is a homomorphism,

$$f(a) = f\left(a_1^{r_1} * a_2^{r_2} * \cdots * a_n^{r_n}\right) = f(a_1)^{r_1} \cdot f(a_2)^{r_2} \cdots f(a_n)^{r_n}.$$

Therefore, $f(a)$ is totally determined by its values on the elements of S. ■

Example 8.1.6 Let $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \cdot)$ be a homomorphism that takes $1 \mapsto 3$. The map f takes any $a \in \mathbb{Z}$ to 3^a. To show this, let $a \in \mathbb{Z}$.

- If $a \geq 0$, and since f is a homomorphism,

$$f(a) = f(\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}}) = \underbrace{f(1) \cdot f(1) \cdots f(1)}_{a \text{ times}} = \underbrace{3 \cdot 3 \cdots 3}_{a \text{ times}} = 3^a.$$

- If $a < 0$, then

$$f(a) = f(\underbrace{-1 + (-1) + \cdots + (-1)}_{-a \text{ times}}) = \underbrace{f(-1) \cdot f(-1) \cdots f(-1)}_{-a \text{ times}}$$

$$= \underbrace{f(1)^{-1} \cdot f(1)^{-1} \cdots f(1)^{-1}}_{-a \text{ times}} = \underbrace{3^{-1} \cdot 3^{-1} \cdots 3^{-1}}_{-a \text{ times}} = 3^a.$$

Using Proposition 8.1.5, to show that two homomorphisms are equal, it is enough to check their values on a generating set, as shown in the following corollary.

Corollary 8.1.7 *Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, $G_1 = \langle S \rangle$ for some $S \subseteq G_1$, and $f, g : G_1 \to G_2$ be group homomorphisms. The maps f and g are equal on G_1 if and only if $f(a) = g(a)$ for all $a \in S$.*

The next proposition examines the image and inverse image of subgroups under a group homomorphism.

Proposition 8.1.8 *Let $(G_1, *)$, $(G_2, \cdot)$ be groups and H, K be subgroups of G_1, G_2, respectively. If $f : G_1 \to G_2$ is a group homomorphism, then*

1. $f(H)$ is a subgroup of G_2.
2. $f^{-1}(K)$ is a subgroup of G_1.
3. If K is a normal subgroup of G_2, then $f^{-1}(K)$ is a normal subgroup of G_1.

4. If H is a normal subgroup of G_1 and f is surjective, then $f(H)$ is a normal subgroup of G_2.

Proof

1. According to Proposition 8.1.4, $e_2 = f(e_1) \in f(H)$, which implies that $f(H)$ is a nonempty subset of G_2. Let $b_1, b_2 \in f(H)$. According to the definition of $f(H) = \{f(a) : a \in H\}$, there exist $a_1, a_2 \in H$ such that

$$b_1 = f(a_1), \qquad b_2 = f(a_2).$$

As H is a subgroup, $a_1 * a_2^{-1} \in H$. Hence,
$b_1 \cdot b_2^{-1} = f(a_1) \cdot (f(a_2))^{-1} = f\big(a_1 * a_2^{-1}\big) \in f(H)$.
The result follows by Proposition 7.1.4.

2. The identity $e_2 \in K$, then $e_1 \in f^{-1}(e_2) \subseteq f^{-1}(K)$, so $f^{-1}(K)$ is a nonempty subset of G_1. For $a_1, a_2 \in f^{-1}(K)$, the images $f(a_1)$, $f(a_2)$ belong to K. Hence,

$$f\big(a_1 * a_2^{-1}\big) = f(a_1) \cdot f\big(a_2^{-1}\big) = f(a_1) \cdot (f(a_2))^{-1} \in K$$

i.e., $a_1 \cdot a_2^{-1} \in f^{-1}(K)$. By Proposition 7.1.4, $f^{-1}(K)$ is a subgroup of G_1.

3. Assume that K is a normal subgroup of G_2. By (2), $f^{-1}(K)$ is subgroup of G_1.

For all $a \in G_1$ and all $h \in f^{-1}(K)$,

$$f\big(a * h * a^{-1}\big) = f(a) \cdot f(h) \cdot f\big(a^{-1}\big) = f(a) \cdot f(h) \cdot f(a)^{-1}.$$

As $f(h) \in K$, $f(a) \in G_2$, and K is a normal subgroup, by Proposition 7.5.2,

$$f\big(a * h * a^{-1}\big) \in K.$$

i.e.,

$$a * h * a^{-1} \in f^{-1}(K)$$

for all $a \in G_1$, and $h \in f^{-1}(K)$. By Proposition 7.5.2, $f^{-1}(K)$ is a normal subgroup of G_1.

4. According to (1), $f(H)$ is a subgroup of G_2. We must show that $f(H)$ is normal. Let $f(h) \in f(H)$, and $b \in G_2$ for arbitrary elements h and b. As f is surjective, there exists $a \in G_1$ such that $b = f(a)$. Therefore,

$$b \cdot f(h) \cdot b^{-1} = f(a) \cdot f(h) \cdot (f(a))^{-1} = f(a) \cdot f(h) \cdot f\big(a^{-1}\big) = f\big(a * h * a^{-1}\big).$$

Since H is a normal subgroup of G_1, then $a * h * a^{-1} \in H$, which implies that $b \cdot f(h) \cdot b^{-1} = f\big(a * h * a^{-1}\big) \in f(H)$.

By Proposition 7.5.2, $f(H)$ is a normal subgroup of G_2. ■

The following example shows that the requirement in Proposition 8.1.8 (4), for f to be a surjective map, cannot be omitted.

Example 8.1.9 Consider the symmetric groups $\mathfrak{S}_2 = \big\{e_{\mathfrak{S}_2}, (12)\big\}$ and $\mathfrak{S}_3$. Define $f : \mathfrak{S}_2 \to \mathfrak{S}_3$ such that $f\big(e_{\mathfrak{S}_2}\big) = e_{\mathfrak{S}_3}$ and $f((12)) = (12) \in \mathfrak{S}_3$. Let $H = \mathfrak{S}_2$, it is a normal subgroup of $\mathfrak{S}_2$. The image of H under f is $f(H) = \big\{e_{\mathfrak{S}_3}, (12)\big\}$. However,

$$(13)f(H) = \{(13), (123)\} \neq \{(13), (132)\} = f(H)(13)$$

i.e., $f(H)$ is not a normal subgroup of $\mathfrak{S}_3$.

8.2 The Kernel and Image of Homomorphism

Let G_1, G_2 be two groups. With any homomorphism $f : G_1 \to G_2$ we associate two special subgroups of G_1 and G_2. These subgroups are built using the group G_1 and the identity element of G_2. Namely, they are $f(G_1)$ and $f^{-1}(\{e_2\})$, respectively. The importance of these subgroups is due to the information that they provide about the homomorphism. These subgroups are formally defined as follows.

Definition 8.2.1 Let G_1, G_2 be groups and $f : G_1 \to G_2$ be group homomorphism. The image of f is defined to be the whole range of the map f and denoted by $Im(f)$. The preimage of $\{e_2\}$ under the map f, where e_2 is the identity element of G_2, is called the kernel of f and denoted by $\ker(f)$. i.e.,

$$\begin{aligned} Im(f) &= f(G_1) = \{f(a) : a \in G_1\} \\ \ker(f) &= f^{-1}(\{e_2\}) = \{a \in G_1 : f(a) = e_2\}. \end{aligned}$$

Recall that $\{e_2\}$ is a normal subgroup of G_2. The following result is a corollary of Proposition 8.1.8.

Corollary 8.2.2 *Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group homomorphism. The image of f is a subgroup of G_2. The kernel of f is a normal subgroup of G_1, i.e.,*

$$Im(f) < G_2 \ \wedge\ \ker(f) \trianglelefteq G_1.$$

The subgroups defined above allow to "reconstruct" the homomorphism f. Observe that they provide an easy method to determine the injectivity and surjectivity of the map f.

Proposition 8.2.3 *Let $(G_1, *)$, $(G_2, \cdot)$ be groups. If $f : G_1 \to G_2$ is a group homomorphism, then*

1. *f is an epimorphism if and only if $Im(f) = G_2$.*
2. *f is a monomorphism if and only if $\ker(f) = \{e_1\}$.*

Proof The first statement follows by the definition of surjective maps, as the map f is onto if and only if $f(G_1) = G_2$. To show the second statement, assume that f is a one to one function. For each a in G_1,

$$a \in \ker(f) \Rightarrow f(a) = e_2 = f(e_1) \underset{f \text{ is one to one}}{\Rightarrow} a = e_1.$$

In the other direction, if $\ker(f) = \{e_1\}$, then

$$f(a) = f(b) \Rightarrow f(a) \cdot (f(b))^{-1} = e_2 \Rightarrow f\left(a * b^{-1}\right) = e_2 \Rightarrow a * b^{-1} \in \ker(f)$$

Hence, $a * b^{-1} = e_1$ and $a = b$. Therefore, f is one to one. ■

Next, we list several examples for computing the kernel and image of several homomorphisms.

Example 8.2.4

1. Consider the additive group $(\mathbb{Z}, +)$. Let $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ be the homomorphism defined in Example 8.1.3 (3), i.e., $f(a) = 3a$ for all $a \in \mathbb{Z}$. The kernel and image of f are

$$\ker(f) = \{0\} \text{ and } Im(f) = 3\mathbb{Z}.$$

Therefore, f is a monomorphism, and it is not surjective.

2. Consider the additive groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, \oplus_n)$. Let f be the homomorphism defined in Example 8.1.3 (5). i.e.,

$$f : \mathbb{Z} \to \mathbb{Z}_n, \text{ where } a \mapsto [a]$$

for all $a \in \mathbb{Z}$, where $[a]$ denotes the equivalence class of a in $\mathbb{Z}_n$. The map f is an epimorphism as

$$Im(f) = \{f(a) : a \in \mathbb{Z}\} = \{[a] : a \in \mathbb{Z}\} = \mathbb{Z}_n.$$

However, the map f is not a monomorphism as

$$\ker(f) = \{a \in \mathbb{Z} : f(a) = [0]\} = \{a \in \mathbb{Z} : [a] = [0]\} = \{a \in \mathbb{Z} : n|a\} = n\mathbb{Z}.$$

3. Consider the additive groups $(\mathbb{Z}_6, \oplus_6)$ and $(\mathbb{Z}_9, \oplus_9)$. Define

$$\begin{aligned} f : (\mathbb{Z}_6, \oplus_6) &\to (\mathbb{Z}_9, \oplus_9) \\ [a]_6 &\mapsto [3a]_9. \end{aligned}$$

Since $9|(3 \cdot 6)$, by the result in Example 3.2.4, f is a well-defined map. This map is a homomorphism with $\ker(f) = \{[0]_6, [3]_6\}$, $Im(f) = \{[0]_9, [3]_9, [6]_9\}$ (Check!).

By Proposition 8.2.3, the map f is neither surjective nor injective.

4. Consider the groups $(\mathbb{Z}_{12}, \oplus_{12})$ and $(\mathbb{Z}_{30}, \oplus_{30})$. Let f be the homomorphism defined in Example 8.1.3 (6), i.e.,

$$\begin{aligned} f : \mathbb{Z}_{12} &\to \mathbb{Z}_{30} \\ [x]_{12} &\mapsto [5x]_{30} \end{aligned}$$

where $[x]_k$ denotes the equivalence class of x in $\mathbb{Z}_k$. The map f is a well-defined homomorphism (Check!). The kernel of f and its image are

$$\begin{aligned} \ker(f) &= \{[x]_{12} \in \mathbb{Z}_{12} : f([x]_{12}) = [0]_{30}\} = \{[x]_{12} \in \mathbb{Z}_{12} : [5x]_{30} = [0]_{30}\} \\ &= \{[x]_{12} \in \mathbb{Z}_{12} : 30|5x\} = \{[0]_{12}, [6]_{12}\}. \end{aligned}$$

$$\begin{aligned} Im(f) &= \{f([x]_{12}) \in \mathbb{Z}_{30} : [x]_{12} \in \mathbb{Z}_{12}\} = \{[5x]_{30} : [x]_{12} \in \mathbb{Z}_{12}\} \\ &= \{[0]_{30}, [5]_{30}, [10]_{30}, [15]_{30}, [20]_{30}, [25]_{30}\}. \end{aligned}$$

According to Proposition 8.2.3, the map f is neither surjective nor injective. Table 8.1 is Cayley's table of the subgroup $(f(\mathbb{Z}_{12}), \oplus_{30})$.

Note that no isomorphism exists between $(\mathbb{Z}_m, \oplus_m)$ and $(\mathbb{Z}_n, \oplus_n)$ for different m and n, as the orders of both groups are different.

5. Consider the additive group $(\mathbb{Z}_2, \oplus_2)$ and the multiplicative group $(\{-1, 1\}, \cdot)$. Clearly, the map $f : \mathbb{Z}_2 \to \{-1, 1\}$ defined as

Table 8.1 Cayley's tables of $(f(\mathbb{Z}_{12}), \oplus_{30})$

$\oplus_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$
$[0]_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$
$[5]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$	$[0]_{30}$
$[10]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$	$[0]_{30}$	$[5]_{30}$
$15]_{30}$	$15]_{30}$	$[20]_{30}$	$[25]_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$
$[20]_{30}$	$[20]_{30}$	$[25]_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$
$[25]_{30}$	$[25]_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$

$$f([x]) = \begin{cases} 1 & [x] = [0] \\ -1 & [x] = [1] \end{cases}$$

is an isomorphism.

6. Consider the two groups $(\mathbb{Z}_4, \oplus_4)$ and $(\mathrm{Inv}(\mathbb{Z}_5), \otimes_5)$. Note that

$$\mathrm{Inv}(\mathbb{Z}_5) = \{[1]_5, [2]_5, [3]_5, [4]_5\} = \langle [3]_5 \rangle \text{ and } 3^4 \cong 1 \mod 5.$$

Define

$$f : (\mathbb{Z}_4, \oplus_4) \to (\mathrm{Inv}(\mathbb{Z}_5), \otimes_5) \text{ by } f([x]_4) = \left[3^x\right]_5.$$

The relation f is a well-defined map as

$$\begin{aligned} [x]_4 = [y]_4 &\Rightarrow x - y = 4q \quad \text{for some } q \text{ in } \mathbb{Z} \\ &\Rightarrow 3^x = 3^y 3^{4q} \Rightarrow 3^x \cong 3^y \mod 5 \Rightarrow \left[3^x\right]_5 = \left[3^y\right]_5. \end{aligned}$$

This map is a homomorphism as

$$f\big([x]_4 \oplus_4 [y]_4\big) = \left[3^{x+y}\right]_5 = \left[3^x 3^y\right]_5 = \left[3^x\right]_5 \otimes_5 \left[3^y\right]_5 = f([x]_4) \otimes_5 f\big([y]_4\big).$$

To show that f is bijective, it is enough to show its injectivity (the two groups are finite with the same cardinality). The map f is injective as

$$\begin{aligned} \ker(f) &= \{[x]_4 \in \mathbb{Z}_4 : f\,([x]_4) = [1]_5\} = \left\{[x]_4 \in \mathbb{Z}_4 : \left[3^x\right]_5 = [1]_5\right\} \\ &= \left\{[x]_4 \in \mathbb{Z}_4 : 3^x \cong 1 \mod 5\right\}. \end{aligned}$$

The quotient-remainder theorem can be applied to x and 4 to obtain that there exist $q, r \in \mathbb{Z}$ such that

$$x = 4q + r \quad \text{and} \quad 0 \leq r < 4.$$

- If $r = 0$, then $3^x = 3^{4q} \cong 1^q = 1 \mod 5$, and thus, $[x]_4 \in \ker(f)$.
- If $r = 1$, then $3^x = 3^{4q+1} \cong 3 \ncong 1 \mod 5$, and thus, $[x]_4 \notin \ker(f)$.
- Similarly, for the cases $r = 2, r = 3$, $3^x \ncong 1 \mod 5$ and $[x]_4 \notin \ker(f)$.

Therefore, only the case where $x = 4q$, we have $[x]_4 \in \ker(f)$, i.e.,

$$\ker(f) = \left\{[4q]_4, q \in \mathbb{Z}\right\} = \{[0]_4\}.$$

The reader should check that $g : (\mathbb{Z}_4, \oplus) \to (\mathrm{Inv}(\mathbb{Z}_5), \otimes_5)$, where $g([x]_4) = [4^x]_5$ is a well-defined homomorphism, that is not injective (Check!).

7. For any prime p and any generator $[a]$ of $\mathrm{Inv}\big(\mathbb{Z}_p\big) = \mathbb{Z}_p^*$, the map

$g : \big(\mathbb{Z}_{p-1}, \oplus_{p-1}\big) \to \big(\mathbb{Z}_p^*, \otimes_p\big)$, where $g\big([x]_{p-1}\big) = [a^x]_p$ is an isomorphism (Exercise 8.28). Note that since $\left|\mathbb{Z}_p^*\right| = p - 1$, then $a^{p-1} \cong 1 \bmod p$.

Example 8.2.5

1. Consider the group homomorphism $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ defined by $f(x) = e^x$ for all $x \in \mathbb{R}$.

$\ker(f) = \{x \in \mathbb{R} : e^x = 1\} = \{0\}$ and $\mathrm{Im}(f) = \{e^x : x \in \mathbb{R}\} = \mathbb{R}^+$.
The map f is an example of a monomorphism that is not an epimorphism. Compare this monomorphism with the isomorphism described in Example 8.1.3 (7).

2. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{C}^*, \cdot)$. Let $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ defined by $f(x) = e^{ix}$ for all $x \in \mathbb{R}$. The map f is a homomorphism as

$$f(x + y) = e^{i(x+y)} = e^{ix}e^{iy} = f(x)f(y).$$

The kernel of f is

$$\begin{aligned}\ker(f) &= \{x \in \mathbb{R} : f(x) = 1\} = \left\{x \in \mathbb{R} : e^{ix} = 1\right\}\\ &= \{x \in \mathbb{R} : \cos x + i \sin x = 1\} = \{x \in \mathbb{R} : \cos x = 1 \ \wedge \ \sin x = 0\}\\ &= \{x \in \mathbb{R} : x = 2\pi k, k \in \mathbb{Z}\} = \{2\pi k, k \in \mathbb{Z}\} = 2\pi\mathbb{Z},\end{aligned}$$

and

$$\begin{aligned}\mathrm{Im}(f) &= \{f(x) \in \mathbb{C} : x \in \mathbb{R}\} = \left\{e^{ix} \in \mathbb{C} : x \in \mathbb{R}\right\}\\ &= \left\{z \in \mathbb{C} : \ z = e^{ix}, \ x \in \mathbb{R}\right\} = \{z \in \mathbb{C} : |z| = 1\} \text{ (the unit circle in } \mathbb{C}).\end{aligned}$$

Therefore, f is an not isomorphism.

3. Consider the multiplicative group $(\mathbb{R}^*, \cdot)$. Define $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ by

$$f(x) = |x|.$$

The map f is a homomorphism with $\ker(f) = \{1, -1\}$ and $\mathrm{Im}(f) = (0, \infty)$. Clearly, f is not an isomorphism.

4. Consider the groups $(GL_n(\mathbb{R}), \ \cdot)$ and $(\mathbb{R}^*, \ \cdot)$. Let $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be the map defined by taking any matrix A to its determinant $\det(A)$ (Definition 1.6.20). The map det is a homomorphism as

$$\det(AB) = \det(A) \cdot \det(B).$$

This map is surjective. For if $\lambda \in \mathbb{R}^* = \mathbb{R}\backslash\{0\}$, let A_λ be the diagonal matrix in $GL_n(\mathbb{R})$, whose first element $a_{11} = \lambda$ and all other diagonal elements are 1. The matrix A_λ is an invertible matrix with $\det(A_\lambda) = \lambda$. The map det has a nontrivial kernel since

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R}).$$

Therefore, the homomorphism $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is not an isomorphism.

The next proposition demonstrates the strong relation between normal subgroups and homomorphisms. The proposition explains that not only is the kernel of a homomorphism a normal subgroup of the domain group G, but any normal subgroup of G is a kernel for some homomorphism. Moreover, it shows that a homomorphism provides a new method to obtain normal subgroups.

Proposition 8.2.6 *Let $(G, *)$ be a group. Any normal subgroup of G is a kernel of a homomorphism on G . i.e.,*

$$H \trianglelefteq G \Longleftrightarrow \exists \text{ a homomorphism } f : G \to G/H \ni H = \ker(f).$$

Proof Assume that H is a normal subgroup of G and define $f : G \to G/H$ to be the map that takes a to aH for all $a \in G$. The map f is a homomorphism as

$$f(a * b) = (a * b)H = aH \cdot_{G/H} bH = f(a) \cdot_{G/H} f(b) \quad \text{for all } a, b \in G$$

and

$$\ker(f) = \{a \in G : f(a) = H\} = \{a \in G : aH = H\} = \{a \in G : a \in H\} = H.$$

The equivalence statement follows since the kernel of any homomorphism of G is normal subgroup of G (Corollary 8.2.2). ■

Example 8.2.7

1. Let $n \in \mathbb{N}$. Consider the symmetric group $\mathfrak{S}_n$ and its normal subgroup $\mathcal{A}_n$ (Corollary 7.5.7). The map

$$\begin{aligned} f : \mathfrak{S}_n &\to \mathfrak{S}_n/\mathcal{A}_n \\ \sigma &\mapsto \sigma\mathcal{A}_n \end{aligned}$$

is a homomorphism such that $\mathrm{Ker}(f) = \mathcal{A}_n$.

2. Consider the group $(\mathbb{Z}_{12}, \oplus_{12})$ and its normal subgroup $K = \langle[6]\rangle = \{[0], [6]\}$. To find the homomorphism f such that $\ker(f) = K$, one constructs the quotient group $\mathbb{Z}_{12}/K$, where the operation $\mathbb{Z}_{12}/K$ is defined by

$$([a]K) +_{\mathbb{Z}_{12}/K} ([b]K) = [a+b]K.$$

Let $f : \mathbb{Z}_{12} \to \mathbb{Z}_{12}/K$ be defined by taking $[a]$ to $[a]K$, then f is a well-defined homomorphism with $\ker(f) = K$.

8.3 Group Isomorphisms and Cayley's Theorem

Group isomorphisms (Definition 8.1.1) are maps that preserve all group structures. This section is devoted to study isomorphisms.

Definition 8.3.1 Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups. The groups G_1 and G_2 are called isomorphic if there exists an isomorphism $f : G_1 \to G_2$.

As any bijective map f has a bijective inverse, any isomorphism is invertible. The following proposition shows that the inverse map of an isomorphism is also an isomorphism.

Proposition 8.3.2 *Let $(G_1, *)$ and $(G_2, \cdot)$ be groups. If $f : G_1 \to G_2$ is a group isomorphism, then $f^{-1} : G_2 \to G_1$ is an isomorphism.*

Proof The map f^{-1} is bijective (Exercise 1.21). To show that f^{-1} is a homomorphism, let $b_1, b_2 \in G_2$, $a_1 = f^{-1}(b_1)$, and $a_2 = f^{-1}(b_2)$. Since f is bijective homomorphism,

$$f^{-1}(b_1) * f^{-1}(b_2) = a_1 * a_2 = f^{-1}(f(a_1 * a_2)) = f^{-1}(f(a_1) \cdot f(a_2)) = f^{-1}(b_1 \cdot b_2).$$

■

On the class of all groups, define the following relation.

$G_1 \cong G_2$ if and only if there exists an isomorphism $f : G_1 \to G_2$.

This relation is an equivalence relation (Exercise 8.5). The groups in Examples 8.2.4 (5–7) and Example 8.1.3 (7) are examples of isomorphic groups. More examples are presented in the remainder of this section. ■

Example 8.3.3

1. Let $m \in \mathbb{Z}$ such that $m \neq 0$. The map GG in Example 8.1.3 (4) is an isomorphism, which implies that the additive groups $\mathbb{Z}$ and $m\mathbb{Z}$ are isomorphic, i.e.,

$$\mathbb{Z} \cong m\mathbb{Z} \text{ for all } m \neq 0.$$

In this example, a proper subgroup is isomorphic to the whole group. According to the transitivity of the isomorphic relation (Exercise 8.5), $m\mathbb{Z} \cong n\mathbb{Z}$, for all nonzero integers m, n.

2. The groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$ are isomorphic for each $n \in \mathbb{N}$. The isomorphism is given by the function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ that takes $a + n\mathbb{Z}$ into $[a]$, where $0 \leq a \leq n - 1$. It is a well-defined bijection map such that

$$f\big((a + n\mathbb{Z}) +_{\mathbb{Z}/n\mathbb{Z}} (b + n\mathbb{Z})\big) = f(a + n\mathbb{Z}) + f(b + n\mathbb{Z}).$$

Note that $\mathbb{Z}/n\mathbb{Z}$ is a finite group that has n elements (Example 7.7.9 (1)).

3. For each $n \in \mathbb{N}$, the group $\mathfrak{S}_{n-1}$ is isomorphic to a subgroup of $\mathfrak{S}_n$. Specifically, $\mathfrak{S}_{n-1}$ is isomorphic to the subgroup of $\mathfrak{S}_n$ that fixes one element of the set $\{1, 2, \ldots, n\}$. The inclusion map provides the required monomorphism.

Example 8.3.4 Let $n \in \mathbb{N}$ such that $n \geq 3$. Let $\langle r, s\rangle$ be the subgroup of $O(2)$ generated by.

$$r = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \text{ and } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercise 7.5 shows that the subgroup $\langle r, s\rangle$ is finite and can be listed as follows:

$$\langle r, s\rangle = \left\{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\right\}.$$

The dihedral group in Example 7.3.11 satisfies that

$$D_{2n} = \left\langle R_{\frac{2\pi}{n}}, l_o\right\rangle = \left\{R_0, R_{\frac{2\pi}{n}}, R_{\frac{4\pi}{n}}, \ldots, R_{\frac{2(n-1)\pi}{n}}, l_o, l_{\frac{\pi}{n}}, \ldots, l_{\frac{(n-1)\pi}{n}}\right\}.$$

Define the map

$$\begin{aligned} f : D_{2n} &\to \langle r, s\rangle \\ (R_{\frac{2\pi}{n}})^k l_o^t &\mapsto r^k \mathrm{s}^t \end{aligned}$$

for each $0 \leq k \leq n - 1$ and for each $0 \leq t \leq 1$. The map f is an isomorphism (Exercise 8.28). Using this isomorphism, we identify the dihedral group with the subgroup $\langle r, s\rangle$.

Corollary 8.3.5 *Let $n \in \mathbb{N}$ where $n \geq 3$.*

$$D_{2n} = \langle r, s\rangle = \left\{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\right\}$$

where r, s satisfy the relations

$$\operatorname{ord}(r) = n, \operatorname{ord}(s) = 2, \quad \text{and} \quad (rs)^2 = e.$$

For example, the group D_{12} of all symmetries of the regular 6-polygon, consists of the 12 elements

$$D_{12} = \left\{e, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, r^5s\right\}$$

that are controlled by the relations $r^6 = s^2 = e$, $(sr)^2 = e$. It is left to the reader to write Cayley's table for the group $(D_{12}, \cdot)$. The reader may need to do the following computations

$$r^4r^5 = r^9 = r^3, \quad r^5r^3s = r^8s = r^2s,$$
$$r^3sr^5 = r^3r^{6-5}s = r^4s, \quad r^3sr^2s = r^3r^{6-2}s^2 = r.$$

Example 8.3.6 Let $n \in \mathbb{N}$ such that $n \geq 3$. Consider the two groups: $K = \langle \alpha, \tau\rangle$ (Exercise 7.6) and the subgroup $\langle r, s\rangle$ of $O(2)$ (Example 8.3.4). Define the map.

$$\begin{aligned} f : \langle r, s\rangle &\to K \\ r^ks^t &\mapsto \alpha^k\tau^t \end{aligned}$$

for all $0 \leq k \leq n-1$ and $t \in \{0, 1\}$

Clearly, that f is a bijective map (Check!). To show that f is a homomorphism, let $x, y \in \langle r, s\rangle$ be an arbitrary element. i.e., $x = r^{k_1}s^{t_1}$, $y = r^{k_2}s^{t_2}$ for some k_1, k_2, t_1, t_2 where $0 \leq k_1, k_2 \leq n-1$ and $t_1, t_2 \in \{0, 1\}$.

$$\begin{aligned} f(x \cdot y) &= f\left(r^{k_1}s^{t_1}r^{k_2}s^{t_2}\right) = f\left(r^{k_1}r^{-k_2}s^{t_1}s^{t_2}\right) = f\left(r^{k_1-k_2}s^{t_1+t_2}\right) \\ &= \alpha^{k_1-k_2}\tau^{t_1+t_2} = \alpha^{k_1}\alpha^{-k_2}\tau^{t_1}\tau^{t_2} = \alpha^{k_1}\tau^{t_1}\alpha^{k_2}\tau^{t_2} \\ &= f\left(r^{k_1}s^{t_1}\right) \circ f\left(r^{k_2}s^{t_2}\right) = f(x) \circ f(y). \end{aligned}$$

Therefore, $\langle r, s\rangle$ and K are isomorphic groups. By the transitivity of the isomorphic relation (Exercise 8.5), all three groups in Examples 8.3.4 and 8.3.6 are isomorphic and can be identified.

As we mentioned in the beginning of this section, an isomorphism of two groups preserves all group structures of the domain and codomain groups, such as the commutativity, cardinality of the groups, orders of the elements, and normality of subgroups. The commutativity is preserved by any homomorphism. It is left to the reader to check that if G_1 is abelian and $f : G_1 \to G_2$ is a homomorphism, then $f(G_1)$ is abelian. To preserve the normality of subgroups, at least an epimorphism is needed (Proposition 8.1.8). Therefore, if $f : G_1 \to G_2$ is an isomorphism, then for any normal subgroup H of G_1, the image $f(H)$ will be a normal subgroup of G_2. The cardinality of the two groups is preserved as any isomorphism must be a bijective map. For the orders of group elements, we have the following proposition.

Proposition 8.3.7 *Let $(G_1, *)$ and $(G_2, \cdot)$ be groups and $f : G_1 \to G_2$ be a group isomorphism. For any $a \in G_1$, $\operatorname{ord}(f(a)) = \operatorname{ord}(a)$.*

Proof Assume that $a \in G_1$ is an arbitrary element. If a has infinite order, then the order of $f(a)$ is infinite (exercise). Let $\operatorname{ord}(a) = k$, Proposition 8.1.4 implies that $(f(a))^k = e_2$. We show that k is the smallest positive integer such that $(f(a))^k = e_2$. Let r be any positive integer such that $(f(a))^r = e_2$. Since f is a homomorphism,

$$f\big(a^r\big) = e_2.$$

As f is a bijective map, f^{-1} is bijective (Theorem 1.5.20), and

$$a^r = f^{-1}\big(f\big(a^r\big)\big) = f^{-1}(e_2) = e_1.$$

As $k = \operatorname{ord}(a)$, then $k \leq r$. ■

The reader should note that the previous corollary is not true if one replaces the word isomorphism with homomorphism. For example, the map $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f(n) = 0$ for all $n \in \mathbb{Z}$ is a homomorphism (Example 8.1.3 (1)). For any $n \neq 0$, $\operatorname{ord}(n)$ is not finite, but $\operatorname{ord}(f(n)) = \operatorname{ord}(0) = 1$.

Corollary 8.3.8 *Let $n \in \mathbb{N}$. Any two isomorphic groups have the same number of elements whose order is n.*

Let p be a prime number. The following proposition states that all groups with order p are isomorphic. The reader must be aware that this statement is not true for any number n. For example, the groups $(\mathbb{Z}_6, \oplus_6)$ and $(\mathfrak{S}_3, \circ)$ both have 6 elements but are not isomorphic ($(\mathbb{Z}_6, \oplus_6)$ is an abelian group, whereas $(\mathfrak{S}_3, \circ)$ is not). The groups $(\mathbb{Z}_4, \oplus_4)$ and $(\{[1], [3], [5], [7]\}, \otimes_8)$ are examples of abelian groups that have the same number of elements but are not isomorphic. There are three elements of order 2 in $(\{[1], [3], [5], [7]\}, \otimes_8)$, while $(\mathbb{Z}_4, \oplus_4)$ has only one element of order 2.

Proposition 8.3.9 *Any group whose order is the prime number p is isomorphic to $\mathbb{Z}_p$.*

Proof Let G be a group such that $|G| = p$ for some prime p. As $p > 1$, there exists an element a in G such that $a \neq e$. According to Lagrange's theorem (Theorem 7.4.17), the order of the subgroup $\langle a \rangle$ divides p. Therefore, $\text{ord}(\langle a \rangle)$ is either 1 or p. As $a \neq e$, there exists only one possibility for $\text{ord}(\langle a \rangle)$, which is p. Hence, $\langle a \rangle$ is a subgroup of G that has the same order of G, i.e.,

$$G = \langle a \rangle = \left\{e, a, a^2, \ldots, a^{p-1}\right\}.$$

The map $f : \mathbb{Z}_p \to G$ that takes $[k]$ to a^k is the required isomorphism (Check!). ■

The next goal is to determine the conditions in which the additive groups $\mathbb{Z}_{mn}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ are isomorphic. We begin with the following lemma.

Lemma 8.3.10 *Let $n, m \in \mathbb{N}$. If* $\gcd(m, n) = 1$, *then the additive groups $\mathbb{Z}_{nm}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ are isomorphic.*

Proof Assume that $\gcd(m, n) = 1$, and define

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m \text{ such that } [x]_{mn} \mapsto ([x]_n, [x]_m)$$

where $[x]_k$ denotes the equivalence class of x in $\mathbb{Z}_k$. The map f is a well-defined, for if $[x]_{mn} = [y]_{mn}$, then mn divides $x - y$. Therefore, $m|(x - y)$ and $n|(x - y)$, which implies that $[x]_m = [y]_m$ and $[x]_n = [y]_n$. Consequently, $([x]_n, [x]_m) = \left([y]_n, [y]_m\right)$. To show that f is a homomorphism, let $[x]_{mn}, [y]_{mn}$ be any elements in $\mathbb{Z}_{mn}$. By the definition of f,

$$\begin{aligned} f\left([x]_{mn} \oplus_{mn} [y]_{mn}\right) &= f\left([x + y]_{mn}\right) = \left([x + y]_n, [x + y]_m\right) \\ &= \left([x]_n \oplus_n [y]_n, [x]_m \oplus_m [y]_m\right) = ([x]_n, [x]_m) + \left([y]_n, [y]_m\right) \\ &= f([x]_{mn}) + f\left([y]_{mn}\right). \end{aligned}$$

We still need to show that f is one to one and onto. As the domain and codomain are finite sets with same cardinalities, it suffices to show only one of these cases (Exercise 1.6). To show that f is injective, assume that $[x]_{mn}$ be an arbitrary element in $\ker(f)$. i.e., $f([x]_{mn}\big] = ([0]_n, [0]_m)$. By definition of relations mod n and mod m, we obtain that $n|x$ and $m|x$. Since $\gcd(m, n) = 1$, then $nm|x$, and thus, $[x]_{mn} = [0]_{mn}$. Therefore $\ker(f) = \{[0]_{mn}\}$ and f is injective. ■

Lemma 8.3.11 *For any $n, m \in \mathbb{N}$, if the additive groups $\mathbb{Z}_{nm}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ are isomorphic, then*

$$\gcd(m, n) = 1.$$

Proof If $\mathbb{Z}_{nm}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ are isomorphic groups, then there exists an isomorphism $f : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_{nm}$. Since $[1]_{nm} \in \mathbb{Z}_{nm}$ and f is onto, then there exists $\left([y]_n, [z]_m\right)$ in $\mathbb{Z}_n \times \mathbb{Z}_m$ such that

$$f\big([y]_n, [z]_m\big) = [1]_{nm}$$

Let $l = \mathrm{lcm}(m, n)$. Multiplying this equation by l, yields

$$l \cdot f\big([y]_n, [z]_m\big) = l \cdot [1]_{nm}$$

which implies

$$f\big([ly]_n, [lz]_m\big) = f\big(l \cdot [y]_n, l \cdot [z]_m\big) = [l]_{nm}$$

As l is a multiple of both n and m, then $[ly]_n = [0]_n$, $[lz]_m = [0]_m$. Therefore,

$$[0]_{nm} = f([0]_n, [0]_m) = f\big([ly]_n, [lz]_m\big) = [l]_{nm}$$

i.e., $[0]_{nm} = [l]_{nm}$ and $nm|l$, which implies that $mn \le l$. Since $l \le mn$, then $l = mn$, which gives

$$\gcd(m, n) = \frac{mn}{\mathrm{lcm}(m, n)} = 1$$

■

Corollary 8.3.12 *Let $n, m \in \mathbb{N}$ and consider the additive groups $\mathbb{Z}_m$, $\mathbb{Z}_n$ and $\mathbb{Z}_{mn}$. The groups $\mathbb{Z}_{mn}$ and $\mathbb{Z}_n \times \mathbb{Z}_m$ are isomorphic if and only if* $\gcd(m, n) = 1$.

According to the corollary above, even though the additive groups $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_8$ have the same number of elements, they are not isomorphic. For the same reason, the groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic. The following example shows that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the Klein group (Example 5.2.2), which implies that the Klein group is not isomorphic to $\mathbb{Z}_4$. In fact, each nonidentity element in the Klein group has order 2, a property that does not hold for $\mathbb{Z}_4$.

Example 8.3.13 Consider the Klein group $(V, *)$ and the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Define the map $f : V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ that takes

$$e \to (0, 0), a \to (0, 1), b \to (1, 0), \text{ and } c \to (1, 1).$$

Checking all the elements in V indicates that the map f is a homomorphism. Clearly, this map is bijective (by definition). Therefore, Klein group $(V, *)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. If Klein group $(V, *)$ is isomorphic to $\mathbb{Z}_4$, then by the transitivity of the isomorphism relation, we would have $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to $\mathbb{Z}_4$, which contradicts Corollary 8.3.12, as $\gcd(2, 2) = 2 \neq 1$.

Next, we state and present a proof for Cayley's theorem, one of the important theorems in group theory, named in honor of Arthur Cayley. The theorem states that every group is isomorphic to a subgroup of some symmetric group, rendering the study of symmetric groups a key to understanding the structure of any group. The theorem shows that any group G is isomorphic to $Lm(G) < \mathfrak{S}_G$, where $Lm(G)$ is the subgroup of all left multiplications on G (Proposition 7.1.14).

Theorem 8.3.14 (Cayley's theorem) *Any group G is isomorphic to a subgroup of its symmetric group $\mathfrak{S}_G$.*

Proof Define $\phi : G \to Lm(G)$ by $\phi(a) = f_a \ \ \forall\, a \in G$. Using Proposition 7.1.14, we obtain

$$\phi(a * b) = f_{a*b} = f_a \circ f_b = \phi(a) \circ \phi(b)$$

i.e., the map ϕ is a homomorphism. This map is injective as

$$\begin{aligned}\phi(a) = \phi(b) &\Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \forall\, x \in G\\ &\Rightarrow a * x = b * x \quad \forall\, x \in G\\ &\Rightarrow a = a * e = b * e = b \Rightarrow a = b.\end{aligned}$$

Finally, the map ϕ is surjective since for each $y \in Lm(G) = \{f_a : a \in G\}$, there exists $a \in G$ such that $\phi(a) = f_a = y$. ■

The following example explains the method used to obtain the subgroup of $\mathfrak{S}_G$ that is isomorphic to a given group G.

Example 8.3.15 Consider the group $(\text{Inv}(\mathbb{Z}_7), \otimes_7)$. According to Cayley's theorem, the group $\text{Inv}(\mathbb{Z}_7)$ is isomorphic to $\text{Lm}(\text{Inv}(\mathbb{Z}_7))$, where $\text{Lm}(\text{Inv}(\mathbb{Z}_7)) = \left\{f_{[1]}, f_{[2]}, f_{[3]}, f_{[4]}, f_{[5]}, f_{[6]}\right\}$. As

$$f_{[a]} : \text{Inv}(\mathbb{Z}_7) \to \text{Inv}(\mathbb{Z}_7)$$

$$[x] \mapsto [ax] \ \ \text{where}[x] \in \text{Inv}(\mathbb{Z}_7).$$

i.e.,

$$f_{[1]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [1] & [2] & [3] & [4] & [5] & [6] \end{pmatrix} = e$$

$$f_{[2]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [2] & [4] & [6] & [1] & [3] & [5] \end{pmatrix} = ([1][2][4])([3][6][5])$$

$$f_{[3]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [3] & [6] & [2] & [5] & [1] & [4] \end{pmatrix} = ([1][3][2][6][4][5])$$

$$f_{[4]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [4] & [1] & [5] & [2] & [6] & [3] \end{pmatrix} = ([1][4][2])([3][5][6])$$

$$f_{[5]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [5] & [3] & [1] & [6] & [4] & [2] \end{pmatrix} = ([1][5][4][6][2][3])$$

$$f_{[6]} = \begin{pmatrix} [1] & [2] & [3] & [4] & [5] & [6] \\ [6] & [5] & [4] & [3] & [2] & [1] \end{pmatrix} = ([1][6])([2][5])([3][4])$$

Therefore,

$$\begin{aligned}\mathrm{Inv}(\mathbb{Z}_7) \cong \{&e, ([1][3][2][6][4][5]), ([1][5][4][6][2][3]), ([1][2][4])([3][6][5]),\\ &([1][5][4][6][2][3]), ([1][6])([2][5])([3][4])\}.\end{aligned}$$

We end the section by studying isomorphisms on G (automorphisms). We shall prove that $\mathrm{Aut}(G)$, the set of all automorphisms on G, forms a group. Moreover, we provide an example of a normal subgroup of $\mathrm{Aut}(G)$.

Proposition 8.3.16 *Let $(G, *)$ be a group. The set $Aut(G)$ of all automorphisms on G forms a group under the composition of maps.*

Proof The composition of two automorphisms on G is an automorphism (Proposition 8.1.2). Therefore, the composition is a binary operation on $\mathrm{Aut}(G)$. The associativity of the composition on $Aut(G)$ follows from the associativity of the composition of maps. The identity map $\iota : G \to G$ defined by $\iota(x) = x \ \forall x \in G$ is an automorphism that serves as an identity element in $\mathrm{Aut}(G)$. Let f be an automorphism. According to Proposition 8.3.2, the inverse map f^{-1} is also an automorphism and satisfies $f \circ f^{-1} = f^{-1} \circ f = \iota$. Therefore, $\mathrm{Aut}(G)$ is a group. ■

An important example of automorphism is an inner automorphism defined in the following example.

Example 8.3.17 Let $(G, *)$ be a group. For $a \in G$, define the map.

$$\begin{aligned}\phi_a : G &\to G\\ x &\mapsto a * x * a^{-1}.\end{aligned}$$

The map ϕ_a is an automorphism. For if x, y are elements in G, then

$$\begin{aligned}\phi_a(x) * \phi_a(y) &= \left(a * x * a^{-1}\right) * \left(a * y * a^{-1}\right)\\ &= a * x * \left(a^{-1} * a\right) * y * a^{-1} = a * x * y * a^{-1}\\ &= \phi_a(x * y).\end{aligned}$$

Therefore, ϕ_a is a homomorphism. It is invertible as.

$$\phi_a(\phi_{a^{-1}}(x)) = \phi_{a^{-1}}(\phi_a(x)) = x \text{ for all } x \in G.$$

Hence, $\phi_{a^{-1}}\phi_a = \phi_a\phi_{a^{-1}} = \iota(G)$, which implies that ϕ_a is one to one and onto. Therefore, ϕ_a is an element of $\mathrm{Aut}(G)$. It is straightforward to show that for any$a, b \in G$, $\phi_a\phi_{\mathrm{b}} = \phi_{a*\mathrm{b}}$.

Definition 8.3.18 Let $(G, *)$ be a group, and $a \in G$. The map ϕ_a defined in the example above is called a conjugation by a or inner automorphism. The set of all inner automorphisms on G is denoted by $\mathrm{Inn}(G)$.

Proposition 8.3.19 *The set of all inner automorphisms on* $(G, *)$ *forms a normal subgroup of* $(Aut(G), \circ)$.

Proof According to the result of Example 8.3.17, $\mathrm{Inn}(G)$ is a subset of $\mathrm{Aut}(G)$. As ϕ_e (the identity map on G) is an inner automorphism, then $\mathrm{Inn}(G)$ is a nonempty set. It is a subgroup as

$$\phi_a(\phi_{\mathrm{b}})^{-1} = \phi_a\phi_{b^{-1}} = \phi_{a*b^{-1}} \in \mathrm{Inn}(G) \text{ for all } \phi_a, \phi_{b^{-1}} \in \mathrm{Inn}(G).$$

To show that $\mathrm{Inn}(G)$ is normal, let f be any automorphism on G and ϕ_a be an element in $\mathrm{Inn}(G)$ for some $a \in G$.

$$f\phi_a f^{-1}(x) = f\big(af^{-1}(x)a^{-1}\big) = f(a)xf(a)^{-1} \text{ for all } \quad x \in G.$$

Therefore, $f\phi_a f^{-1} = \phi_{f(a)} \in \mathrm{Inn}(G)$. ■

8.4 The Fundamental Theorems of Homomorphisms

There are three fundamental theorems that are related to homomorphisms. This section studies the three theorems and provide several examples. Recall the result of Corollary 8.2.2, in which for a group homomorphism $f : G_1 \to G_2$, the kernel of f is a normal subgroup of G_1. This result enables us to build a quotient group $G_1/\ker(f)$. This quotient group is isomorphic to the subgroup of all images of f.

Theorem 8.4.1 (First fundamental theorem of group homomorphisms) *Let* $(G_1, *)$ *and* $(G_2, \cdot)$ *be two groups. If* $f : G_1 \to G_2$ *is a group homomorphism, then*

$$G_1/\ker(f) \cong \mathrm{Im}(f).$$

Proof Since $\ker(f)$ is a normal subgroup of G_1, then by Proposition 7.7.3, $G_1/\ker(f)$ forms a group. Define $f^* : G_1/\ker(f) \to G_2$.

$$a\ \ker(f) \mapsto f(a) \quad \forall\, a \in G_1.$$

The map f^* is well-defined. For if $a_1\ker(f), a_2\ker(f)$ are arbitrary elements in $G_1/\ker(f)$ such that $a_1\ker(f) = a_2\ker(f)$, then by Proposition 7.4.7, $a_1 \in a_2\ker(f)$, i.e., $\exists\, k \in \ker(f) \ni a_1 = a_2 * k$. Therefore,

$$f(a_1) = f(a_2 * k) = f(a_2)\cdot f(k) = f(a_2)\cdot e_2 = f(a_2).$$

To show that f^* is a homomorphism, we assume that $a_1\ker(f),\ a_2\ker(f)$ are arbitrary elements in $G_1/\ker(f)$. Hence,

$$\begin{aligned} f^*\big((a_1\ker(f)) \cdot_{G_1/\ker(f)} (a_2\ker(f))\big) &= f^*((a_1 * a_2)\ker(f)) \\ &= f(a_1 * a_2) = f(a_1)\cdot f(a_2) \\ &= f^*(a_1\ker(f))\cdot f^*(a_2\ker(f)). \end{aligned}$$

Finally, $a\ker(f) \in \ker(f^*) \Longleftrightarrow f(a) = f^*(a\ker(f)) = e_2 \Longleftrightarrow a \in \ker(f) \Longleftrightarrow a\ker(f) = \ker(f)$ i.e., $\ker(f^*) = \{\ker(f)\}$ which is the identity element of $G_1/\ker(f)$. Therefore, by Proposition 8.2.3, the map f^* is one to one. Consequently,

$G_1/\ker(f) \cong f^*(G_1/\ker(f)) = f(G_1) = Im(f)$. ■

Note that in this proof, the original homomorphism f can be reconstructed as a composition of the homomorphism f^* and quotient map of G_1 into $G_1/\ker(f)$, i.e.,

$$f = f^* \circ \pi$$

where π is the map defined for any $a \in G_1$ by $\pi(a) = a\ \ker(f)$.

Example 8.4.2

1. Consider the group homomorphism $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ defined by $f(x) = e^{ix}$. In Example 8.2.5 (2), we showed that $\ker(f) = 2\pi\mathbb{Z}$ and $Im(f) = \{z \in \mathbb{C}^* : |z| = 1\}$. Applying the result of the first fundamental theorem, we obtain

$$\mathbb{R}/_{2\pi\mathbb{Z}} \cong \{z \in \mathbb{C} : |z| = 1\}$$

i.e., the unit circle is isomorphic to the quotient group $\mathbb{R}/_{2\pi\mathbb{Z}}$.

2. Consider the groups $(\mathbb{Z}_{12}, \oplus_{12})$ and $(\mathbb{Z}_{30}, \oplus_{30})$ and the homomorphism

$$f : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$$

$$[x]_{12} \mapsto [5x]_{30}$$

Table 8.2 Images of the map f

$[x]_{12}$	$[0]_{12}$	$[1]_{12}$	$[2]_{12}$	$[3]_{12}$	$[4]_{12}$	$[5]_{12}$	$[6]_{12}$	$[7]_{12}$	$[8]_{12}$	$[9]_{12}$	$[10]_{12}$	$[11]_{12}$
$f([x]_{12})$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$	$[0]_{30}$	$[5]_{30}$	$[10]_{30}$	$[15]_{30}$	$[20]_{30}$	$[25]_{30}$

where $[x]_k$ denotes the equivalence class of x in $\mathbb{Z}_k$. Table 8.2 contains the images of f

Using the table below, we obtain
$\ker(f) = \{[0]_{12}, [6]_{12}\}$ and $Im(f) = \{[0]_{30}, [5]_{30}, [10]_{30}, [15]_{30}, [20]_{30}, [25]_{30}\}$.
Therefore, $\mathbb{Z}_{12}/\ker(f)$ is equal to the set $\{[a]_{12}\ker(f) : [a]_{12} \in \mathbb{Z}_{12}\}$ which is

$$\{\{[0]_{12}, [6]_{12}\}, \{[1]_{12}, [7]_{12}\}, \{[2]_{12}, [8]_{12}\}, \{[3]_{12}, [9]_{12}\}, \{[4]_{12}, [10]_{12}\}, \{[5]_{12}, [11]_{12}\}\}.$$

Note that the map that takes
$\{[0]_{12}, [6]_{12}\} \mapsto [0]_{30}$, $\{[1]_{12}, [7]_{12}\} \mapsto [5]_{30}$, $\{[2]_{12}, [8]_{12}\} \mapsto [10]_{30}$,
$\{[3]_{12}, [9]_{12}\} \mapsto [15]_{30}$, $\{[4]_{12}, [10]_{12}\} \mapsto [20]_{30}$, $\{[5]_{12}, [11]_{12}\} \mapsto [25]_{30}$.
is the isomorphism f^* between the two groups $\mathbb{Z}_{12}/\ker(f)$ and $Im(f)$ defined in the proof of Theorem 8.4.1.

3. Although Exercise 7.36 can be solved without using the information in this chapter, the solution is considerably easier to obtain by using Theorem 8.4.1. The condition $(a * b)^m = a^m * b^m$ for all $a, b \in G$ shows that the map $f : G \to G$ defined by $f(a) = a^m$ is a homomorphism with $\ker(f) = G[m]$ and $\text{Im}(f) = mG$ (Check!). Therefore, all the results of Exercise 7.36 follow except the normality of $\text{Im}(f)$. We must separately show that $\text{Im}(f)$ is normal.

If G_1, G_2 are two finite groups and $f : G_1 \to G_2$ is a homomorphism, then Corollary 8.2.2 and Lagrange's theorem guarantee that $|Im(f)|$ divides $\text{ord}(G_2)$. The following corollary states that $|Im(f)|$ also divides $\text{ord}(G_1)$. Therefore, $|Im(f)|$ divides $\gcd(|G_1|, |G_2|)$.

Corollary 8.4.3 *Let G_1, G_2 be groups, and $f : G_1 \to G_2$ be a homomorphism. If G_1 is a finite group, then $|Im(f)|$ divides* $\text{ord}(G_1)$.

Proof According to Corollary 8.2.2, $\ker(f)$ is a normal subgroup of G. As G_1 is finite, then by Lagrange's theorem (Theorem 7.4.17), both $\ker(f)$ and $G_1/\ker(f)$ are finite and

$$|G_1/\ker(f)| = \frac{|G_1|}{|\ker(f)|}.$$

According to the first fundamental theorem,$|G_1/\ker(f)| = |Im(f)|$, and thus,

$$|G_1| = |G_1/\ker(f)| \cdot |\ker(f)| = |Im(f)| \cdot |\ker(f)|.$$

The result now follows. ■

Note that if the map f in the above result is an epimorphism, then $Im(f) = G_2$ and $|G_2|$ divides $|G_1|$.

Corollary 8.4.4 *Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group homomorphism. If the two groups are finite, then $|Im(f)|$ divides* $\gcd(|G_1|, |G_2|)$.

Proposition 8.4.5 *Let G_1, G_2 be finite groups. If $|G_1|$ and $|G_2|$ are relatively prime, then the trivial homomorphism is the only homomorphism between G_1 and G_2.*

Proof Assume that $f : G_1 \to G_2$ is an arbitrary group homomorphism. By Corollary 8.4.4, $|Im(f)|$ divides $\gcd(|G_1|, |G_2|) = 1$. As the only positive divisor of 1 is 1, then $Im(f) = \{e_2\}$ and f must be trivial. ■

Using the first fundamental theorem of homomorphisms, one can generalize Corollary 8.3.12 to obtain the following proposition. Recall that $m_1, \ldots, m_k$ are relatively primes if $\gcd\big(m_i, m_j\big) = 1$ for all $i \neq j$.

Proposition 8.4.6 *Let $m_1, \ldots, m_k$ be relatively primes. The additive group $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ is isomorphic to $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$.*

Proof Define the map.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \\ f(x) &\mapsto \big([x]_{m_1}, \ldots, [x]_{m_k}\big). \end{aligned}$$

The map f is a group homomorphism. For all $x, y \in \mathbb{Z}$,

$$\begin{aligned} f(x+y) =&\big([x+y]_{m_1}, \ldots, [x+y]_{m_k}\big) = \big([x]_{m_1} \oplus_{m_1} [y]_{m_1}, \ldots, [x]_{m_k} \oplus_{m_k} [x]_{m_k}\big) \\ =&\big([x]_{m_1}, \ldots, [x]_{m_k}\big) \oplus_{m_1 \cdots m_k} \big([y]_{m_1}, \ldots, [y]_{m_k}\big) = f(x) \oplus_{m_1 \cdots m_k} f(y). \end{aligned}$$

We show that $\ker(f) = m_1 \cdots m_k \mathbb{Z}$, as follows:
If $x \in \ker(f)$, then $x \in \mathbb{Z}$ and $f(x) = \big([0]_{m_1}, \ldots, [0]_{m_k}\big)$. i.e.,

$$\big([x]_{m_1}, \ldots, [x]_{m_k}\big) = \big([0]_{m_1}, \ldots, [0]_{m_k}\big)$$

implying that $[x]_{m_i} = [0]_{m_i}$ for all $1 \leq i \leq k$. Hence, x is divisible by all $m_1, \ldots, m_k$. Since $m_1, \ldots, m_k$ are relatively prime, x is divisible by their product $m_1 m_2 \cdots m_k$ (Corollary 2.5.7 (3)). Therefore, x is a multiple of $m_1 m_2 \cdots m_k$ and $\ker(f) \subseteq m_1 \cdots m_k \mathbb{Z}$. The other inclusion is clear as any element in $m_1 \cdots m_k \mathbb{Z}$ is in $\text{Ker}(f)$ (Check!), i.e.,

$$\ker(f) = m_1 \cdots m_k \mathbb{Z}.$$

According to the first fundamental theorem of homomorphisms, $\mathbb{Z}/\ker(f)$ is isomorphic to $f(\mathbb{Z})$. To show that f is surjective, let $\big([u_1]_{m_1}, \ldots, [u_k]_{m_k}\big)$ be any element in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$. For each $1 \leq i \leq k$, $\gcd(m_i, s_i) = 1$ where $s_i =$

$m_1 \cdots m_{i-1}\, m_{i+1} \cdots m_k$, and thus, by Theorem 2.5.1, there exist $a_i, b_i \in \mathbb{Z}$ such that $1 = a_i m_i + b_i s_i$. i.e.,

$$b_i s_i \equiv 1 \mod m_i.$$

Moreover, $b_i s_i \equiv 0 \mod m_j$ for each $j \neq i$. Let

$$x = \sum_{i=1}^{k} u_i b_i s_i.$$

Then, x is an integer that satisfies $x \equiv u_i \mod m_i$ for each $1 \leq i \leq k$, i.e.,

$$f(x) = \left([u_1]_{m_1}, \ldots, [u_k]_{m_k}\right)$$

Therefore, f is surjective. By the first fundamental theorem,

$$\mathbb{Z}_{m_1 m_2 \cdots m_k} = \mathbb{Z}/(m_1 \cdots m_k \mathbb{Z}) \cong f(\mathbb{Z}) = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.$$

■

Next, we study the second and third fundamental theorems of homomorphisms. As mentioned in the beginning of the section, both theorems concern subgroups of a given group G. These theorems provide a way to create a quotient subgroup of a quotient group. In this section, both theorems are stated and proved. In addition, several examples are provided.

Theorem 8.4.7 (Second Fundamental Theorem of group homomorphisms) *Let G be a group and H, K be subgroups of G. If H is a normal subgroup of G, then HK is a subgroup of G, $H \cap K$ is a normal subgroup of K, and*

$$K/(H \cap K) \cong HK/H.$$

Proof As $H \trianglelefteq G$, then by Proposition 7.5.12, HK is a group and H is normal in $HK = \langle H \cup K \rangle$. Let f be the composition of the inclusion map $\iota : K \to HK$ and the quotient map $\pi : HK \to HK/H$, i.e.,

$$f : K \xrightarrow{\iota} HK \xrightarrow{\pi} HK/H.$$

As f is a composition of two homomorphisms, it is a homomorphism. This map is surjective since $HK = KH$, and then any element of HK/H is of the form $khH = kH = \pi(\iota(k)) = f(k)$.

The kernel of f is

$$\ker(f) = \{a \in K : \pi\iota(a) = H\} = \{a \in K : aH = H\} = \{a \in K : a \in H\} = H \cap K.$$

By Corollary 8.2.2, $H \cap K$ is a normal subgroup of K, and by the first fundamental theorem of homomorphism,

$$K/(H \cap K) \cong f(K) = HK/H$$

■

Example 8.4.8 In the additive group $(\mathbb{Z}, +)$, let $H = 4\mathbb{Z}$ and $K = 5\mathbb{Z}$. The subsets H and K are normal subgroups of $\mathbb{Z}$ and $H \cap K = 20\,\mathbb{Z}$. As $HK = H + K = \mathbb{Z}$, then the second fundamental theorem of group homomorphism yields $5\mathbb{Z}/20\,\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$.

Corollary 8.4.9 *Let G be a finite group and H, K be subgroups of G. If H is a normal subgroup of G, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof As the group G is finite, all its subgroups are also finite. According to the second fundamental theorem of group homeomorphisms, $|HK/H| = |K/(H \cap K)|$. Lagrange's theorem implies that

$$\frac{|HK|}{|H|} = \frac{|K|}{|H \cap K|}.$$

.

The result now follows. ■

Example 8.4.10 Consider the group $\mathfrak{S}_4$. Let $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ and $K = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$. Both H and K are subgroups of $\mathfrak{S}_4$. As H is a normal subgroup (Example 7.7.5), the premises of Corollary 8.4.9 are satisfied, and thus,

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{4 \times 4}{2} = 8.$$

It can be easily to show that

$$\begin{aligned} HK &= \{h * k : h \in H, k \in K\} \\ &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2), (3\ 4), (1\ 4\ 2\ 3), (1\ 3\ 2\ 4)\}. \end{aligned}$$

The following theorem is another theorem that involves relations between a group G and its normal subgroups.

Theorem 8.4.11 (The third fundamental theorem of group homomorphisms) *Let G be a group and H, K be normal subgroups of G. If $K \subseteq H$, then*

$$H/K \trianglelefteq G/K \text{ and } (G/K)/(H/K) \cong G/H.$$

Proof As both H and K are normal subgroups of G, then by Propositions 7.5.9 and 7.7.3, we have $\left(G/K, +_{G/K}\right)$, $\left(G/H, +_{G/H}\right)$ and $\left(H/K, +_{H/K}\right)$ form groups. Define the map

$$\begin{aligned} f : G/K &\to G/H \\ aK &\mapsto aH \qquad \text{for all } \ a \in G. \end{aligned}$$

It can be easily verified that f is a surjective homomorphism. The kernel of f is

$$\begin{aligned} \ker(f) &= \{aK \in G/K : aH = H\} \\ &= \{aK \in G/K : a \in H\} = H/K. \end{aligned}$$

The result follows by the first fundamental theorem. ■

Example 8.4.12 Consider the additive group $(\mathbb{Z}, +)$. For each $m, n \in \mathbb{Z}$, the subgroups $n\mathbb{Z}$ and $m\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$ satisfying $m\mathbb{Z} \subseteq n\mathbb{Z}$ if $n|m$ (Check!). Therefore, if $n|m$, then by the third fundamental theorem of homomorphisms, $n\mathbb{Z}/m\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. This isomorphism is expressed by the map

$$f : (\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$$

where $f((a + m\mathbb{Z}) + (n\mathbb{Z}/m\mathbb{Z})) = a + n\mathbb{Z}$.

8.5 Group Actions and Group Homomorphisms

In this section left (right) group action on a set is defined and briefly studied. We begin by defining the opposite group and show that a left action of a group induced a right action of the opposite group. Since any group is isomorphic to its opposite group, we only consider the left action of a group. One of the main results in this section relates the group action on a set A to the group of all symmetries on A. We end the section by examining two sets related to the action of a group on the set A, namely the orbit and the stabilizer of an element in A.

Definition 8.5.1 Let $(G, *)$ be a group. The opposite group of G, usually denoted by G^{op}, is the group whose underlying set is G and its binary operation defined as follows:

Table 8.3 Cayley's tables of the group ($G = \{1, -1, i, -i, j, -j, k, -k\}, .^{\text{op}}$)

$.^{\text{op}}$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	i	-1	1	$-k$	k	j	$-j$
$-i$	$-i$	$-i$	1	-1	k	$-k$	$-j$	j
j	j	$-j$	k	$-k$	-1	1	$-i$	$-i$
$-j$	$-j$	j	$-k$	k	1	-1	i	i
k	k	$-k$	$-j$	j	i	$-i$	-1	1
$-k$	$-k$	k	j	$-j$	$-i$	i	1	-1

$$a *^{\text{op}} b = b * a.$$

It is straightforward to verify that ($G^{\text{op}}, *^{\text{op}}$) is a group.

Example 8.5.2

1. Cleary, for an abelian group G, the operation on G coincides with that of the opposite group, making the group G and its opposite identical.

2. Consider the group ($G = \{1, -1, i, -i, j, -j, k, -k\}, \bullet$), defined in Example 5.2.4. The operation on the opposite group of G is given by Table 8.3

Lemma 8.5.3 *Any group G is isomorphic to its opposite group.*

Proof The map $f : (G, *) \to (G^{op}, *^{op})$ defined by $f(g) = g^{-1}$ is a bijective map satisfying that

$$f(g_1 * g_2) = (g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1} = g_1^{-1} *^{op} g_2^{-1} = f(g_1) *^{op} f(g_2).$$

Thus, f is an isomorphism. ■

Definition 8.5.4 Let $(G, *)$ be a group and A be any set. A left group action of G on A is a function $\mu : G \times A \to A$ satisfies

1. $\mu(e, a) = a$ for all $a \in A$, and
2. $\mu(g * h, a) = \mu(g, \mu(h, a))$ for all $g, h \in G$, and $a \in A$.

If a function μ exists, we say that G acts on A. The set A is called a left G-set. If the action is clear from context, the expression $\mu(g, a)$ will be shortened to $g \cdot a$, and items (1) and (2) in the definition can be rewritten as

1. $e \cdot a = a$ for all $a \in A$, and
2. $(g * h) \cdot a = g \cdot (h \cdot a)$ for all $g, h \in G$, and $a \in A$.

Similarly, the group right action is defined as follows:

Definition 8.5.5 Let $(G, *)$ be a group and A be any set. A right group action of G on A is a function $\mu : A \times G \to A$ satisfies

1. $\mu(a, e) = a$ for all $a \in A$, and
2. $\mu(a, g * h) = \mu(\mu(a, g), h)$ for all $g, h \in G$, and $a \in A$.

If a function μ exists, we say that G acts on A, and the set A is called a right G-set. If the action is clear from context, the expression $\mu(a, g)$ will be shortened to $a \cdot g$, and items (1) and (2) in the definition can be rewritten as

1. $a \cdot e = a$ for all $a \in A$, and
2. $a \cdot (g * h) = (a \cdot g) \cdot h$ for all $g, h \in G$, and $a \in A$.

It is left to the reader to verify that the left action of a group $(G, *)$ on a set A yields a right group action of $(G^{\text{op}}, *^{\text{op}})$ on the same set A. In this section, we only consider the left action of a group.

Example 8.5.6

1. Let $(G, *)$ be a group and A be any set. The map

pleae delete this box

$$\begin{aligned} \cdot : G \times A &\to A \\ (g, a) &\mapsto g \cdot a = a \end{aligned}$$

forms a left action of G on A. This action is called the trivial action of G.

2. Let $(G, *)$ be a group.

(a) The map

$$\begin{aligned} \cdot : G \times G &\to G \\ (g, h) &\mapsto g \cdot h = g * h \end{aligned}$$

forms a left action of G on itself. This action is called the left multiplication of G.

Similarly, the action $g \cdot h = h * g$ defines a right action of G on itself, called the right multiplication of G

(b) The map

$$\begin{aligned} \cdot : G \times G &\to G \\ (g, a) &\mapsto g \cdot a = g * a * g^{-1} \end{aligned}$$

forms a left action of G on itself. This action is called the action of G by conjugation.

3. Let A be a set and consider $(\mathfrak{S}_A, \circ)$, the group of all symmetries on A (Corollary 5.1.11). The map

$$\begin{aligned} \cdot : \mathfrak{S}_A \times A &\to A \\ (\phi, a) &\mapsto \phi \cdot a = \phi(a) \end{aligned}$$

defined a left action of $\mathfrak{S}_A$ on the set A. To verify that $\cdot$ is a left action of $\mathfrak{S}_A$ on A, one must verify the conditions in Definition 8.5.4 as follows:

(a) $I_A \cdot a = I_A(a) = a$ for all $a \in A$

(b) $(\phi \circ \psi) \cdot a = (\phi \circ \psi)(a) = \phi(\psi(a)) = \phi(\psi \cdot a) = \phi \cdot (\psi \cdot a)$ for all $\phi, \psi \in \mathfrak{S}_A$ and all $a \in A$.

In particular, for each $n \in \mathbb{N}$, the group $\mathfrak{S}_n$ acts on $\{1, 2, 3, \ldots, n\}$.

4. Consider the additive group $(\mathbb{R}, +)$. Let $A = \mathbb{R}^2$ and define the action of $\mathbb{R}$ on A given by

$$t \cdot (a, b) = \left(e^t a + te^t b, e^t b\right).$$

Clearly $0 \cdot (a, b) = (a, b)$, and by direct computations, we have

$$\begin{aligned} t_1 \cdot (t_2 \cdot (a, b)) &= t_1 \cdot \left(e^{t_2} a + t_2 e^{t_2} b, e^{t_2} b\right) \\ &= \left(e^{t_1}\left(e^{t_2} a + t_2 e^{t_2} b\right) + t_1 e^{t_1} e^{t_2} b, e^{t_1} e^{t_2} b\right) \\ &= \left(e^{t_1+t_2} a + (t_1 + t_2) e^{t_1+t_2} b, e^{t_1+t_2} b\right) \\ &= (t_1 + t_2) \cdot (a, b). \end{aligned}.$$

The proof of the following lemma is left an exercise.

Lemma 8.5.7 *Let $(G, *)$ be a group and A be a left G -set. For each $g \in G$, the map*

$$\begin{aligned} f_g : A &\to A \\ a &\mapsto g \cdot a \end{aligned}$$

is a permutation on A. i.e., $f_g \in \mathfrak{S}_A$.

The following two proposition reveal the relationship between action of a group and homomorphisms.

Proposition 8.5.8 *Let $(G, *)$ be a group and A be a left G -set. The group action of G on A induces a group homomorphism from G to the group of all symmetries on A.*

Proof Define the map

$$\begin{aligned} f : G &\to \mathfrak{S}_A \\ g &\mapsto f_g : A \to A \\ &\qquad\quad a \mapsto g \cdot a \end{aligned}$$

i.e., $f(g)$ is the permutation that takes any element a to the action of G on a. For all $g, h \in G$ and all $a \in A$

$$f(g * h)(a) = (g * h) \cdot a = g \cdot (h \cdot a) = f(g)(h \cdot a) = f(g) \circ f(h)(a)$$

i.e., $f(g * h) = f(g) \circ f(h)$, and thus, f is a homomorphism. ■

Proposition 8.5.9 *Let A be any set and $(G, *)$ be a group. Any group homomorphism $f : G \to \mathfrak{S}_A$ induces a left action of G on the set A.*

Proof Define the action of G on the set A by $g \cdot a = f(g)(a)$. We verify that this is indeed a left action on A as follows:

- For each $a \in A$, $e \cdot a = f(e)(a) = I_A(a) = a$.
- For each $g, h \in G$, and for each $a \in A$,

$$(g * h) \cdot a = f(g * h)(a) = f(g) \circ f(h)(a) = f(g)(f(h)(a)) = g.(h \cdot a). \quad ■$$

In the following, for any element a in a G-set, two subsets can be related. These subsets are the orbit of a and its stabilizer. We begin with the following lemma whose proof is left as an easy exercise.

Lemma 8.5.10 *Let G be a group, A be a nonempty left G -set. The group action of G on A defines an equivalence relation on A given by $a \cong b$ if and only if there exists $g \in G$ such that $b = g \cdot a$.*

Definition 8.5.11 Let G be a group, A be a nonempty G-set, and $\cong$ as in Lemma 8.5.10. For any element $a \in A$, the equivalence class of a is called the G-orbit of a. For $g \in G$, we say G fixes a if $g \cdot a = a$. The subset of all elements of G that fix a is called stabilizer of a.

For each $a \in A$, the G-orbit of a is denoted by $\mathcal{O}(a)$, and the stabilizer of a is denoted by G_a. i.e.,

$$\mathcal{O}(a) = \{g \cdot a : g \in G\}, \quad G_a = \{g \in G : g \cdot a = a\}.$$

Note that both sets the G-orbit of a and its stabilizer are nonempty subsets of A and G, respectively. In fact, the stabilizer of a is a subgroup of G for any $a \in A$(Exercise 8.31).

Proposition 8.5.12 *Let G be a group, and A be a G -set. For each $a \in A$,*

$$|\mathcal{O}(a)| = [G : G_a]$$

where $[G : G_a]$ is the index of the subgroup G_a.

Proof Let $a \in A$. Define the map $f : \mathcal{O}(a) \to G/G_a$ as $f(g \cdot a) = g\ G_a$, where $g\ G_a$ is the left coset of G_a. Let $g_1 \cdot a$ and $g_2 \cdot a$ be arbitrary elements in $\mathcal{O}(a)$. Since

$$\begin{aligned} g_1 \cdot a = g_2 \cdot a &\Leftrightarrow g_2^{-1} \cdot (g_1 \cdot a) = g_2^{-1} \cdot (g_2 \cdot a) \\ &\Leftrightarrow \left(g_2^{-1} * g_1\right) \cdot a = \left(g_2^{-1} * g_2\right) \cdot a \\ &\Leftrightarrow \left(g_2^{-1} * g_1\right) \cdot a = a \\ &\Leftrightarrow g_2^{-1} \cdot g_1 \in G_a \\ &\Leftrightarrow g_2\ G_a = g_1\ G_a \quad \text{(Proposition 7.4.8(2))} \end{aligned}$$

then f is a well-defined injective map. For any $g\ G_a \in G/G_a$, $g \cdot a$ is an element of $\mathcal{O}(a)$ satisfies that $f(g \cdot a) = g\ G_a$. i.e., f is surjective. Therefore, $|\mathcal{O}(a)| = |G/G_a| = [G : G_a]$. ■

Corollary 8.5.13 *Let G be a finite group with $|G| = p$, and let A be a left G -set. For each $a \in A$, $|\mathcal{O}(a)|$ is either p or* 1.

For a finite group G, the conjugacy class equation is the following is

$$|G| = |C(G)| + \sum_{C_a \neq G} [G : C_a]$$

where $C(G)$ is the center of G, and $C_a = \{x \in G : x * a = a * x\}$. It was stated and proved in Exercise 7.13. This equation can be easily proved using the action of G on itself by conjugation (Exercise 8.32).

Exercises

Solved Exercises

8.1 Let $(G, *)$ be an abelian finite group that has an odd order. Show that the map $f : G \to G$ defined by $a \mapsto a^2$ for all $a \in G$ is an automorphism.

Solution

Clearly, f is a function on G. Using the result of Lemma 5.4.5(2), for all $a, b \in G$,

$$f(a * b) = (a * b)^2 = a^2 * b^2 = f(a)f(b).$$

Hence, f is a homomorphism. To show that f is bijective, it is enough to show that f is surjective (or injective) as G is finite (Exercise 1.6). To show that f is surjective, let b be an arbitrary element in G. As $|G|$ is odd, then $\gcd(|G|, 2) = 1$. According to Bézout's lemma (Theorem 2.5.1) there exist $x, y \in \mathbb{Z}$ such that $2x + |G|y = 1$. Therefore,

$$b = b^1 = b^{2x+|G|y} = b^{2x} * b^{|G|y} = b^{2x} * e = b^{2x} = \left(b^x\right)^2.$$

Let $a = b^x \in G$, then $f(a) = a^2 = (b^x)^2 = b$, and thus, f is bijective. i.e., f is an automorphism.

8.2 Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group isomorphism. Show that

- The group G_1 is abelian if and only if G_2 is abelian.
- $G_1 = \langle a \rangle$ for some $a \in G$ if and only if $G_2 = \langle f(a) \rangle$.

Solution

- Assume that G_1 is an abelian group. As f is a surjective map, then for all $a, b \in G_2$ there exist $c, d \in G_1$ such that $a = f(c), b = f(d)$. Hence,

$$a * b = f(c) * f(d) = f(c * d) = f(d * c) = f(d) * f(c) = b * a.$$

Therefore, G_2 is abelian. For the other direction, assume that G_2 is an abelian group. As $f^{-1} : G_2 \to G_1$ is also an isomorphism, then G_1 is abelian.

- If $G_1 = \langle a \rangle$ for some $a \in G$, then

$$\langle f(a) \rangle = \left\{(f(a))^k : k \in \mathbb{Z}\right\} = \left\{f\left(a^k\right) : k \in \mathbb{Z}\right\} = f(\langle a \rangle) = f(G_1) = G_2.$$

Conversely, if $G_2 = \langle b \rangle$ for some $b = f(a)$ and $a \in G_1$, then

$$\begin{aligned}\langle a \rangle = \left\langle f^{-1}(b) \right\rangle =& \left\{\left(f^{-1}(b)\right)^k : k \in \mathbb{Z}\right\} = \left\{f^{-1}\left(b^k\right) : k \in \mathbb{Z}\right\} \\ =& f^{-1}(G_2) = G_1.\end{aligned}$$

8.3 Let G_1, G_2 be groups, and $f : G_1 \to G_2$ be a group homomorphism. Show that for each $n \in \mathbb{N}$ and $a \in G_1$, if the equation $x^n = a$ has a solution in G_1, then the equation $x^n = f(a)$ has a solution in G_2.

Solution:

Let $n \in \mathbb{N}$ be an arbitrary element. Any $b \in G_1$ is a solution for $x^n = a$ if and only if $b^n = a$. By applying the homomorphism f to both sides of the equation, we obtain the equivalent equation

$$(f(b))^n = f\left(b^n\right) = f(a).$$

This occurs if and only if $f(b) \in G_2$ is a solution of $x^n = f(a)$.

8.4 Consider the two groups $(\mathbb{R}^3, +)$ and $\left(\mathbb{R}^2, +\right)$. Define $\theta : (\mathbb{R}^3, +) \to \left(\mathbb{R}^2, +\right)$ to be the map that takes (x, y, z) to (x, z). Show that θ is an epimorphism and find its kernel.

Solution:

Let (x, y, z) and $\left(x^{'}, y^{'}, z^{'}\right)$ be arbitrary elements in $\mathbb{R}^3$. As

$$\begin{aligned}\theta\big((x, y, z) + \left(x', y', z'\right)\big) &= \theta\left(x + x', y + y', z + z'\right)\\ &= \left(x + x', z + z'\right) = (x, z) + \left(x', z'\right)\\ &= \theta(x, y, z) + \theta\left(x', y', z'\right).\end{aligned}$$

then θ is a homomorphism. To show that θ is surjective, let (x, z) be an arbitrary element in $\mathbb{R}^2$. Pick the triple $(x, 1, z) \in \mathbb{R}^3$. The corresponding image under θ is $\theta(x, 1, z) = (x, z)$, which implies that θ is a surjective map, and $Im(\theta) = \mathbb{R}^2$. One can compute the kernel of θ as follows:

$$\begin{aligned}\ker(\theta) &= \left\{(x, y, z) \in \mathbb{R}^3 : (x, z) = (0, 0)\right\} = \left\{(0, y, 0) \in \mathbb{R}^3\right\}\\ &= \{(0, y, 0) : y \in \mathbb{R}\} \cong \mathbb{R}.\end{aligned}$$

Note that $\{(0, y, 0) : y \in \mathbb{R}\}$ represents the y-axis in $\mathbb{R}^3$, and $\ker(\theta)$ is isomorphic to the additive group $(\mathbb{R}, +)$ via the isomorphism that takes $(0, y, 0)$ to y.

8.5 Let $\mathfrak{G}$ be the class of all groups. On $\mathfrak{G}$, define the relation $\cong$ by.

$$G_1 \cong G_2 \text{ if and only if the two groups are isomorphic.}$$

Show that the relation $\cong$ is a reflexive, symmetric and transitive relation. Therefore, $\cong$ is an equivalence relation on $\mathfrak{G}$.

Solution:

For any group G, the identity map $\iota : G \to G$ defined by $\iota(a) = a$ for all $a \in G$ is an isomorphism, and thus, $G \cong G$. If $G_1 \cong G_2$, then there exists an isomorphism $f : G_1 \to G_2$. By Proposition 8.3.2, the inverse map $f^{-1} : G_2 \to G_1$ is an isomorphism. Hence, $G_2 \cong G_1$. Finally, if $G_1 \cong G_2$ and $G_2 \cong G_3$, then there exist two isomorphisms

$$f_1 : G_1 \to G_2, \quad f_2 : G_2 \to G_3.$$

According to Proposition 8.1.2, the composition $f_2 \circ f_1 : G_1 \to G_3$ is an isomorphism. Therefore, $G_1 \cong G_3$. According to Definition 1.4.1, $\cong$ is an equivalence relation.

8.6 Let G be a group and H, K be normal subgroups of G such that G is the internal direct product of H and K. Consider the direct product $H \times K$. Show that the internal direct product $G = HK$ is isomorphic to the direct product $H \times K$. State the generalization of the result in the case of n normal subgroups.

Solution:

Define $f : H \times K \to HK$ to be the map $f(h, k) = h * k$. As G is the internal direct product of H and K, then $H \cap K = \{e\}$, which implies that the elements of H and K commute (Lemma 7.5.15), and thus,

$$\begin{aligned} f((h_1, k_1) \bullet (h_2, k_2)) &= f(h_1 * h_2, k_1 * k_2) = (h_1 * h_2) * (k_1 * k_2) \\ &= (h_1 * k_1) * (h_2 * k_2) = f(h_1, k_1) * f(h_2, k_2). \end{aligned}$$

Therefore, f is a homomorphism. The operation $\bullet$ denotes the binary operation defined on the product of the groups H and K. The map f is surjective, as for any $h * k \in HK$, the pair $(h, k) \in H \times K$ and $f(h, k) = h * k$. To show that f is an injective map, one can check the kernel of f as follows:

If $(h, k) \in \ker(f)$, then $h * k = e$. By Exercise 7.8, $h = k = e$. i.e., the kernel of f is contained in $\{(e, e)\}$. Since (e, e) is in the kernel of f, then $\ker(f) = \{(e, e)\}$ and f is an isomorphism.

A generalization of this result, which can be shown by induction, is presented as follows:

“ Let $n \in \mathbb{N}$. Let G be a group and $H_1, H_2, \ldots, H_n$ be normal subgroups of G. If G is the internal direct product of $H_1, H_2, \ldots,$ and H_n, then G is isomorphic to the direct product $H_1 \times H_2 \times \cdots \times H_n$”.

8.7 Let G be a group and H be a normal subgroup of G. Show that any subgroup of G/H is of the form K/H, where K is a subgroup of G containing H.

(Note that the solution below is another proof of Proposition 7.7.6).

Solution:

Assume that $\mathcal{K}$ is a subgroup of G/H. Let $K = \pi^{-1}(\mathcal{K})$, where π is the quotient map (epimorphism) $\pi : G \to G/H$, defined by taking any element a in G to aH (Example 8.1.3(2c)). By Proposition 8.1.8 (2), K is a subgroup of G. Let $h \in H$ be an arbitrary element, as $\pi(h) = hH = H \in \mathcal{K}$, then $h \in \pi^{-1}(\mathcal{K}) = K$. i.e., H is contained in K. Since H is normal in G, then it is normal in K. Finally, as π is surjective, using the result of Exercise 1.24, we obtain

$$\mathcal{K} = \pi(K) = \{aH : a \in K\} = K/H.$$

8.8 Consider the group $(\mathbb{R}, +)$ and its normal subgroup $\mathbb{Z}$. Show that

$$\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} : |z| = 1\}.$$

Solution

Consider the group $(\mathbb{C}^*, \cdot)$. Define the map $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ by $f(r) = e^{2\pi ir}$ for each real number r. Since

$$f(r + s) = e^{2\pi i(r+s)} = e^{2\pi ir} \cdot e^{2\pi is} = f(r) \cdot f(s),$$

then the map f is a homomorphism. By computing the kernel and image of f, we obtain

$$\begin{aligned}\ker(f) &= \left\{r \in \mathbb{R} : e^{2\pi ir} = 1\right\} = \{r \in \mathbb{R} : cos2\pi r + isin2\pi r = 1\}\\ &= \{r \in \mathbb{R} : cos2\pi r = 1 \wedge\ sin2\pi r = 0\}\\ &= \{r \in \mathbb{R} : r \in \mathbb{Z}\} = \mathbb{Z},\end{aligned}$$

and

$$Im(f) = \{f(r) \in \mathbb{C} : r \in \mathbb{R}\} = \left\{e^{2\pi ir} \in \mathbb{C} : r \in \mathbb{R}\right\} = \{z \in \mathbb{C} : |z| = 1\}.$$

Therefore, applying the first fundamental theorem of group homomorphisms yields

$$\mathbb{R}/\mathbb{Z} \cong \{z \in \mathbb{C} : |z| = 1\}.$$

8.9 Let G_1, G_2 be any groups, $f : G_1 \to G_2$ be a group homomorphism, and K be a subgroup of G_2. Show that.

- $\ker(f)$ is a normal subgroup of $f^{-1}(K)$.
- If f is a surjective map, then $\left(f^{-1}(K)/\ker(f)\right) \cong K$.

Solution:

1. By Corollary 8.2.2, $\ker(f)$ is a normal subgroup of G_1, and thus, we only need to show that $\ker(f)$ is contained in $f^{-1}(K)$ for any subgroup K of G_2. Let K be an arbitrary subgroup of G_2 and x be any element in $\ker(f)$. As $e_2 \in K$, then $x \in \ker(f) \Rightarrow f(x) = e_2 \in K \Rightarrow x \in f^{-1}(K)$. Therefore, $\ker(f) \trianglelefteq f^{-1}(K)$.
2. Assume that f is surjective and K is a subgroup of G_2. Define

$$\begin{aligned} g : f^{-1}(K) &\to G_2\\ a &\mapsto f(a) \quad \text{for each } a \in f^{-1}(K)\end{aligned}$$

i.e., G is the restriction of f on the subgroup $f^{-1}(K)$. By Exercise 8.16, the map g is a homomorphism. Therefore, by the first fundamental theorem,

$$\left(f^{-1}(K)/\ker(g)\right) \cong Im(g).$$

One can easily check that $\ker(g) = \ker(f)$. For the image of g,

$$Im(g) = \left\{g(a) : a \in f^{-1}(K)\right\} = g\left(f^{-1}(K)\right) = f\left(f^{-1}(K)\right)$$

where the last equality holds as $g = f$ on $f^{-1}(K)$. Since f is surjective, then

$$f\big(f^{-1}(K)\big) = K.$$

Therefore,

$$\big(f^{-1}(K)/\ker(f)\big) \cong K.$$

8.10 Consider the additive group $\big(\mathbb{R}^2, +\big)$. Show that every line V passing through the origin in $\mathbb{R}^2$ is a normal subgroup of $\mathbb{R}^2$ that is isomorphic to $\mathbb{R}$. Describe $\mathbb{R}^2/V$.

Solution:

Any line V passing through the origin in $\mathbb{R}^2$ is either the y-axis, or it has the form $y = mx$ for some $m \in \mathbb{R}$. i.e.,

$$V = \{(0, y) : y \in \mathbb{R}\} \text{ or } V = \{(x, mx) : x \in \mathbb{R}\}.$$

Both are nonempty subsets of $\mathbb{R}^2$, as $(0, 0) \in V$.

1. If $V = \{(0, y) : y \in \mathbb{R}\}$ and $(0, y_1), (0, y_2)$ are arbitrary elements in V, then

$$(0, y_1) + (0, y_2)^{-1} = (0, y_1) + (0, -y_2) = (0, y_1 - y_2) \in V$$

By Proposition 7.1.4(3), V is a subgroup of $\mathbb{R}^2$ that is isomorphic to $(\mathbb{R}, +)$ via the map

$$\begin{aligned} f : (V, +) &\to (\mathbb{R}, +) \\ (0, y) &\mapsto y. \end{aligned}$$

2. If $V = \{(x, mx) : x \in \mathbb{R}\}$ and $(x, mx), (y, my)$ are arbitrary elements in V, then $(x, mx) + (y, my)^{-1} = (x, mx) + (-y, -my) = (x - y, m(x - y)) \in V$.

By Proposition 7.1.4.(3), V is a subgroup of $\mathbb{R}^2$ that is isomorphic to $(\mathbb{R}, +)$ via the map

$$\begin{aligned} f : (V, +) &\to (\mathbb{R}, +) \\ (x, mx) &\mapsto x. \end{aligned}$$

Therefore, in both cases, $V \cong \mathbb{R}$. Clearly, V is normal since the operation $+$ is a commutative operation. For describing the quotient, we have

1. If $V = \{(0, y) : y \in \mathbb{R}\}$, then the map

$$\begin{aligned} g : \mathbb{R}^2 &\to \mathbb{R} \\ (x, y) &\mapsto x \end{aligned}$$

is an epimorphism with ker(g) = V. Therefore, $\mathbb{R}^2/V \cong \mathbb{R}$. Geometrically, any element in $\mathbb{R}^2/V$ is of the form

$$(a,b)V = \{(a,b) + (0,y) : y \in \mathbb{R}\} = \{(a, y+b) : y \in \mathbb{R}\}$$

where (a,b) belongs to $\mathbb{R}^2$. This relation represents a line in $\mathbb{R}^2$ with x-coordinates fixed at a and y- coordinates varying freely. Specifically, $(a,b)V$ is represented by a line in $\mathbb{R}^2$ parallel to V, expressed as $x = a$.

2. If $V = \{(x, mx) : x \in \mathbb{R}\}$, then the map

$$\begin{aligned} g : \mathbb{R}^2 &\to \mathbb{R} \\ (x,y) &\mapsto mx - y \end{aligned}$$

is an epimorphism with ker(g) = V. Therefore, $\mathbb{R}^2/V \cong \mathbb{R}$. Geometrically, any element in $\mathbb{R}^2/V$ is of the form

$$(a,b)V = \{(a,b) + (x,mx) : x \in \mathbb{R}\} = \{(x+a, mx+b) : x \in \mathbb{R}\}$$

where (a,b) belongs to $\mathbb{R}^2$. To simplify the notation, let $x_1 = x + a \in \mathbb{R}$, then

$$(a,b)V = \{(x_1, m(x_1 - a) + b) : x_1 \in \mathbb{R}\}.$$

This relation represents a line in $\mathbb{R}^2$ expressed as $y = m(x-a) + b$, which is a line in $\mathbb{R}^2$ parallel to V and meets the y-axis at $(0, b - ma)$.

The reader may note the similarity of this result and that of Example 7.4.4, where the elements of $\mathbb{R}^2$ are represented as vectors. In fact, both quotient groups are isomorphic via the map $(a,b)V \mapsto (ai + bj)H$.

8.11 Let G be a finite group and A be a left G-set. Show that for each $a \in A$, $|\mathcal{O}(a)|$ is a divisor of $|G|$.

Solution:

Let a be an arbitrary element in A. According to Proposition 8.5.12, $|\mathcal{O}(a)| = [G : G_a]$. Using Lagrange theorem, we obtain

$$|G| = [G : G_a]|G_a| = |\mathcal{O}(a)||G_a|.$$

and thus, $|\mathcal{O}(a)|$ is a divisor of divides $|G|$.

Unsolved Exercises

8.12 Let G be a group. Show that G is abelian if and only if the map

$$\begin{aligned} f : G &\to G \\ x &\mapsto x^{-1} \end{aligned}$$

is a homomorphism.

8.13 Let G_1, G_2 be two abelian groups and $\phi : G_1 \to G_2$ be a homomorphism. Show that for any integer m, $\phi(mG_1)$ is a subgroup of mG_2. Show that if ϕ is an isomorphism then $\phi(mG_1) = mG_2$. See Proposition 5.5.3 for the definition of mG.

8.14 Let G be a group and $f : G \to G$ be the map defined on G by $f(a) = a^2$. Determine the conditions on G that make f a homomorphism.

8.15 Let G and H be finite groups such that $|G| \neq |H|$. Show that there are no isomorphisms from G to H.

8.16 Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group homomorphism (monomorphism). Show that the restriction of f (Definition 1.5.3) in any subgroup of G_1 is a group homomorphism (monomorphism). Provide an example of a group epimorphism such that its restriction to a subgroup of the domain group is not surjective.

8.17 Consider the additive group $(\mathbb{Z}, +)$. Define the map $f : \mathbb{Z} \to \mathbb{Z}$ by $f(a) = na$, where n is a nonzero integer. Show that the map f is a monomorphism that is not surjective for any $n \neq 1, -1$. What is the kernel and image of f?

8.18 Consider the additive group $(\mathbb{Z}, +)$. Let

$$\begin{aligned} f : \left(\mathbb{Z}/n\mathbb{Z}, +_{\mathbb{Z}/n\mathbb{Z}}\right) &\to \left(\mathbb{Z}/m\mathbb{Z}, +_{\mathbb{Z}/m\mathbb{Z}}\right) \\ a + n\mathbb{Z} &\mapsto a + m\mathbb{Z}. \end{aligned}$$

- Show that f is well-defined if and only if m, n are positive integers such that $m|n$.
- Show that when f is well defined, it is a homomorphism. Compute its kernel and its image.

(Compare the result of this question with the result of Example 3.2.4)

8.19 Consider the additive groups $(\mathbb{R}^3, +)$, $\left(\mathbb{R}^2, +\right)$ and the map $f : (\mathbb{R}^3, +) \to \left(\mathbb{R}^2, +\right)$ defined by $f(x, y, z) = (x + z, y - x)$. Show that f is a homomorphism and find its kernel and image.

8.20 Prove the generalization stated in Exercise 8.6.

8.21 Consider the additive group $(\mathbb{Z}, +)$. Show that $6\mathbb{Z}/18\mathbb{Z} \cong 3\mathbb{Z}/9\mathbb{Z}$.

8.22 Consider the additive groups $(\mathbb{Z}_{24}, \oplus_{24})$ and $(\mathbb{Z}_{12}, \oplus_{12})$. Show that $\{[0]_{24}, [12]_{24}\}$ is a normal subgroup of $\mathbb{Z}_{24}$ and

$$\mathbb{Z}_{24}/\{[0]_{24}, [12]_{24}\} \cong \mathbb{Z}_{12}.$$

8.23 Let $n \in \mathbb{N}$ such that $n \geq 3$. Show that the three groups

$$\mathfrak{S}_n/\mathcal{A}_n, \mathbb{Z}_2, \text{ and } (\{\pm 1\}),$$

are isomorphic groups.

8.24 Let G_1, G_2 be two groups, $f : G_1 \to G_2$ be a surjective group homomorphism, and K be a normal subgroup of G_2. Show that

$$G_1/f^{-1}(K) \cong G_2/K.$$

where $f^{-1}(K) = \{a \in G_1 : f(a) \in K\}$.

8.25 Let G be a finite group and H, K be normal subgroups of G. Show that

$$|G| < |K||H| \Rightarrow |H \cap K| > 1.$$

8.26 Let G_1, G_2 be two groups. Show that $G_1 \times \{e_2\}$ is isomorphic to G_1.

8.27 Let G_1, G_2 be two groups and H, K be normal subgroups of G_1 and G_2, respectively. Show that $H \times K$ is a normal subgroup of $G_1 \times G_2$, and

$$(G_1 \times G_2)/(H \times K) \cong (G_1/H) \times (G_2/\mathrm{K}).$$

In particular,

$$(G_1 \times G_2)/(G_1 \times \{e_2\}) \cong G_2.$$

8.28 Show that

i. the map f in Example 8.2.4 (7) is an isomorphism.
ii. the map f in Example 8.3.4 is an isomorphism.

8.29 Provide an example for a group G and two normal subgroups H, K of G such that $H \cong K$, but G/H is not isomorphic to G/K.

8.30 Let $G = \left\{ \begin{pmatrix} \frac{1+t^2}{2t} & \frac{t^2-1}{2t} \\ \frac{t^2-1}{2t} & \frac{1+t^2}{2t} \end{pmatrix} : t \in \mathbb{R}^* \right\}$.

i. Show that G, endowed with matrix multiplication, forms a group.
ii. Show that the group G, endowed with matrix multiplication, is isomorphic to the group $(\mathbb{R}^*, \cdot)$ where $\cdot$ is the multiplication defined on the real numbers.
iii. Show that G contains a subgroup that is isomorphic to $\left(\mathbb{R}^+, \cdot\right)$.

8.31 Let G be a group and A is a left G-set. Show that

- the set $\{\mathcal{O}(a) : a \in A\}$ is a partition of A.
- the stabilizer of any $a \in A$ is a subgroup of G.

8.32 Solve Exercise 7.13 using the information provided in Sect. 8.5.

Reference

Adkins, W., & Weintraub, S. (1992). *Agebra an approach via module theory*. Springer.

Chapter 9
Classification of Finite Abelian Groups

In this chapter, we study the finite abelian groups. According to Definition 5.4.2, a group is called abelian if the binary operation defined on G is commutative. We show that any finite abelian group is isomorphic to the product of additive groups $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ for some positive integers $n_1, n_2, \ldots, n_k$. The first section is devoted to study cyclic groups (finite and infinite). The cyclic groups form examples of abelian groups that are described in Chap 7. We shall see that, up to isomorphism, there is only one infinite cyclic group $(\mathbb{Z}, +)$, and for each $n \in \mathbb{N}$, the additive group $(\mathbb{Z}_n, \oplus_n)$ is the only cyclic group of order n. In Sect. 9.2, we define and study primary groups, and in Sect. 9.3, we study independent and spanning subsets of an abelian group. The primary groups, the independent subset, and spanning subset in abelian groups are required to prove the fundamental theorem of finite abelian groups in Sect. 9.4.

9.1 Cyclic Groups

A cyclic group is a group that is generated by a single element. We show that any cyclic group is abelian, and the cyclic group, whose order is a power of prime, forms the building block for any abelian group. We begin by reminding the reader of Definition 7.3.2 in Chap 7.

Definition 9.1.1 Let G be a group and $S \subseteq G$. The group G is said to be generated by S if $G = \langle S \rangle$. If $S = \{a_1, a_2 \ldots, a_n\}$ is a finite set, then $G = \langle a_1, a_2, \ldots, a_n \rangle$ is finitely generated.

Definition 9.1.2 The group G is said to be cyclic if there exists $a \in G$ such that $G = \langle a \rangle$. In this case, we say that a generates the group G.

A cyclic group G has the form $G = \langle a \rangle = \left\{a^k : k \in \mathbb{Z}\right\}$ (Proposition 7.3.6). If G is a finite group of order n, then $G = \left\{e, a, a^2, \ldots, a^{n-1}\right\}$.

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_9

Proposition 9.1.3 *Any cyclic group is abelian.*

Proof Let G be any cyclic group, then $G = \langle a \rangle = \left\{a^k : k \in \mathbb{Z}\right\}$ for some $a \in G$. If x, y are arbitrary elements in G, then $x = a^n$, $y = a^m$ for some $m, n \in \mathbb{Z}$. Hence

$$x{*}y = a^n{*}a^m = a^{n+m} = a^{m+n} = a^m{*}a^n = y{*}x$$

i.e., G is abelian. ■

The converse of the proposition above is not true. For example, although Klein group is an abelian group, it contains no element of order 4. Therefore, Klein group is not cyclic.

Proposition 9.1.4 *A group G is abelian if and only if the quotient of the group by its center is cyclic*, i.e.,

$$\text{A group } G \text{ is abelian} \Longleftrightarrow G/C(G) \text{ is cyclic.}$$

Proof If G is abelian, then $C(G) = G$, and $G/C(G) = \langle e \rangle$ is a cyclic group. For the other direction, assume that $G/C(G)$ is a cyclic group, then there exists d in G such that $G/C(G) = \langle d\ C(G) \rangle$. If g is an element in G, then there exists $k \in \mathbb{Z}$ such that

$$g\ C(G) = (d\ C(G))^k = d^k C(G).$$

According to Proposition 7.4.7, $\left(d^k\right)^{-1} * g \in C(G)$. Therefore, for any $g \in G$, there exists $k \in \mathbb{Z}$ and $c \in C(G)$ such that $g = d^k * c$. Let a, b be any elements in G, then there exist $k_1, k_2 \in \mathbb{Z}$ and $c_1, c_2 \in C(G)$ such that $a = d^{k_1} * c_1,\ b = d^{k_2} * c_2$. Therefore,

$$\begin{aligned} a * b &= \left(d^{k_1} * c_1\right) * \left(d^{k_2} * c_2\right) = d^{k_1} * \left(d^{k_2} * c_1\right) * c_2 \\ &= d^{k_1+k_2} * c_2 * c_1 = d^{k_2+k_1} * c_2 * c_1 = d^{k_2} * \left(d^{k_1} * c_2\right) * c_1 \\ &= \left(d^{k_2} * c_2\right) * \left(d^{k_1} * c_1\right) = b * a. \end{aligned}$$

i.e., G is abelian. ■

Note that the quotient group in this proposition is a quotient of G by its center. If the center is replaced by an arbitrary normal subgroup, then the result is not true. Exercise 9.5 shows an example for a cyclic group G/H in which G is not abelian.

Example 9.1.5

1. The additive groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, \oplus_n)$ are examples of cyclic groups, as $\mathbb{Z} = 1$ and $\mathbb{Z}_n = \langle [1] \rangle$ (Examples 7.3.8, and 7.3.9).
2. The additive group $(\mathbb{Q}, +)$ is an example of an abelian noncyclic group. To show this result, assume that $(\mathbb{Q}, +)$ is cyclic. In this case, there exists a nonzero number $a \in \mathbb{Q}$ such that

$$\mathbb{Q} = \langle a \rangle = \{na : n \in \mathbb{Z}\}.$$

As $a/2$ is an element in $\mathbb{Q}$, there exists $n \in \mathbb{Z}$ such that $na = a/2$, which implies that $n = 1/2$, contradicting that n is an integer. Similarly, one can show that the additive group $(\mathbb{R}, +)$ is an abelian noncyclic group.

3. The multiplicative group $(\mathbb{Q}^*, \cdot)$ is an example of an abelian noncyclic group. If $(\mathbb{Q}^*, \cdot)$ was cyclic, then there exists a number $a \in \mathbb{Q}^*$ such that $\mathbb{Q}^* = \langle a \rangle$. The element a can be written as r/s, where $\gcd(r, s) = 1$, $r \neq 0$, and $s > 0$. Therefore,

$$\mathbb{Q}^* = \langle r/s \rangle = \{(r/s)^k : r, s, k \in \mathbb{Z} \wedge r \neq 0, s > 0\}.$$

As $1/(s+1)$ is an element in $\mathbb{Q}^*$, then there exists $k \in \mathbb{Z}$ such that $1/(s+1) = (r/s)^k$.

- If $k = 0$, then $1/(s+1)$ equals 1, which implies that $s = 0$, contradicting the assumption $s > 0$.
- If $k > 0$, then the equation $1/(s+1) = (r/s)^k$ implies that $r^k(s+1) = s^k$. Therefore, $(s+1)|s^k$ contradicts that $\gcd(s, s+1) = 1$ (Exercise 2.19).
- If $k < 0$, then the equation $1/(s+1) = (r/s)^k$ implies that $1/(s+1) = (s/r)^m$ where $m = -k > 0$. i.e., $s^m(s+1) = r^m$. Therefore, as $s|(s^m(s+1))$, then $s|r^m$, which contradicts that $\gcd(r, s) = 1$ (Exercise 2.19).

Therefore, the group $(\mathbb{Q}^*, \cdot)$ cannot be cyclic.

4. The dihedral group D_{2n} and the symmetric group $\mathfrak{S}_n$ are both nonabelian groups for all $n \geq 3$. Therefore, these groups are both noncyclic for $n \geq 3$.
5. Let $n \in \mathbb{N}$. Consider the dihedral group D_{2n} (Example 5.1.4(6)). The subgroup of D_{2n} that consists of all rotations by angles $2\pi k/n$ where $0 \leq k \leq n-1$, forms a finite cyclic group that is generated by rotation by $2\pi/n$.
6. For any prime p, the group $\left(\mathrm{Inv}\left(\mathbb{Z}_p\right), \otimes_p\right)$ is a cyclic group (Proposition 7.3.21).
7. Any group of order 2 is cyclic (Check!).
8. Let p be a prime number. Any group of order p is cyclic. For if $|G| = p > 1$, then there exists $a \neq e$ in G. Let $H = \langle a \rangle$ be the subgroup of G generated by a. By Lagrange's theorem, $|H|$ divides $|G| = p$. Since $|H| \neq 1$ ($a \neq e$), then $|H| = p$, and $H = G$ is cyclic.

Proposition 9.1.6 *All subgroups and quotient groups of cyclic groups are cyclic.*

Proof Let $G = \langle a \rangle$ be a cyclic group, and H be a subgroup of G.

- If $H = \{e\}$, then H $= \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then there exists $k \in \mathbb{Z}^*$ such that $a^k \in H$. Without loss of generality, assume that $k > 0$ (if $k < 0$, then $m = -k > 0$ and $a^{-\mathrm{k}} \in H$). Choose k_0 to be the smallest positive integer such that $a^{k_0} \in H$. The goal is to show that $H = \left\langle a^{k_0} \right\rangle$. Since $a^{k_0} \in H$ and $\left\langle a^{k_0} \right\rangle$ is the smallest subgroup of G containing a^{k_0} (Proposition 7.3.3), then $\left\langle a^{k_0} \right\rangle \subseteq H$. For the other direction, let $h = a^n \in H$ for some integer n. By Theorem 2.1.2, applied to k_0 and n, $\exists q, r \in \mathbb{Z} \ni n = qk_0 + r, 0 \leq r < k_0$. Thus, $a^r = a^{n-qk_0} = a^n a^{-qk_0}$. Since both a^n and a^{-qk_0} belong to H, then $a^r = a^n a^{-qk_0} \in H$. However, k_0 is the smallest positive integer such that $a^{k_0} \in H$, and thus, $r = 0$ and $n = qk_0$. i.e., $h = a^n = a^{qk_0} = \left(a^{k_0}\right)^q \in \left\langle a^{k_0} \right\rangle$. Since h is an arbitrary element, then $H \subseteq \left\langle a^{k_0} \right\rangle$. Therefore, $H = \left\langle a^{k_0} \right\rangle$ is cyclic.
- For the quotient group G/H, note that H is normal (G is cyclic, and thus, abelian), which means that the quotient group is defined and is a group. We show that $G/H = \langle aH \rangle$, as follows:

$$\langle aH \rangle = \left\{(aH)^k : k \in \mathbb{Z}\right\} = \left\{a^k H : k \in \mathbb{Z}\right\} \subseteq \{bH : b \in G\} = G/H.$$

Since $a^k H = (aH)^k \in \langle aH \rangle$, then $G/H \subseteq \langle aH \rangle$. ■

Note that the converse of Proposition 9.1.8 is not true. For example, for all $n \geq 3$, the subgroup $H = \langle (1\ 2) \rangle$ is a cyclic subgroup of $\mathfrak{S}_n$, and the quotient group $\mathfrak{S}_n/\mathcal{A}_n$ is a cyclic group for any n, but $\mathfrak{S}_n$ is not cyclic. Also, the abelian group $(\mathbb{R}^*, \cdot)$ is not cyclic since its subgroup $(\mathbb{Q}^*, \cdot)$ is not cyclic. The following corollary is concluded from the proof of Proposition 9.1.6.

Corollary 9.1.7 *Let G be a cyclic group such that $G = \langle a \rangle$. Any subgroup of G is of the form of $\left\langle a^k \right\rangle$ for some integer k.*

Corollary 9.1.8

1. *The intersection of cyclic subgroups is cyclic.*
2. *The product of a finite number of subgroups of a cyclic group is cyclic.*

Proof

1. As the intersection of any groups is a subgroup of each of them, (1) follows by Proposition 9.1.6.
2. Assume that $H_1, H_2, \ldots, H_n$ are subgroups of a cyclic group G. Since G is abelian, then by Proposition 7.5.13, the product $H_1 H_2 \ldots H_n$ is a subgroup of G. Therefore, the result in (2) follows by Proposition 9.1.6. ■

Example 9.1.9 Any subgroup of the additive $(\mathbb{Z}, +)$ has the form $\langle 1^n \rangle = \langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Any subgroup of the additive $(\mathbb{Z}_n, \oplus_n)$ has the form $\langle [1]^n \rangle = \langle n \rangle = [n]\mathbb{Z}$ for some $n \in \mathbb{Z}$.

The following proposition is a stronger version of Lagrange's theorem in the case of finite cyclic groups.

Theorem 9.1.10 *Let G be a finite cyclic group of order n. For each $m \in \mathbb{N}$,*

$$\exists\,!\, H < G \ni |H| = m \Leftrightarrow m|n.$$

Proof Assume that G is a cyclic finite group, and $G = \langle a \rangle$ for some $a \in G$. If there exists $H < G$ such that $|H| = m$, then by Lagrange's theorem (Theorem 7.4.17), the integer m divides n. For the other direction, assume that m is an integer dividing n. Let $H = \left\langle a^{\mathrm{n/m}} \right\rangle$, thus H is a subgroup of G and

$$|H| = ord\left(a^{n/m}\right) = \frac{n}{(\mathrm{n/m})} = m \text{ (Proposition 5.5.9).}$$

To show that this H is unique, assume that there exists a subgroup K of G such that $|K| = m$. Let a^t be any element in K, then we have $\left(a^t\right)^m = e$, which yields that $n|mt$. i.e., $t = s(n/m)$ for some integer s. Therefore, $a^t = \left(a^{n/m}\right)^s \in H$, and K is a subset of H, where $|K| = |H|$. Hence, $K = H$, and H is the only subgroup of order m. ■

According to Theorem 9.1.10, the number of different subgroups of a finite cyclic group equals the number of different positive divisors of the order of G. In fact, as shown in the proof, any subgroup of $G = \langle a \rangle$ is of the form a^k, where $k = n/m$ is a divisor of n. Note that if m is a repeated divisor of the order of G, then there is only one subgroup of the form $\left\langle a^{|G|/m} \right\rangle$ that is corresponding to all repeated m.

Example 9.1.11

1. Consider the cyclic group $(\mathbb{Z}_{18}, \oplus_{18})$. The divisors of 18 are $1, 2, 3, 6, 9, 18$. According to Theorem 9.1.10, there are only six different subgroups of the additive group $(\mathbb{Z}_{18}, \oplus_{18})$. Since $\mathbb{Z}_{18} = \langle [1] \rangle$, then these subgroups can be listed as follows:

$$\langle [1]^{18} \rangle = \langle [18] \rangle = \langle [0] \rangle = \{[0]\}, \langle [1]^{9} \rangle = \langle [9] \rangle = \{[0], [9]\},$$

$$\langle [1]^{6} \rangle = \langle [6] \rangle = \{[0], [6], [12]\}, \langle [1]^{3} \rangle = \langle [3] \rangle = \{[0], [3], [6], [9], [12], [15]\},$$

$$\langle [1]^{2} \rangle = \langle [2] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14], [16]\}$$

$$\langle [1]^{1} \rangle = \langle [1] \rangle = \mathbb{Z}_{18}.$$

2. Similarly, one shows that there are only three different subgroups of $(\mathbb{Z}_9, \oplus_9)$ expressed as follows:

$$\langle [1]^{9} \rangle = \langle [9] \rangle = \{[0]\}, \langle [1]^{3} \rangle = \langle [3] \rangle = \{[0], [3], [6]\}, \langle [1]^{1} \rangle = \mathbb{Z}_9.$$

In general, the subgroups of the additive group $(\mathbb{Z}_n, \oplus_n)$ are $\left\{\langle [1]^{\frac{n}{m}} \rangle : m \in \mathbb{N}, m|n\right\}$.

3. Consider the multiplicative group $\left(\mathbb{Z}_{11}^*, \otimes_{11}\right)$. The group $\left(\mathbb{Z}_{11}^*, \otimes_{11}\right)$ is a finite cyclic group that is generated by [2] (Check!). There exist 10 elements in $\mathbb{Z}_{11}^*$. The divisors of 10 are $1, 2, 5, 10$. Therefore, there are four different subgroups of $\mathbb{Z}_{11}^*$:

$$\langle [2]^{10} \rangle = \langle [1] \rangle = \{1\}, \quad \langle [2]^5 \rangle = \langle [10] \rangle = \{[1], [10]\}$$

$$\langle [2]^2 \rangle = \langle [4] \rangle = \{[1], [4], [5], [9], [3]\}, \quad \langle [2]^1 \rangle = \mathbb{Z}_{11}^*.$$

Similarly, since $\mathbb{Z}_7^* = \langle [3] \rangle$ and $\mathrm{ord}\left(\mathbb{Z}_7^*\right) = 6$, then there exist 4 subgroups of $\left(\mathbb{Z}_7^*, \otimes_7\right)$:

$$\langle [3]^1 \rangle = \mathbb{Z}_7^*, \quad \langle [3]^2 \rangle = \{[1], [2], [4]\}, \quad \langle [3]^3 \rangle = \{[1], [6]\}, \quad \langle [3]^6 \rangle = \{[1]\}.$$

4. Consider the multiplicative group $(\mathbb{C}^*, \cdot)$, where $\mathbb{C}^*$ denotes the set of all nonzero complex numbers. Let

$$H = \left\{ \frac{1 \pm i\sqrt{3}}{2}, \frac{-1 \pm i\sqrt{3}}{2}, \pm 1 \right\}.$$

The set H is a cyclic subgroup of $\mathbb{C}^*$ as

$$H = \left\{ \left(\frac{1 + i\sqrt{3}}{2} \right)^k : k = 1, 2, 3, \ldots, 6 \right\}.$$

The subgroups of H are in one to one correspondence with the set of divisors of 6 which are 1, 2, 3, and 6. Hence, there are 4 subgroups of H. Namely,

$$\begin{aligned}
\langle h^6 \rangle &= \langle 1 \rangle = \{1\}, \\
\langle h^3 \rangle &= \langle -1 \rangle = \{1, -1\}, \\
\langle h^2 \rangle &= \left\{ 1, \frac{-1 + i\sqrt{3}}{2}, \frac{1 - i\sqrt{3}}{2} \right\}, \\
\langle h^1 \rangle &= H.
\end{aligned}$$

where $h = \left(1 + i\sqrt{3}\right)/2$.

Remark 9.1.12 The direct product of cyclic groups is not necessarily cyclic. For example, even though the additive group $\mathbb{Z}_2 = \langle[1]\rangle$ is cyclic, the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, as $\mathbb{Z}_2 \times \mathbb{Z}_2$ contains no element of order 4 (Check!). In fact, if $m, n \in \mathbb{N}$ such that $\gcd(m, n) \neq 1$, then their least common multiple l is less than mn, which implies that for any element $([a], [b])$ in $\mathbb{Z}_m \times \mathbb{Z}_n$,

$$([a], [b])^l = ([la], [lb]) = ([0], [0]).$$

Thus, $\operatorname{ord}(([a], [b])) \leq l < mn$, and $\mathbb{Z}_m \times \mathbb{Z}_n$ has no element of order mn.

The following proposition shows that an isomorphism preserves the cyclic property of groups and sends the generator of the domain group to a generator of the codomain group. For example, in the isomorphic groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ the isomorphism sends 1 to m (Example 8.1.3(4)).

Proposition 9.1.13 *Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group isomorphism. The group G_1 is cyclic if and only if G_2 is also cyclic. An element a generates G_1 if and only if $f(a)$ generates G_2.*

Example 9.1.14

1. The groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic. As $(\mathbb{Z}, +)$ is cyclic and $(\mathbb{Q}, +)$ is not cyclic, no isomorphism can exist between the two groups.
2. The groups $(\mathbb{Z}_4, \oplus_4)$ and $(\{[1], [3], [7], [9]\}, \otimes_{10})$ are cyclic isomorphic groups (Check!).
3. The groups $(\mathbb{Z}_4, \oplus_4)$ and $(\{[1], [5], [7], [11]\}, \otimes_{12})$ are not isomorphic as $(\mathbb{Z}_4, \oplus_4)$ is cyclic and $(\{[1], [5], [7], [11]\}, \otimes_{12})$ is not cyclic. Similarly, the groups $(\mathbb{Z}_2, \oplus_2)$ and $(\operatorname{Inv}(\mathbb{Z}_6), \otimes_6)$ are not isomorphic.
4. The groups $\left(\mathbb{Z}_{p-1}, \oplus_{p-1}\right)$ and $\left(\operatorname{Inv}\left(\mathbb{Z}_p\right), \otimes_{\mathrm{p}}\right)$ are two isomorphic cyclic groups for any prime p (Exercise 9.7).
5. The group H in Example 9.1.11 (4) is isomorphic to the additive group $(\mathbb{Z}_6, \oplus_6)$. The isomorphism is given by the map : $\mathbb{Z}_6 \to H$ that takes $k \mapsto h^k$.

A cyclic group may have more than one generator. If a is a generator of G then

$$\left\langle a^{-1}\right\rangle = \left\{\left(a^{-1}\right)^k : k \in \mathbb{Z}\right\} = \left\{a^s : s = -k \in \mathbb{Z}\right\} = \langle a\rangle = G$$

i.e., a^{-1} is also a generator of G. For example, the additive group $(\mathbb{Z}, +)$ is generated by both 1 and -1. The additive group $(\mathbb{Z}_n, \oplus_n)$, where $n \geq 3$, is generated by any element $[k] \in \mathbb{Z}_n$ such that $\gcd(k, n) = 1$ (Example 7.3.20). The following proposition is a corollary of Proposition 7.3.1 or Corollary 7.4.22.

Proposition 9.1.15 *Let G be a finite cyclic group of order n that is generated by an element a. For any $m \in \mathbb{N}$, $a^m \in G$ is a generator of G if and only if* $\gcd(m, n) = 1$.

To use Proposition 9.1.15 for finding all the generators for a given cyclic group, one must know at least one generator to begin with.

Example 9.1.16 Since the additive group $\mathbb{Z}_8 = \langle [1] \rangle$, the different generators of $\mathbb{Z}_8$ are

$$\left\{ [1]^m : m \in \mathbb{N}, \gcd(m, 8) = 1 \right\} = \{[1], [3], [5], [7]\}.$$

To determine only the number of generators of a finite group, rather than the generators themselves, Euler totient function can be used (Definition 5.3.8). Since for each $n \in \mathbb{N} \backslash \{1\}$, $\varphi(n) = |\{[\mathrm{m}] \in \mathbb{Z}_n : \gcd(m, n) = 1\}|$, then Corollary 5.3.9 implies the following results.

Corollary 9.1.17 *Let G be a finite cyclic group of order n. The number of generators of G is*

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

where $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ is the prim factorization on n.

Example 9.1.18 Since $|\mathbb{Z}_{12}| = 12 = 2^2 3^1$, and

$$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

then there exist 4 generators of $\mathbb{Z}_{12}$.

Our next goal is to classify all cyclic groups. The following theorem shows that, up to isomorphism, the only infinite cyclic group is the additive infinite group $\mathbb{Z}$, and the additive group $\mathbb{Z}_n$ is the only cyclic group of order n.

Theorem 9.1.19 *Let $(G, *)$ be a cyclic group. The group G is either isomorphic to the additive group $(\mathbb{Z}_n, \oplus_n)$ or isomorphic to the additive group $(\mathbb{Z}, +)$.*

Proof Assume that G is cyclic group and $G = \langle a \rangle$ for some $a \in G$.

- If G is finite with $|G| = n$, then $G = \left\{ e, a, a^2, \ldots, a^{n-1} \right\}$. Define the map

$$\begin{aligned} f : G &\to \mathbb{Z}_n \\ a^r &\mapsto [r]. \end{aligned}$$

We show that f is an isomorphism as follows: for $0 \leq r, s \leq n - 1$

$$f\left(a^r * a^s\right) = f\left(a^{r+s}\right) = [\mathrm{r} + \mathrm{s}] = [\mathrm{r}] \oplus_n [s] = f\left(a^r\right) \oplus_n f\left(a^s\right).$$

Therefore, f is a homomorphism. As

$$[\mathrm{r}] = [s] \Leftrightarrow \exists\, q \in \mathbb{Z} \ni\ r - s = qn$$

$$\Leftrightarrow a^{r-s} = a^{qn} = e \Leftrightarrow a^r = a^s.$$

then f is a well-defined injective map. As the domain and codomain are finite sets of the same cardinality, f is bijective (Exercise 1.6). Therefore, $G \cong \mathbb{Z}_n$.

– If G is infinite, then $G = \{a^n : n \in \mathbb{Z}\}$, where $a^n \neq a^m$ for all $m \neq n$ (otherwise, $a^{n-m} = e$, and a has a finite order that implies that G will be finite). The map $f : G \to \mathbb{Z}$ taking a^r to r is the required isomorphism (Check!). ■

Corollary 9.1.20 *All cyclic groups with the same order are isomorphic. In particular, if p is a prime number, then up to isomorphism, the additive group $\left(\mathbb{Z}_p, \oplus_p\right)$ is the only group of order p.*

Proof According to Theorem 9.1.19, any cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n$. Therefore, by the transitive property of the isomorphism relation, all cyclic groups of the same order n are isomorphic, and the first statement follows. For the second statement, as any group of order p is cyclic (Example 9.1.5 (8)) and all cyclic groups of the same order are isomorphic, then all groups of order p are isomorphic and there exists only one group of order p. ■

9.2 Primary Groups

In this section, we study a class of groups where the order of any element is a power of a given prime p. These groups are called primary groups. To emphasize that a primary group is linked to a prime p, these groups are also called p-primary groups, or simply, p-groups. Not every p-group is an abelian group, nor any abelian group is a p-group; however, the p-groups form a basic tool in proving the fundamental result of finite abelian groups, provided in Sect. 9.4.

Definition 9.2.1 Let p be a prime number. A p-primary group, or simply, a p-group, is a group in which the order of any element is a power of p. A group G is called a primary if it is p-primary for some prime p. A subgroup of a p-group is called a p-subgroup.

It follows directly from this definition that the order of any element in a p-group must be finite. This does not mean that the order of the group itself is finite. In fact, many examples for infinite p-groups exist, see Example 9.2.3 (9,10).

Proposition 9.2.2 *Let p be any prime.*

1. A group G is a p-group if and only if for each a in G, there exists a nonnegative integer k such that $a^{p^k} = e$.
2. A finite group G is a p-group if and only if $|G| = p^k$ for some nonnegative integer k.

3. Any finite cyclic p-group is isomorphic to the additive group $\mathbb{Z}_{p^k}$ for some nonnegative integer k, i.e.,
   G is a finite cyclic p-group $\Longleftrightarrow G = \mathbb{Z}_{p^k}$ for some nonnegative integer k.

Proof

1. If G is a p-group, then for any $a \in G$, the order of a is a power of p, i.e., $\operatorname{ord}(a) = p^k$ and $a^{p^k} = e$ for some nonnegative integer k. For the other direction, assume that for each a in G, there exists an integer k such that $a^{p^k} = e$. Lemma 5.5.5 implies that $\operatorname{ord}(a)$ is finite, and Lemma 5.5.6, shows that $\operatorname{ord}(a)$ divides p^k. Therefore, $\operatorname{ord}(a)$ is a power of p.
2. Assume that G is a finite p-group. If $G = \{e\}$, then $|G| = p^0$. Otherwise, let q be any prime divisor of $|G|$. According to Cauchy's theorem (Proposition 7.7.11), the group G must contain an element of order q. As every element in G has order p^s for some positive s, then $q = p^s$. However, q is a prime, which implies that $q = p$. Therefore, p is the only prime divisor of $|G|$, and the order of G is p^k for some integer k. For the other direction, assume that the order of G is p^k for some integer k, and let a be an arbitrary element in G. By Corollary 7.4.19, $a^{p^k} = a^{|G|} = e$. By the first statement, G is a p-group.
3. This statement directly follows by Theorem 9.1.19 and item (2). ■

Example 9.2.3

1. The trivial group $G = \{e\}$ is a p-group for any prime p, as $|G| = p^0$ for any p.
2. The Klein group is an example of a 2-group that is a finite group of order 2^2. Note that the order of any nonidentity element is 2^1.
3. The group $(\mathbb{Z}, +)$ is not a p-group for any prime number p, as $\operatorname{ord}(1) = \infty \neq p^k$ for any prime p and any positive integer k.
4. The additive group $(\mathbb{Z}_4, \oplus_4)$ is a 2-group that is a finite group of order 2^2. Note that

$$\operatorname{ord}([0]) = 2^0, \operatorname{ord}([1]) = \operatorname{ord}([3]) = 2^2, \text{ and } \operatorname{ord}([2]) = 2^1.$$

One can also check that the additive group $(\mathbb{Z}_7, \oplus_7)$ is a 7-group as it is a group of order 7^1. The additive group $(\mathbb{Z}_6, \oplus_6)$ is not a p-group for any p. The group $\mathbb{Z}_6$ is finite with an order 6 that is not p^k for any prime p and any positive integer k.

5. Let p be any prime. The additive group $\mathbb{Z}_p$ is a p-group for which the order of every nonidentity element is p. In general, the additive group $\mathbb{Z}_{p^k}$ is a p-group for any nonnegative integer k. For example, the additive groups $\mathbb{Z}_3, \mathbb{Z}_9, \mathbb{Z}_{27}, \mathbb{Z}_{81}, \ldots$ are all 3-groups.
6. The multiplicative group $(\operatorname{Inv}(\mathbb{Z}_{12}), \otimes_{12})$ has an order equal to 2^2. Therefore, $(\operatorname{Inv}(\mathbb{Z}_{12}), \otimes_{12})$ is a 2-group. One can easily show that the order of any element other than [1] is 2.

7. The multiplicative group $(\text{Inv}(\mathbb{Z}_{18}), \otimes_{18})$ has an order 6. Since 6 is not equal to p^k for any prime p and any positive integer k, then $\text{Inv}(\mathbb{Z}_{18})$ is not a p-group for any prime p.
8. The multiplicative group $(\text{Inv}(\mathbb{Z}_5), \otimes_5)$ is a 2-group since it is a finite group of order 2^2. Note that

$$\text{ord}([1]) = 2^0, \text{ord}([2]) = \text{ord}([3]) = 2^2, \text{ and } \text{ord}([4]) = 2^1.$$

The multiplicative group $(\text{Inv}(\mathbb{Z}_{11}), \otimes_{11})$ is not a p-group for any p, since the order of $\text{Inv}(\mathbb{Z}_{11})$ is $10 \neq p^k$ for any prime p and any positive integer k.

9. Consider the additive group $(G, \oplus)$, where $G = \mathbb{Z}_7 \times \mathbb{Z}_7 \times \cdots \times \mathbb{Z}_7 \times \cdots$ (G is the infinite direct product of the groups $\mathbb{Z}_7$), and $\oplus$ is the operation defined on the infinite direct product using $\oplus_7$. Any element in $a \in G$ is an infinite sequence of elements of $\mathbb{Z}_7$. i.e., $a = [a_1], [a_2], [a_3], \ldots,$ where $[a_i] \in \mathbb{Z}_7$. Since

$$a^7 = 7[a_1], 7[a_2], 7[a_3], \cdots = [0], [0], [0], \cdots = e_G$$

the order of any element a in G is either 1 or 7. Therefore, $(G, \oplus)$ is an example of an infinite 7-group.

10. Consider the additive group $(\mathbb{Q}, +)$. Let p be a prime and $A_p = \{m/p^k : k, m \in \mathbb{Z}, k \geq 0\}$. The set A_p is a subgroup of $\mathbb{Q}$ that contains the integers $\mathbb{Z}$ (Verify!). The subgroup A_p is not a primary group, as it contains $1/p^k$, an element of infinite order. The quotient group

$$A_p/\mathbb{Z} = \{(m/p^k) + \mathbb{Z} : k, m \in \mathbb{Z}, k > 0\}$$

is a p-group. For each element $(m/p^k) + \mathbb{Z}$ in $(A_p/\mathbb{Z}, \oplus_{A_p/\mathbb{Z}})$, we have

$$((m/p^k) + \mathbb{Z})^{p^k} = m + \mathbb{Z} = \mathbb{Z} = e_{A_p/\mathbb{Z}}.$$

Therefore, $(A_p/\mathbb{Z}, \oplus_{A_p/\mathbb{Z}})$ is an example of an infinite p-group.

11. Let p be a prime and

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}.$$

The set G is a group under matrix multiplication (Check!). It can be easily verified that the order of G equals p^3. Therefore, the group G is a p- group, and the center of G is

$$C(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_p \right\}$$

which is a subgroup of order p. Therefore, $C(G) \neq G$ and G is not abelian. The group G is an example of a p-group that is not abelian. For more examples of nonabelian p-groups, see Exercises 9.21 and 9.22.

The proof of the following proposition is straightforward and left as an easy exercise.

Proposition 9.2.4 *Let p be prime. Any subgroup of a p-group is a p-group. Any quotient group of a p-group is a p-group.*

Proposition 9.2.5 *Let G be a group, and p be a prime number.*

1. If $p^k G = \{e\}$ for some nonnegative integer k, then G is a p-group.
2. If G is abelian, then $G[p]$ is a p-subgroup of G.

Proof

1. If $p^k G = \{e\}$ for some nonnegative integer k, then for any $a \in G$, $a^{p^k} = e$ for some nonnegative integer k. Proposition 9.2.2 (1) implies the result.
2. Assume that G is abelian. By Proposition 5.5.13, $G[p]$ is a group. Let b be any element in $G[p]$, then $b^p = e$. According to Lemma 5.5.6, $\text{ord}(b)|p$, which implies that $\text{ord}(b)$ is either 1 or p. As b is arbitrary, then $G[p]$ is a p- group. ■

For the definition of mG and $G[m]$, see Proposition 5.5.13.

Corollary 9.2.6 *Let p be a prime number and G be a finite group. The group G is a p-group if and only if the exponent of G is of the form p^k for some nonnegative integer k,* i.e., *for a finite group G,*

$$G \text{ is a } p \text{ - group} \iff \text{Exp}(G) = p^k \text{ for } k \in \mathbb{N} \cup \{0\}.$$

Proof Assume that G is a finite p-group. Since G is finite, then the exponent of G exists and is equal to the least common multiple of the orders of all its elements (Proposition 5.5.17). Since the order of any element in G is a power of p, then the least common multiple of such orders is also a power of p, i.e., there exists a nonnegative integer k such that the exponent of G equals p^k. For the other direction, let $a \in G$ be an arbitrary element in G. If the exponent of G is p^k, then $\text{ord}(a)$ divides p^k, i.e., $\text{ord}(a) = p^s$ for some $s \leq k$. Therefore, G is a p-group. ■

The next two results explain the relationship between p-groups and cyclic groups in the finite case. Before discussing these results, let us point out the following:

- Not all primary groups are cyclic. The Klein group is an example of a 2-group that is not cyclic.
- Not all cyclic groups are primary groups. The additive group $\mathbb{Z}_6$ is a cyclic group that is not a p-group for any prime p.
- For any prime p and any $k \in \mathbb{N}$, the group $\mathbb{Z}_{p^k}$ is a cyclic p-group, and any finite cyclic primary group is isomorphic to $\mathbb{Z}_{p^k}$ for some prime p and nonnegative integer k (Proposition 9.2.2 (3)).

Lemma 9.2.7 *Let $n \in \mathbb{N}$. The additive group $\mathbb{Z}_n$ is isomorphic to a direct product of cyclic p_i-groups. Namely,*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_s^{k_s}}$$

where $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the prime factorization of n.

Proof If $n = 1$, then $\mathbb{Z}_1 = \{e\} \cong \mathbb{Z}_{p^0}$ is a p-group for any prime p. If $n > 1$, let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be the prime factorization of n (Theorem 2.8.8, and Definition 2.8.10). As $p_1, p_2, \ldots, p_s$ are all distinct, then $p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}$ are relatively prime. By Proposition 8.4.6,

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_s^{k_s}} \cong \mathbb{Z}_{p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_s^{k_s}} = \mathbb{Z}_n$$

as required. ■

As any finite cyclic group $G \cong \mathbb{Z}_n$ for some positive integer n (Theorem 9.1.19), the following corollary follows.

Corollary 9.2.8 *Any finite cyclic group is isomorphic to a direct product of cyclic p_i-groups, i.e., if G is a finite cyclic group, then*

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_s^{k_s}}$$

where $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the prime factorization of $|G|$.

We devote the remainder of this section to prove Corollary 9.2.17, the analog for the above corollary. It is a generalization of Corollary 9.2.8 to the case of abelian groups. Corollary 9.2.17 is called the primary decomposition of finite abelian groups. We begin with the following lemma.

Lemma 9.2.9 *Let G be a finite abelian group. For each p, a prime divisor of $|G|$, the subset*

$$G_p = \left\{a \in G : a^{p^s} = \text{e for some } s \in \mathbb{N}\right\}$$

is a normal p-subgroup of G that contains $G[p]$.

Proof Assume that G is a finite abelian group and p is any divisor of $|G|$. According to Cauchy's theorem (Proposition 7.7.11), the subset G_{p} is not empty. Let $a, b \in G_{\mathrm{p}}$, then we have $a^{p^s} = \mathrm{e}$ and $b^{p^r} = \mathrm{e}$ for some $s, r \in \mathbb{N}$. Since G is abelian, then $(a * b)^{p^{s+r}} = (a)^{p^{s+r}} * (b)^{p^{s+r}} = e$. i.e., $a * b \in G_{\mathrm{p}}$. By Proposition 7.1.6, G_{p} is a subgroup of G. For any a in G_{p}, $a^{p^s} = \mathrm{e}$ for some $s \in \mathbb{N}$, and thus, G_{p} is a p-group (Proposition 9.2.2 (1)) which is normal as G is abelian. Clearly,

$$G[p] = \left\{a \in G : a^p = \mathrm{e}\right\} \subseteq G_p.$$

■

Definition 9.2.10 Let G be a finite abelian group and p be a prime divisor of $|G|$. The subgroup G_p is called the p-component of G. A primary component of G is a p-component of G for some prime divisor of $|G|$.

Example 9.2.11 In the following we compute the p-component for a given abelian group G and prime divisor of the order of G.

1. Consider the additive group $(\mathbb{Z}_4, \oplus_4)$. The order of $\mathbb{Z}_4$ is 4, and it has only one prime divisor, namely 2. Therefore, $\mathbb{Z}_4$ has only one prime component, the 2-component of $\mathbb{Z}_4$ is

$$\left\{[a] : \left[2^s a\right] = [0] \text{ for some } s \in \mathbb{N}\right\} = \{[0[, [1], [2], [3]\} = \mathbb{Z}_4.$$

   Note that $\left[2^2 a\right] = [0]$ for all $[a] \in \mathbb{Z}_4$.

2. Consider the additive group $(\mathbb{Z}_6, \oplus_6)$. The order of $\mathbb{Z}_6$ is 6, which has two prime divisors. Therefore, there exist two prime components of $\mathbb{Z}_6$, namely, the 2-component and the 3-component of $\mathbb{Z}_6$. Similar to (1), one can easily show that the 2-component of $\mathbb{Z}_6$ is $\{[0], [3]\}$ and the 3-component of $\mathbb{Z}_6$ is $\{[0], [2], [4]\}$. Note that the intersection of the two components of $\mathbb{Z}_6$ is $\{[0]\}$, and their product is $\mathbb{Z}_6$.
3. Any finite p-group G has only one component (Exercise 9.26).

Proposition 9.2.12 Let G be a finite abelian group and p be any prime divisor of $|G|$. The order of the p-component of G is equal to p^k for a positive integer k, where $\gcd\left(p, |G|/p^k\right) = 1$.

Proof Since G_p is a p-group, then by Proposition 9.2.2, $\left|G_p\right| = p^k$ for some nonnegative integer k. Since $p||G|$, then by Cauchy's theorem (Proposition 7.7.11), G must contain an element of order p, which implies that G_p contains a nonidentity element. Therefore, $\left|G_p\right| > 1$, and k must be positive. If $\gcd\left(p, |G|/p^k\right) \neq 1$, then $p|\left(|G|/p^k\right)$. Since $|G|/p^k$ is the order of the quotient group G/G_p, then by Cauchy's theorem (Proposition 7.7.11), there exists an element $aG_p \neq G_p$ that belongs to the group G/G_p such that $\mathrm{ord}\left(aG_p\right) = p$. Therefore, $a^p G_p = \left(aG_p\right)^p = G_p$, which implies that $a^p \in G_p$, i.e., there exists an $s \in \mathbb{N}$, such that $(a^p)^{p^s} = e$. Consequently, $a \in G_p$. By Proposition 7.4.5, $aG_p = G_p$, which contradicts that $\operatorname{ord}(aG_p) = p$. Therefore, $\gcd(p, |G|/p^k) = 1$. ■

Since the integer k in Proposition 9.2.12 must be positive, any p-component cannot be a trivial subgroup, and no primary components exist for the trivial group $G = \{e\}$.

Corollary 9.2.13 *Let G be a finite abelian group. If $p_1, \ldots, p_n$ are all distinct prime divisors of $|G|$, then*

$$|G| = p_1^{k_1} \cdots p_n^{k_n}$$

where $p_i^{k_i}$ is the order of the p_i-component of G.

Proof Since $p_1, \ldots, p_n$ are all distinct prime divisors of $|G|$, then $|G| = p_1^{s_1} \ldots p_n^{s_n}$ for some positive integers $s_1, \ldots, s_n$. For each $1 \le i \le n$, let G_{p_i} be the p_i-component of G. According to Proposition 9.2.12, $\left|G_{p_i}\right| = p_i^{k_i}$ for some positive integer k_i, where $\gcd\left(p_i, |G|/p_i^{k_i}\right) = 1$. Since G_{p_i} is a subgroup of G, and $p_1, \ldots, p_n$ are all distinct, then $p_i^{k_i} | p_i^{s_i}$ and $k_i \le s_i$. As $\gcd\left(p_i, |G|/p_i^{k_i}\right) = 1$, the prime p_i does not divide $|G|/p_i^{k_i}$. However,

$$|G|/p_i^{k_i} = p_1^{s_1} \cdots p_{i-1}^{s_{i-1}} p_i^{s_i - k_i} p_{i+1}^{s_{i+1}} \cdots p_n^{s_n}$$

which implies that $s_i - k_i = 0$. Therefore, $s_i = k_i$ and $|G| = p_1^{k_1} \cdots p_n^{k_n}$. ■

Our next goal is to show that every finite abelian group is an internal direct product of its p_i-components. The internal direct product of subgroups is defined in Definition 7.6.5. We begin with the following lemma.

Lemma 9.2.14 *Let G be a finite abelian group. If $p_1, \ldots, p_n$ are all distinct prime divisors of $|G|$, then $G = G_{p_1} G_{p_2} \cdots G_{p_n}$, where G_{p_i} is the p_i-component of G.*

Proof Since $G_{p_i} = \left\{a \in G : a^{p_i^s} = \text{e for some } s \in \mathbb{N}\right\}$ is a normal subgroup of G for each $1 \le i \le n$, then the product $G_{p_1} G_{p_2} \cdots G_{p_n}$ forms a subgroup of G (Proposition 7.5.13). Therefore, it remains only to show that G is a subset of $G_{p_1} G_{p_2} \cdots G_{p_n}$. Let $a \in G$ be an arbitrary element. By Proposition 9.2.12, for each $1 \le i \le n$, there exists a positive integer k_i such that $\left|G_{p_i}\right| = p_i^{k_i}$. Let $m_i = |G|/p_i^{k_i} = \prod_{j \ne i} p_j^{k_j}$, (Corollary 9.2.13). By Exercise 2.12, we have $\gcd(m_1, \ldots, m_n) = 1$. Hence, there exist $l_i \in \mathbb{Z}$, $1 \le i \le n$ such that $\sum_{i=1}^n l_i m_i = 1$ (Exercise 2. 9). For each $1 \le i \le n$, let $a_i = a^{l_i m_i}$ then we have

$$a_i^{p_i k_i} = \left(a^{l_i m_i}\right)^{p_i k_i} = a^{l_i m_i p_i^{k_i}} = a^{l_i |G|} = \left(a^{|G|}\right)^{l_i} = e$$

which implies that $a_i \in G_{p_i}$ and

$$\begin{aligned}a = a^1 = a^{\sum\limits_{i=1}^{n} l_i m_i} &= a^{l_1 m_1} * a^{l_2 m_2} * \cdots * a^{l_n m_n}\\ &= a_1 * a_2 * \cdots * a_n \in G_{p_1} G_{p_2} \cdots G_{p_n}.\end{aligned}$$

Therefore, $G = G_{p_1} G_{p_2} \cdots G_{p_n}$. ■

Lemma 9.2.15 *Let G be a finite abelian group, $p_1, \ldots, p_n$ be all the distinct prime divisors of $|G|$, and G_{p_i}, $1 \le i \le n$ be the p_i-components of G. For all $1 \le i \le n$,*

$$G_{p_i} \cap \left\langle \cup_{j \ne i} G_{p_j} \right\rangle = \{e\}.$$

Proof Using Proposition 7.5.18, it suffices to show that for each $a_i \in G_{p_i}$, $1 \le i \le n$

$$a_1 * a_2 * \cdots * a_n = e \Longrightarrow a_1 = \cdots = a_n = e.$$

Assume that $a_1 * a_2 * \cdots * a_n = e$, where $a_i \in G_{p_i}$, $1 \le i \le n$. By Corollary 9.2.13,

$$|G| = p_1^{k_1} \cdots p_n^{k_n}$$

where $p_i^{k_i} = \left|G_{p_i}\right|$. Let $m_i = |G|/p_i^{k_i} = \prod_{j \ne i} p_j^{k_j}$. By Exercise 2.12, $\gcd(m_1, \ldots, m_n) = 1$. Therefore, there exists $l_i \in \mathbb{Z}, 1 \le i \le n$ such that $\sum_{i=1}^{n} l_i m_i = 1$ (Exercise 2.9). For each $a_i \in G_{p_i}$, $\operatorname{ord}(a_i) | p_i^{k_i}$. Since for all $j \ne i$, $p_i^{k_i} | m_j$, then $\operatorname{ord}(a_i) | m_j$, and $a_i^{m_j} = e$ for all $i \ne j$. Therefore, if $a_1 * a_2 * \cdots * a_n = e$, then for each $1 \le i \le n$,

$$\begin{aligned}e = e^{l_j m_j} &= (a_1 * a_2 * \cdots * a_n)^{l_j m_j}\\ &= a_1^{l_j m_j} * a_2^{l_j m_j} * \cdots * a_n^{l_j m_j} = a_i^{l_i m_i}\end{aligned}$$

Hence,

$$a_i = a_i^1 = a_i^{\sum\limits_{j=1}^{n} l_j m_j} = a_i^{l_1 m_1} * a_i^{l_2 m_2} * \cdots * a_i^{l_n m_n} \underset{a_i^{m_j} = e \text{ if } i \ne j}{=} e * e * \cdots e * a_i^{l_i m_i} * e \cdots * e = a_i^{l_i m_i} = e.$$

The following theorem is a direct corollary of the above two lemmas. ■

Theorem 9.2.16 *Every nontrivial finite abelian group is an internal direct product of its primary components.*

The result in Exercise 8.20 shows the following:

Corollary 9.2.17 (Primary decomposition of finite abelian groups) *Every nontrivial finite abelian group is isomorphic to the direct product of its primary components. Namely, if $G \ne \{e\}$ is a finite abelian group, and $p_1, \ldots, p_n$ are all distinct prime divisors of $|G|$, then*

$$G \cong \prod_{i=1}^{n} G_{p_i} = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_n}$$

where G_{p_i} is the p_i-component of G.

The next goal is to show that each primary component G_p in the decomposition above is isomorphic to a direct product of cyclic p-groups, i.e., $G_p \cong \prod_{k_i} \mathbb{Z}_{p^{k_i}}$ for some k_i. However, this task is challenging, and we defer its proof to Sect. 9.4, until all necessary definitions and results have been introduced.

9.3 Independent Subsets, Spanning Subsets, and Bases of a Group

The current section contains the basic definitions and results that are required to prove the fundamental theorem of finite abelian groups in the next section.

Definition 9.3.1 (*Independent subset of a group*) Let G be an abelian group and $a_1, a_2, \ldots, a_n$ be distinct elements in G such that $a_i \neq e$ for each $1 \leq i \leq n$. The set $\{a_1, a_2, \ldots, a_n\}$ is called independent if whenever there are integers $k_1, k_2, \ldots, k_n$ such that $a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n} = e$, then $a_i^{k_i} = e$ for all $1 \leq i \leq n$. An independent set $\{a_1, a_2, \ldots, a_n\}$ is called maximal independent if it is not contained in any other independent subset of G.

According to this definition, none of the elements $a_1, a_2, \ldots, a_n$ is an identity element in G. Therefore, by definition, any subset of G that contains e is not independent. In particular, the set $\{e\}$ is not independent.

Example 9.3.2

1. As the empty set $\emptyset$ contains no elements, the conditional statement in the definition is satisfied, and $\emptyset$ is an independent set.
2. Any subset consisting of one nonidentity element satisfies the condition of the independence. Therefore, it is an independent set. In particular, the subsets $\{1\}$, $\{2\}$, $\{-1\}$, $\{z\}$ for any nonzero z in $\mathbb{Z}$ are examples of independent subsets of $(\mathbb{Z}, +)$.
3. The subset $\{2, 3\}$ is not independent in $(\mathbb{Z}, +)$ as

   $$2^3 * 3^{-2} = 2 + 2 + 2 + (-3) + (-3) = 0, \text{ but } 2^3 = 2 + 2 + 2 \neq 0.$$

4. In general, any subset of $(\mathbb{Z}, +)$ that has more than one element is not independent. If $S = \{k_1, k_2, \ldots, k_n\}$, $n \geq 2$, is any subset of nonzero elements in $\mathbb{Z}$, then $k_1^{k_2} + k_2^{-k_1} + k_3^0 + \cdots + k_n^0 = 0$, but $k_1^{k_2} \neq 0$ and $k_2^{-k_1} \neq 0$.
5. Since any subset of $(\mathbb{Z}, +)$ that has more than one element is not independent, any set that consists of only a nonzero element of $\mathbb{Z}$ is a maximal independent set.

6. Consider the additive group $\mathbb{Z}_4 \times \mathbb{Z}_4$. The set $\{([1], [2]), ([3], [3])\}$ is an independent set. If k_1, k_2 are any integers such that $([1], [2])^{k_1} \oplus_4 ([3], [3])^{k_2} = ([0], [0])$, then

$$([k_1], [2k_1]) \oplus_4 ([3k_2], [3k_2]) = ([0], [0]).$$

This result implies that $[k_1 + 3k_2]$=[0] and $[2k_1 + 3k_2]$=[0], i.e.,
$[k_1] = -[3k_2] = [k_2]$ and $[2k_1] = -[3k_2] = [k_2]$. Solving these two equations gives that $[k_1] = [k_2] = [0]$, which implies that

$$([1], [2])^{k_1} = ([k_1], [2k_1]) = ([0], [0]),$$

and

$$([3], [3])^{k_2} = ([3k_2], [3k_2]) = ([0], [0]).$$

The reader may easily check that the subset $\{([0], [2]), ([3], [0])\}$ is also an independent set (Check!).

7. Consider the additive group $(\mathbb{Z} \times \mathbb{Z}, +)$. For any nonzero elements x, y in $\mathbb{Z}$, the subset $\{(x, 0), (0, y)\}$ is an independent set. For if k_1, k_2 are any integers such that

$$(x, 0)^{k_1} + (0, y)^{k_2} = (0, 0), \text{ then } (k_1x, 0) + (0, k_2y) = (0, 0)$$

which implies that $k_1x = k_2y = 0$, i.e.,

$$(x, 0)^{k_1} = (k_1x, 0) = (0, 0) \text{ and } (0, y)^{k_2} = (0, k_2y) = (0, 0).$$

The set $\{(x, 0), (0, y)\}$ is maximal independent in $\mathbb{Z} \times \mathbb{Z}$. For any (a, b), a nonzero element in $\mathbb{Z} \times \mathbb{Z}$, the set $\{(x, 0), (0, y), (a, b)\}$ is not independent. For if $k_1 = ay, k_2 = bx, k_3 = -xy$, then
$(x, 0)^{k_1} + (0, y)^{k_2} + (a, b)^{k_3} = (0, 0)$, but $(a, b)^{k_3} \neq (0, 0)$ (Check!).

8. Consider the additive group $(\mathbb{R} \times \mathbb{R}, +)$. Similar to the case for $\mathbb{Z} \times \mathbb{Z}$, the subset $\{(x, 0), (0, y)\}$ is an independent set for any nonzero elements x, y in $\mathbb{R}$. However, $\{(x, 0), (0, y)\}$ is not maximal independent in $\mathbb{R} \times \mathbb{R}$. It can be easily verified that the sets

$$\left\{(x, 0), (0, y), \left(x\sqrt{2}, 0\right)\right\} \text{ and } \left\{(x, 0), (0, y), \left(0, \sqrt[5]{7}y\right)\right\}$$

are also independent sets in $\mathbb{R} \times \mathbb{R}$.

9. Consider the group $(\mathcal{M}_{3\times 2}(\mathbb{Z}), +)$. The subset $\{E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32}\}$ is an independent set in $\mathcal{M}_{3\times 2}(\mathbb{Z})$. For if the sum

$$E_{11}^{k_{11}} + E_{12}^{k_{12}} + E_{21}^{k_{21}} + E_{22}^{k_{22}} + E_{31}^{k_{31}} + E_{32}^{k_{32}} = 0_{3\times 2}$$

then

$$k_{11}E_{11} + k_{12}E_{12} + k_{21}E_{21} + k_{22}E_{22} + k_{31}E_{31} + k_{32}E_{32} = 0_{3\times 2}.$$

According to which

$$\begin{pmatrix} k_{11} & k_{21} \\ k_{21} & k_{22} \\ k_{31} & k_{32} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus, each $k_{ij} = 0$, and each $E_{ij}^{k_{ij}} = k_{ij}E_{ij} = 0_{3\times 2}$ for each $1 \leq i \leq 2, 1 \leq j \leq 3$. The set $\{E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32}\}$ is an example of a maximal independent subset of $\mathcal{M}_{3\times 2}(\mathbb{Z})$ (Check!). The subset $\{E_{12}, E_{21}, E_{22}, E_{32}\}$ is also independent, but it is not maximal independent as it is contained in $\{E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32}\}$. In general, one can show that the set $\left\{E_{ij} : 1 \leq i \leq m \wedge 1 \leq j \leq n\right\}$ is a maximal independent subset in $\mathcal{M}_{m\times n}(\mathbb{Z})$.

The proof of the following lemma is straightforward and left to the reader.

Lemma 9.3.3 *Let G be an abelian group. The set $\{a_1, a_2, \ldots, a_n\}$ is an independent subset of G if and only if it is independent in every subgroup of G containing $a_1, a_2, \ldots, a_n$.*

Lemma 9.3.4 *Let G be an abelian group and $c_1, c_2, \ldots, c_n$ be any integers. If $\{a_1, a_2, \ldots, a_n\}$ is an independent subset of G and $a_i^{c_i} \neq e$ for $1 \leq i \leq n$, then the set $\left\{a_1^{c_1}, a_2^{c_2}, \ldots, a_n^{c_n}\right\}$ is independent.*

Proof Assume that there exist integers $k_1, k_2, \ldots, k_n$ such that

$$\left(a_1^{c_1}\right)^{k_1} * \left(a_2^{c_2}\right)^{k_2} * \cdots * \left(a_n^{c_n}\right)^{k_n} = e,$$

and $a_i^{c_i} \neq e$ for each $1 \leq i \leq n$. By Proposition 5.5.2,

$$a_1^{c_1k_1} * a_2^{c_2k_2} * \cdots * a_n^{c_nk_n} = e.$$

Since $\{a_1, a_2, \ldots, a_n\}$ is independent, then $\left(a_i^{c_i}\right)^{k_i} = a_i^{c_ik_i} = e$ for each $1 \leq i \leq n$, as required. ■

Example 9.3.5 Consider the additive group $\mathbb{Z}_2 \times \mathbb{Z}_3$. Let $a_1 = ([1], [1])$ and $a_2 = ([0], [1])$. The set $\{a_1, a_2\}$ is not independent (Check with $k_1 = 2$ and $k_2 = -2$). However,

$$a_1^3 = ([1],[1])^3 = ([1],[0]) \text{ and } a_2^1 = ([0],[1]).$$

Therefore, the set $\{a_1^3, a_2^1\}$ is independent.

The above example shows that the converse of the result in Lemma 9.3.4 is not always true. However, in several special cases, such as those of p-groups, the following statement holds:

Proposition 9.3.6 *Let p be a prime, G a finite abelian p-group, and $\{a_1, a_2, \ldots, a_n\}$ any subset of G such that for all $1 \le i \le n$, $a_i^p \neq e$. The set $\{a_1^p, a_2^p, \ldots, a_n^p\}$ is independent if and only if $\{a_1, a_2, \ldots, a_n\}$ is independent.*

Proof Assume that $\{a_1^p, a_2^p, \ldots, a_n^p\}$ is independent. For each $1 \le i \le n$, $a_i^p \neq e$, which implies that $a_i \neq e$ for each $1 \le i \le n$. Let $k_1, k_2, \ldots, k_n$ be integers such that

$$a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n} = e.$$

We show that $a_i^{k_i} = e$ for each $1 \le i \le n$, as follows:

The group G is abelian. Therefore, the equality $a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n} = e$ implies that

$$\left(a_1^p\right)^{k_1} * \left(a_2^p\right)^{k_2} * \cdots * \left(a_n^p\right)^{k_n} = \left(a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n}\right)^p = e.$$

As $\{a_1^p, a_2^p, \ldots, a_n^p\}$ is an independent set, then $\left(a_i^p\right)^{k_i} = e$ for all $1 \le i \le n$. By Lemma 5.5.6, $\text{ord}\left(a_i^p\right) | k_i$ for each $1 \le i \le n$. Since $a_i^p \neq e$ and G is a p-group, then $\text{ord}\left(a_i^p\right) = p^{s_i}$ for some integer $s_i \ge 1$. Therefore, $p | k_i$. For each $1 \le i \le n$, let $k_i = pm_i$ for some $m_i \in \mathbb{Z}$. Hence,

$$e = a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n} = \left(a_1^p\right)^{m_1} * \left(a_2^p\right)^{m_2} * \ldots * \left(a_n^p\right)^{m_n}.$$

Since $\{a_1^p, a_2^p, \ldots, a_n^p\}$ is independent, then by Lemma 9.3.4, $\left\{\left(a_1^p\right)^{m_1}, \left(a_2^p\right)^{m_2}, \ldots, \left(a_n^p\right)^{m_n}\right\}$ is independent, and thus, $a_i^{k_i} = \left(a_i^p\right)^{m_i} = e$, as required. The other direction directly follows by Lemma 9.3.4. ■

Definition 9.3.7 Let G be a group, and $a_1, a_2, \ldots, a_n$ be distinct elements in G. The set $\{a_1, a_2, \ldots, a_n\}$ is called a spanning set of G if $G = \langle a_1, a_2, \ldots, a_n \rangle$. In this case, we say that $\{a_1, a_2, \ldots, a_n\}$ spans G.

Example 9.3.8

1. A cyclic group generated by an element a has a spanning set $\{a\}$. For example, each of the sets $\{1\}$, $\{-1\}$, and $\{-1, 1\}$ are spanning sets of $(\mathbb{Z}, +)$.
2. Let $n \in \mathbb{N}$. Consider the regular n-polygon with the center at the origin and one of its vertices at $(1, 0)$. The set that consists of the rotation of such a polygon in the plane around the origin with angle $\frac{2\pi}{n}$ and reflection around the x-axis forms a spanning set for all symmetries of the polygon.

3. Example 7.3.14 shows that $\{(1\ 2), (2\ 3\ 4 \cdots n)\}$ is a spanning set of $\mathfrak{S}_n$.
4. Let G be a group and $a_1, a_2, \dots, a_n$ be generators of G (Definition 7.3.2). The set $\{a_1, a_2, \dots, a_n\}$ is a spanning set of G.

Definition 9.3.9 Let G be an abelian group and $a_1, a_2, \dots, a_n$ be distinct elements in G. The set $\{a_1, a_2, \dots, a_n\}$ is called a basis of G if $\{a_1, a_2, \dots, a_n\}$ is an independent subset of G that spans the whole group G. If such a subset exists, we say that G admits a basis.

Remark 9.3.10

1. If G is an abelian group, then by Proposition 7.3.6 the set $\{a_1, a_2, \dots, a_n\}$ spans G if and only if for each $a \in G$, $a = a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n}$ for some integers $k_1, k_2, \dots, k_n$.
2. The empty set $\emptyset$ is a basis for the trivial group $G = \{e\}$. The set $\emptyset$ is an independent set, and as $\langle \emptyset \rangle = \{e\}$ (Sect. 7.3), $\emptyset$ is a spanning set of $\{e\}$.
3. If G is a cyclic group generated by a nonidentity element a, then $\{a\}$ forms a basis for G.
4. A basis for an abelian group G may not be unique. For example, both $\{1\}$ and $\{-1\}$ are bases for $(\mathbb{Z}, +)$. Note that the set $\{1, -1\}$ generates $(\mathbb{Z}, +)$, but it does not form a basis for $(\mathbb{Z}, +)$ since it is not an independent set (Check!).
5. A basis for an abelian group G is a maximal independent subset (Exercise 9.33).

Example 9.3.11 Let q be a prime and $G = \mathbb{Z}_{q^2} \times \mathbb{Z}_{q^2}$. Let $a_1 = ([1], [q])$, $a_2 = ([q], [q])$. The set $\{a_1, a_2\}$ is independent and maximal independent but not a spanning set of G.

- Note that none of the elements a_i is an identity of G. To show that $\{a_1, a_2\}$ is independent, let $a_1^{k_1} \oplus_{q^2} a_2^{k_2} = ([0], [0])$ for some integers k_1, k_2, then we have

$$\begin{aligned}([1], [q])^{k_1} \oplus_{q^2} ([q], [q])^{k_2} &= ([k_1], [k_1 q]) \oplus_{q^2} ([k_2 q], [k_2 q])\big) \\ &= ([k_1 + k_2 q], [k_1 q + k_2 q]) = ([0], [0])\end{aligned}$$

which implies that

$$k_1 + k_2 q \equiv 0 \bmod q^2 \ \text{ and } \ k_1 q + k_2 q \equiv 0 \bmod q^2.$$

By subtracting these equations, we obtain $k_1 - k_1 q \equiv 0 \bmod q^2$, i.e., $q^2 | k_1(1-q)$. As $\gcd\big(q^2, 1-q\big) = 1$ (Exercise 2.11), then q^2 divides k_1, which yields that $a_1^{k_1} = ([k_1], [k_1 q]) = ([0], [0])$ in $\mathbb{Z}_{q^2} \times \mathbb{Z}_{q^2}$ implying that

$$a_2^{k_2} = ([0], [0]) \oplus_{q^2} a_2^{k_2} = a_1^{k_1} \oplus_{q^2} a_2^{k_2} = ([0], [0]).$$

Therefore, $\{a_1, a_2\}$ is an independent set.

- To show that $\{a_1, a_2\}$ is maximal independent, assume that $y = ([b], [c])$ is a nonzero element in G. We show that the set $\{a_1, a_2, y\}$ cannot be independent as follows: Let $k_3 = \begin{cases} 1 \text{ if } q|b \text{ and } q|c \\ q \text{ if } q\nmid b \text{ or } q\nmid c \end{cases}$. The integer $k_3 \in \mathbb{Z}$, and $y^{k_3} \neq ([0], [0])$ (Verify!). However, both components of $y^{k_3} = k_3([b], [c])$ are divisible by q, i.e., $y^{k_3} = ([qm], [qn])$ for some $m, n \in \mathbb{Z}$. By putting $k_1 = -q(m-n)$ and $k_2 = -n$, one gets

$$y^{k_3} * a_2^{k_2} * a_1^{k_1} = ([qm], [qn]) - ([nq], [nq]) - \big([q(m-n)], \big[q^2(m-n)\big]\big) = ([0], [0]).$$

Since $y^{k_3} \neq ([0], [0])$, the set $\{a_1, a_2, y\}$ is not independent.

- The set $\{a_1, a_2\}$ is not a spanning set of G since $([1], [1]) \in G$, and $([1], [1])$ cannot be generated by $\{a_1, a_2\}$. If $([1], [1]) = a_1^{k_1} \oplus_{q^2} a_2^{k_2} = k_1a_1 \oplus_{q^2} k_2a_2$ for some integers k_1, k_2, then

$$([1], [1]) = ([k_1 + k_2q], [k_1q + k_2q]).$$

That is, $(k_1 + k_2)q = k_1q + k_2q \equiv 1 \bmod q^2$, which implies that $q|1$ (Exercise 3.3) contradicting $q > 1$.

If $a_1, a_2, \dots, a_n$ are elements in an abelian group G, then the subgroups $\langle a_i \rangle$ are normal for each $1 \leq i \leq n$. The following proposition follows directly from Proposition 7.5.18, where $\langle a_i \rangle$ is replacing the subgroup H_i.

Proposition 9.3.12 *Let G be a finite abelian group, and $a_1, a_2, \dots, a_n$ be elements in G such that $a_i \neq e$ for each $1 \leq i \leq n$. The set $\{a_1, a_2, \dots, a_n\}$ is an independent subset in G if and only if*

$$\langle a_i \rangle \cap \big\langle \cup_{j\neq i} \langle a_j \rangle \big\rangle = \{e\} \text{ for each } 1 \leq i \leq n.$$

Corollary 9.3.13 *Let G be a finite abelian group. The group G is an internal direct product of cyclic subgroups if and only if G admits a basis.*

Proof Assume that $\{a_1, a_2, \dots, a_n\}$ forms a basis of G. Since $G = \langle a_1, a_2, \dots, a_n \rangle$, and each $\langle a_i \rangle$ is normal subgroup of G, then by Proposition 7.5.13,

$$G = \langle a_1, a_2, \dots, a_n \rangle = \langle a_1 \rangle \langle a_2 \rangle \langle a_3 \rangle \cdots \langle a_n \rangle.$$

Since $\{a_1, a_2, \dots, a_n\}$ is independent, then by Proposition 9.3.12, $\langle a_i \rangle \cap \big\langle \cup_{j\neq i} \{a_j\} \big\rangle = \{e\}$. Therefore, G is an internal direct product of cyclic subgroups (Definition 7.6.5). For the other direction, assume that G is an internal direct product of $H_i = \langle a_i \rangle$ for some $a_1, a_2, \dots, a_n$ in G. Consider the set of generators of H_i, i.e.,

$a_1, a_2, \ldots, a_n$ $1 \le i \le n$. We show that $\{a_1, a_2, \ldots, a_n\}$ forms a basis for G. Since G is an internal direct product of H_i, and $\bigcup_i H_i \subseteq \langle a_1, a_2, \ldots, a_n\rangle$, then

$$G = H_1 H_2 \cdots H_n = \langle \cup_i H_i \rangle \subseteq \langle a_1, a_2, \ldots, a_n\rangle$$

i.e., $\{a_1, a_2, \ldots, a_n\}$ spans G. To show the independence, assume that $a_1^{k_1} * a_2^{k_2} * \ldots * a_n^{k_n} = e$ for some integers $k_1, k_2, \ldots, k_n$. Since G is abelian, then for each $a_i \in \{a_1, a_2, \ldots, a_n\}$,

$$a_i^{k_i} = a_1^{-k_1} * a_2^{-k_2} * \cdots * a_{i-1}^{-k_{i-1}} * a_{i+1}^{-k_{i+1}} * \cdots * a_n^{-k_n} \in \left\langle \cup_{j \neq i} H_j \right\rangle.$$

Moreover $a_i^{k_i} \in H_i$, and thus, $a_i^{k_i} \in H_i \cap \langle \cup_{j\neq i} H_i \rangle = \{e\}$. Consequently, $a_i^{k_i} = e$. ■

The following corollary follows by Exercise 8.6 and the fact that any subgroup of a p-group is also a p-group.

Corollary 9.3.14 *Let p be prime and G a finite abelian p-group.*

1. The group G is an internal direct product of cyclic p-subgroups if and only if G admits a basis.
2. If G admits a basis, then G is isomorphic to a direct product of cyclic p-groups.

i.e., $G \cong \prod\limits_{k_i} \mathbb{Z}_{p^{k_i}}$ for some nonnegative integers k_i.

Example 9.3.15 The Klein group (Example 5.2.2) is an example of a finite abelian 2-group that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is a direct product of cyclic 2-groups. One can easily check that the subset of two nonidentity elements in the Klein group forms a basis for it.

9.4 The Fundamental Theorem of Finite Abelian Groups

The goal of this section is to prove that any finite abelian group is isomorphic to a direct product of primary cyclic groups. This result is known as the fundamental theorem of finite abelian groups, referred to by "The Basis Theorem"(Rotman, 1995).

Theorem 9.4.1 (Fundamental theorem of finite abelian groups) *Every finite abelian group is isomorphic to a direct product of primary cyclic groups. i.e., if G is a nontrivial finite abelian group, then there exists a positive integer n, primes $p_1, p_2, \ldots, p_n$ (not necessarily distinct) and positive integers $k_1, k_2, \ldots, k_n$ such that*

$$G \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{k_i}}.$$

By Corollary 9.2.17, any nontrivial finite abelian group is isomorphic to the direct product of its primary components. Therefore, to prove Theorem 9.4.1, we show that any p- component of a nontrivial finite abelian group is isomorphic to a direct product of cyclic p-groups. In fact, we will prove that any finite abelian p-group is isomorphic to a direct product of cyclic p-groups. For this, using the result in Corollary 9.3.14 (2), it suffices to show that any finite abelian p-group admits a basis. This will be the goal for this section and will be realized by proving the following statements regarding any prime p.

- Any finite abelian group G such that $pG = \{e\}$ admits a basis.
- If G is a finite abelian p-group, then any basis of pG can be extended to a basis for G.
- Every finite abelian p-group admits a basis.

We begin by proving several necessary results regarding p-groups. Recall that if G is abelian, then $mG = \{a^m : a \in G\}$ is a subgroup of G for any integer m, and the exponent of G is the smallest positive integer m such that $mG = \{e\}$.

Lemma 9.4.2 *Let p be a prime and G be a finite abelian group such that $pG = \{e\}$.*

1. The order of any nonidentity element in G equals p. Therefore,

$$pG = \{e\} \Longleftrightarrow G = \{e\} \text{ or } \mathrm{Exp}(G) = p.$$

2. For any $a \in G$ and $n \in \mathbb{Z}$ such that $p \nmid n$, there exists $s \in \mathbb{Z}$ such that $a^{sn} = a$.

Proof

1. Let $a \in G$ such that $a \neq e$. As $pG = \{e\}$, then $a^p = e$, and thus, by Lemma 5.5.6, $\mathrm{ord}(a)$ divides p, which implies that $\mathrm{ord}(a)$ is either 1 or p. Since $a \neq e$, then $\mathrm{ord}(a) = p$. Therefore, if $G \neq \{e\}$, then p is the smallest positive integer such that $pG = \{e\}$, i.e., $\mathrm{Exp}(G) = p$. The other direction is straightforward.
2. Assume that $n \in \mathbb{Z}$ is an arbitrary element. If p does not divide n, then $\gcd(p, n) = 1$. By Bézout's lemma (Theorem 2.5.1), there exist $r, s \in \mathbb{Z}$ such that $rp + sn = 1$, and thus,

$$a = a^1 = a^{rp+sn} = a^{rp} * a^{sn} = e * a^{sn} = a^{sn} \qquad \blacksquare$$

Proposition 9.4.3 *Let p be a prime and G be a finite abelian group such that $pG = \{e\}$. Any maximal independent subset of G spans G. Therefore, any maximal independent subset of G forms a basis of G.*

Proof Assume that $\{a_1, a_2, \dots, a_n\}$ is a maximal independent subset of G. To prove the proposition, it suffices to show that $G \subseteq \langle a_1, a_2, \dots, a_n\rangle$. The other inclusion follows since G is a group. Let $y \in G$ be an arbitrary element. As $\{a_1, a_2, \dots, a_n, y\}$ is not independent, then there exist $k_1, \dots, k_n, k_{n+1} \in \mathbb{Z}$ such that $a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n} * y^{k_{n+1}} = e$, where at least one of $a_1^{k_1}, a_2^{k_2}, \dots, a_n^{k_n}, y^{k_{n+1}}$ is not the identity e. In particular, $y^{k_{n+1}} \neq e$ (if $y^{k_{n+1}} = e$, then by the independence of the set $\{a_1, a_2, \ldots, a_n\}$, all $a_1^{k_1}, a_2^{k_2}, \ldots, a_n^{k_n}$ are equal to e). Therefore, $p \nmid k_{n+1}$. According to Lemma 9.4.2, there exists $c \in \mathbb{Z}$ such that $y = y^{c\ k_{n+1}}$. Therefore,

$$y = \left(y^{k_{n+1}}\right)^c = \left(a_1^{-k_1} * a_2^{-k_2} * \cdots * a_n^{-k_n}\right)^c = a_1^{-ck_1} * a_2^{-ck_2} * \cdots * a_n^{-ck_n} \in \langle a_1, a_2, \ldots, a_n \rangle$$

and $\{a_1, a_2, \ldots, a_n\}$ spans G. ■

Remark 9.4.4

- Proposition 9.4.3 is not true if one does not require that $pG = \{e\}$ for some prime p. Example 9.3.11 is an example of a maximal set that does not form a basis (not a spanning set). Note that the additive group $\mathbb{Z}_{q^2} \times \mathbb{Z}_{q^2}$ is a q- group, but it does not satisfy $pG = \{e\}$ for any prime p.
- Let p be a prime and G be a finite abelian group. As any basis of G forms a maximal independent set (Exercise 9.33), if $pG = \{e\}$, then any subset of G forms a basis if and only if it is a maximal independent subset of G.

Corollary 9.4.5 *Let p be a prime and G be a finite abelian group such that $pG = \{e\}$. Any independent subset of G can be completed to a basis. i.e., if $\{a_1, a_2, \ldots, a_r\}$ is an independent subset in G, then there exist $a_{r+1}, a_{r+2}, \ldots, a_n$ elements in G, such that $\{a_1, a_2, \ldots, a_r, a_{r+1}, a_{r+2}, \ldots, a_n\}$ forms a basis for G.*

Proof Assume that $B_0 = \{a_1, \ldots, a_r\}$ is an independent set in G. If B_0 is a maximal independent, then it forms a basis (Proposition 9.4.3); otherwise, $G \neq \langle a_1, a_2, \ldots, a_r \rangle$, and thus, select $a_{r+1} \in G \backslash \langle a_1, a_2, \ldots, a_r \rangle$ and let $B_1 = \{a_1, \ldots, a_r, a_{r+1}\}$. The subset B_1 is independent (Exercise 9.13). If B_1 is a maximal independent, then B_1 forms a basis; otherwise, $G \neq \langle a_1, a_2, \ldots, a_{r+1} \rangle$. Pick $a_{r+2} \in G \backslash \langle a_1, a_2, \ldots, a_{r+1} \rangle$, and let $B_2 = \{a_1, \ldots, a_{r+1}, a_{r+2}\}$. The subset B_2 is independent (Check!). If B_2 is maximal independent, then it forms a basis; otherwise, the same process is continued. If B_k is not maximal independent, we form the independent set B_{k+1} such that $B_k \subseteq B_{k+1}$. Since G is finite, the process will be terminated, and the last independent set that we obtain is maximal. ■

As the empty set is an independent subset of any group G and under the conditions of the last corollary, the above construction can be initiated with an empty set B_0 that can be made into a basis. Hence, the following corollary is easily obtained.

Corollary 9.4.6 *Let p be a prime. Any finite abelian group G such that $pG = \{e\}$ admits a basis.*

Lemma 9.4.7 *Let p be a prime and G a finite abelian p-group. If $\{a_1, \ldots, a_n\}$ is a basis for pG, then there exists a basis $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ for G such that $a_i = b_i^p$, $1 \leq i \leq n$.*

Proof Let $H = pG = \{b^p : b \in G\}$ and $\{a_1, \ldots, a_n\}$ be a basis for H. According to the definition of H, for each $1 \leq i \leq n$, there exists $b_i \in G$ such that $a_i = b_i^p$. By Proposition 9.3.6, the set $\{b_1, \ldots, b_n\}$ is an independent set. On other hand,

$$p\langle b_1, \ldots, b_n\rangle = \left\langle b_1^p, \ldots, b_n^p\right\rangle = \langle a_1, \ldots, a_n\rangle = H = pG.$$

These equations do not imply that $\langle b_1, \ldots, b_n\rangle = G$ (Example 7.3.22) because several elements in G can be eliminated by p and will not appear in $pG = H$. Such elements are $G[p] = \{b \in G : b^p = e\}$. To form a basis for G, we use the set $\{b_1, \ldots, b_n\}$ and add to it the elements of a basis of $G[p]$. However, after adding these elements to $\{b_1, \ldots, b_n\}$, the new set may not be independent. To avoid this problem, we only add the basis elements from $G[p]$ that ensure that the new obtained set is independent. To do this, the following steps are used: Consider the set $\{b_1, \ldots, b_n\}$. As $\{b_1, \ldots, b_n\}$ is a subset of the p-group G and $b_i^p = a_i \neq e$, then for each $1 \leq i \leq n$, $\text{ord}(b_i) = p^{s_i}$ for some $s_i > 1$. Let $w_i = b_i^{p^{s_i-1}}$. Clearly, that $w_i \neq e$, and $w_i \in G[p]$. As $\{b_1, \ldots, b_n\}$ is an independent set, then by Lemma 9.3.4, the set $\{w_1, \ldots, w_n\}$ is also independent in G. According to Lemma 9.3.3, $\{w_1, \ldots, w_n\}$ is an independent subset of $G[p]$. As $pG[p] = \{e\}$, then by Corollary 9.4.5, the set $\{w_1, \ldots, w_n\}$ can be extended to a basis for $G[p]$. Let $\{w_1, \ldots, w_n, v_1, \ldots, v_m\}$ be a basis for $G[p]$. By adding the elements $v_1, \ldots, v_m$ to the set $\{b_1, \ldots, b_n\}$, we obtain the required basis for G. Namely, we show that $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ forms a basis for G, as follows:

- To show that $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ is independent, assume

$$b_1^{k_1} * b_2^{k_2} * \cdots * b_n^{k_n} * v_1^{l_1} * v_2^{l_2} * \cdots * v_m^{l_m} = e. \quad (*)$$

for some integers $k_1, k_2, \ldots k_n, l_1, l_2, \ldots, l_m$. As $v_j \in G[p]$, the equation in $(*)$ implies that

$$\begin{aligned} e &= \left(b_1^{k_1} * b_2^{k_2} * \cdots * b_n^{k_n} * v_1^{l_1} * v_2^{l_2} * \cdots * v_m^{k_m}\right)^p \\ &= b_1^{pk_1} * b_2^{pk_2} * \cdots * b_n^{pk_n} * e * e * \cdots * e = b_1^{pk_1} * b_2^{pk_2} * \cdots * b_n^{pk_n}. \end{aligned}$$

As $\{b_1, \ldots, b_n\}$ is independent, then so is $\left\{b_1^p, \ldots, b_n^p\right\}$, which implies that $b_i^{pk_i} = e$ for each $1 \leq i \leq n$. Hence, $\text{ord}(b_i) = p^{s_i}$ divides pk_i. i.e., $k_i = t_i p^{s_i-1}$. Substituting k_i in Equation $(*)$, where $w_i = b_i^{p^{s_i-1}}$ yields

$$\begin{aligned} e &= b_1^{t_1 p^{s_1-1}} * b_2^{t_2 p^{s_2-1}} * \cdots * b_n^{t_n p^{s_n-1}} * v_1^{l_1} * v_2^{l_2} * \cdots * v_m^{l_m} \\ &= w_1^{t_1} * w_2^{t_2} * \cdots * w_n^{t_n} * v_1^{l_1} * v_2^{l_2} * \cdots * v_m^{l_m}. \end{aligned}$$

As $\{w_1, \cdots, w_n, v_1, \cdots, v_m\}$ are independent, then $w_i^{t_i} = e$ for all $1 \leq i \leq n$, and $v_j^{l_j} = e$ for all $1 \leq j \leq m$. Therefore, $b_i^{k_i} = b_i^{t_i p^{s_i-1}.} = w_i^{t_i} = e$ and $v_j^{l_j} = e$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Therefore, the set $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ is an independent subset of G.

– To show that $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ spans G, assume that $a \in G$. Since $a^p \in pG$ and

$pG = H = \langle a_1, \ldots, a_n \rangle$, there exist $k_1, k_2, \ldots, k_n$ such that

$$a^p = a_1^{k_1} * \cdots * a_n^{k_n} = b_1^{pk_1} * \cdots * b_n^{pk_n}.$$

Therefore, $a^p * b_1^{-pk_1} * \cdots * b_n^{-pk_n} = e$, which yields $\left(a * b_1^{-k_1} * \cdots * b_n^{-k_n}\right)^p = e$, and thus, $a * b_1^{-k_1} * \cdots * b_n^{-k_n} \in G[p]$. As $\{w_1, \ldots, w_n, v_1, \ldots, v_m\}$ is a basis for $G[p]$, then there exist integers $l_1, l_2, \ldots, l_n, t_1, t_2, \ldots, t_m$ such that

$$\begin{aligned} a * b_1^{-k_1} * \cdots * b_n^{-k_n} &= w_1^{l_1} * \cdots * w_n^{l_n} * v_1^{t_1} * \cdots * v_m^{t_m} \\ &= b_1^{l_1 p^{s_1 - 1}} * \cdots * b_n^{l_n p^{s_n - 1}} * v_1^{t_1} * \cdots * v_m^{t_m} \end{aligned}$$

i.e.,

$$a = b_1^{k_1 + l_1 p^{s_1 - 1}} * \cdots * b_n^{k_n + l_n p^{s_n - 1}} * v_1^{t_1} * \cdots * v_m^{t_m} \in \langle b_1, \ldots, b_n, v_1, \ldots, v_m \rangle.$$

Therefore, $\{b_1, \ldots, b_n, v_1, \ldots, v_m\}$ forms a basis for G. ■

Recall that for a finite group, an exponent always exists, and for a finite p-group, the exponent is of the form p^k, where k is a nonnegative integer.

Theorem 9.4.8 *Let p be a prime. Every finite abelian p-group admits a basis.*

Proof Let p be a prime and G be a finite abelian p-group. By Corollary 9.2.6, $\text{Exp}(G) = p^k$ for some integer $k \geq 0$. We show the result by induction on k as follows: If $pG = \{e\}$ ($k = 0$, or $k = 1$), then the result is given in Corollary 9.4.6. For the inductive step, assume that $k \geq 1$ and the statement is true for k, i.e., any finite abelian group of exponent p^k admits a basis. Let G be a finite abelian group whose exponent is p^{k+1} and let $H = pG$. Since $p^k H = p^{k+1} G$, then H has the exponent p^k. By the induction hypothesis, H admits a basis, which means that pG admits a basis. Therefore, Lemma 9.4.7 implies that the group G admits a basis, and the result is satisfied. ■

By Theorem 9.4.8 and Corollary 9.3.14 (2), the following corollary is obtained.

Corollary 9.4.9 *Let p be prime. Every finite abelian p-group is isomorphic to a direct product of cyclic p-groups.*

By Proposition 9.2.2, any finite abelian cyclic p-group is $\mathbb{Z}_{p^k}$ for some nonnegative integer k. Therefore, if G is a finite abelian p-group, then there exist $k_1, k_2, \ldots, k_s$ such that $G \cong \prod_{i=1}^{s} \mathbb{Z}_{p^{k_i}}$. Since any p-component of an abelian group is a nontrivial p-group (Proposition 9.2.12), the following result is obtained.

Corollary 9.4.10 *Let G be a nontrivial finite abelian group, p be a prime divisor of $|G|$, and G_p be the p-component of G. There exist positive integers $k_1, k_2, \ldots, k_s$ such that $G_p \cong \prod_{j=1}^{s} \mathbb{Z}_{p^{k_j}}$.*

Proof of Theorem 9.4.1 Assume that G is a finite abelian group. If $G = \{e\}$, then $G = \{e\} \cong \mathbb{Z}_1$ is a direct product of one primary cyclic group. Assume that $G \neq \{e\}$ and let $p_1, \ldots, p_m$ be all distinct prime divisors of $|G|$. According to Corollary 9.2.17,

$$G \cong \prod_{i=1}^{m} G_{p_i} = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_m}$$

where G_{p_i} is the p_i-component of G. Since every component of G_{p_i} is isomorphic to $\prod_{j=1}^{s_i} \mathbb{Z}_{p_i^{k_j}}$ for some positive integers $k_1, k_2, \ldots, k_{s_i}$ (Corollary 9.4.10), then

$$G \cong \prod_{j=1}^{s_1} \mathbb{Z}_{p_1^{k_j}} \times \prod_{j=1}^{s_2} \mathbb{Z}_{p_2^{k_j}} \times \cdots\cdots \times \prod_{j=1}^{s_m} \mathbb{Z}_{p_m^{k_j}}.$$

If one does not require that $p_1, \ldots, p_m$ are distinct, the result follows. ∎

Example 9.4.12 Let G be a finite abelian group of order 270. As $270 = 2 \times 3^3 \times 5$, then there are three primary components of G, which are G_2, G_3, and G_5. According to Corollary 9.2.13, $|G_2| = 2$, $|G_3| = 3^3$, and $|G_5| = 5$. By Corollary 9.1.20, as both G_2, G_3 have a prime order, then

$$G_2 \cong \mathbb{Z}_2 \text{ and } G_5 \cong \mathbb{Z}_5.$$

We must find all the isomorphic groups to G_3. By Corollary 9.4.10, $G_3 \cong \prod_{i=1}^{s} \mathbb{Z}_{3^{k_i}}$ for some s and k_i. Since the order of G_3 equals 27, all possible nonisomorphic forms of G_3 are

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_9 \times \mathbb{Z}_3, \text{ and } \mathbb{Z}_{27}.$$

Therefore, G is isomorphic to one of the following groups:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$$

Exercises

Solved Exercises

9.1 Let G be an abelian group such that $|G| = pq$, where p and q distinct prime numbers. Show that G is cyclic.

Solution

As p and q divide $\operatorname{ord}(G)$, then by Cauchy's theorem (Theorem 7.7.12), there exist two nonidentity elements $a, b \in G$ such that $|\langle a\rangle| = p$ and $|\langle b\rangle| = q$. As $\langle b\rangle \cap \langle a\rangle$ is a subgroup of both $\langle a\rangle$ and $\langle b\rangle$, then by Lagrange's theorem, $|\langle b\rangle \cap \langle a\rangle|$ divides both $|\langle a\rangle|$ and $|\langle b\rangle|$, which implies that $|\langle b\rangle \cap \langle a\rangle| = 1$ and $\langle b\rangle \cap \langle a\rangle = \{e\}$. As G is abelian, then by Exercise 7.11, $|\langle a * b\rangle| = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) = \operatorname{lcm}(p, q) = pq$. That is, $\langle a * b\rangle = G$ and G is cyclic.

9.2 Let G be a finite group. Show that if $|G| = pq$, where p and q are primes, not necessarily distinct, then every proper subgroup of G is cyclic.

Solution

Let H be a proper subgroup of G. By Lagrange's theorem (Theorem 7.4.17), $|H|$ divides $|G|$. Since H is a proper subgroup of G, then all possibilities of $|H|$ are 1, p or q. If $|H| = 1$, then $|H| = \{e\}$ is cyclic. If $|H| = p$ or $|H| = q$, then H is cyclic (Example 9.1.5 (8)).

9.3 Let G be a group and a be an element in G. Show that for any $m, n \in \mathbb{N}$, the subgroup

$\langle a^m\rangle \cap \langle a^n\rangle$ is a cyclic subgroup of $\langle a\rangle$, and $\langle a^m\rangle \cap \langle a^n\rangle = \left\langle a^{\operatorname{lcm}(m,n)}\right\rangle$.

Solution

Since both $\langle a^m\rangle$ and $\left\langle a^k\right\rangle$ are subgroups of $\langle a\rangle$ (Check!), their intersection $\langle a^m\rangle \cap \langle a^n\rangle$ is a subgroup of $\langle a\rangle$. By Corollary 9.1.8 (1), this subgroup is a cyclic group. To find the corresponding generator, note that since $\operatorname{lcm}(m, n) = rm = sn$ for some integers r, s, then

$$a^{\operatorname{lcm}(m,n)} = a^{rm} \in \left\langle a^m\right\rangle \text{ and } a^{\operatorname{lcm}(m,n)} = a^{sn} \in \left\langle a^n\right\rangle$$

which implies that $\left\langle a^{\operatorname{lcm}(m,n)}\right\rangle \subseteq \langle a^m\rangle \cap \langle a^n\rangle$. On the other hand, if $a^k \in \langle a^m\rangle \cap \langle a^n\rangle$ for some integer k, then $k = rm = sn$ for some integers r, s. i.e., $m|k$ and $n|k$. By Exercise 2.24, $\operatorname{lcm}(m, n)$ divides k. i.e., $k = t\ \operatorname{lcm}(m, n)$ for some integer t. Hence, $a^k = a^{t\ \operatorname{lcm}(m,n)} \in \left\langle a^{\operatorname{lcm}(m,n)}\right\rangle$ and $\langle a^m\rangle \cap \langle a^n\rangle \subseteq \left\langle a^{\operatorname{lcm}(m,n)}\right\rangle$.

9.4 Let G be an infinite cyclic group. Show that the identity element is the only element whose order is finite.

Solution 1

As G is a cyclic infinite group, then by Theorem 9.1.19, $G \cong (\mathbb{Z}, +)$. Since 0 is the only element in $\mathbb{Z}$ whose order is finite, then Proposition 8.3.7 implies the results.

Solution 2

Since G is an infinite cyclic group, then $G = \langle a \rangle$ for some $a \in G$, where a has an infinite order. Assume that there exists $b \neq e$ in G such that $\operatorname{ord}(b) = m$. As $b \in \langle a \rangle$, then $b = a^k$ for some nonzero integer k. Therefore, $e = b^m = \left(a^k\right)^m = a^{km}$, which implies that $\operatorname{ord}(a)$ is finite (Lemma 5.5.5).

9.5 Give an example for a group G and a subgroup H of G such that G/H is cyclic and G is not abelian. (Compare the result of this question with the result of Proposition 9.1.4).

Solution

Let $n \in \mathbb{N}$ where $n \geq 4$. Consider the symmetric group $\mathfrak{S}_n$ and its subgroup of all even permutations $\mathcal{A}_n$. Since the quotient group $\mathfrak{S}_n/\mathcal{A}_n$ has only two elements (Proposition 7.7.9), then it is cyclic (Example 9.1.5 (8)). However, neither $\mathfrak{S}_n$ nor $\mathcal{A}_n$ is abelian.

9.6 Let G be any group. Show that if K is a subgroup of G contained in the center of G and G/K is cyclic, then G is abelian.

Solution

Note first that every subgroup contained in the center of G is normal subgroup of G (verify!). Therefore, both K and $C(G)$ are normal subgroup of G. Applying the third fundamental theorem of group homomorphisms (Theorem 8.4.11) with $H = C(G)$, we obtain.

$$G/C(G) \cong (G/K)/(C(G)/K).$$

Since G/K is cyclic then

$$G/C(G)$$

is isomorphic to a quotient group of cyclic group, hence it is cyclic (Proposition 9.1.6). By Proposition 9.1.4, G is abelian.

9.7 Let p be a prime number. Show that the two groups $\left(\mathbb{Z}_{p-1}, \oplus_{p-1}\right)$ and $(\operatorname{Inv}(\mathbb{Z}_p), \otimes_p)$ are isomorphic.

Solution

A nice solution for this question can be easily given using Proposition 7.3.21, Theorem 9.1.19, and Lemma 5.3.3 (exercise). Alternatively, Let a be any generator of the group $\operatorname{Inv}(\mathbb{Z}_p)$ (Proposition 7.3.21). Define

$$\begin{aligned} f : \big(\mathbb{Z}_{p-1}, \oplus_{p-1}\big) &\to \big(\mathrm{Inv}\big(\mathbb{Z}_p\big), \otimes_p\big) \\ [x]_{p-1} &\mapsto \big[a^x\big]_p. \end{aligned}$$

We show that f is an isomorphism, as follows.

- To show that f is well-defined, let $[x]_{p-1}, [y]_{p-1}$ be elements in $\mathbb{Z}_{p-1}$ such that $[x]_{p-1} = [y]_{p-1}$. This implies that $x - y = (p-1)q$ for some $q \in \mathbb{Z}$. Therefore,

$$a^x = a^y a^{(p-1)q} \equiv a^y \cdot 1 \mod p$$

i.e., $a^x = a^y$ mod p, and $[a^x]_p = [a^y]_p$. Note that since $\big|\mathrm{Inv}(\mathbb{Z}_p)\big| = p - 1$, then $a^{p-1} \equiv 1\ mod\ p.$

- The map f is a homomorphism since

$$\begin{aligned} f\big([x]_{p-1} \oplus_{p-1} [y]_{p-1}\big) &= f\big([x+y]_{p-1}\big) = \big[a^{x+y}\big]_p \\ &= \big[a^x a^y\big]_p = \big[a^x\big]_p \otimes_p \big[a^y\big]_p \\ &= f\big([x]_{p-1}\big) \otimes_p f\big([y]_{p-1}\big). \end{aligned}$$

- To show that f is a bijective map, it is enough to show the injectivity of f (Exercise 1.6). As

$$\begin{aligned} Ker(f) &= \Big\{[x]_{p-1} \in \mathbb{Z}_{p-1} : \big[a^x\big]_p = [1]_p\Big\} \\ &= \big\{[x]_{p-1} \in \mathbb{Z}_{p-1} : p \mid \big(a^x - 1\big) \wedge 1 \le a^x < p\big\} \\ &= \big\{[x]_{p-1} \in \mathbb{Z}_{p-1} : p \mid \big(a^x - 1\big) \wedge 0 \le a^x - 1 < p - 1\big\} \\ &= \big\{[0]_{p-1}\big\} \end{aligned}$$

then f is an injective map. Note that proving that f is surjective is easier than proving its injectivity (Check!).

9.8 The prime numbers 3, 5, 17, 257, 65537, 4294967297, ..., which are known as Fermat numbers (Burton, 2007), are of the form of $2^{2^k} + 1$ for some $k \in \mathbb{N}$. Show that if p is a prime number such that $p \neq 2$, then

$$\mathrm{Inv}\big(\mathbb{Z}_p\big) \text{ is a primary group} \Longleftrightarrow p \text{ is a Fermat number.}$$

In this case, $\mathrm{Inv}\big(\mathbb{Z}_p\big)$ will be a 2-group.

Solution

For any prime p, the multiplicative group $\text{Inv}\big(\mathbb{Z}_p\big) = \mathbb{Z}_p^*$ is a group of order $p - 1$.

- If $p = 2$, then $\text{Inv}(\mathbb{Z}_2) = \{[1]\}$, which is a q-group for any prime q as $1 = q^0$.
- If $p \neq 2$, then $\text{Inv}\big(\mathbb{Z}_p\big)$ is a primary group if and only if $p - 1 = q^m$ for some prime q and a positive integer m, and
  - Since $p > 2$, then $q^m = p - 1$ is an even number, i.e., q must be 2,
  - Since $p = q^m + 1$, the integer m must be power of 2, i.e., $m = 2^k$ (Check that if m is not power of 2, then $q^m + 1$ is not prime).

  Therefore, $\text{Inv}\big(\mathbb{Z}_p\big)$ is a primary group if and only if $p - 1 = 2^{2^k}$ as required, and

$$\text{Inv}(\mathbb{Z}_2), \text{Inv}(\mathbb{Z}_3), \text{Inv}(\mathbb{Z}_5), \text{Inv}(\mathbb{Z}_{17}), \text{Inv}(\mathbb{Z}_{257}), \dots.$$

are all 2-groups. For a prime p such that $p \neq 2$ and p not being a Fermat number, the group $\text{Inv}\big(\mathbb{Z}_p\big)$ is not a primary group.

9.9 Show that the direct product of p-groups is a p-group.

Solution

Let $(G_1, *)$ and $(G_2, \cdot)$ be p-groups and $(a, b) \in G_1 \times G_2$ be an arbitrary element. Since both G_1, G_2 are p-groups and $a \in G_1, b \in G_2$, by definition of p-groups,

$$|ord(a)| = p^k \text{ and } |ord(b)| = p^s$$

for some nonnegative integers k, s. Let $m = \text{lcm}(k, s)$, then both p^k and p^s divide p^m(Check!). Therefore,

$$(a, b)^{p^m} = (\underbrace{a * a * \cdots * a}_{p^m \text{ times}}, \underbrace{b \cdot b \cdots b}_{p^m \text{ times}}) = \big(a^{p^m}, b^{p^m}\big) = (e_1, e_2).$$

By Lemma 5.5.6, $ord((a, b))$ divides p^m, which implies that $ord((a, b))$ is a power of p. As (a, b) is arbitrary, then $G_1 \times G_2$ is a p-group. Note that in case of both groups are finite, Proposition 9.2.2 (2) can be used to provide a one line proof (exercise).

9.10 Let p be a prime. Show that any finite nontrivial p-group has a nontrivial center.

Solution

Let G be a finite p-group. For each $a \in G$, let $C_a = \{x \in G : x * a = a * x\}$. By Exercise 7.13, C_a is a subgroup of G, and

$$|C(G)| = |G| - \sum_{C_a \neq G} [G : C_a] \qquad (*)$$

We check the orders of each term in Equation $(*)$.

- As G is a nontrivial p-group, then $|G| = p^k$ for a positive integer k (Proposition 9.2.2).
- For each $a \in G$, C_a is also a p-group (Proposition 9.2.4), which implies that $|C_a| = p^s$ for some nonnegative integer s. Therefore, for all $a \in G$, such that $C_a \neq G$, we have $1 < [G : C_a] = |G|/|C_a| = p^{k-s}$. Therefore, p divides all terms in the right side of Equation $(*)$.
- Since p divides every term in the right side of the equation, it also divides the left side. i.e., $|C(G)| \geq p$, and $C(G)$ is nontrivial.

9.11 Let p be a prime and G be a nonabelian group of order p^3. Show that $|C(G)| = p$.

Solution

Since $|G| = p^3$, then G is a p-group (Proposition 9.2.2), which implies that the center of G is not trivial (Exercise 9.10). As G is not abelian, then $C(G) \neq G$. Therefore, $C(G)$ is a subgroup of G such that $1 < |C(G)| < p^3$. By Lagrange's theorem, $|C(G)|$ divides p^3. Therefore, $|C(G)|$ is either p^2 or p. If $|C(G)| = p^2$, then $|G/C(G)| = p$ which implies that $G/C(G)$ is cyclic (Example 9.1.5 (8)). Therefore, G is abelian (Proposition 9.1.4), which contradicts the assumption. Therefore, there exists only one possibility of $|C(G)|$, which is p.

9.12 Let p be a prime and G be a finite abelian nontrivial p-group. Show that G is cyclic if and only if G has exactly one subgroup of order p.

Solution

As G is a nontrivial p-group, then $|G| = p^n > 1$ for some $n \geq 1$. Assume that G is cyclic. Since $p||G|$, then by Theorem 9.1.10, G contains a unique subgroup of order p. To show the other direction, assume that G has exactly one subgroup of order p, and hence, nontrivial. As any finite abelian p-group is isomorphic to a direct product of cyclic groups (Corollary 9.4.9), then

$$G \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_l \rangle \quad \text{for some } a_i \text{ in } G.$$

Since $\langle a_i \rangle$ is a p-group, then $|\langle a_i \rangle| = p^{k_i} > 1$, where $1 \leq i \leq l$. If $l > 1$, let

$$x = \left(a_1^{p^{k_1-1}}, \ldots, e, e\right) \text{ and } y = \left(e, a_2^{p^{k_2-1}}, \ldots, e, e\right)$$

then $\langle x \rangle \cap \langle y \rangle = \{(e, e, e, e \ldots, e)\}$ and $|\langle x \rangle| = p = |\langle y \rangle|$, which implies that G has two subgroups of order p. Therefore, $l = 1$ and G is cyclic.

9.13 Let p be any prime, G be a finite abelian group such that $pG = \{e\}$, and let $\{a_1, a_2, \ldots, a_r\}$ be an independent subset in G. Show that if $\{a_1, a_2, \ldots, a_r\}$

is not maximal independent, then there exists $a_{r+1} \in G \backslash \langle a_1, a_2, \ldots, a_r \rangle$ such that $\{a_1, a_2, \ldots, a_r, a_{r+1}\}$ is an independent subset in G.

Solution

Assume that $\{a_1, a_2, \ldots, a_r\}$ is not maximal independent. Let $\{a_1, a_2, \ldots, a_r\}$ be independent subset of G. By Corollary 9.4.5, there exist $a_{r+1}, a_{r+2}, \ldots, a_n$ in $G \ni \{a_1, a_2, \ldots, a_n\}$ is a basis. Hence, a maximal independent (Exercise 9.33). Since $\{a_1, a_2, \ldots, a_r\}$ is not independent, then $n \geq r+1$ and $\{a_1, a_2, \ldots, a_r, a_{r+1}\}$ is independent. The result follows as $a_{r+1} \notin \langle a_1, a_2, \ldots, a_r \rangle$.

Unsolved Exercises

9.14 Find all the generators of $\mathbb{Z}_{22}$.

9.15 Let G be a cyclic group generated by a, and $m, n \in \mathbb{Z}$. Show that $\left\langle a^{\gcd(m,n)} \right\rangle$ is the smallest subgroup of G that contains a^m and a^n.

9.16 Show that any abelian group of order 22 is cyclic.

9.17 Let G be a group such that $|G| = 33$. Show that every proper subgroup of G is cyclic.

9.18 Give an example of a group G and normal subgroup H of G such that both G/H and H are abelian groups, and G is not abelian.

9.19 Let G be a group and H, K be cyclic subgroups of G. Is the product HK a subgroup? Is HK cyclic? Explain your answer.

9.20 Show that any group of order p or p^2 is an abelian group.

9.21 Let p be a prime. Consider the additive group $\left(\mathbb{Z}_p, \oplus_p\right)$. Let $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. On G define the operation $*$ by

$$([a], [b], [c]) * \left([a'], [b'], [c']\right) = \left([a] \oplus_p [a'], [b] \oplus_p [b'], [c] \oplus_p [c'] \oplus_p [-ba']\right).$$

Show that $(G, *)$ is a nonabelian p-group of order p^3.

9.22 Let p be a prime. Let $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ and define the operation $*$ on G by

$$([a], [b]) * \left([a'], [b']\right) = \left([a] \oplus_p [a'], [b] \oplus_{p^2} [b'] \oplus_{p^2} [ba'p]\right).$$

Show that G is a nonabelian p-group of order p^3.

9.23 Let $p \neq 2$ be a prime number. Show that the group G in Exercise 9.21 satisfies

$$([a], [b], [c])^p = ([0], [0], [0]) \text{ for all } ([a], [b], [c]) \text{ in } G.$$

Is this statement true if $p = 2$?

9.24 Let $p \neq 2$ be a prime number. Does the group G in Exercise 9.22 satisfy

$$([a], [b])^p = ([0], [0]) \text{ for all } ([a], [b]) \text{ in } G?$$

Explain your answer and compare it with the answer for Exercise 9.21.

9.25 Compute all p-components of the additive groups $\mathbb{Z}_{12}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$, and $\mathbb{Z}_{60}$.

9.26 Show that any p-group has only one component.

9.27 Give an example (different than that in Example 9.3.5) for which the converse of the result in Lemma 9.3.4 is not true.

9.28 Let G be a finite abelian group and $|G| = 22$. Determine all groups that are isomorphic to G.

9.29 Let G be a finite abelian group. Let b be an element in G such that

$$\operatorname{ord}(b) = \max\{\operatorname{ord}(a) : a \in G\}.$$

Show that $\operatorname{ord}(a)$ divides $\operatorname{ord}(b)$ for all $a \in G$.

9.30 Show that $\operatorname{Exp}\big(\mathbb{Z}_p^*, \otimes_p\big) = p - 1$.

9.31 Let G_1, G_2 be groups and $f : G_1 \to G_2$ be a group isomorphism. Show that if the set $\{a_1, a_2, \dots, a_n\}$ forms a basis for G_1, then $\{f(a_1), f(a_2), \dots, f(a_n)\}$ forms a basis for G_2.

9.32 Show that two bases for an abelian group G may not have the same number of elements.

Hint: Show that the group $\mathbb{Z}_p \times \mathbb{Z}_q$, where $\gcd(p, q) = 1$, has two bases with two different numbers of elements.

9.33 Show that any basis of abelian group G is a maximal independent set in G.

9.34 Give an example of a prime p and two p-groups with the same order that are not isomorphic.

References

Burton, D. M. (2007). *Elementary Number Theory*. MacGraw-Hill.
Rotman, J. (1995). *An introduction to the theory of groups*. Springer-Verlag.

Chapter 10
Group Theory and Sage

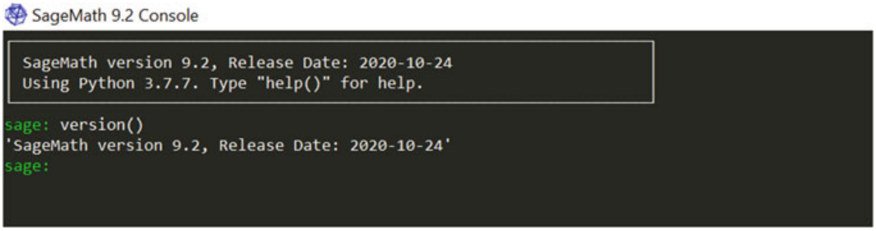
At present, almost no mathematician works without using software. Software such as MATLAB and MATHEMATICA are among the best tools for engineers and mathematicians. Moreover, there are computer software as Sage (SageMath) and CoCalc (SageMathCloud) that can help explore, compute, solve a variety of algebraic problems, and address group theory problems. Sage and CoCalc were founded by William Stein and were hosted by Sage. CoCalc is an online version that uses Sage, Latex, and Jupyter. In this chapter, we learn how to use Sage (which can be downloaded and works offline) to solve problems (typically complicated problems) in group theory. For further information regarding Sage, we refer the reader to (Zimmermann et al., 2018).

10.1 What Is Sage?

The expanded form of the term Sage is "**S**ystem for **A**lgebra and **G**eometry **E**xperimentation", which explains the role of this software. Sage is a mathematical open-source software that uses syntax and helps solve problems in Mathematics and Engineering. Problems in algebra, combinatorics, graph theory, and many other fields can be easily solved using Sage. For example, in the context of group theory, Sage contains enormous numbers of cods (commands) that are related to aspects of algebra. These commands can manipulate numbers to solve complicated linear equations. The commands can be used to identify whether a given group is cyclic, normal, or abelian. Several commands are available to compute Cayley's table for the additive and multiplicative groups of integers modulo n and find the generators of a group, among other applications.

Sage can be downloaded using the link "https://www.sagemath.org/". Note that many versions of Sage are available, these versions are regularly updated. To check the version of your software, type the command "version ()", as shown below. In this chapter, we use "SageMath version 9.2",

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0_10



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: version()
'SageMath version 9.2, Release Date: 2020-10-24'
sage:
```

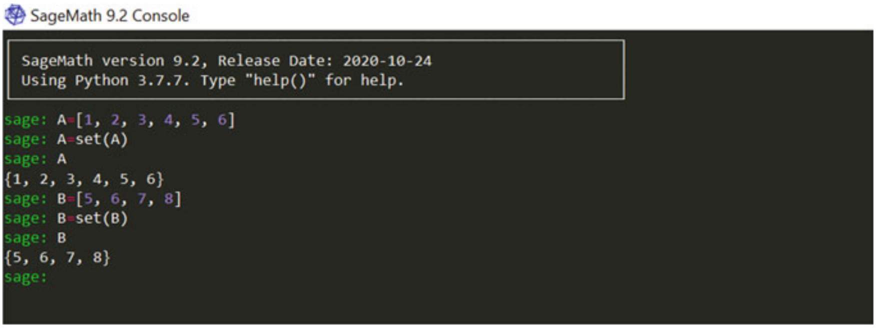
10.2 Examples for Using Sage in Group Theory

In this section, several questions that already have been solved in Chaps.1–9 will be repeated using Sage. By applying Sage's commands, many problems can be solved in an efficient manner. We begin by considering basic operations on sets and learn several commands and then move to deeper problems pertaining to group theory. We explain the usage and template for each adopted command. All the images of the commands in this chapter have been extracted from Sage sessions of the Sage official software (SageMath, 2021). The reader may refer to (Zimmermann et al., 2018) and (Anastassiou & Mezei, 2015) to try other Sage commands.

10.2.1 Commands Related to Sets and Basic Operations

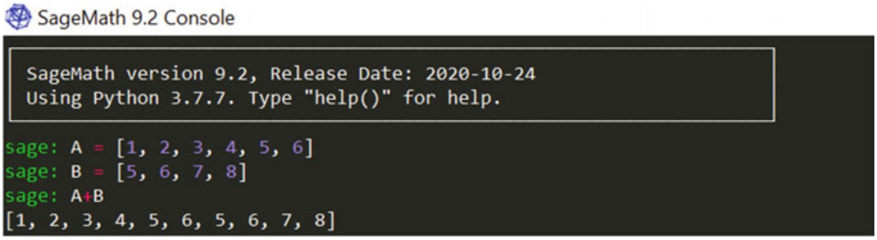
To begin working with Sage, we must define (inform the software about) the objects that we intend to deal with. The objects can be defined by typing the elements of such object in a list with two square brackets. In this manner, Sage stores the values of the objects and uses them if needed. For example, typing $A = [1, 2, 3, 4, 5, 6]$ stores A as the list of elements $1, 2, 3, 4, 5, 6$ in the same given order. The list A remains stored and is not viewed unless a command asks Sage to do so. Many commands in Sage can be used to view the output. For example, if $A = [1, 2, 3, 4, 5, 6]$ is encoded in Sage, then any time a user types "A" or "A.list()" and presses ENTER, the stored value of A will be presented.

The command "set()" in Sage is used to store an object as a set. After applying this command, the input is considered a set and remains as a set unless its format is changed by another command. For example, typing A $= [1, 2, 3, 4, 5, 6]$ drives Sage to consider A to be the list $1, 2, 3, 4, 5, 6$. To consider A as a set, the command "$A = \text{set}(A)$" is used. See the following example.



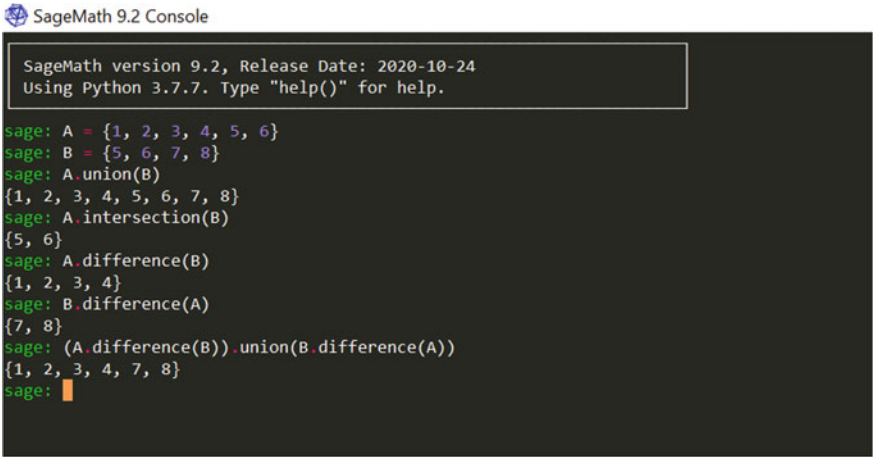
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A=[1, 2, 3, 4, 5, 6]
sage: A=set(A)
sage: A
{1, 2, 3, 4, 5, 6}
sage: B=[5, 6, 7, 8]
sage: B=set(B)
sage: B
{5, 6, 7, 8}
sage:
```

It is possible to merge two lists that are previously encoded using the symbol "+". For example, in the following display box, the command "+" joins the two lists A and B and the elements of the two lists in the same order without deleting any common elements.



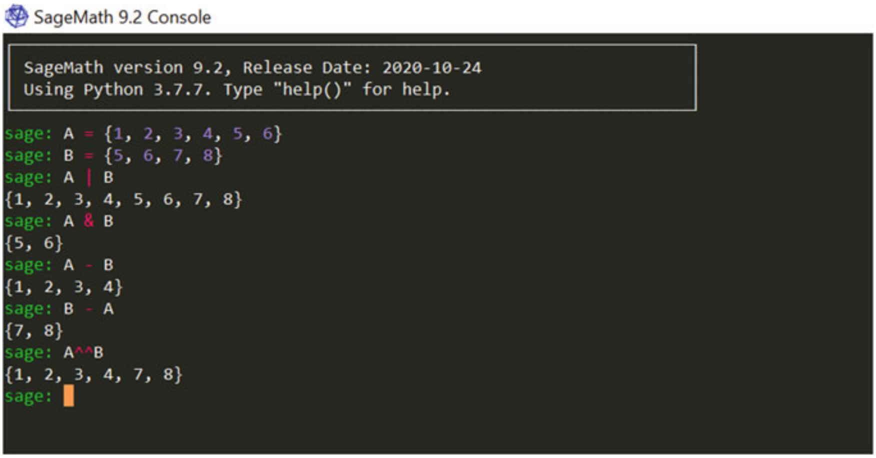
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = [1, 2, 3, 4, 5, 6]
sage: B = [5, 6, 7, 8]
sage: A+B
[1, 2, 3, 4, 5, 6, 5, 6, 7, 8]
```

If one deals with the lists only as sets, then the best way is to store these lists directly as sets, specifically by implanting the elements between curly brackets "{}", as shows below.



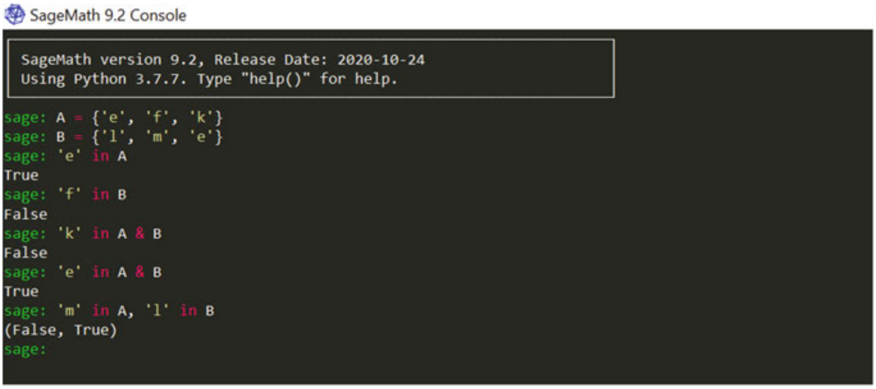
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = {1, 2, 3, 4, 5, 6}
sage: B = {5, 6, 7, 8}
sage: A.union(B)
{1, 2, 3, 4, 5, 6, 7, 8}
sage: A.intersection(B)
{5, 6}
sage: A.difference(B)
{1, 2, 3, 4}
sage: B.difference(A)
{7, 8}
sage: (A.difference(B)).union(B.difference(A))
{1, 2, 3, 4, 7, 8}
sage:
```

The commands “difference()”, “intersection()”, and “union()” in the above display box are used to compute the difference, intersection, union, and symmetric difference of two sets. To use such commands, one must ensure that the inputs are defined as sets by using the command “set()” or curly brackets; otherwise, the commands will not work. Other shorter commands are available too. For example, the union, intersection, difference, and symmetric difference can be computed using the symbols “|”, “&”, “−”, and “∧∧”, respectively. All these symbols deal with the inputs as sets.



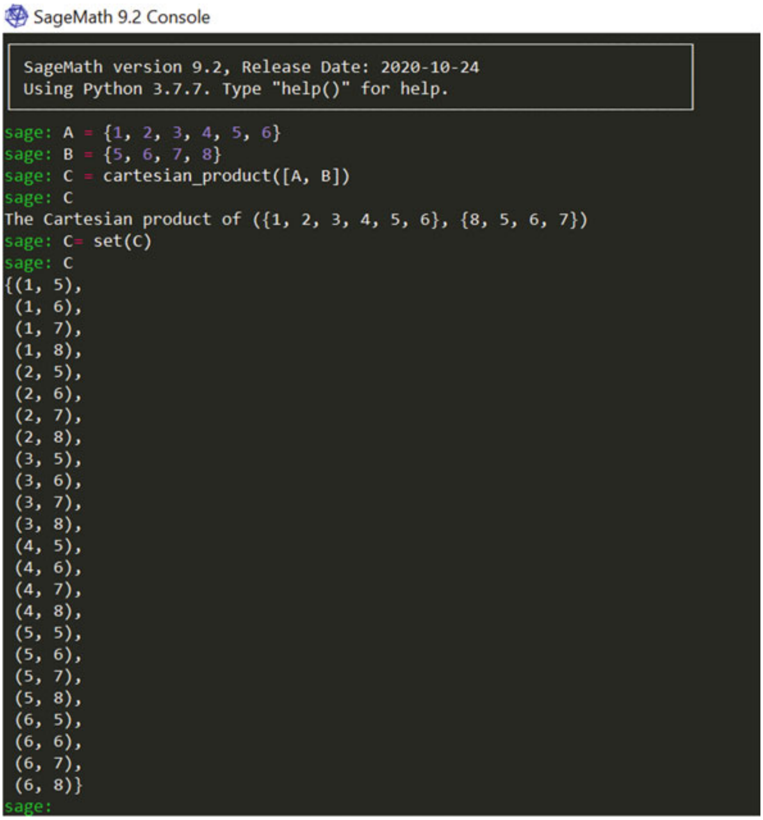
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = {1, 2, 3, 4, 5, 6}
sage: B = {5, 6, 7, 8}
sage: A | B
{1, 2, 3, 4, 5, 6, 7, 8}
sage: A & B
{5, 6}
sage: A - B
{1, 2, 3, 4}
sage: B - A
{7, 8}
sage: A^^B
{1, 2, 3, 4, 7, 8}
sage:
```

The types of elements in any set vary, and they may be numbers, characters, or names. If the elements of a set are not numbers, then they must be identified between two quotation marks, as shown in the following display box. To check whether any element belongs to a certain set, the command “in” should be used. The answer of such command is either “true” or “false”. Two commands can be implemented in the same line by using a comma “,” or semicolon “;”.



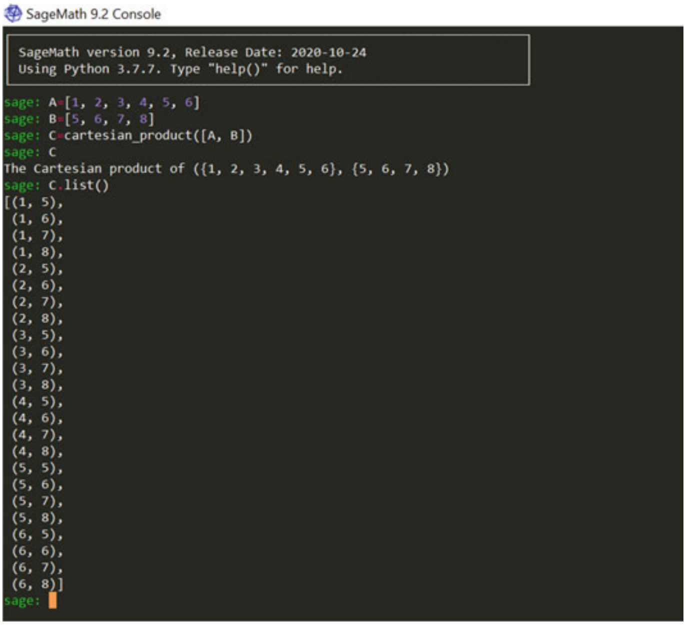
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = {'e', 'f', 'k'}
sage: B = {'l', 'm', 'e'}
sage: 'e' in A
True
sage: 'f' in B
False
sage: 'k' in A & B
False
sage: 'e' in A & B
True
sage: 'm' in A, 'l' in B
(False, True)
sage:
```

The command “cartesian_product([,])” is used by Sage to find the Cartesian product of two sets defined in the system. For example, the command “cartesian_product([A, B])” stores the Cartesian product of the sets A and B in the program. Sage does not present the output unless a suitable command is applied, as shown in the following display box. Note that to view the elements of the Cartesian product, one must apply the command “set()”.

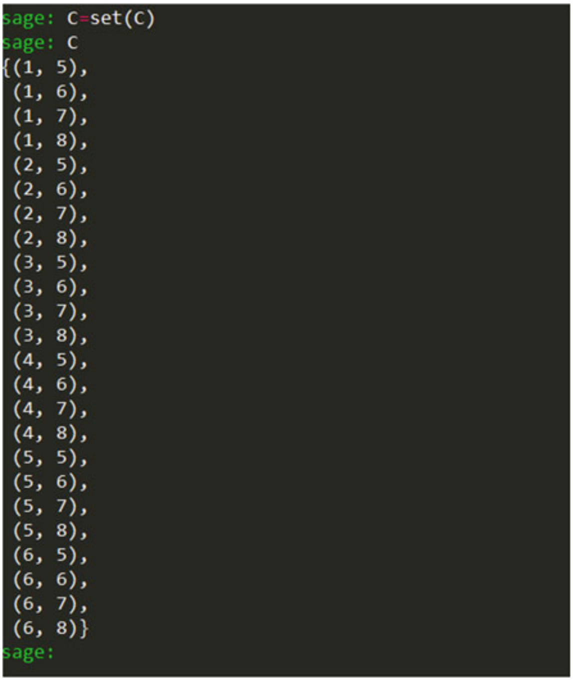


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = {1, 2, 3, 4, 5, 6}
sage: B = {5, 6, 7, 8}
sage: C = cartesian_product([A, B])
sage: C
The Cartesian product of ({1, 2, 3, 4, 5, 6}, {8, 5, 6, 7})
sage: C= set(C)
sage: C
{(1, 5),
 (1, 6),
 (1, 7),
 (1, 8),
 (2, 5),
 (2, 6),
 (2, 7),
 (2, 8),
 (3, 5),
 (3, 6),
 (3, 7),
 (3, 8),
 (4, 5),
 (4, 6),
 (4, 7),
 (4, 8),
 (5, 5),
 (5, 6),
 (5, 7),
 (5, 8),
 (6, 5),
 (6, 6),
 (6, 7),
 (6, 8)}
sage:
```

If A and B are encoded using the square brackets, their Cartesian product can be calculated using the same command. However, to view the elements of their product, the command “list()” is used. To list the elements as a set, one needs to apply the command “set()”. See the operations explained below.

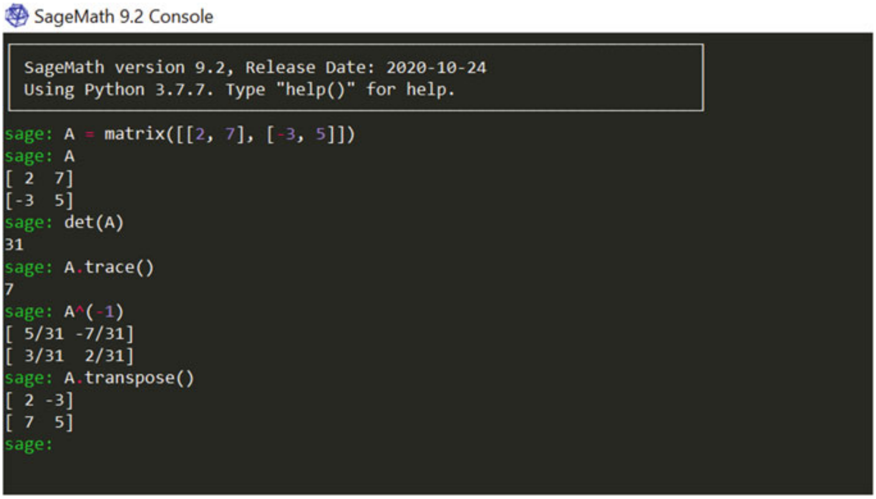


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A=[1, 2, 3, 4, 5, 6]
sage: B=[5, 6, 7, 8]
sage: C=cartesian_product([A, B])
sage: C
The Cartesian product of ({1, 2, 3, 4, 5, 6}, {5, 6, 7, 8})
sage: C.list()
[(1, 5),
 (1, 6),
 (1, 7),
 (1, 8),
 (2, 5),
 (2, 6),
 (2, 7),
 (2, 8),
 (3, 5),
 (3, 6),
 (3, 7),
 (3, 8),
 (4, 5),
 (4, 6),
 (4, 7),
 (4, 8),
 (5, 5),
 (5, 6),
 (5, 7),
 (5, 8),
 (6, 5),
 (6, 6),
 (6, 7),
 (6, 8)]
sage: 
```



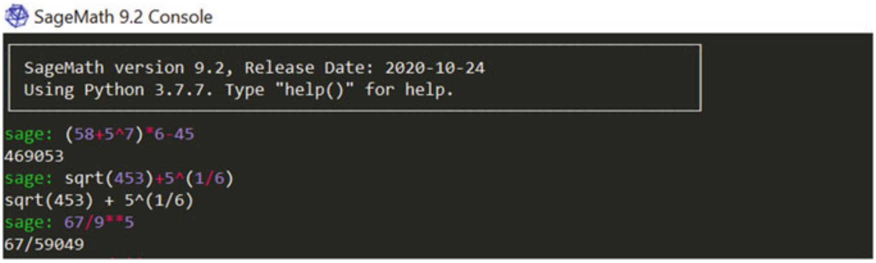
```
sage: C=set(C)
sage: C
{(1, 5),
 (1, 6),
 (1, 7),
 (1, 8),
 (2, 5),
 (2, 6),
 (2, 7),
 (2, 8),
 (3, 5),
 (3, 6),
 (3, 7),
 (3, 8),
 (4, 5),
 (4, 6),
 (4, 7),
 (4, 8),
 (5, 5),
 (5, 6),
 (5, 7),
 (5, 8),
 (6, 5),
 (6, 6),
 (6, 7),
 (6, 8)}
sage:
```

The command “matrix()” is used to define a matrix in Sage. The entries of a matrix are entered row by row within square brackets. Operations on matrices such as determinant, trace, inverse, and transpose are implemented using the commands “det (A)”, “A.trace()”, “$A^\wedge(-1)$”, and “A.transpose()”, respectively. For example, the matrix in Example 1.6.22 (1) is encoded as shown in the following display box, and all its matrix operations are computed.



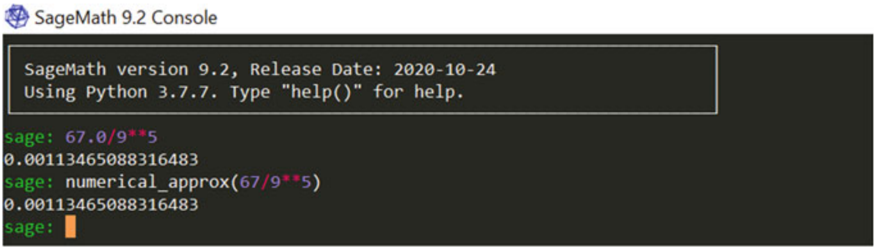
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: A = matrix([[2, 7], [-3, 5]])
sage: A
[ 2  7]
[-3  5]
sage: det(A)
31
sage: A.trace()
7
sage: A^(-1)
[ 5/31 -7/31]
[ 3/31  2/31]
sage: A.transpose()
[ 2 -3]
[ 7  5]
sage:
```

Sage can also be considered a calculator. Basic operations on integers, reals, and complex numbers can be conducted. The signs “$+, -, *, /$” are used for sum, difference, multiplication, and division, respectively. For the exponents, the signs “$**$” or “$^\wedge$” are used. The square root and nth root are calculated using the commands “sqrt()” and “$^\wedge(1/n)$”, respectively.



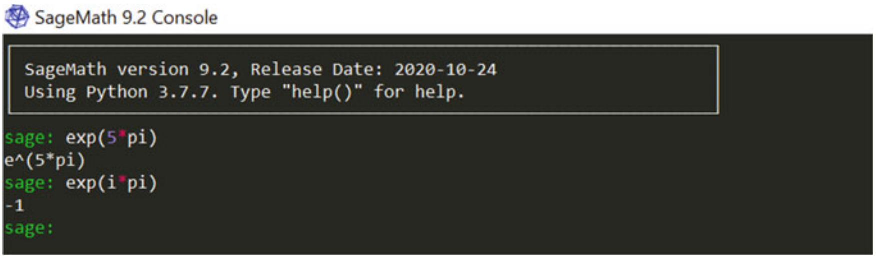
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: (58+5^7)*6-45
469053
sage: sqrt(453)+5^(1/6)
sqrt(453) + 5^(1/6)
sage: 67/9**5
67/59049
```

The last quotient in the output above yields a fractional answer. To obtain the value in decimal, either replace “67” by “67.0”, or use the command “numerical_approx()”, as follows:

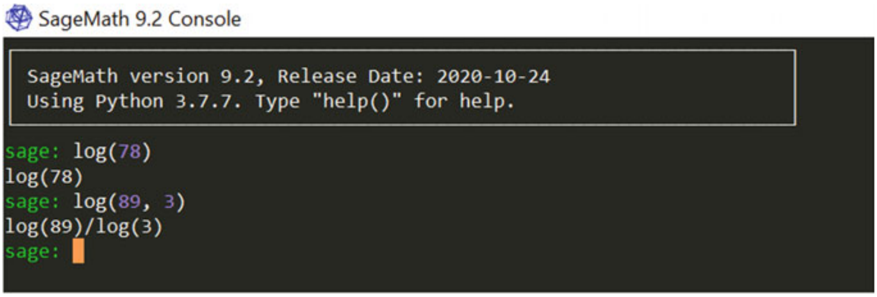


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: 67.0/9**5
0.00113465088316483
sage: numerical_approx(67/9**5)
0.00113465088316483
sage: 
```

The constant numbers π and e are defined in Sage as “pi” and “e”, respectively. The imaginary number i is also defined as “i” or “I”. The exponent function is implemented using “exp()”. The logarithm function with base 10 and base a can be calculated using the commands “log()” and “log(, a)”, respectively.

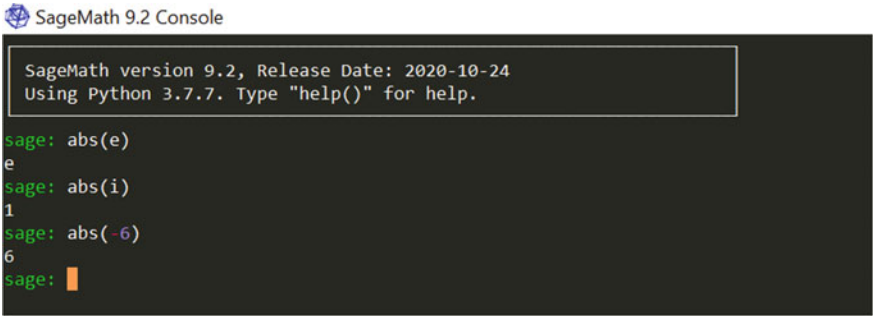


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: exp(5*pi)
e^(5*pi)
sage: exp(i*pi)
-1
sage:
```



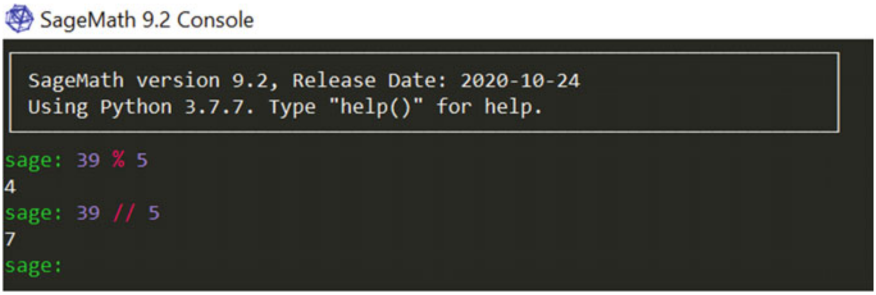
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: log(78)
log(78)
sage: log(89, 3)
log(89)/log(3)
sage: 
```

The absolute value of a number can be calculated using the command “abs()”, as shown below.

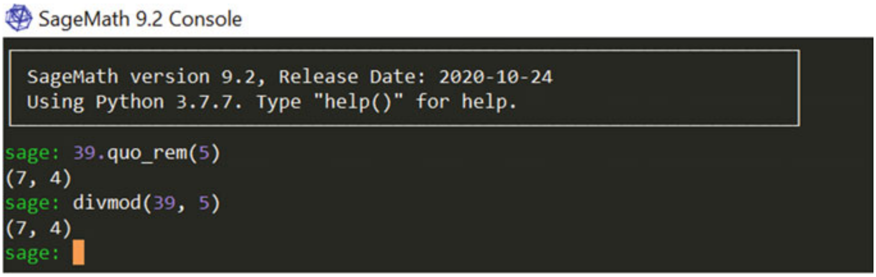


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: abs(e)
e
sage: abs(i)
1
sage: abs(-6)
6
sage:
```

Next, we review commands related to the quotient-remainder theorem (Sect. 2.1). In Sage, when dividing a by b, the remainder can be computed by typing “$a\%b$”. The quotient is obtained by using the symbol “//”. Several commands can be used to find the quotient and reminder simultaneously, such as “a.quo_rem(b)” and “divmod(a, b)”.

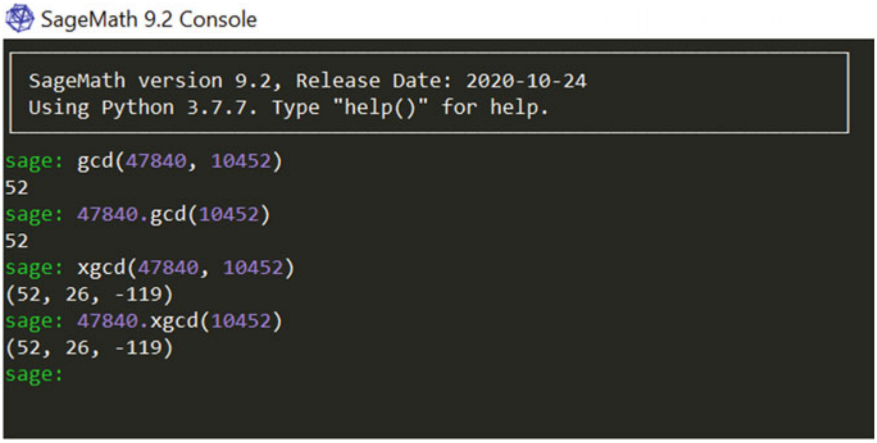


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: 39 % 5
4
sage: 39 // 5
7
sage:
```



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: 39.quo_rem(5)
(7, 4)
sage: divmod(39, 5)
(7, 4)
sage:
```

The greatest common divisor is obtained using the commands “gcd(a, b)” or “a.gcd(b)” for the integers a and b. The coefficients specified by Bézout’s lemma to write the greatest common divisor as a linear combination of the two integers can be computed in seconds by using the commands “xgcd(a, b)” or “a.xgcd(b)”.

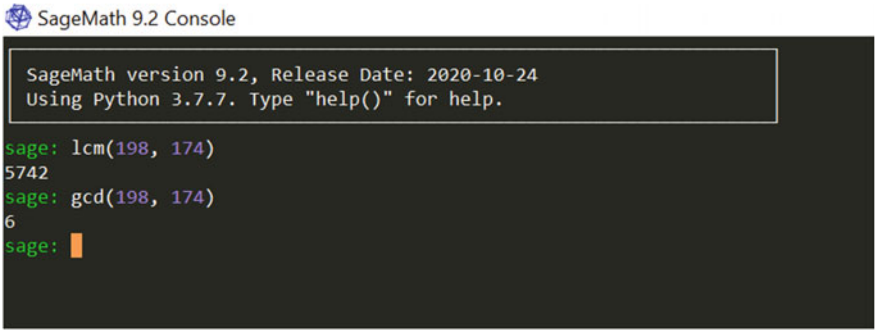


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: gcd(47840, 10452)
52
sage: 47840.gcd(10452)
52
sage: xgcd(47840, 10452)
(52, 26, -119)
sage: 47840.xgcd(10452)
(52, 26, -119)
sage:
```

The output of the commands “xgcd(a, b)” or “a.xgcd(b)” is a triple consisting of the greatest common divisor of the first component and the coefficients of the linear combination in other two components. Hence, the output of such commands in the display box above means

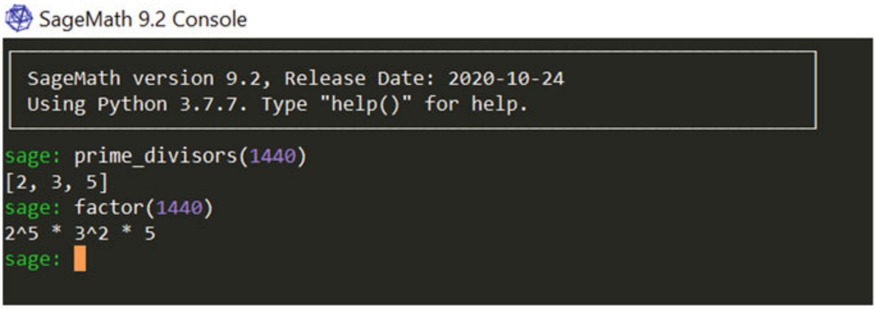
$$52 = (26 \times 47840) + (-119 \times 10452).$$

The command “lcm(,)” is used to compute the least common multiple.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: lcm(198, 174)
5742
sage: gcd(198, 174)
6
sage: 
```

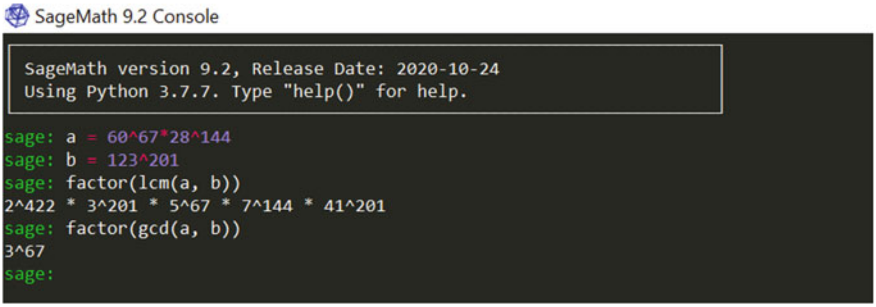
To compute the prime divisors of a given number, the command "prime_divisors()" is used in Sage. The command "factor()" is used for finding the prime factorization.



SageMath 9.2 Console

```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: prime_divisors(1440)
[2, 3, 5]
sage: factor(1440)
2^5 * 3^2 * 5
sage: 
```

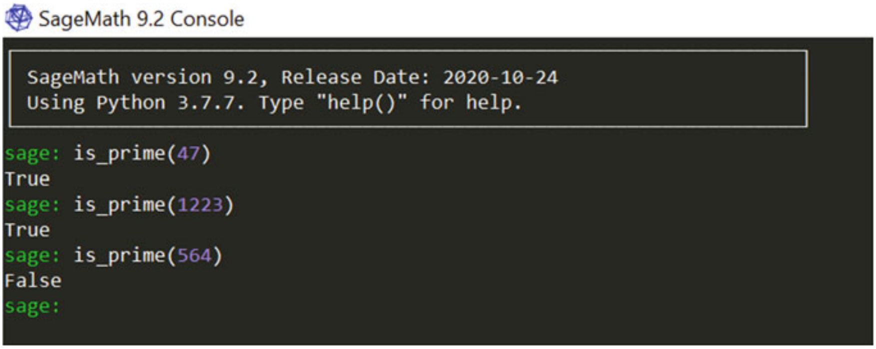
The following shows the solution of Example 2.9.9 by using Sage.



SageMath 9.2 Console

```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: a = 60^67*28^144
sage: b = 123^201
sage: factor(lcm(a, b))
2^422 * 3^201 * 5^67 * 7^144 * 41^201
sage: factor(gcd(a, b))
3^67
sage:
```

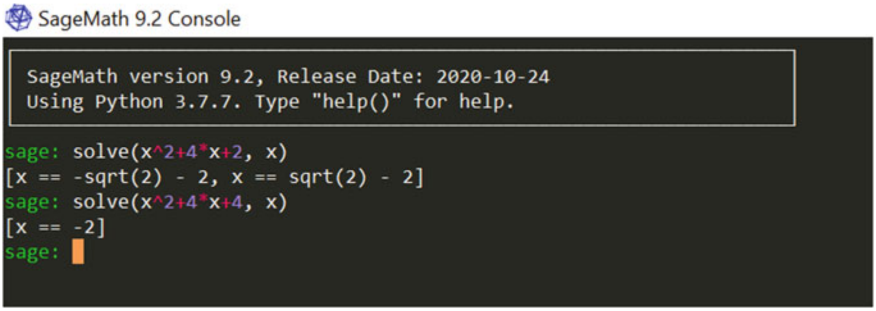
To check whether a number is a prime, the command "is_prime()" can be used.



SageMath 9.2 Console

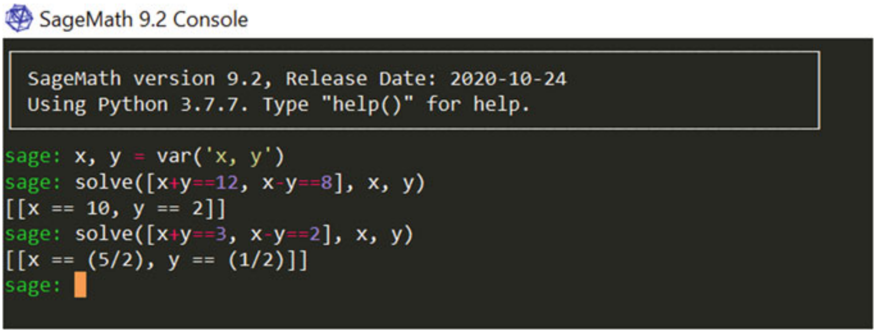
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: is_prime(47)
True
sage: is_prime(1223)
True
sage: is_prime(564)
False
sage:
```

Sage solves equations using the command “solve()”. To solve any equation in one variable, write the equation followed by a comma with a variable inside the brackets of the command “solve()”. The double equality symbol “==” in the following display box means the equal sign.



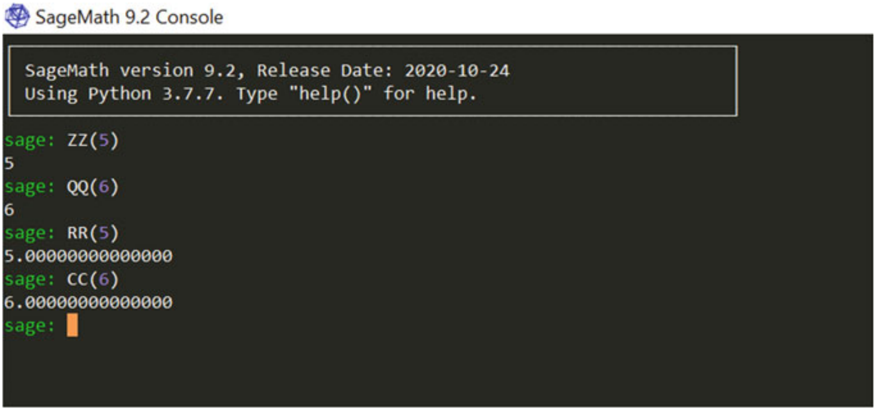
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: solve(x^2+4*x+2, x)
[x == -sqrt(2) - 2, x == sqrt(2) - 2]
sage: solve(x^2+4*x+4, x)
[x == -2]
sage:
```

In cases involving more than one variable, Sage must be informed about the variables before using the command “solve()”. The definition can be performed using “var()”.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: x, y = var('x, y')
sage: solve([x+y==12, x-y==8], x, y)
[[x == 10, y == 2]]
sage: solve([x+y==3, x-y==2], x, y)
[[x == (5/2), y == (1/2)]]
sage:
```

To define any number “x” as an integer, rational number, real number, or complex number in Sage, the commands “ZZ(x))”, “QQ(x))”, “RR(x)”, or “CC(x)” are used, respectively.

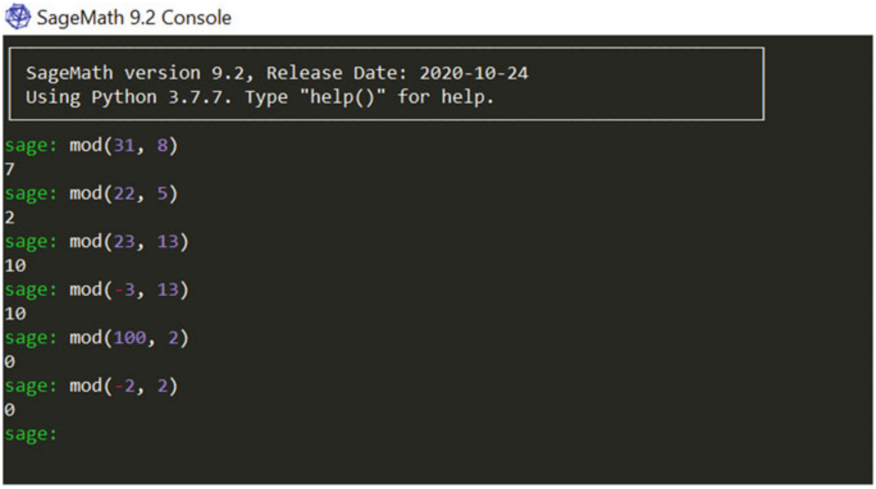


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: ZZ(5)
5
sage: QQ(6)
6
sage: RR(5)
5.00000000000000
sage: CC(6)
6.00000000000000
sage:
```

In the above display box, the statements mean $5 \in \mathbb{Z}$, $6 \in \mathbb{Q}$, $5 \in \mathbb{R}$, and $6 \in \mathbb{C}$.

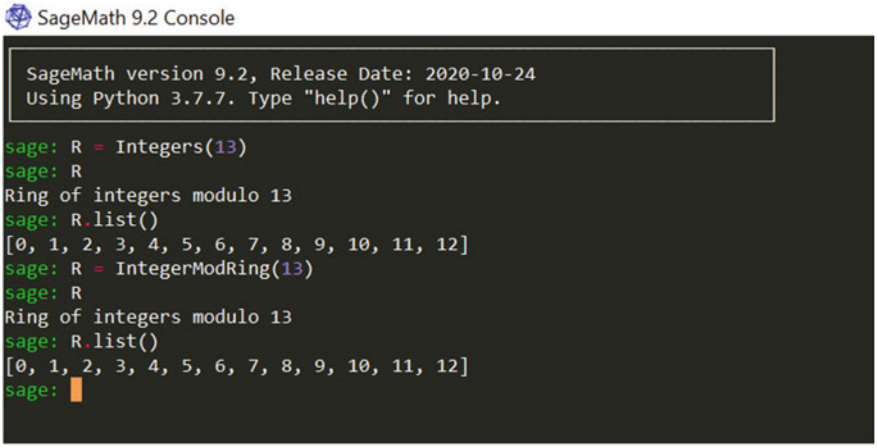
10.2.2 Commands Related to Integers Modulo n

This subsection discusses Sage commands related to the integers modulo n. These commands can help solve the problems discussed in Chapter 3. For example, the command "mod(a, n)" is used to find the integer congruent to a modulo n. Example 3.5.1 is resolved below.



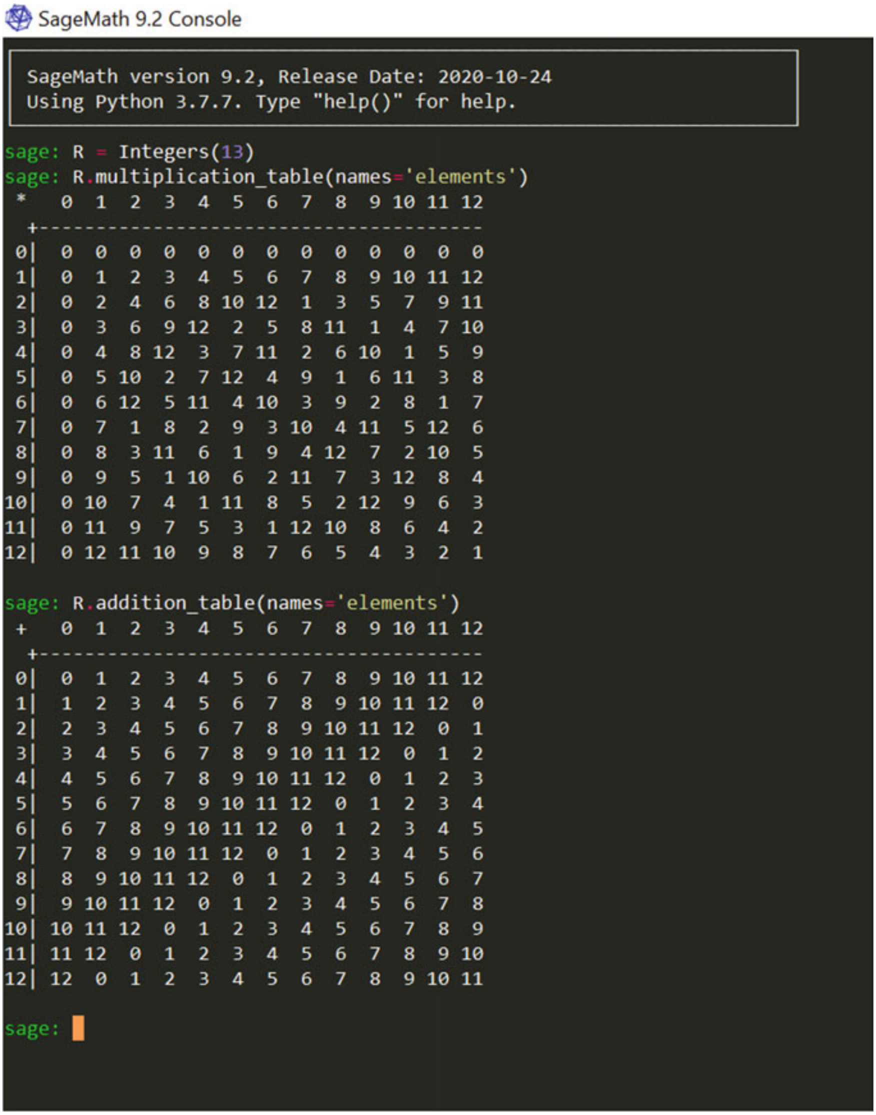
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: mod(31, 8)
7
sage: mod(22, 5)
2
sage: mod(23, 13)
10
sage: mod(-3, 13)
10
sage: mod(100, 2)
0
sage: mod(-2, 2)
0
sage:
```

The residue classes module n are obtained using one of the two commands “Integers(n)” or “IntegerModRing (n)”. Both commands can be used to generate the additive group module n. . Like most other commands in Sage, these commands create the additive group and store it in the system. Sage does not display the group unless a display command is applied. Several items in (Example 3.3.4) are resolved in the display box below.



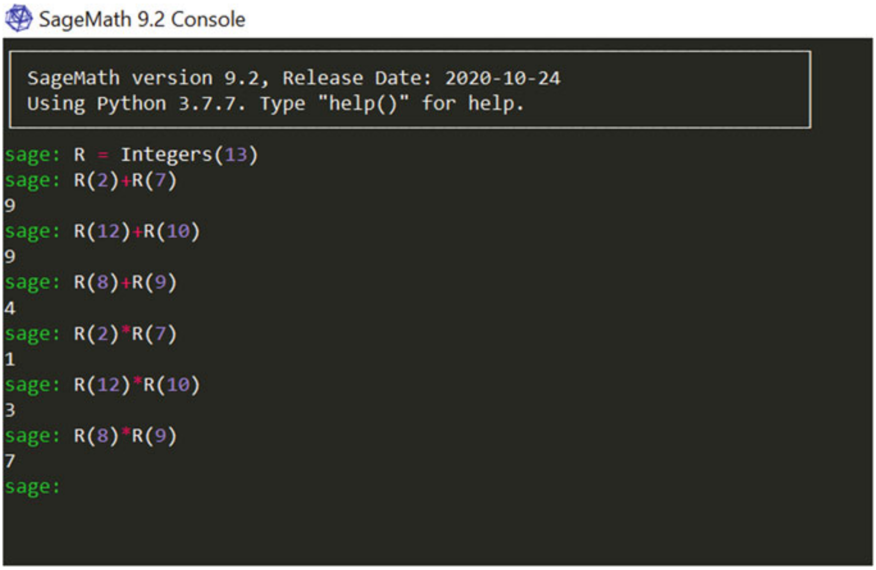
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: R = Integers(13)
sage: R
Ring of integers modulo 13
sage: R.list()
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
sage: R = IntegerModRing(13)
sage: R
Ring of integers modulo 13
sage: R.list()
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
sage: 
```

To find the tables for the addition and multiplication on $\mathbb{Z}_n$, Sage uses the commands “R.multiplication_table(names =‘elements’)” and “R.addition_table(names =‘elements’)”, respectively. Note that “R” refers to the name assigned to $\mathbb{Z}_n$.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: R = Integers(13)
sage: R.multiplication_table(names='elements')
 *   0  1  2  3  4  5  6  7  8  9 10 11 12
  +---------------------------------------
 0|  0  0  0  0  0  0  0  0  0  0  0  0  0
 1|  0  1  2  3  4  5  6  7  8  9 10 11 12
 2|  0  2  4  6  8 10 12  1  3  5  7  9 11
 3|  0  3  6  9 12  2  5  8 11  1  4  7 10
 4|  0  4  8 12  3  7 11  2  6 10  1  5  9
 5|  0  5 10  2  7 12  4  9  1  6 11  3  8
 6|  0  6 12  5 11  4 10  3  9  2  8  1  7
 7|  0  7  1  8  2  9  3 10  4 11  5 12  6
 8|  0  8  3 11  6  1  9  4 12  7  2 10  5
 9|  0  9  5  1 10  6  2 11  7  3 12  8  4
10|  0 10  7  4  1 11  8  5  2 12  9  6  3
11|  0 11  9  7  5  3  1 12 10  8  6  4  2
12|  0 12 11 10  9  8  7  6  5  4  3  2  1

sage: R.addition_table(names='elements')
 +   0  1  2  3  4  5  6  7  8  9 10 11 12
  +---------------------------------------
 0|  0  1  2  3  4  5  6  7  8  9 10 11 12
 1|  1  2  3  4  5  6  7  8  9 10 11 12  0
 2|  2  3  4  5  6  7  8  9 10 11 12  0  1
 3|  3  4  5  6  7  8  9 10 11 12  0  1  2
 4|  4  5  6  7  8  9 10 11 12  0  1  2  3
 5|  5  6  7  8  9 10 11 12  0  1  2  3  4
 6|  6  7  8  9 10 11 12  0  1  2  3  4  5
 7|  7  8  9 10 11 12  0  1  2  3  4  5  6
 8|  8  9 10 11 12  0  1  2  3  4  5  6  7
 9|  9 10 11 12  0  1  2  3  4  5  6  7  8
10| 10 11 12  0  1  2  3  4  5  6  7  8  9
11| 11 12  0  1  2  3  4  5  6  7  8  9 10
12| 12  0  1  2  3  4  5  6  7  8  9 10 11

sage:
```

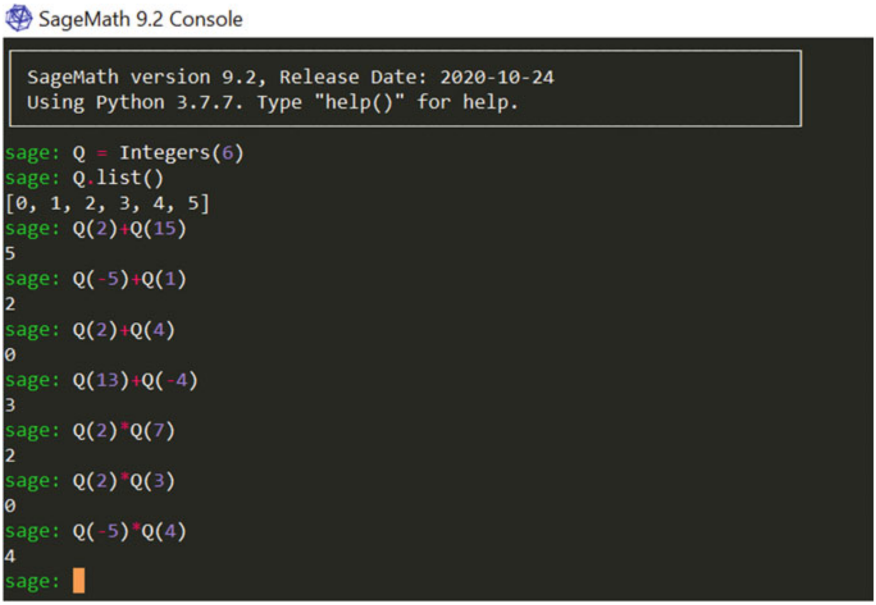
To add or multiply specific elements in $\mathbb{Z}_n$, the elements must be selected using the name assigned to $\mathbb{Z}_n$, as shown in resolving Example 3.3.4 (1).



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: R = Integers(13)
sage: R(2)+R(7)
9
sage: R(12)+R(10)
9
sage: R(8)+R(9)
4
sage: R(2)*R(7)
1
sage: R(12)*R(10)
3
sage: R(8)*R(9)
7
sage:
```

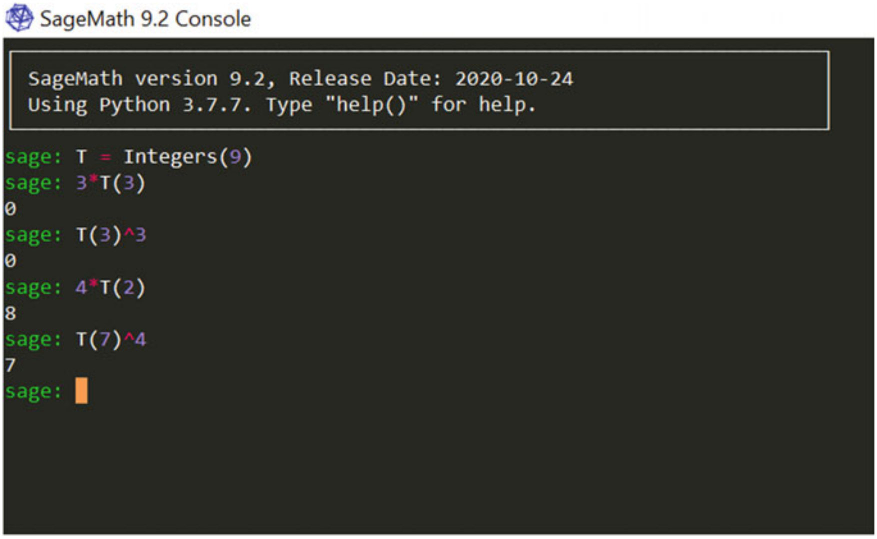
Example 3.3.4 (2) can also be solved using Sage, as follows:



SageMath 9.2 Console

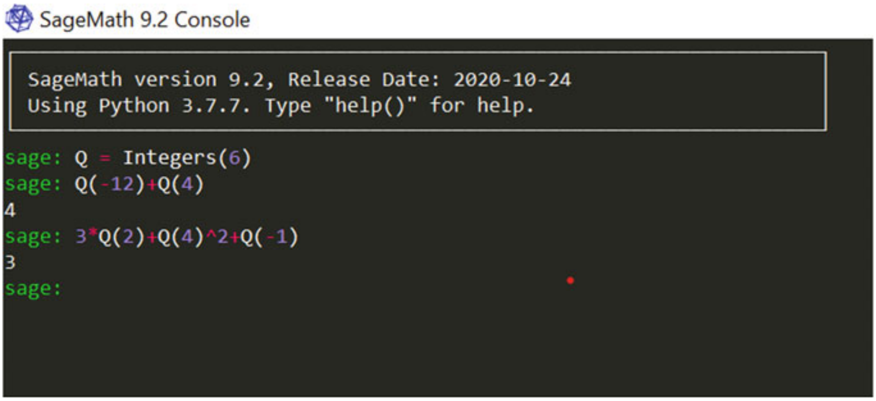
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Q = Integers(6)
sage: Q.list()
[0, 1, 2, 3, 4, 5]
sage: Q(2)+Q(15)
5
sage: Q(-5)+Q(1)
2
sage: Q(2)+Q(4)
0
sage: Q(13)+Q(-4)
3
sage: Q(2)*Q(7)
2
sage: Q(2)*Q(3)
0
sage: Q(-5)*Q(4)
4
sage:
```

Example 3.3.10 is resolved using Sage, as shown in the following box:



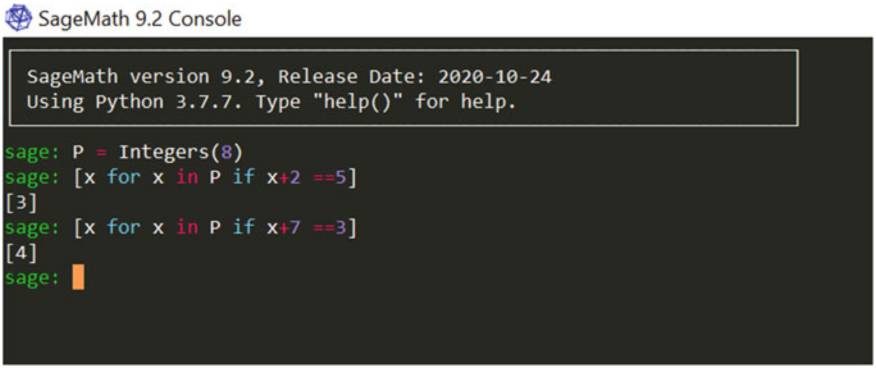
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: T = Integers(9)
sage: 3*T(3)
0
sage: T(3)^3
0
sage: 4*T(2)
8
sage: T(7)^4
7
sage:
```

The operation on $\mathbb{Z}_n$ can be simultaneously performed for more than two elements simultaneously, as shown in the following display box.



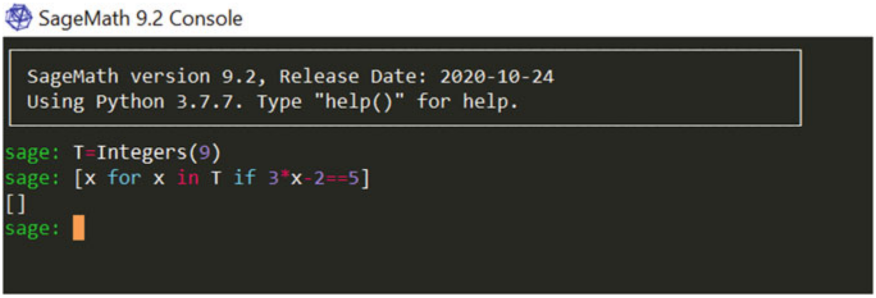
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Q = Integers(6)
sage: Q(-12)+Q(4)
4
sage: 3*Q(2)+Q(4)^2+Q(-1)
3
sage:
```

Equations on $\mathbb{Z}_n$ can also be solved in Sage. To solve an equation on $\mathbb{Z}_n$, a template involving “for”, “in”, and “if” is used. Example 3.6.4 (1) is resolved below, and the reader may see that there exists only one solution in $\mathbb{Z}_8$ for each defined equation.

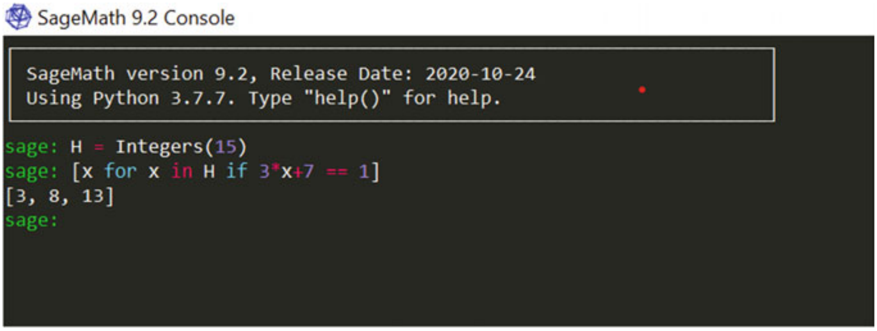


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: P = Integers(8)
sage: [x for x in P if x+2 ==5]
[3]
sage: [x for x in P if x+7 ==3]
[4]
sage: 
```

The results in the display boxes below show that the equation in Example 3.6.4 (2) has no solution in $\mathbb{Z}_9$, and the equation in Example 3.6.4 (4) has three solutions in $\mathbb{Z}_{15}$.



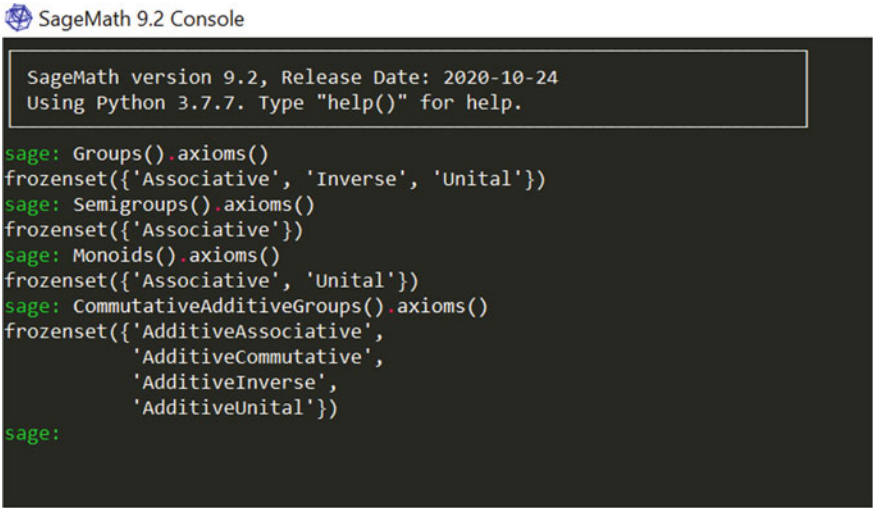
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: T=Integers(9)
sage: [x for x in T if 3*x-2==5]
[]
sage: 
```



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: H = Integers(15)
sage: [x for x in H if 3*x+7 == 1]
[3, 8, 13]
sage:
```

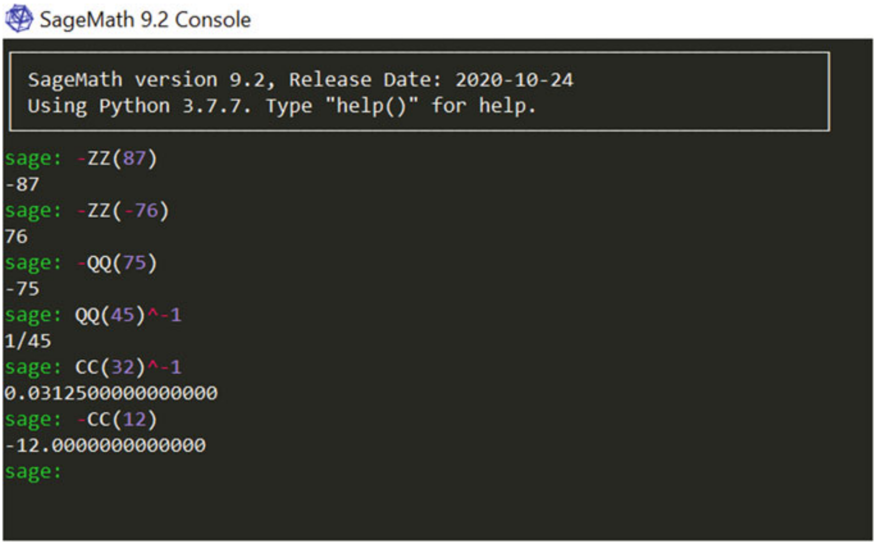
10.2.3 Commands Related to Groups

This subsection discusses commands related to groups that can be used to solve problems in Chaps. 4–6. In particular, Sage can be used to solve problems such as determining if a given group is abelian or cyclic, computing the order of group elements, or obtaining information about the group. The command “axioms()” is used to demonstrate the characteristics of categories such as groups and monoids, as shown below.



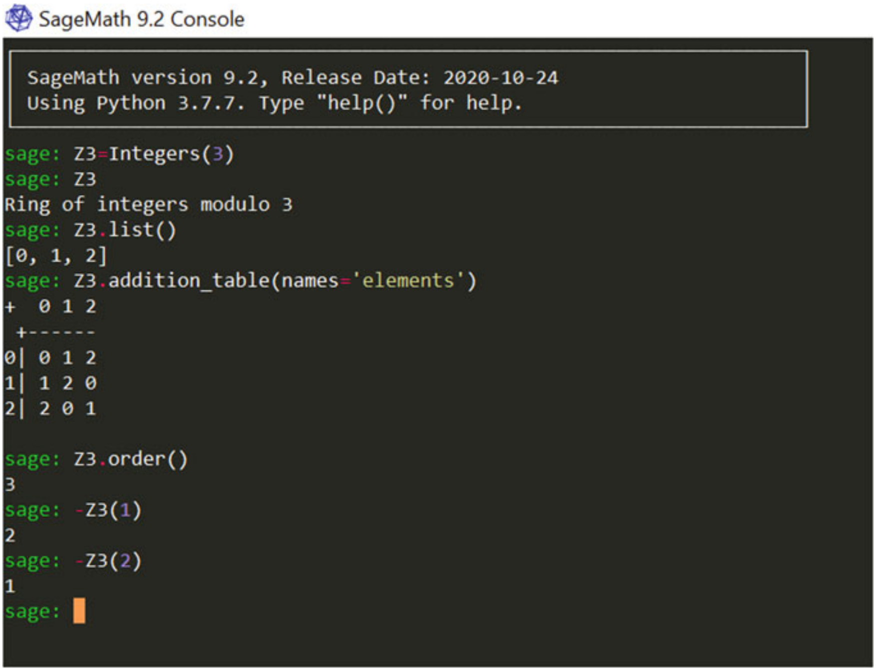
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Groups().axioms()
frozenset({'Associative', 'Inverse', 'Unital'})
sage: Semigroups().axioms()
frozenset({'Associative'})
sage: Monoids().axioms()
frozenset({'Associative', 'Unital'})
sage: CommutativeAdditiveGroups().axioms()
frozenset({'AdditiveAssociative',
           'AdditiveCommutative',
           'AdditiveInverse',
           'AdditiveUnital'})
sage:
```

To find the inverse of any element in an additive group (such as $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, or $(\mathbb{Z}_n, \oplus_n)$) the sign (command) “−” is used. Similarly, for finding the inverse of an element in a multiplicative group (such as $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ or $(\mathrm{Inv}(\mathbb{Z}_n), \oplus_n)$ the command “^ − 1” is used in Sage. Recall that to inform Sage about an element a in $\mathbb{Q}$, one must write “QQ(a)”. Therefore, the command for the inverse of a in the group $(\mathbb{Q}, +)$ will be “−QQ(a)”, while the inverse of a in the group $(\mathbb{Q}^*, \cdot)$ is encoded as “QQ(a)^ − 1”.



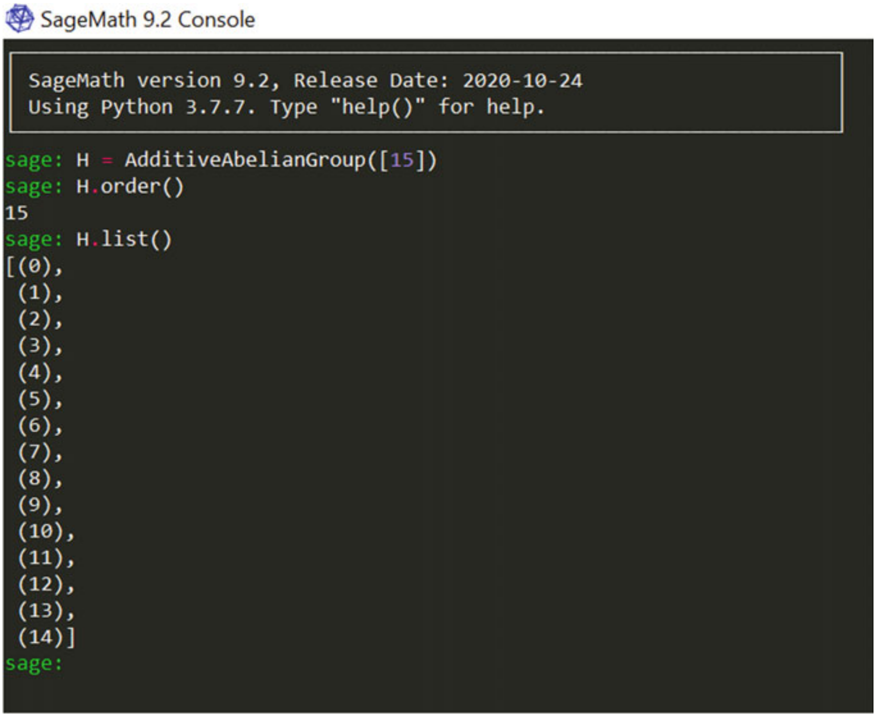
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: -ZZ(87)
-87
sage: -ZZ(-76)
76
sage: -QQ(75)
-75
sage: QQ(45)^-1
1/45
sage: CC(32)^-1
0.0312500000000000
sage: -CC(12)
-12.0000000000000
sage:
```

The command “H.order()” is used to compute the order of a given group or set H. The commands in the display box below list the elements of the additive group $\mathbb{Z}_3$, provide its Caley’s table, compute its order, and find the inverse elements of [1] and [2].

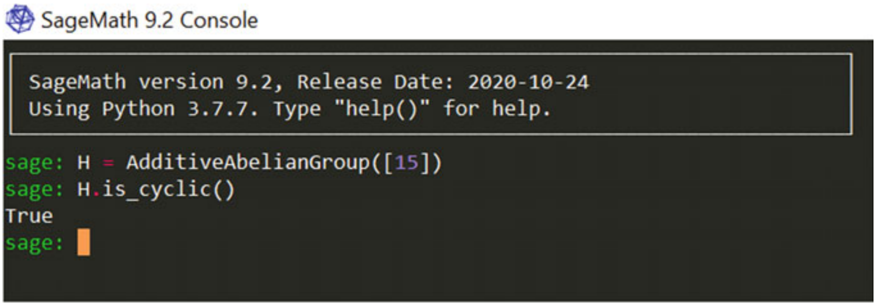


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Z3=Integers(3)
sage: Z3
Ring of integers modulo 3
sage: Z3.list()
[0, 1, 2]
sage: Z3.addition_table(names='elements')
+  0 1 2
 +------
0| 0 1 2
1| 1 2 0
2| 2 0 1

sage: Z3.order()
3
sage: -Z3(1)
2
sage: -Z3(2)
1
sage:
```

The additive group $\mathbb{Z}_n$ can be created in Sage using the command “AdditiveAbelianGroup ([n])”, and the elements of $\mathbb{Z}_n$ can explicitly be seen as equivalence classes.



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: H = AdditiveAbelianGroup([15])
sage: H.order()
15
sage: H.list()
[(0),
 (1),
 (2),
 (3),
 (4),
 (5),
 (6),
 (7),
 (8),
 (9),
 (10),
 (11),
 (12),
 (13),
 (14)]
sage:
```

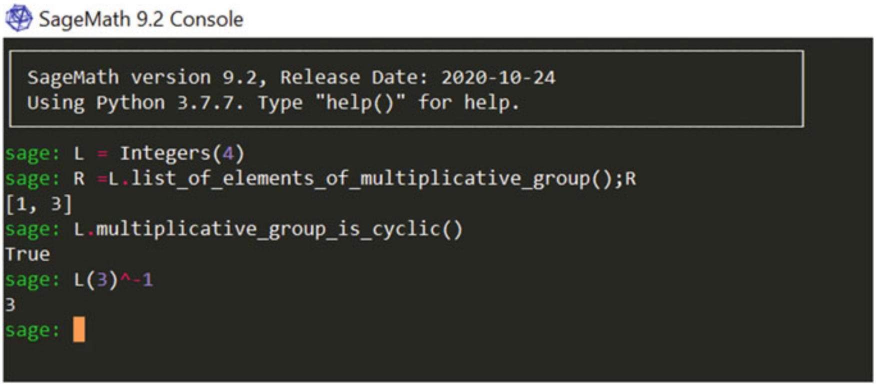


```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: H = AdditiveAbelianGroup([15])
sage: H.is_cyclic()
True
sage:
```

As shown above, Sage can check whether a given group is cyclic, by applying the command “is_cyclic()”.

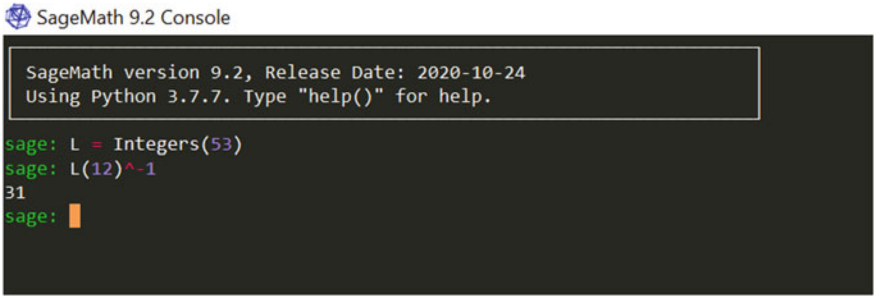
The multiplicative group of integers modulo n can be determined using Sage. The command “list_of_elements_of_multiplicative_group()” stores the elements of

$(\mathrm{Inv}(\mathbb{Z}_n), \otimes_n)$. To obtain this group, one must create $\mathbb{Z}_n$ and then apply the above command to find the invertible elements in $\mathbb{Z}_n$.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: L = Integers(4)
sage: R =L.list_of_elements_of_multiplicative_group();R
[1, 3]
sage: L.multiplicative_group_is_cyclic()
True
sage: L(3)^-1
3
sage: 
```

In the box above, the line "R = list_of_elements_of_multiplicative_group; R" contains two commands: to create the group $\mathrm{Inv}(\mathbb{Z}_n)$ and to view it. Note that writing the command "R = list_of_elements_of_multiplicative_group " stores R as a list of invertible elements in the additive group, and it is not considered as a group. Therefore, to check if the multiplicative group is cyclic, one must use L and not R via the command "L.multiplicative_group_is_cyclic()". For the same reason, to find the inverse of an element in $\mathrm{Inv}(\mathbb{Z}_n)$, the symbol "$\wedge - 1$" is used with $\mathbb{Z}_n$, as mentioned earlier.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: L = Integers(53)
sage: L(12)^-1
31
sage: 
```

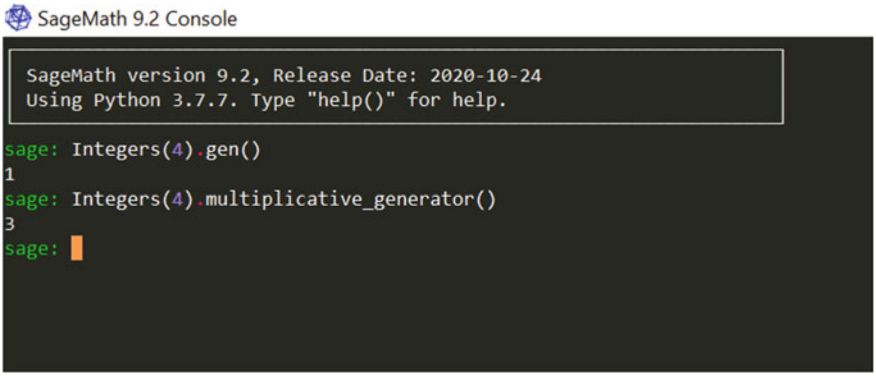
An error message will appear if one tries to find the multiplicative inverse of a noninvertible element. For example, the use of the following commands

"$L = I$nteger(4)"

"$L(2)^\wedge - 1$L(2)^−1"

will generate an error message.

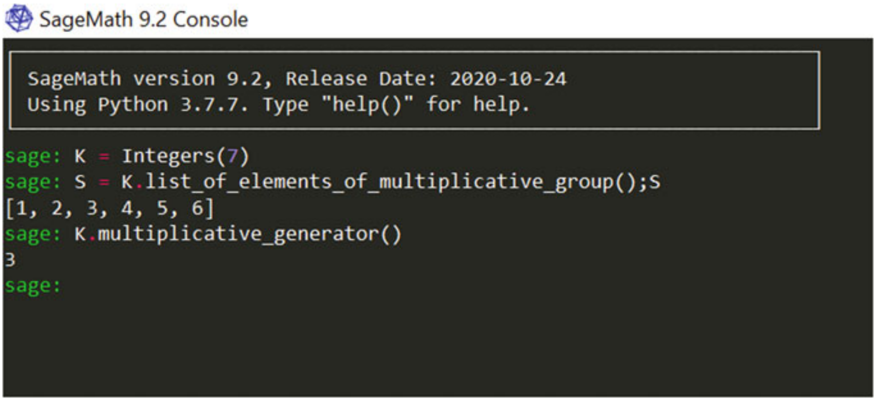
To find a generator of the additive group $\mathbb{Z}_n$, the command "gen()" is used. The command "multiplicative_generator()" is used to obtain the multiplicative group $\mathrm{Inv}(\mathbb{Z}_n)$.



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Integers(4).gen()
1
sage: Integers(4).multiplicative_generator()
3
sage:
```

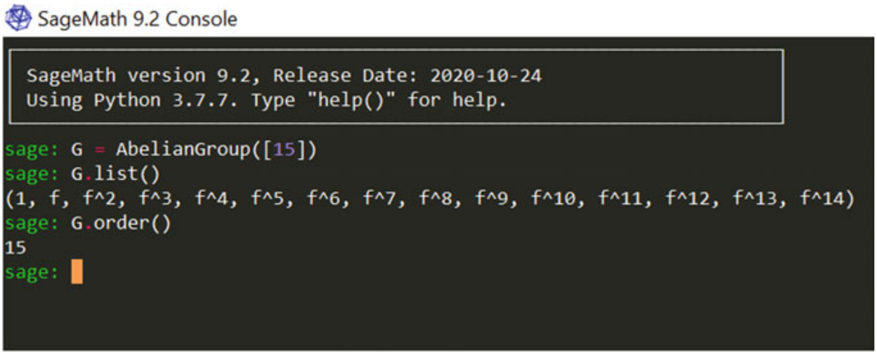
The commands in the display box below create the invertible elements in $\mathbb{Z}_7$ and find a generator of $\mathrm{Inv}(\mathbb{Z}_7)$.



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: K = Integers(7)
sage: S = K.list_of_elements_of_multiplicative_group();S
[1, 2, 3, 4, 5, 6]
sage: K.multiplicative_generator()
3
sage:
```

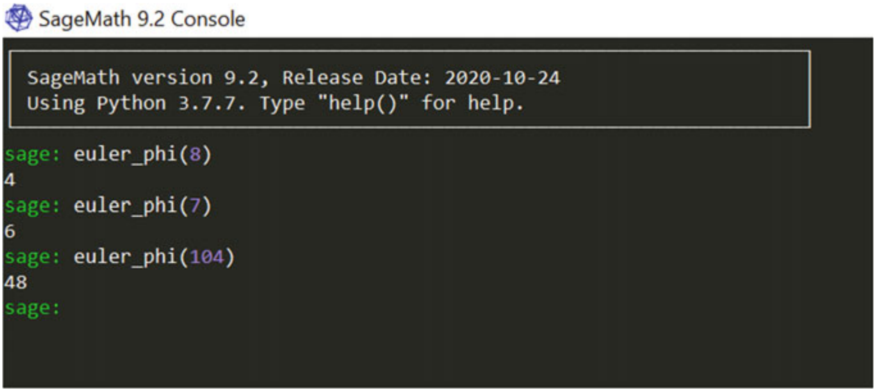
The command “list_of_elements_of_multiplicative_group()” creates the multiplicative cyclic group $\mathrm{Inv}(\mathbb{Z}_n)$, which is not of order n. The command “AbelianGroup ([n])” creates a multiplicative cyclic group of order n for a given n. Note that the output is given in terms of a generator f.



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: G = AbelianGroup([15])
sage: G.list()
(1, f, f^2, f^3, f^4, f^5, f^6, f^7, f^8, f^9, f^10, f^11, f^12, f^13, f^14)
sage: G.order()
15
sage: 
```

The command “euler_phi (n)” is used to find the Euler function that yields the order of the multiplicative group $\mathrm{Inv}(\mathbb{Z}_n)$ (Corollary 5.3.9).



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: euler_phi(8)
4
sage: euler_phi(7)
6
sage: euler_phi(104)
48
sage:
```

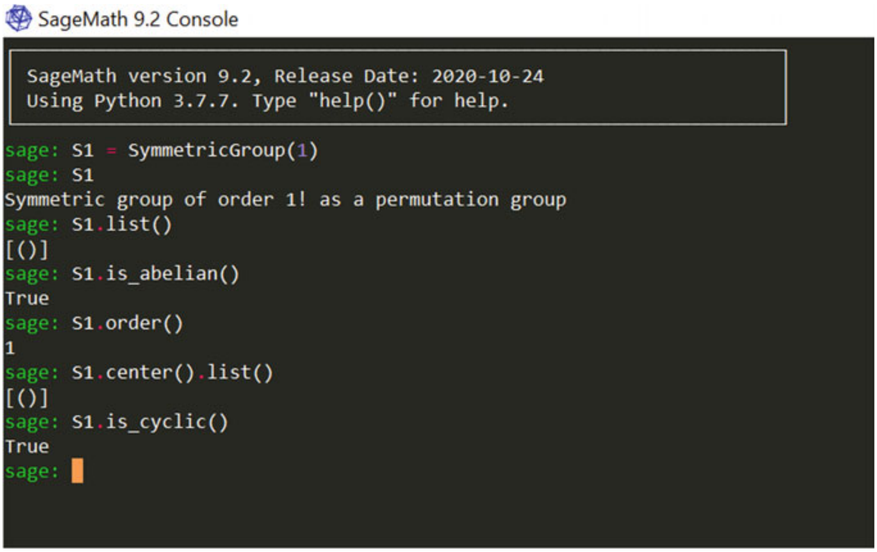
The command “SymmetricGroup (n)” creates the symmetric group $\mathfrak{S}_n$ and stores it in the software. Permutations can be defined in Sage using two methods. The first method uses rounded brackets to implement a permutation as a finite product of cycles. For example, to represent

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \in S_5$$

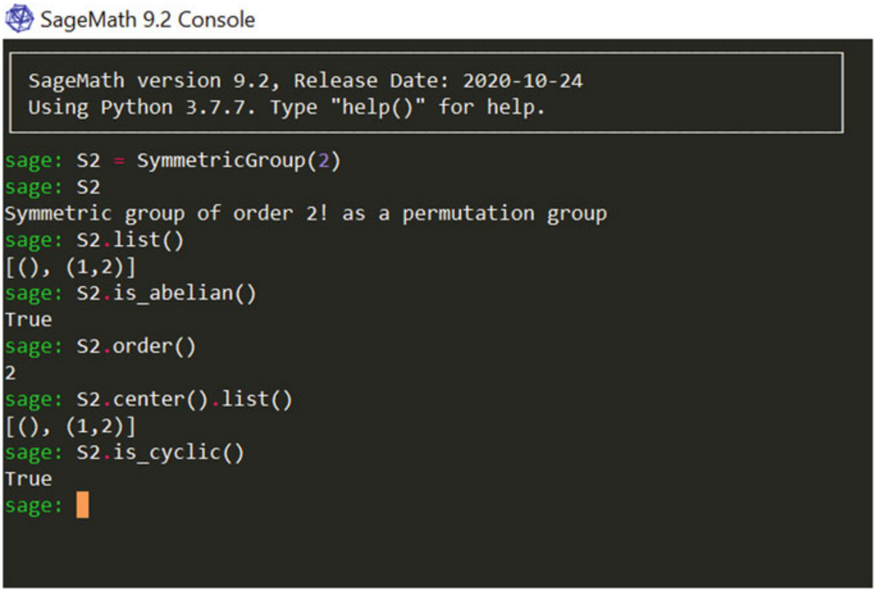
in Sage, one must type ″(1, 3, 5)(2, 4)″. The second method uses square brackets with the numbers between the square brackets representing the value for their position. For example, to represent the permutation ρ using square brackets, one must type ″[3, 4, 5, 2, 1]″. The identity permutation is implemented in Sage using the command “()”. Other commands are also available, as shown in the following display boxes:

- “is_abelian()”, which verifies whether any group is abelian.
- “center() ”, which computes the center of any given group.

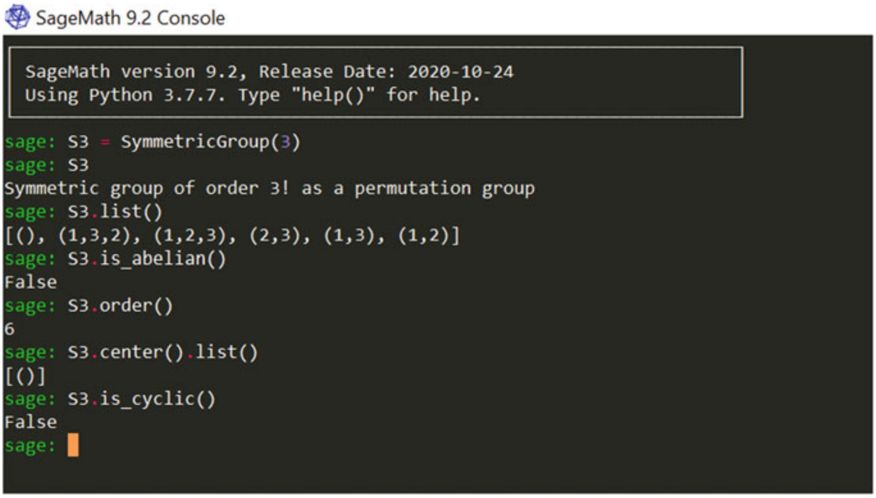
- “order().list”, which computes the center of the given group and lists its elements.



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S1 = SymmetricGroup(1)
sage: S1
Symmetric group of order 1! as a permutation group
sage: S1.list()
[()]
sage: S1.is_abelian()
True
sage: S1.order()
1
sage: S1.center().list()
[()]
sage: S1.is_cyclic()
True
sage:
```



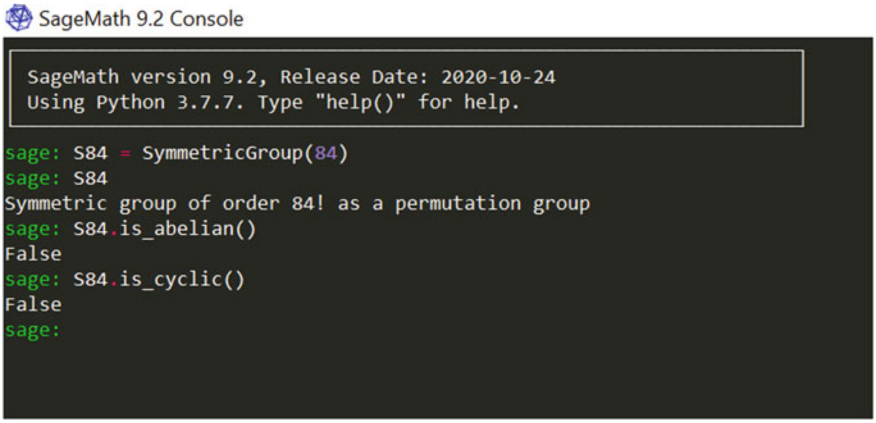
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S2 = SymmetricGroup(2)
sage: S2
Symmetric group of order 2! as a permutation group
sage: S2.list()
[(), (1,2)]
sage: S2.is_abelian()
True
sage: S2.order()
2
sage: S2.center().list()
[(), (1,2)]
sage: S2.is_cyclic()
True
sage:
```



SageMath 9.2 Console

```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: S3
Symmetric group of order 3! as a permutation group
sage: S3.list()
[(), (1,3,2), (1,2,3), (2,3), (1,3), (1,2)]
sage: S3.is_abelian()
False
sage: S3.order()
6
sage: S3.center().list()
[()]
sage: S3.is_cyclic()
False
sage: 
```

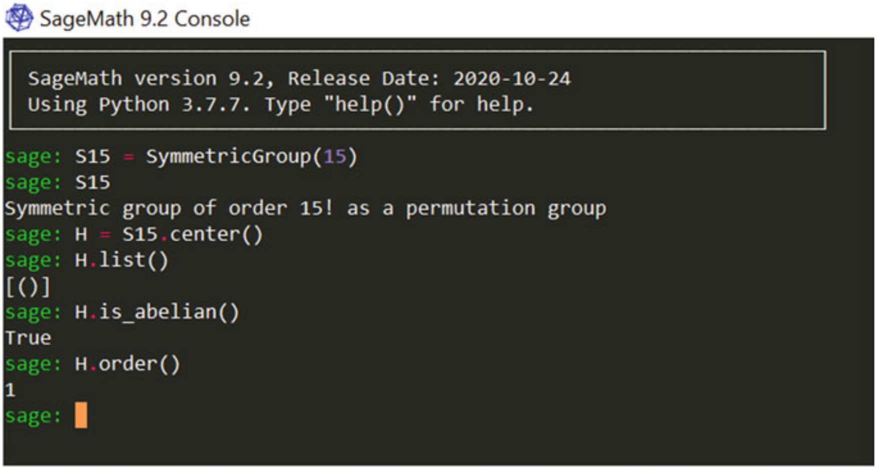
The following display box shows an example for the symmetric group of order $n = 84$.



SageMath 9.2 Console

```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S84 = SymmetricGroup(84)
sage: S84
Symmetric group of order 84! as a permutation group
sage: S84.is_abelian()
False
sage: S84.is_cyclic()
False
sage:
```

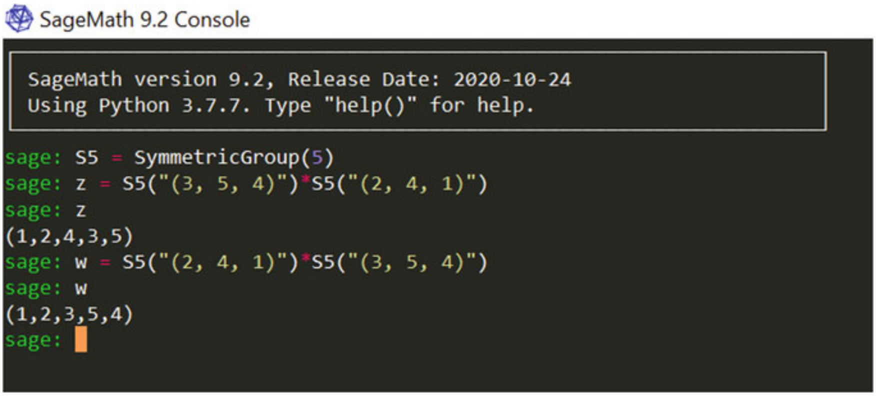
In the display box below, the center of the group is computed first, and then the command “list” lists all the elements of the center of the group.



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S15 = SymmetricGroup(15)
sage: S15
Symmetric group of order 15! as a permutation group
sage: H = S15.center()
sage: H.list()
[()]
sage: H.is_abelian()
True
sage: H.order()
1
sage: 
```

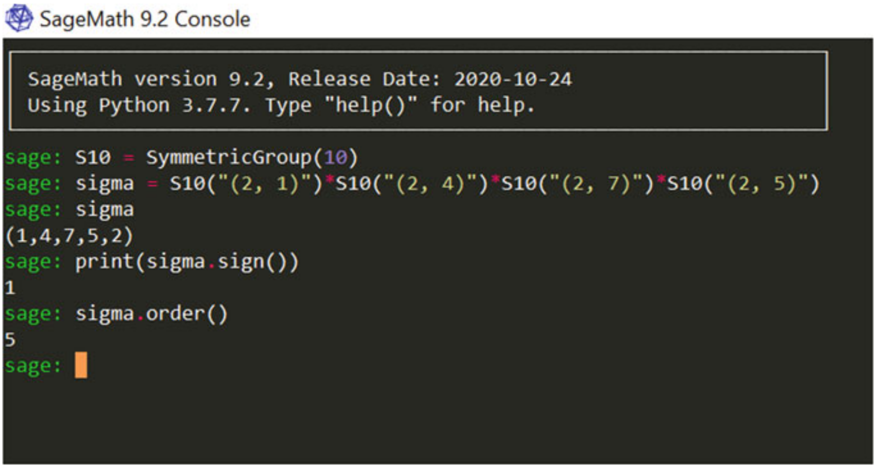
The composition of two maps in mathematics is conducted from right to left. However, in Sage, the composition of permutations are applied from left to right. Therefore, the multiplication (composition) of two permutations in Sage is reversed. For example, to find the product $(2\ 4\ 1)(3\ 5\ 4)$ as an element in $\mathfrak{S}_n$, Sage uses the command

$$\mathfrak{S}_n("(3, 5, 4)") * \mathfrak{S}_n("(2, 4, 1)") \text{ or } \mathfrak{S}_n\left('(3, 5, 4)'\right) * \mathfrak{S}_n\left('(2, 4, 1)'\right).$$



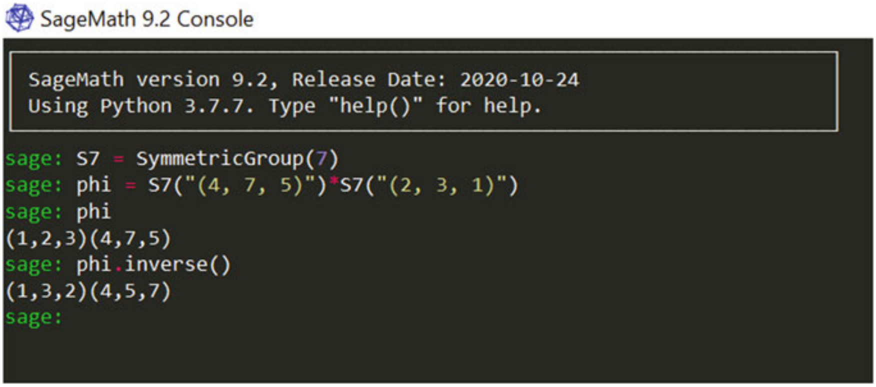
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S5 = SymmetricGroup(5)
sage: z = S5("(3, 5, 4)")*S5("(2, 4, 1)")
sage: z
(1,2,4,3,5)
sage: w = S5("(2, 4, 1)")*S5("(3, 5, 4)")
sage: w
(1,2,3,5,4)
sage: 
```

To find the sign and order of a permutation, the commands “sign()” and “order()” are used, respectively.

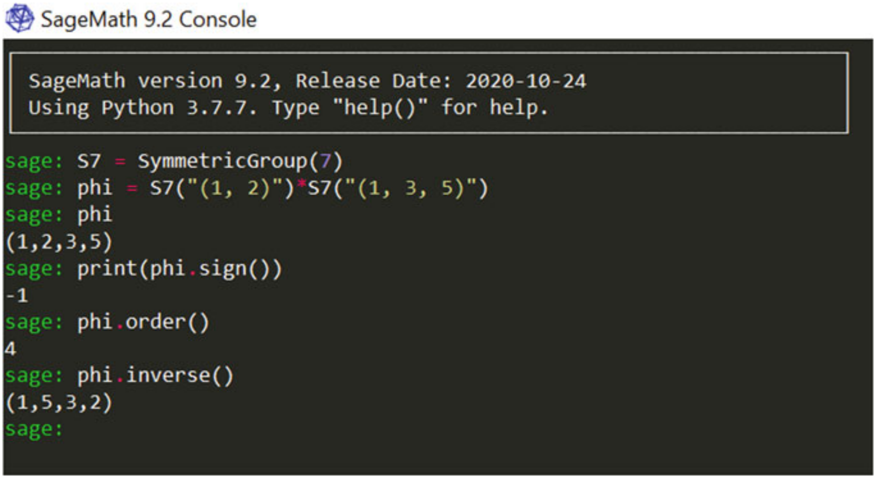


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S10 = SymmetricGroup(10)
sage: sigma = S10("(2, 1)")*S10("(2, 4)")*S10("(2, 7)")*S10("(2, 5)")
sage: sigma
(1,4,7,5,2)
sage: print(sigma.sign())
1
sage: sigma.order()
5
sage:
```

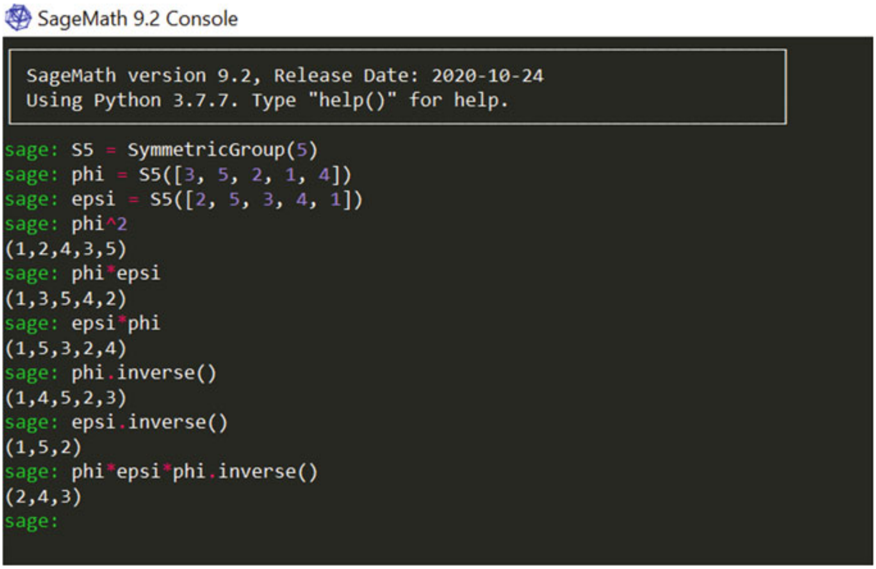
The inverse of any element *m* in a symmetric group can be computed using the command “m.inverse()”, where *m* is the permutation. See the list of examples below.



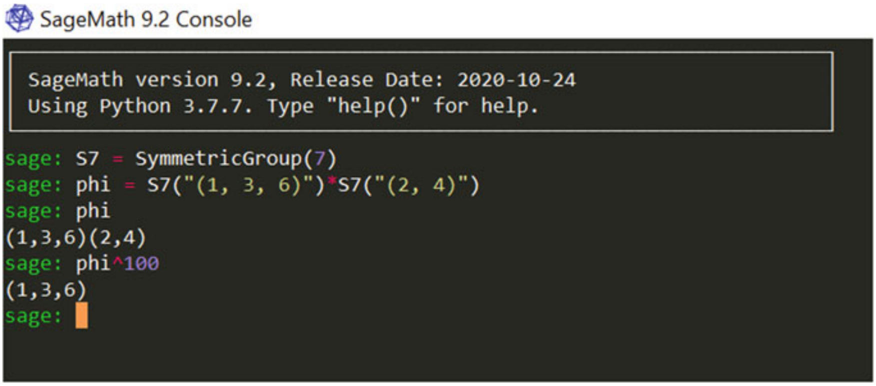
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S7 = SymmetricGroup(7)
sage: phi = S7("(4, 7, 5)")*S7("(2, 3, 1)")
sage: phi
(1,2,3)(4,7,5)
sage: phi.inverse()
(1,3,2)(4,5,7)
sage:
```



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S7 = SymmetricGroup(7)
sage: phi = S7("(1, 2)")*S7("(1, 3, 5)")
sage: phi
(1,2,3,5)
sage: print(phi.sign())
-1
sage: phi.order()
4
sage: phi.inverse()
(1,5,3,2)
sage:
```

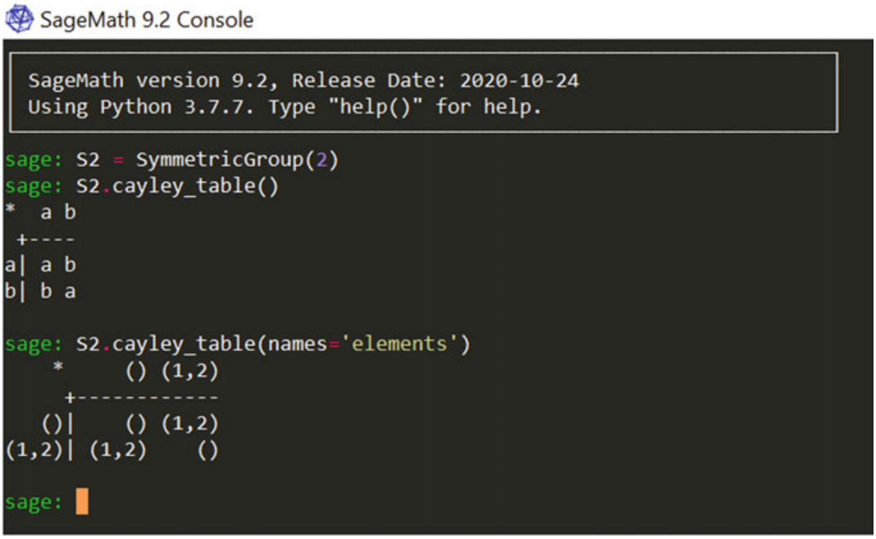


```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S5 = SymmetricGroup(5)
sage: phi = S5([3, 5, 2, 1, 4])
sage: epsi = S5([2, 5, 3, 4, 1])
sage: phi^2
(1,2,4,3,5)
sage: phi*epsi
(1,3,5,4,2)
sage: epsi*phi
(1,5,3,2,4)
sage: phi.inverse()
(1,4,5,2,3)
sage: epsi.inverse()
(1,5,2)
sage: phi*epsi*phi.inverse()
(2,4,3)
sage:
```



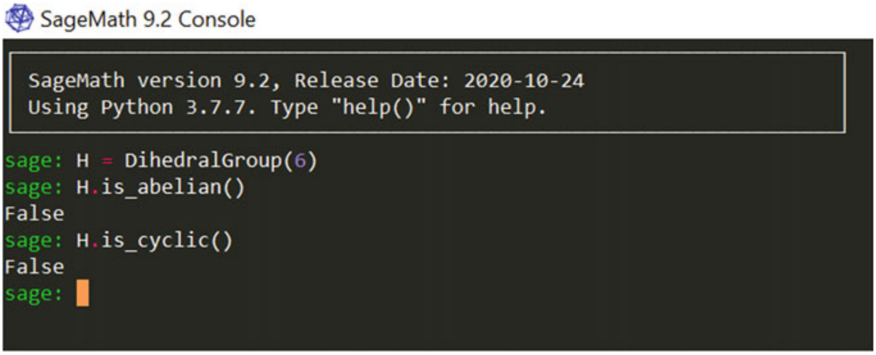
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S7 = SymmetricGroup(7)
sage: phi = S7("(1, 3, 6)")*S7("(2, 4)")
sage: phi
(1,3,6)(2,4)
sage: phi^100
(1,3,6)
sage: 
```

To find Cayley’s table for the symmetric group $\mathfrak{S}_n$, the command “$\mathfrak{S}_n$.cayley_table()” is used, after defining $\mathfrak{S}_n$ in Sage. This command generates Cayley’ table for $\mathfrak{S}_n$ in terms of letters “a, b, c, …”. To view the table in terms of $\mathfrak{S}_n$ permutations, the command “names =‘elememts’” is used.



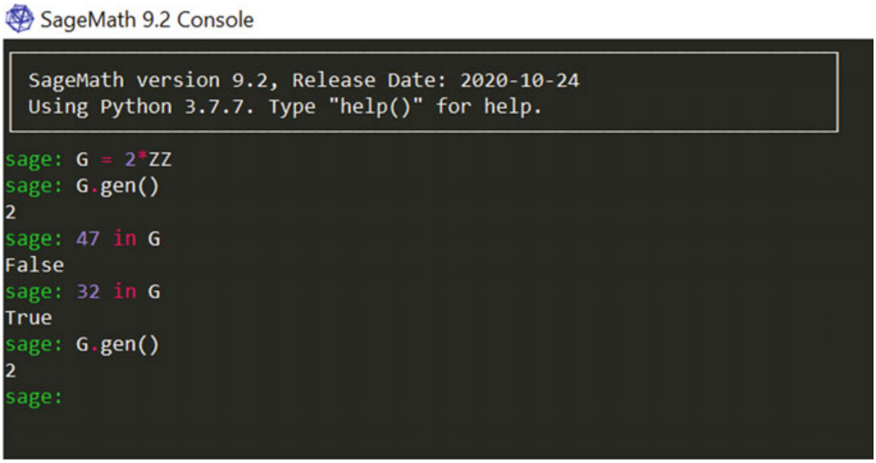
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S2 = SymmetricGroup(2)
sage: S2.cayley_table()
*  a b
 +----
a| a b
b| b a

sage: S2.cayley_table(names='elements')
    *      () (1,2)
     +------------
   ()|     () (1,2)
(1,2)| (1,2)    ()

sage: 
```

The dihedral group can be defined in Sage by using the command “DihedralGroup()”.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: H = DihedralGroup(6)
sage: H.is_abelian()
False
sage: H.is_cyclic()
False
sage: 
```

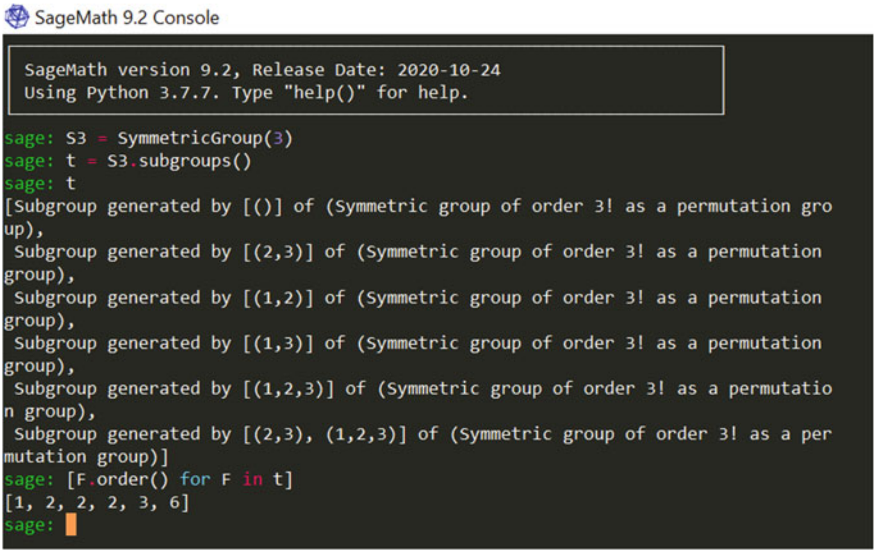
The commands “2*ZZ”, “3*ZZ” , $\cdots$,“m*ZZ” are used for $2\mathbb{Z}$, $3\mathbb{Z}$, $\cdots$, $m\mathbb{Z}$, respectively, as shown below.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: G = 2*ZZ
sage: G.gen()
2
sage: 47 in G
False
sage: 32 in G
True
sage: G.gen()
2
sage:
```

10.2.4 Commands Related to Subgroups

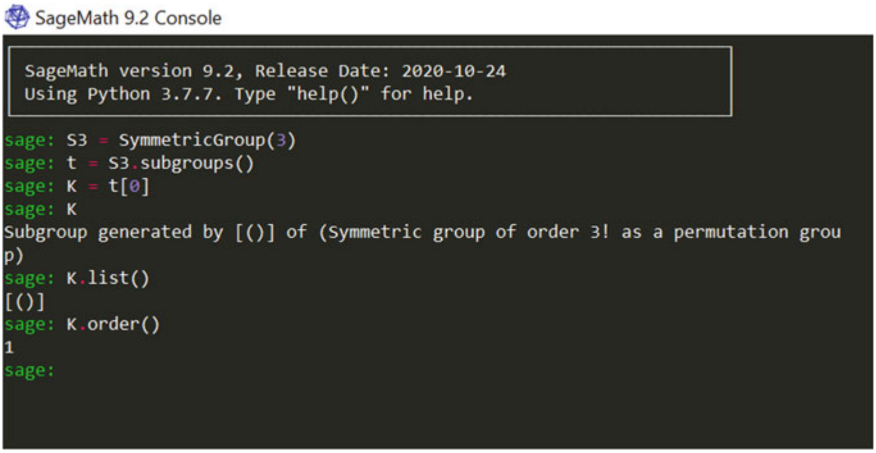
In this subsection, we consider the commands related to subgroups and their properties such as the generating of subgroups, normality of subgroups, and cosets. To create cyclic subgroups of a given group G, the command “subgroups()” is used. In the following display box, all cyclic subgroups of the symmetric group $\mathfrak{S}_3$ are computed in Sage. There exist six different subgroups of S_3. The command “[F.order() for F in t]” is implemented to find the orders of all subgroups, where t denotes the set of all cyclic subgroups.



SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: t = S3.subgroups()
sage: t
[Subgroup generated by [()] of (Symmetric group of order 3! as a permutation gro
up),
 Subgroup generated by [(2,3)] of (Symmetric group of order 3! as a permutation
group),
 Subgroup generated by [(1,2)] of (Symmetric group of order 3! as a permutation
group),
 Subgroup generated by [(1,3)] of (Symmetric group of order 3! as a permutation
group),
 Subgroup generated by [(1,2,3)] of (Symmetric group of order 3! as a permutatio
n group),
 Subgroup generated by [(2,3), (1,2,3)] of (Symmetric group of order 3! as a per
mutation group)]
sage: [F.order() for F in t]
[1, 2, 2, 2, 3, 6]
sage: 
```

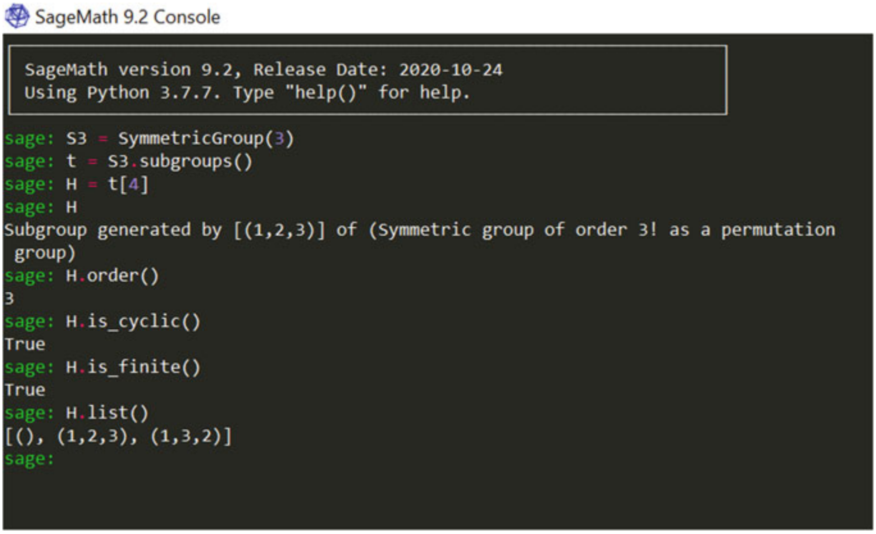
After creating the set of all subgroups of $\mathfrak{S}_n$, any of these subgroups can be selected, and their algebraic properties can be examined. The following example creates the set t of all subgroups of $\mathfrak{S}_3$, selects the first one, list its elements, and computes its order. Note that the command "$k = t\,[n]$" selects the $(n-1)^{\text{th}}$ subgroup of the list t.



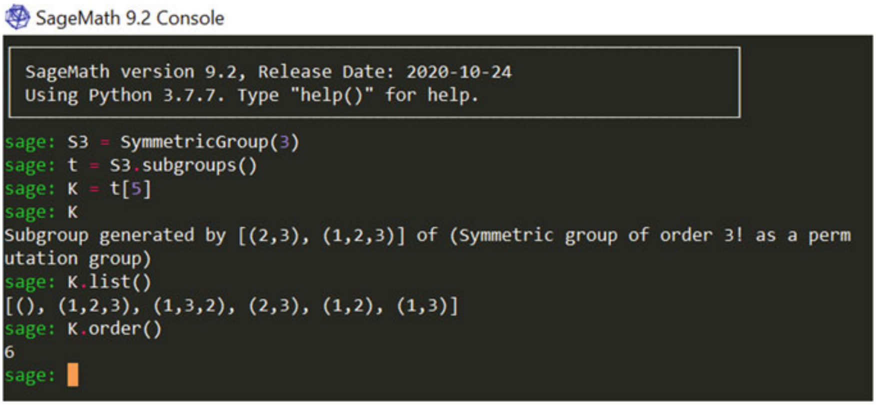
SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: t = S3.subgroups()
sage: K = t[0]
sage: K
Subgroup generated by [()] of (Symmetric group of order 3! as a permutation grou
p)
sage: K.list()
[()]
sage: K.order()
1
sage: 
```

The following two examples redo the example above, with selecting the fourth and third subgroups of $\mathfrak{S}_3$, respectively.

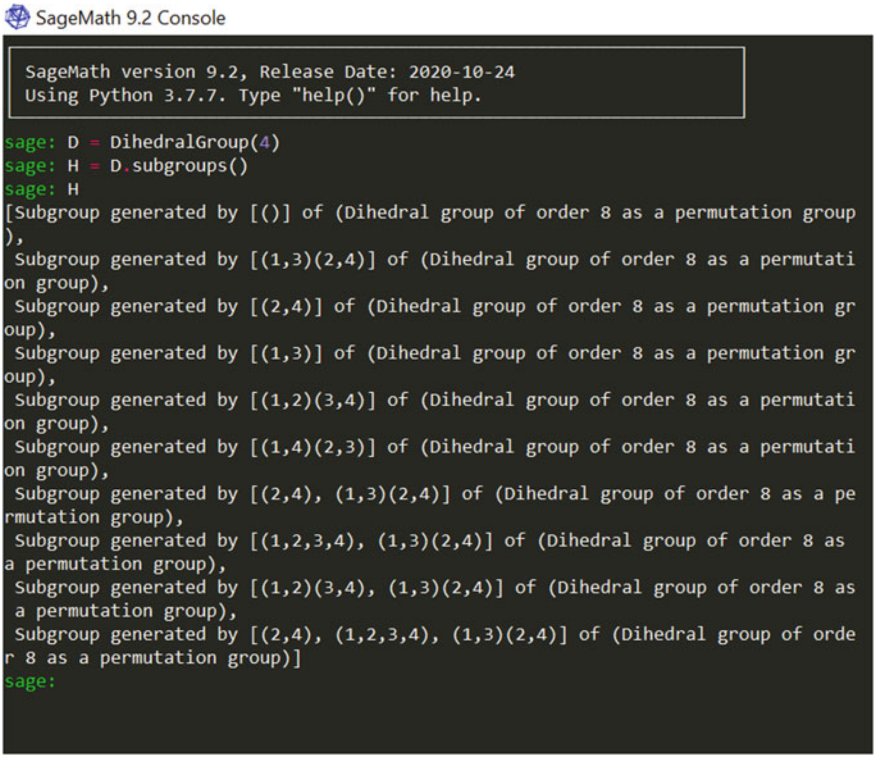


```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: t = S3.subgroups()
sage: H = t[4]
sage: H
Subgroup generated by [(1,2,3)] of (Symmetric group of order 3! as a permutation
 group)
sage: H.order()
3
sage: H.is_cyclic()
True
sage: H.is_finite()
True
sage: H.list()
[(), (1,2,3), (1,3,2)]
sage:
```



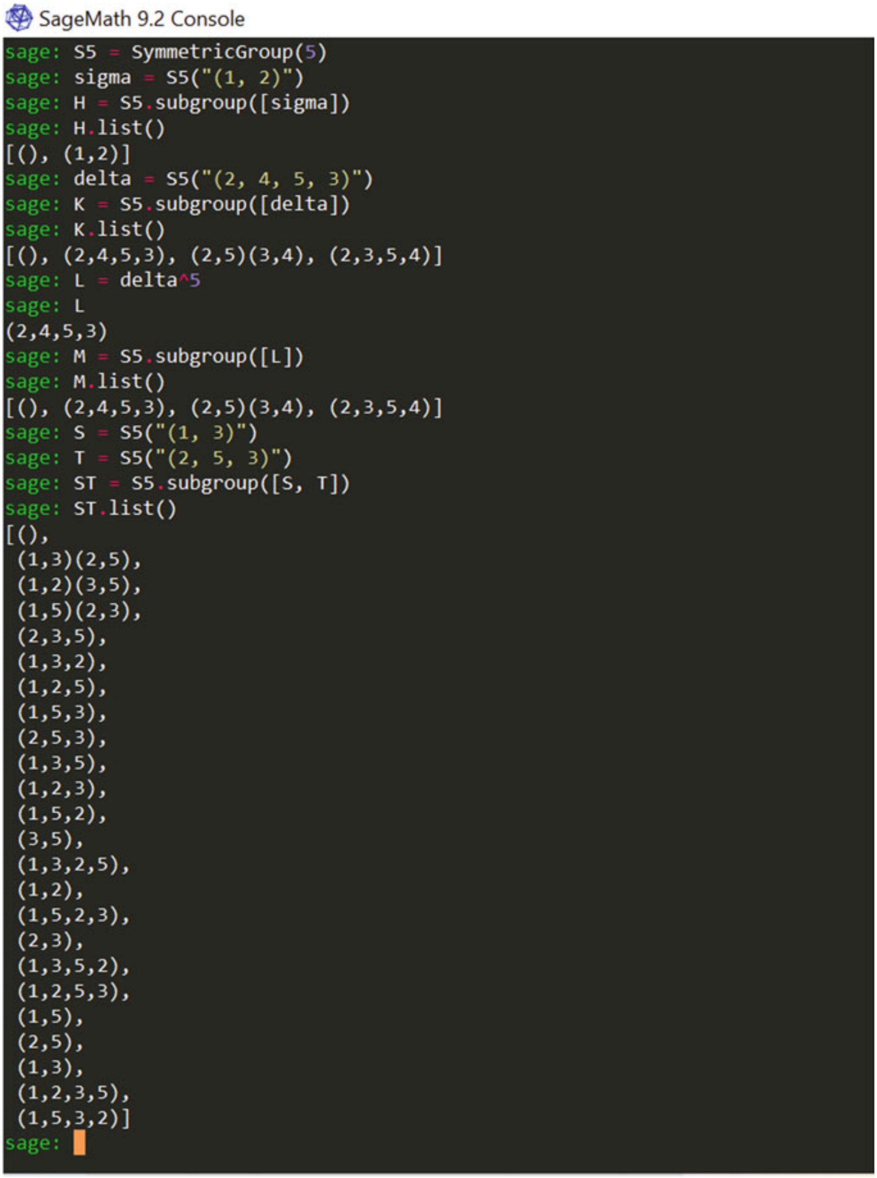
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: t = S3.subgroups()
sage: K = t[5]
sage: K
Subgroup generated by [(2,3), (1,2,3)] of (Symmetric group of order 3! as a perm
utation group)
sage: K.list()
[(), (1,2,3), (1,3,2), (2,3), (1,2), (1,3)]
sage: K.order()
6
sage:
```

All cyclic subgroups of the dihedral group D_4 can be computed, as shown in the following example.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: D = DihedralGroup(4)
sage: H = D.subgroups()
sage: H
[Subgroup generated by [()] of (Dihedral group of order 8 as a permutation group
),
 Subgroup generated by [(1,3)(2,4)] of (Dihedral group of order 8 as a permutati
on group),
 Subgroup generated by [(2,4)] of (Dihedral group of order 8 as a permutation gr
oup),
 Subgroup generated by [(1,3)] of (Dihedral group of order 8 as a permutation gr
oup),
 Subgroup generated by [(1,2)(3,4)] of (Dihedral group of order 8 as a permutati
on group),
 Subgroup generated by [(1,4)(2,3)] of (Dihedral group of order 8 as a permutati
on group),
 Subgroup generated by [(2,4), (1,3)(2,4)] of (Dihedral group of order 8 as a pe
rmutation group),
 Subgroup generated by [(1,2,3,4), (1,3)(2,4)] of (Dihedral group of order 8 as
a permutation group),
 Subgroup generated by [(1,2)(3,4), (1,3)(2,4)] of (Dihedral group of order 8 as
 a permutation group),
 Subgroup generated by [(2,4), (1,2,3,4), (1,3)(2,4)] of (Dihedral group of orde
r 8 as a permutation group)]
sage:
```

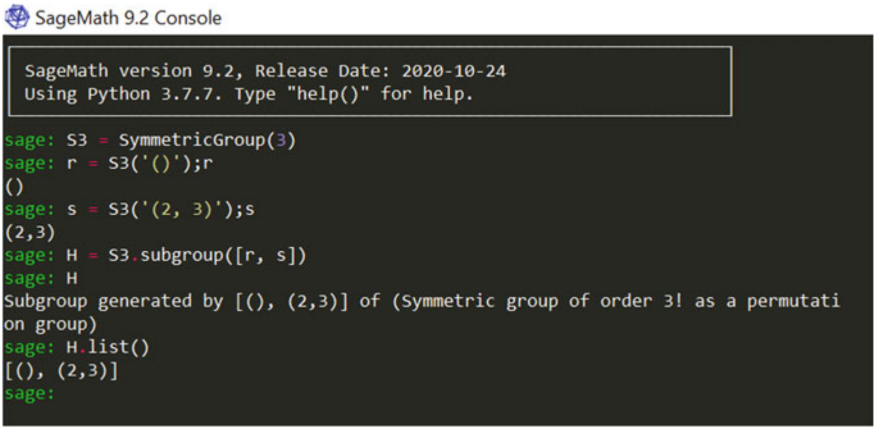
To create the subgroup generated by the subset $\{a, b, c, \ldots\}$ of a given group G, the command "G.subgroup ([$a, b, c, \ldots$])" is used. The command "G.subgroup ([b])" creates the cyclic subgroup of G generated by b.



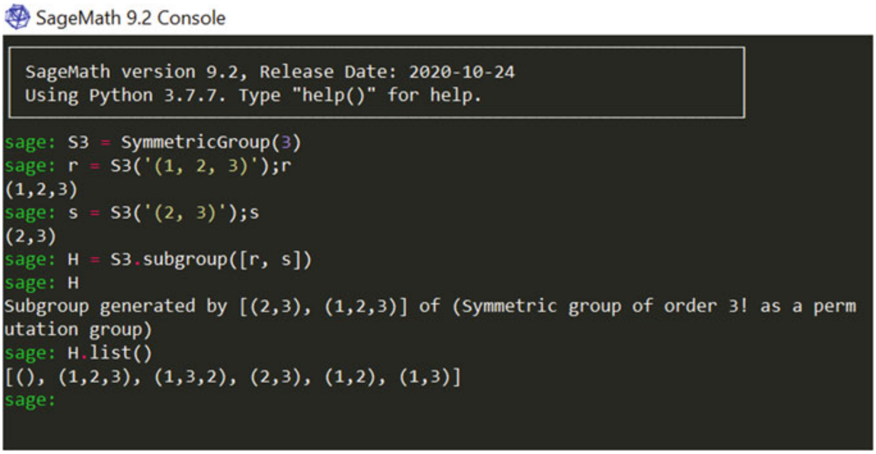
SageMath 9.2 Console

```
sage: S5 = SymmetricGroup(5)
sage: sigma = S5("(1, 2)")
sage: H = S5.subgroup([sigma])
sage: H.list()
[(), (1,2)]
sage: delta = S5("(2, 4, 5, 3)")
sage: K = S5.subgroup([delta])
sage: K.list()
[(), (2,4,5,3), (2,5)(3,4), (2,3,5,4)]
sage: L = delta^5
sage: L
(2,4,5,3)
sage: M = S5.subgroup([L])
sage: M.list()
[(), (2,4,5,3), (2,5)(3,4), (2,3,5,4)]
sage: S = S5("(1, 3)")
sage: T = S5("(2, 5, 3)")
sage: ST = S5.subgroup([S, T])
sage: ST.list()
[(),
 (1,3)(2,5),
 (1,2)(3,5),
 (1,5)(2,3),
 (2,3,5),
 (1,3,2),
 (1,2,5),
 (1,5,3),
 (2,5,3),
 (1,3,5),
 (1,2,3),
 (1,5,2),
 (3,5),
 (1,3,2,5),
 (1,2),
 (1,5,2,3),
 (2,3),
 (1,3,5,2),
 (1,2,5,3),
 (1,5),
 (2,5),
 (1,3),
 (1,2,3,5),
 (1,5,3,2)]
sage: 
```

In the following display boxes, the subgroups of the symmetric group $\mathfrak{S}_3$ that are generated by (2 3) and (1 2 3) are computed. Note that the semicolon is used to implement the two commands simultaneously.

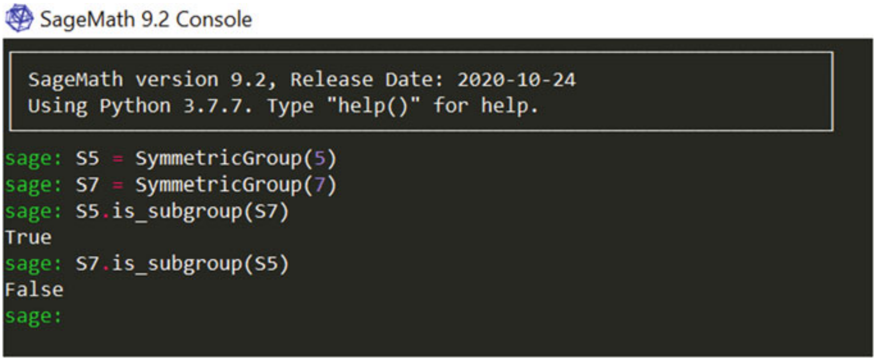


```
SageMath 9.2 Console

 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: r = S3('()');r
()
sage: s = S3('(2, 3)');s
(2,3)
sage: H = S3.subgroup([r, s])
sage: H
Subgroup generated by [(), (2,3)] of (Symmetric group of order 3! as a permutati
on group)
sage: H.list()
[(), (2,3)]
sage:
```



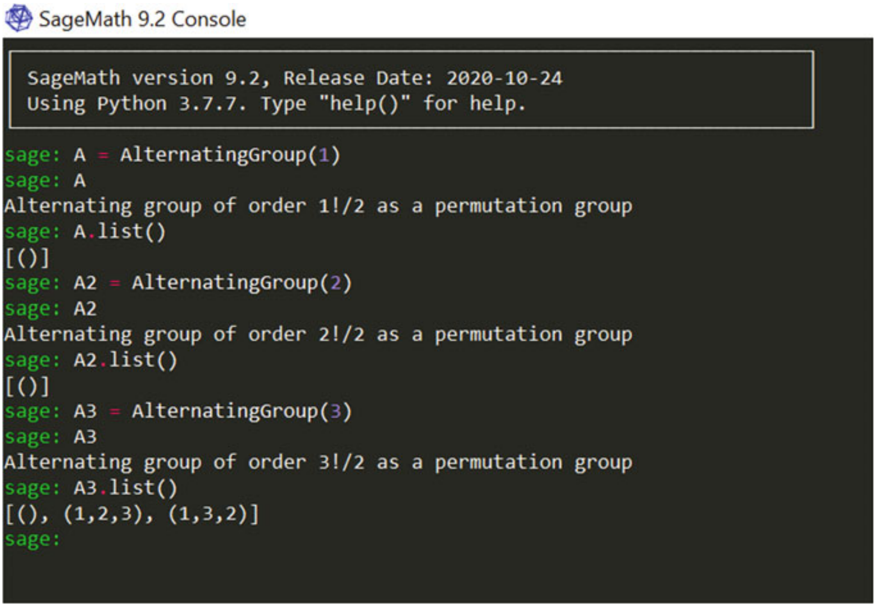
```
SageMath 9.2 Console

 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: r = S3('(1, 2, 3)');r
(1,2,3)
sage: s = S3('(2, 3)');s
(2,3)
sage: H = S3.subgroup([r, s])
sage: H
Subgroup generated by [(2,3), (1,2,3)] of (Symmetric group of order 3! as a perm
utation group)
sage: H.list()
[(), (1,2,3), (1,3,2), (2,3), (1,2), (1,3)]
sage:
```

To check whether group A is a subgroup of group B, the command "A.is_subgroup(B)" is used in Sage, as shown in the following box.



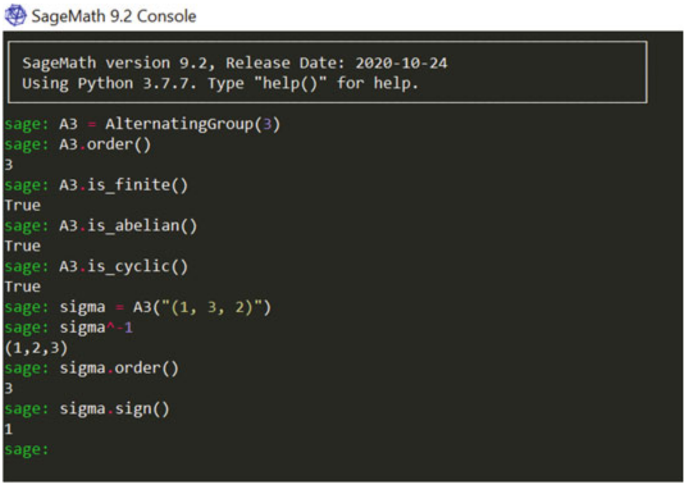
```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S5 = SymmetricGroup(5)
sage: S7 = SymmetricGroup(7)
sage: S5.is_subgroup(S7)
True
sage: S7.is_subgroup(S5)
False
sage:
```

The alternating group $\mathcal{A}_n$, the set of all even permutations in the nth symmetric group, is defined in Sage using the command “AlternatingGroup(n)”. See the following box for the alternating groups $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$.

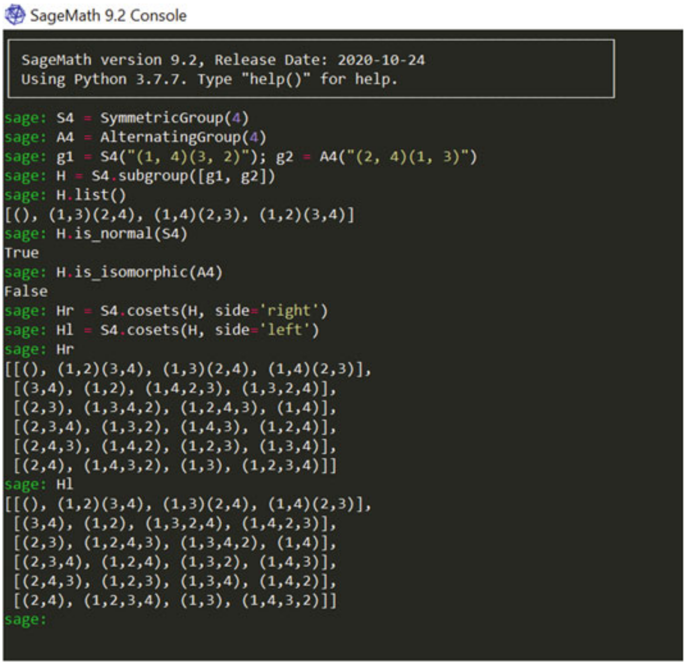


```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: A = AlternatingGroup(1)
sage: A
Alternating group of order 1!/2 as a permutation group
sage: A.list()
[()]
sage: A2 = AlternatingGroup(2)
sage: A2
Alternating group of order 2!/2 as a permutation group
sage: A2.list()
[()]
sage: A3 = AlternatingGroup(3)
sage: A3
Alternating group of order 3!/2 as a permutation group
sage: A3.list()
[(), (1,2,3), (1,3,2)]
sage:
```

In the display box below, the alternating group for $n = 3$ is created, and many commands are applied to check its properties.



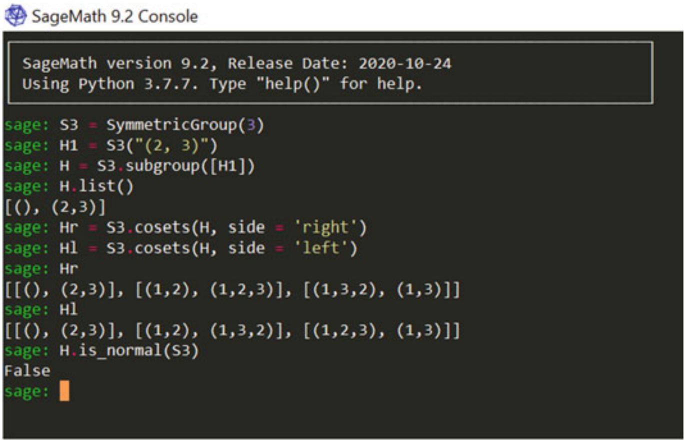
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A3 = AlternatingGroup(3)
sage: A3.order()
3
sage: A3.is_finite()
True
sage: A3.is_abelian()
True
sage: A3.is_cyclic()
True
sage: sigma = A3("(1, 3, 2)")
sage: sigma^-1
(1,2,3)
sage: sigma.order()
3
sage: sigma.sign()
1
sage:
```



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S4 = SymmetricGroup(4)
sage: A4 = AlternatingGroup(4)
sage: g1 = S4("(1, 4)(3, 2)"); g2 = A4("(2, 4)(1, 3)")
sage: H = S4.subgroup([g1, g2])
sage: H.list()
[(), (1,3)(2,4), (1,4)(2,3), (1,2)(3,4)]
sage: H.is_normal(S4)
True
sage: H.is_isomorphic(A4)
False
sage: Hr = S4.cosets(H, side='right')
sage: Hl = S4.cosets(H, side='left')
sage: Hr
[[(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)],
 [(3,4), (1,2), (1,4,2,3), (1,3,2,4)],
 [(2,3), (1,3,4,2), (1,2,4,3), (1,4)],
 [(2,3,4), (1,3,2), (1,4,3), (1,2,4)],
 [(2,4,3), (1,4,2), (1,2,3), (1,3,4)],
 [(2,4), (1,4,3,2), (1,3), (1,2,3,4)]]
sage: Hl
[[(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)],
 [(3,4), (1,2), (1,3,2,4), (1,4,2,3)],
 [(2,3), (1,2,4,3), (1,3,4,2), (1,4)],
 [(2,3,4), (1,2,4), (1,3,2), (1,4,3)],
 [(2,4,3), (1,2,3), (1,3,4), (1,4,2)],
 [(2,4), (1,2,3,4), (1,3), (1,4,3,2)]]
sage:
```

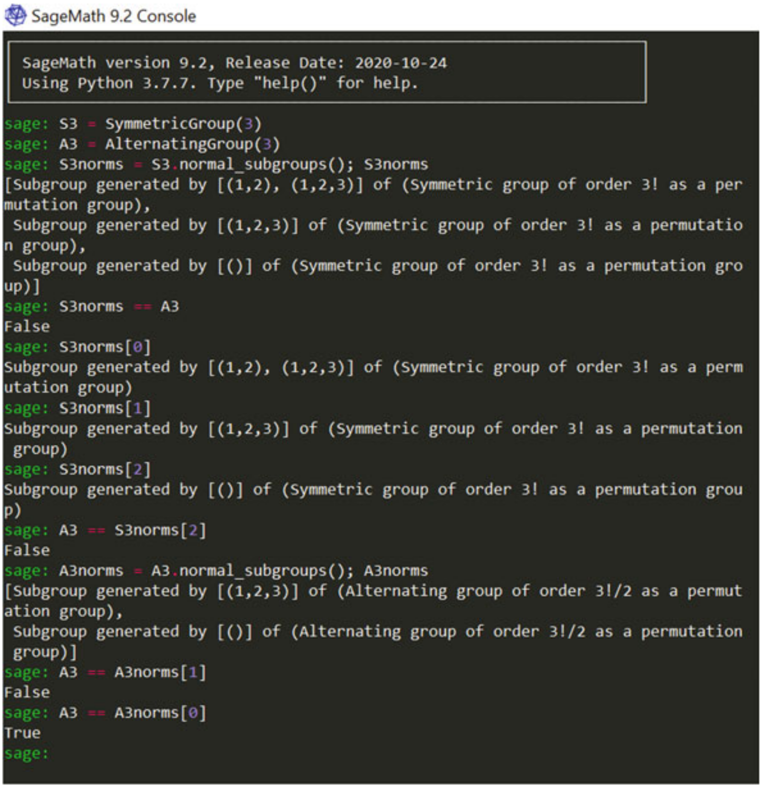
The display box above contains many commands for the symmetric group $\mathfrak{S}_4$ and alternating group $\mathcal{A}_4$. The right and left cosets are computed using the commands

"G.cosets(H, side =‘right’)" and
"G.cosets(H, side =‘left’)", respectively.



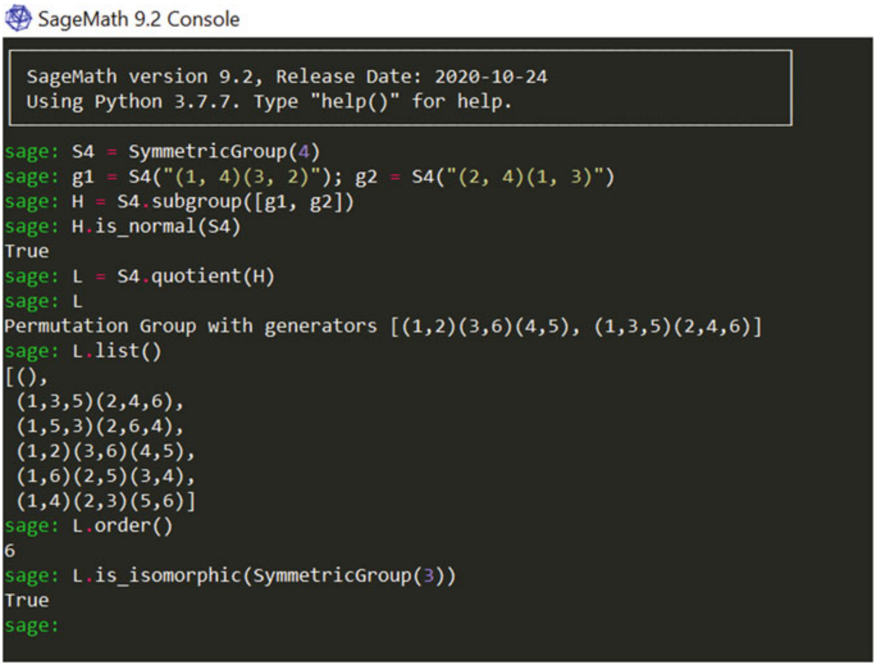
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: H1 = S3("(2, 3)")
sage: H = S3.subgroup([H1])
sage: H.list()
[(), (2,3)]
sage: Hr = S3.cosets(H, side = 'right')
sage: Hl = S3.cosets(H, side = 'left')
sage: Hr
[[(), (2,3)], [(1,2), (1,2,3)], [(1,3,2), (1,3)]]
sage: Hl
[[(), (2,3)], [(1,2), (1,3,2)], [(1,2,3), (1,3)]]
sage: H.is_normal(S3)
False
sage: 
```

To list all the normal subgroups of a given group, the command “normal_subgroups()” is used in Sage. In the following example, Sage creates all normal subgroups of $\mathfrak{S}_3$ and arranges them in a list. To select the i^{th} normal group in the list, apply “S3norms[$i-1$]”, where S3norms is the given name for the normal subgroups of $\mathfrak{S}_3$. Recall that the equal sign is written in Sage as a double equality $'' =='' $. This sign can also be used to check the equality between two objects in Sage.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S3 = SymmetricGroup(3)
sage: A3 = AlternatingGroup(3)
sage: S3norms = S3.normal_subgroups(); S3norms
[Subgroup generated by [(1,2), (1,2,3)] of (Symmetric group of order 3! as a per
mutation group),
 Subgroup generated by [(1,2,3)] of (Symmetric group of order 3! as a permutatio
n group),
 Subgroup generated by [()] of (Symmetric group of order 3! as a permutation gro
up)]
sage: S3norms == A3
False
sage: S3norms[0]
Subgroup generated by [(1,2), (1,2,3)] of (Symmetric group of order 3! as a perm
utation group)
sage: S3norms[1]
Subgroup generated by [(1,2,3)] of (Symmetric group of order 3! as a permutation
 group)
sage: S3norms[2]
Subgroup generated by [()] of (Symmetric group of order 3! as a permutation grou
p)
sage: A3 == S3norms[2]
False
sage: A3norms = A3.normal_subgroups(); A3norms
[Subgroup generated by [(1,2,3)] of (Alternating group of order 3!/2 as a permut
ation group),
 Subgroup generated by [()] of (Alternating group of order 3!/2 as a permutation
 group)]
sage: A3 == A3norms[1]
False
sage: A3 == A3norms[0]
True
sage:
```

The quotient group is computed in Sage using the command “G.quotient(H)”, where H is a normal subgroup of the group G. Note that the elements of the quotient group cannot be identified with the cosets. The command “G.quotient()” creates a group that is isomorphic to the quotient group.



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S4 = SymmetricGroup(4)
sage: g1 = S4("(1, 4)(3, 2)"); g2 = S4("(2, 4)(1, 3)")
sage: H = S4.subgroup([g1, g2])
sage: H.is_normal(S4)
True
sage: L = S4.quotient(H)
sage: L
Permutation Group with generators [(1,2)(3,6)(4,5), (1,3,5)(2,4,6)]
sage: L.list()
[(),
 (1,3,5)(2,4,6),
 (1,5,3)(2,6,4),
 (1,2)(3,6)(4,5),
 (1,6)(2,5)(3,4),
 (1,4)(2,3)(5,6)]
sage: L.order()
6
sage: L.is_isomorphic(SymmetricGroup(3))
True
sage:
```

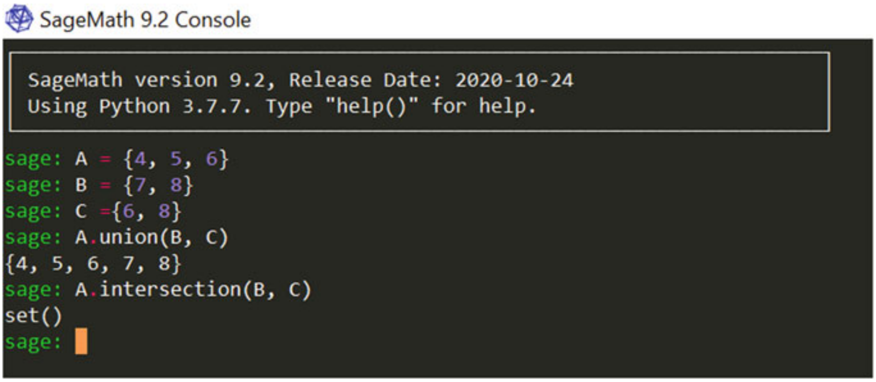
Remark: The codes which are used in this chapter are well known and inherited from the tutorials, reference manual, and construction of SageMath found in (SageMath, Welcome to Sage Tutorial!, 2019), (SageMath, Welcome to Sage Reference Manual!, 2019), and (SageMath, Welcome to Sage Constructions!, 2019).

Exercises

Solved Exercises

10.1 Let $A = \{4, 5, 6\}$, $B = \{7, 8\}$, and $C = \{6, 8\}$ be sets. Using Sage, find $A \cup B \cup C$ and $A \cap B \cap C$.

Solution:



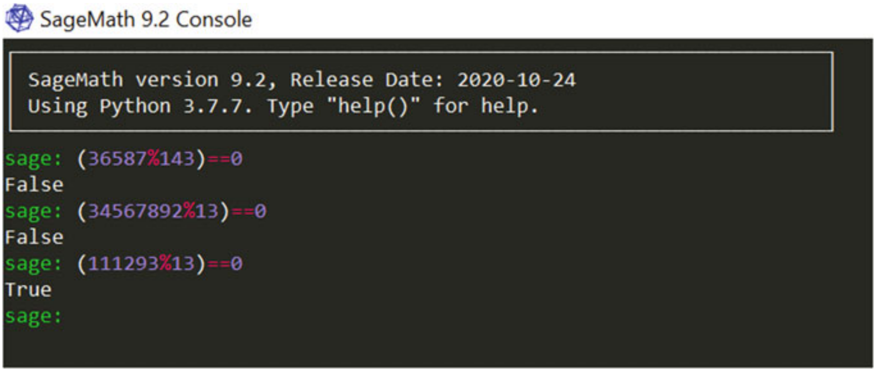
SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A = {4, 5, 6}
sage: B = {7, 8}
sage: C ={6, 8}
sage: A.union(B, C)
{4, 5, 6, 7, 8}
sage: A.intersection(B, C)
set()
sage:
```

10.2 Using Sage commands, find weather a is divisible by b in the following cases:

- $a = 36587$, $b = 143$.
- $a = 34567892$, $b = 13$.
- $a = 111293$, $b = 13$.

Solution:

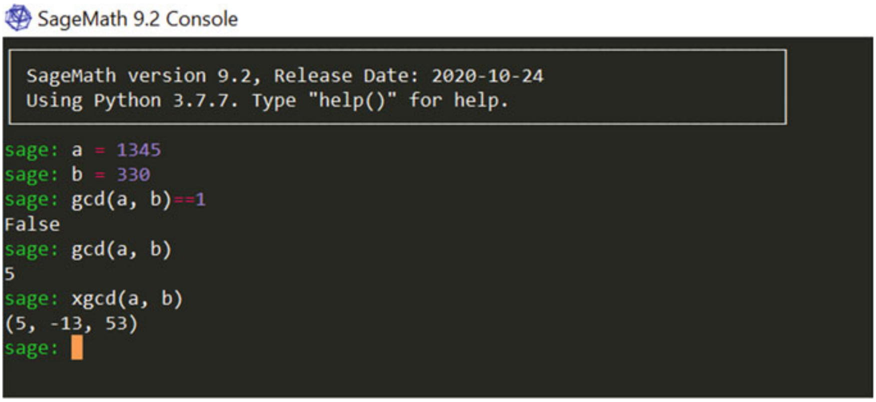


SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: (36587%143)==0
False
sage: (34567892%13)==0
False
sage: (111293%13)==0
True
sage:
```

10.3 Let $a = 1345$ and $b = 330$. Using Sage, check whether a and b are relatively prime. If not, find the greatest common divisor. What are the coefficients of the linear combination of the greatest common divisor of a and b?

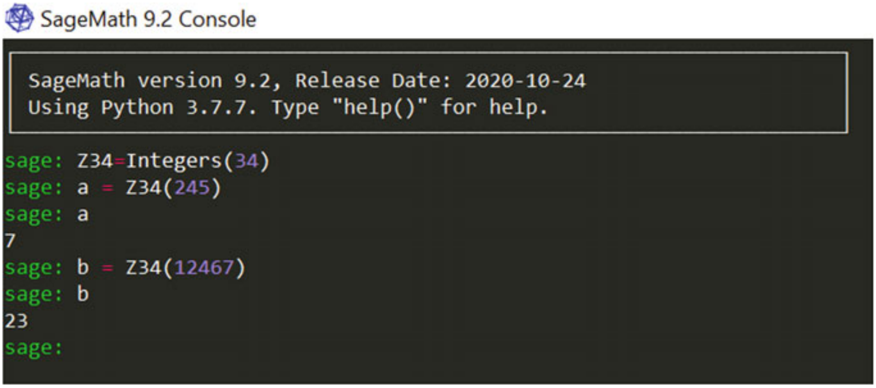
Solution:



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: a = 1345
sage: b = 330
sage: gcd(a, b)==1
False
sage: gcd(a, b)
5
sage: xgcd(a, b)
(5, -13, 53)
sage:
```

10.4 Consider the additive group $\mathbb{Z}_{34}$. Using Sage, find the elements $[a]$, $[b]$ in $\mathbb{Z}_{34}$, where $a = 245$ and $b = 12467$.

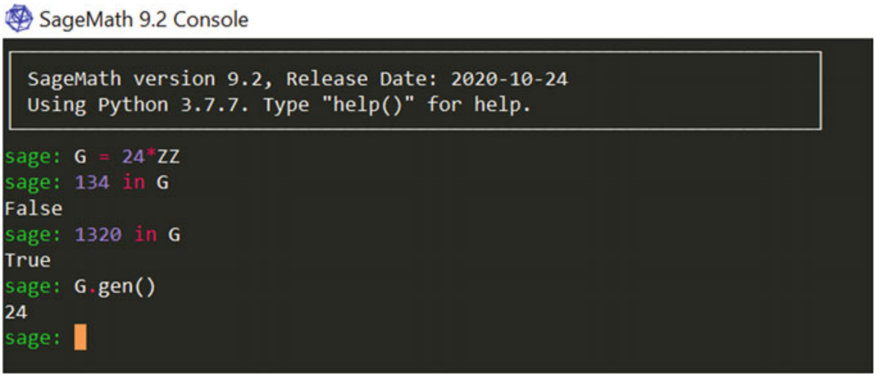
Solution:



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Z34=Integers(34)
sage: a = Z34(245)
sage: a
7
sage: b = Z34(12467)
sage: b
23
sage:
```

10.5 Consider the additive group $(\mathbb{Z}, +)$ and its subgroup $24\mathbb{Z}$. Using Sage, check if 134, and 1320 are elements in $24\mathbb{Z}$. What is the generator of $24\mathbb{Z}$?

Solution:



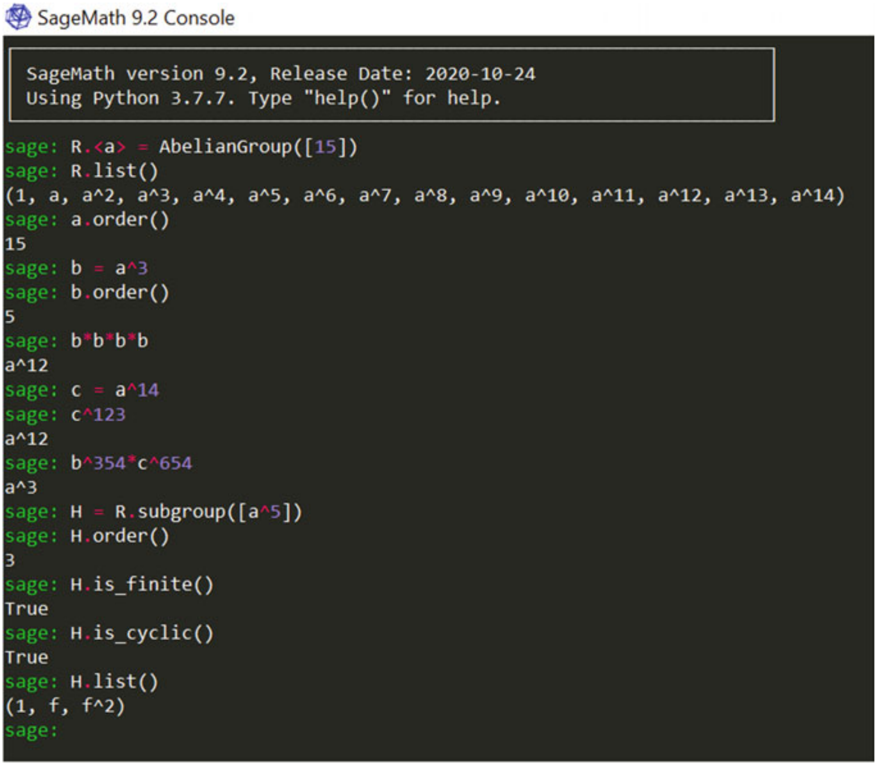
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: G = 24*ZZ
sage: 134 in G
False
sage: 1320 in G
True
sage: G.gen()
24
sage:
```

10.6 Let R be the multiplicative cyclic group of order 15, which is generated by a. Using Sage, answer the following questions:

- List the elements of R.
- Find $|R|$.
- Find ord(a^3).
- Let $b = a^3$, find $b * b * b * b$.
- Let $c = a^{14}$, find c^{123}
- Find $b^{354} * c^{654}$
- Find the subgroup of R generated by a^5 and name it H.
- Is H finite? Is it cyclic?
- Find $|H|$.

[To determine the generator in the cyclic group, the command “R. $<$ a $>=$ AbelianGroup([n]) ” is used, where “n” is the order of the group, and a is the generator]

Solution:



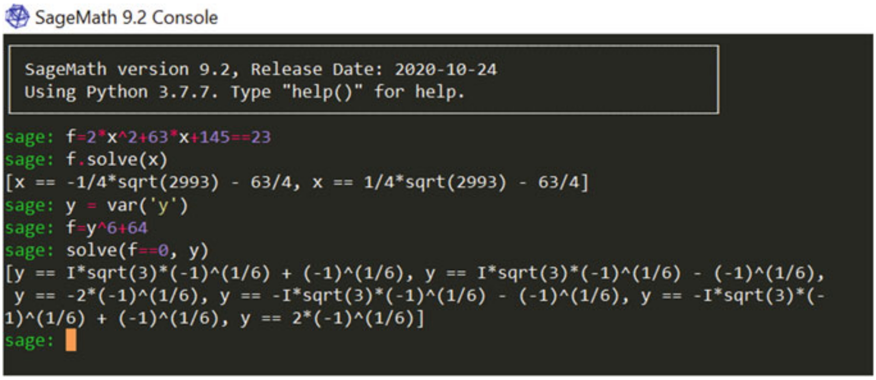
```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: R.<a> = AbelianGroup([15])
sage: R.list()
(1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^10, a^11, a^12, a^13, a^14)
sage: a.order()
15
sage: b = a^3
sage: b.order()
5
sage: b*b*b*b
a^12
sage: c = a^14
sage: c^123
a^12
sage: b^354*c^654
a^3
sage: H = R.subgroup([a^5])
sage: H.order()
3
sage: H.is_finite()
True
sage: H.is_cyclic()
True
sage: H.list()
(1, f, f^2)
sage:
```

10.7 Using Sage and a method different than that mentioned in Sect. 10.1.2.1, solve the following equations:

$$2x^2 + 63x + 145 = 23.$$

$$y^6 + 64 = 0.$$

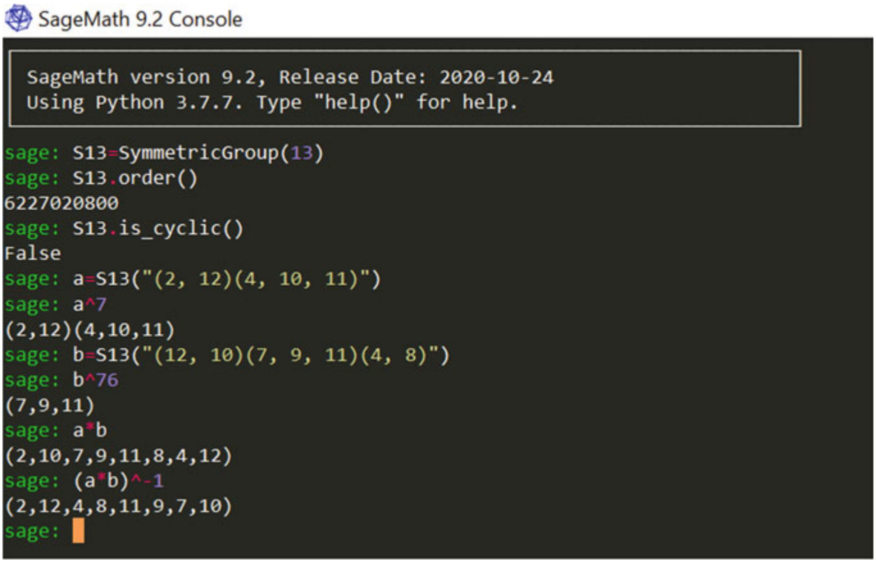
Solution:



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: f=2*x^2+63*x+145==23
sage: f.solve(x)
[x == -1/4*sqrt(2993) - 63/4, x == 1/4*sqrt(2993) - 63/4]
sage: y = var('y')
sage: f=y^6+64
sage: solve(f==0, y)
[y == I*sqrt(3)*(-1)^(1/6) + (-1)^(1/6), y == I*sqrt(3)*(-1)^(1/6) - (-1)^(1/6),
 y == -2*(-1)^(1/6), y == -I*sqrt(3)*(-1)^(1/6) - (-1)^(1/6), y == -I*sqrt(3)*(-
1)^(1/6) + (-1)^(1/6), y == 2*(-1)^(1/6)]
sage: 
```

10.8 Consider the symmetric group $\mathfrak{S}_{13}$. Using Sage, find the order of $\mathfrak{S}_{13}$. Is $\mathfrak{S}_{13}$ cyclic? If $a = \big(2\ 12\big)\big(4\ 10\ 11\big)$ and $b = \big(12\ 10\big)\big(7\ 9\ 11\big)\big(4\ 8\big)$, find a^7, a^{76}, ab, and $(ab)^{-1}$.

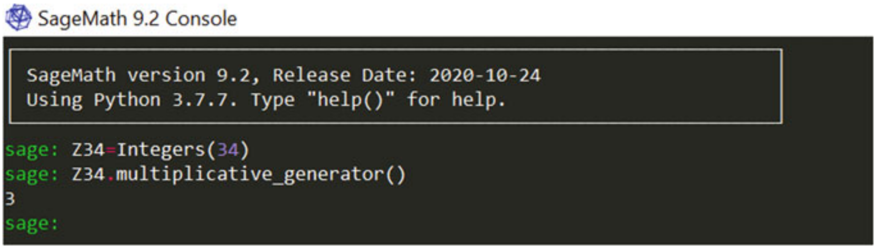
Solution:



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: S13=SymmetricGroup(13)
sage: S13.order()
6227020800
sage: S13.is_cyclic()
False
sage: a=S13("(2, 12)(4, 10, 11)")
sage: a^7
(2,12)(4,10,11)
sage: b=S13("(12, 10)(7, 9, 11)(4, 8)")
sage: b^76
(7,9,11)
sage: a*b
(2,10,7,9,11,8,4,12)
sage: (a*b)^-1
(2,12,4,8,11,9,7,10)
sage: 
```

10.9 Using Sage, find a generator of $\mathrm{Inv}(\mathbb{Z}_{34})$?

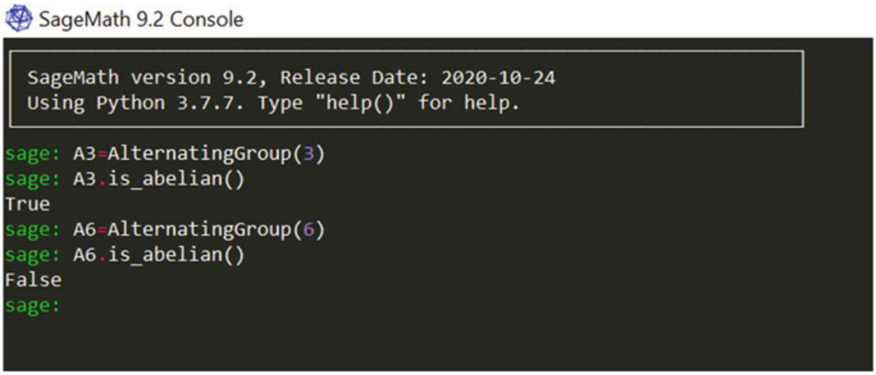
Solution:



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: Z34=Integers(34)
sage: Z34.multiplicative_generator()
3
sage:
```

10.10 Using Sage, determine if $\mathcal{A}_3$ and $\mathcal{A}_6$ are abelian.

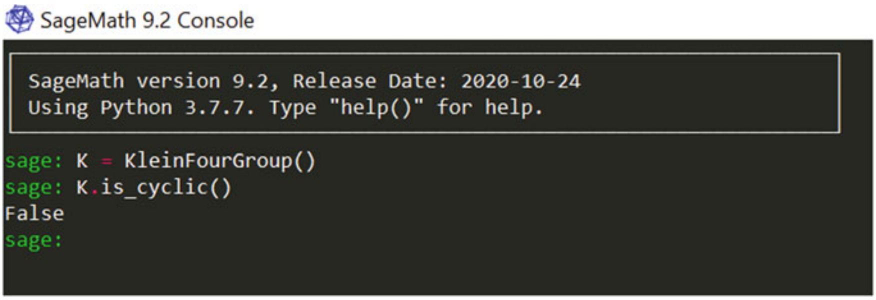
Solution:



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: A3=AlternatingGroup(3)
sage: A3.is_abelian()
True
sage: A6=AlternatingGroup(6)
sage: A6.is_abelian()
False
sage:
```

10.11 Consider the Klein group. Using Sage, check if the Klein group is cyclic.

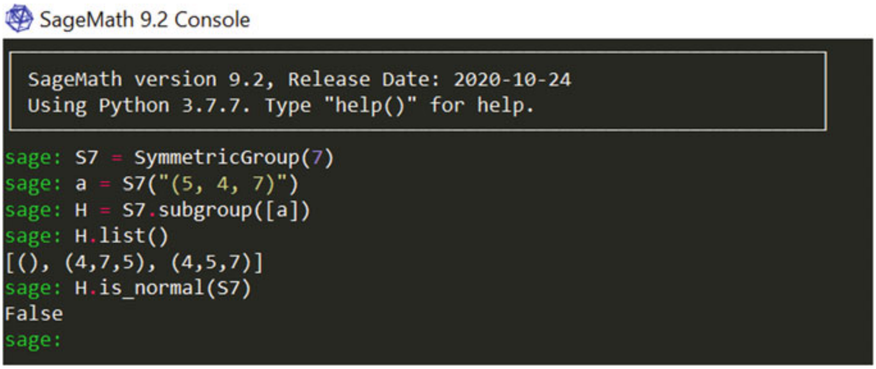
Solution:



```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: K = KleinFourGroup()
sage: K.is_cyclic()
False
sage:
```

10.12 Consider the symmetric group $\mathfrak{S}_7$. Using Sage, find the subgroup H of $\mathfrak{S}_7$ generated by $\begin{pmatrix}5\ 4\ 7\end{pmatrix}$. Is H normal?

Solution:



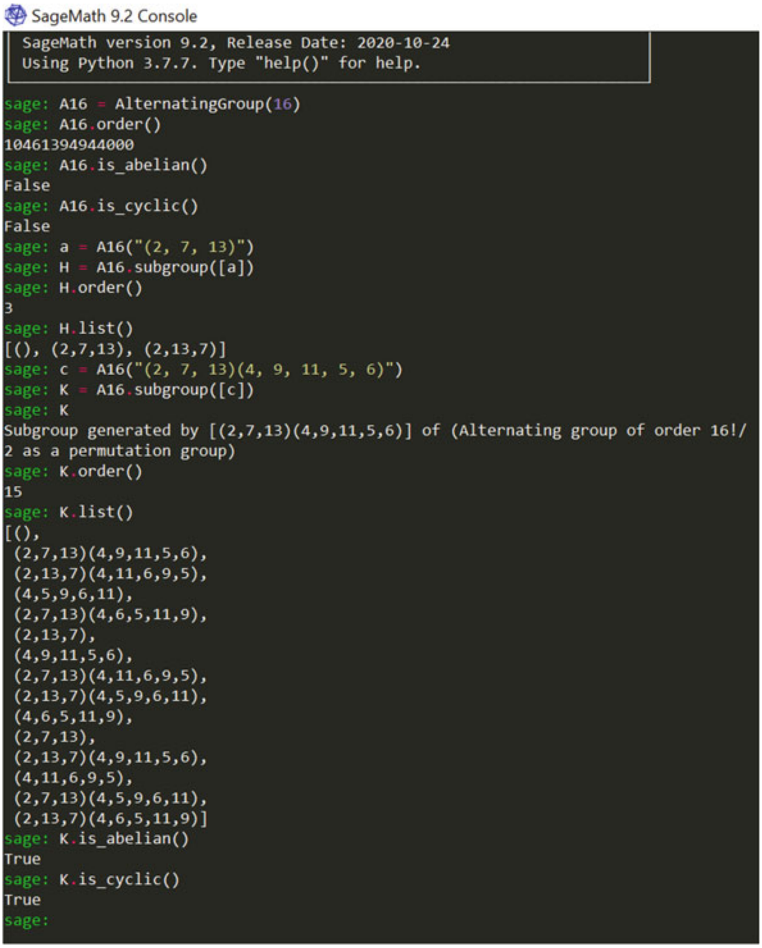
SageMath 9.2 Console

```
SageMath version 9.2, Release Date: 2020-10-24
Using Python 3.7.7. Type "help()" for help.

sage: S7 = SymmetricGroup(7)
sage: a = S7("(5, 4, 7)")
sage: H = S7.subgroup([a])
sage: H.list()
[(), (4,7,5), (4,5,7)]
sage: H.is_normal(S7)
False
sage:
```

10.13 Consider the group $\mathcal{A}_{16}$. Using Sage, find the order of $\mathcal{A}_{16}$. Is $\mathcal{A}_{16}$ abelian? Is it cyclic?

- If $a = \begin{pmatrix}2\ 7\ 13\end{pmatrix}$, find the subgroup H of $\mathcal{A}_{16}$ generated by a and its order.
- If $c = \begin{pmatrix}2\ 7\ 13\end{pmatrix}\begin{pmatrix}4\ 9\ 11\ 5\ 6\end{pmatrix}$, find the subgroup K of generated by c and its order.

Solution:



```
 SageMath version 9.2, Release Date: 2020-10-24
 Using Python 3.7.7. Type "help()" for help.

sage: A16 = AlternatingGroup(16)
sage: A16.order()
10461394944000
sage: A16.is_abelian()
False
sage: A16.is_cyclic()
False
sage: a = A16("(2, 7, 13)")
sage: H = A16.subgroup([a])
sage: H.order()
3
sage: H.list()
[(), (2,7,13), (2,13,7)]
sage: c = A16("(2, 7, 13)(4, 9, 11, 5, 6)")
sage: K = A16.subgroup([c])
sage: K
Subgroup generated by [(2,7,13)(4,9,11,5,6)] of (Alternating group of order 16!/
2 as a permutation group)
sage: K.order()
15
sage: K.list()
[(),
 (2,7,13)(4,9,11,5,6),
 (2,13,7)(4,11,6,9,5),
 (4,5,9,6,11),
 (2,7,13)(4,6,5,11,9),
 (2,13,7),
 (4,9,11,5,6),
 (2,7,13)(4,11,6,9,5),
 (2,13,7)(4,5,9,6,11),
 (4,6,5,11,9),
 (2,7,13),
 (2,13,7)(4,9,11,5,6),
 (4,11,6,9,5),
 (2,7,13)(4,5,9,6,11),
 (2,13,7)(4,6,5,11,9)]
sage: K.is_abelian()
True
sage: K.is_cyclic()
True
sage:
```

Unsolved Exercises

10.14 Let $A = \{a, b, c, d, e\}$, $B = \{a, b, l\}$,and $C = \{a, l, m\}$. Using Sage, find the following sets:

a) $A \cup B \cup C$, $B \cap C$, $A - C$
b) $B \cap C \times A$, $(A \times B) - (B \times C)$

10.15 Solve the following equations using Sage:

– $f(x) = x^2 - 9x + 27$
– $x + 3 = y - 2$

10.16 Find the quotient and remainder of the following integers using Sage.

– $a = 123, b = 21$
– $a = 123, b = -21$

- $a = -123, b = 21$
- $a = -123, b = -21$

10.17 Let $A = \begin{bmatrix} 3 & 4 & 2 \\ 0 & 2 & 1 \\ 5 & 0 & 1 \end{bmatrix} \in \mathcal{M}_3(\mathbb{R})$. Using Sage, find the determinate, trace, and inverse of A.

10.18 Write the addition and multiplication Cayley's tables for $\mathbb{Z}_{11}$. Find the inverse of [5] and [126] for both operations.

10.19 Using Sage, solve the equation $[6x] \oplus_{12} [2] = [32]$ in $\mathbb{Z}_{14}$.

10.20 Find the generators for the following groups:

a) $(\mathbb{Z}_{22}, \oplus_{23})$.
b) $(\mathrm{Inv}(\mathbb{Z}_{23}), \otimes_{23})$.

10.21 Consider the symmetric group $\mathfrak{S}_{20}$. Using Sage, answer the following questions.

a) Is $\mathfrak{S}_{20}$ abelian, is it cyclic?
b) Find the center of $\mathfrak{S}_{20}$, and the order of its center.
c) Find the sign, order, and inverse of $\sigma = (4\ 7\ 8)(2\ 4\ 6)(5\ 11\ 6)$ and $\alpha = (4\ 8\ 2)(15\ 11\ 6\ \ 2)$.
d) Find $\sigma^{214}\alpha^{214}$, and then find its order, sign and inverse.
e) Find the subgroup of $\mathfrak{S}_{20}$ generated by $(4\ \ 7\ \ 12\ \ 8)$.
f) Find the alternating group of $\mathfrak{S}_{20}$.

10.22 Consider the symmetric group $\mathfrak{S}_{13}$ with $\sigma = (3\ \ 7\ \ 8)$ and $\alpha = (4\ \ 1\ \ 2)$. Using Sage,

a) Find the subgroup H of $\mathfrak{S}_{13}$ generated by σ.
b) Find the subgroup K of $\mathfrak{S}_{13}$ generated by α.
c) Find the subgroup N of $\mathfrak{S}_{13}$ generated by σ and α.
d) Are H, K, and N normal?
e) Find the alternating group of $\mathfrak{S}_{13}$.

10.23 Using Sage, find all the normal subgroups of $\mathfrak{S}_{14}$ and $\mathfrak{S}_6$.

10.24 Consider the symmetric group $\mathfrak{S}_{11}$, with $\sigma = (1\ 7\ 2)$, $\alpha = (4\ 1\ 2)$, and $\beta = (11\ 5\ 2)$. Using Sage, answer the following questions:

a) Find the subgroup H of $\mathfrak{S}_{13}$ generated by σ, α, and β.
b) Find the left and right cosets of H
c) Is H a normal subgroup of $\mathfrak{S}_{13}$?

10.25 Consider the symmetric group $\mathfrak{S}_5$.

a) Find the subgroup H generated by $\sigma = (1\ 3)$.
b) Is H normal?

References

Anastassiou, G., & Mezei, R. (2015). *Numerical analysis using sage.*Springer.

SageMath. (2019a, Nov 12). Welcome to Sage Constructions! Retrieved from https://doc.sagemath.org/html/en/constructions/

SageMath. (2019b, Nov 12). *Welcome to Sage Reference Manual!* Retrieved from https://doc.sagemath.org/html/en/reference/

SageMath. (2019c, Nov 12). Welcome to Sage Tutorial! Retrieved from https://doc.sagemath.org/html/en/tutorial/

SageMath. (2021). The sage mathematics software system (version 9.2). The Sage Developers, https://www.sagemath.org

Zimmermann, P., Casamayou, A., Cohen, N., Connan, G., Dumont, T., Fousse, L., Maltey, F., Meulien, M., Mezzarobba, M., Pernet, C., Thiéry, N. M., & Thomas, H. (2018). *Computational mathematics with sagemath.* Creative Commons.

Bibliography

Aljouiee, A., & Alkadi, M. (2004). *Introduction to group theory.* Arushed.

Artin, M. (1991). *Algebra.* Prentice-Hall, Inc.

Badawi, A. (2004). *Abstract algebra manual: Problems and solutions.* Nova Science Publishers Inc.

Baumslag, B., & Chandler, B. (1968). *Schaum's outline of theory and problems of group theory.* McGraw-Hill.

Beezer, R. A. (2013). *Sage for abstract algebra.* GUN Free Documentation License.

Bloch, E. D. (2000). *Proofs and fundamentals: A first course in abstract mathematics.* Birkhaeuser.

Blyth, T. S., & Robertson, E. F. (1984a). *Algebra Through practice: A collection of problems in Algebra with solutions, matrices and vector spaces.* Cambridge University Press.

Blyth, T., & Robertson, E. (1984b). *Algebra through practice: A collection of problems in Algebra with solutions, groups.* Cambridge University Press.

Blyth, T., & Robertson, E. (1984c). *Algebra through practice: A collection of problems in Algebra with solutions, groups, rings and fields.* Cambridge University Press.

Blyth, T. S., & Robertson, E. F. (1985). *Algebra through practice groups.* Cambridge University Press.

Calugareanu, G., Breaz, S., Modoi, C., & Pelea, C. (2003). *Exercises in Abelian group theory.* Springer-Science+Business Media, B. V.

Carter, N. C. (2009). *Visual group theory.* Mathematical Association of America.

Clark, A. (1984). *Elements of Abstract algebra.* Dover Publications Inc.

Cohn, P. (2003). *Further algebra and applications.* Springer.

Dammit, D.S. & Foot, M. R. (2004). *Abstract Algebra.* John Wiely and Sons, Inc.

De Temple, D., & Webb, W. (2014). *Combinatorial reasoning, an introduction to the art of counting.* John Wiley & Sons Inc.

Dixon, J. D., & Mortimer, B. (1996). *Graduate texts in mathematics permutation groups.* Springer.

Dresselhaus, M. S., Dresselhaus, G., & Jorio, A. (2008). *Group theory application to the physics of condensed matter.* Springer.

Fraleigh, J. B., & Katz, V. J. (2003). *A first course in abstract Algebra.* Addison-Wesley.

Fraleigh, J. (2002). *A first course in abstract Algebra.* Addison-Wesley Company.

Fraleigh, J. B. (2013). *A first course in abstract Algebra.* Pearson.

Gallier, J. H. (1986). *Logic for computer science: Foundation of automatic theorem proving.* Harper & Row.

Halmos, P. R. (1974). *Naive set theory.* Springer.

Hefferon, J. (2015). *Linear Algebra.* Orthogonal Publishing L3C.

Herstein, I. (1975). *Topic in Algebra.* John Wiley & Sons.

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0

Higgins, P. M. (1992). *Techniques of semigroup theory*. Oxford University Press.

Howie, J. M. (1976). *An introduction to semigroup theory*. Academic Press.

Howie, J. M. (1995). *Fundamentals of semigroup theory*. The Clarendon Press, Oxford University Press.

Hungerford, T. (2012). *Abstract Algebra an introduction.* Gengage Learning.

Jacobson, N. (1980). *Basic Algebra I*. W H Freeman & Co.

LeVeque, W. (1977). *Fundamentals of number theory*. Dover Publications INC.

Machì, A. (2012). *Groups an introduction to ideas and methods of the theory of groups.* Springer-Verlag Mailand.

Macllwaine, P., & Plumpton, C. (1984). *Coordinate geometry and complex number.* Macmillan Education Limited.

Mulholland, J. (2019). *Permutation puzzles a mathematical perspective.* Self-Published (Creative Commons).

Pinter, C. C. (1990). *A book of abstract Algebra.* Dover Publications Inc.

Rodgers, N. (2000). *Learning to reason: An introduction to logic, sets, and relations.* John Wiley & Sons.

Roman, S. (2012). *Fundamentals of group theory.* Birkhäuser Basel Springer Science+Business Media, LLC.

Rosen, K. H. (1986). *Elementary number theory and its applications.* Addison-Wesley.

Rotman, J. (1995). *An introduction to the theory of groups.* Springer-Verlag.

Rotman, J. (2000). *A first course in abstract Algebra.* Prentice Hall.

SageMath. 2021. The sage mathematics software system (version 9.2). The Sage Developers, https://www.sagemath.org

Suzuki, M. (1982). *Group theory I*. Springer-Verlag.

Zukav, G. (2009). *The dancing Wu Li masters an overview of the new physics.* HarperCollins Publishers Ltd.

Index

B. Al Subaiei and M. Al Nuwairan, *A Gentle Introduction to Group Theory*,
https://doi.org/10.1007/978-981-99-0147-0