Group Theory 1

LECTURE NOTES

Nor Haniza Sarmin
Hidayat Ullah Khan

Third Edition
October 2020

Department of Mathematical Sciences
Faculty of Science
Universiti Teknologi Malaysia

Group Theory 1

LECTURE NOTES

Group Theory 1

LECTURE NOTES

Nor Haniza Sarmin
Hidayat Ullah Khan

Third Edition
October 2020

Department of Mathematical Sciences
Faculty of Science
Universiti Teknologi Malaysia
Johor, Malaysia

Third Edition 2020

Typeset by
N. H. SARMIN & H. U. KHAN
Department of Mathematical Sciences,
Faculty of Science
Universiti Teknologi Malaysia
81310 UTM Johor Bahru
Johor Darul Takzim, Malaysia

Printed in Malaysia by
JASAMAX Enterprise
55, Jalan Kebudayaan 2
Taman Universiti
81300 Skudai
Johor Darul Takzim, Malaysia

Authors' Preface

This is a group theory course for master's level students. The lecture notes are written according to Universiti Teknologi Malaysia's curriculum. It is anticipated that the students have taken an undergraduate modern algebra or abstract algebra course. However, for those who haven't, these lecture notes also contain basic concepts of modern algebra.

This lecture notes consist of two parts. The first part includes introduction to groups, types of groups, isomorphisms between groups, automorphisms; composition of groups to form a direct product, and types of subgroups including normal subgroups and factor groups. Furthermore, some advanced topics in group theory are included including series of groups, nilpotent and solvable groups; rings, and integral domains. The second part is a selected topic of Sylow Theorems and their applications, topics on generators and relations, and group presentations.

As the reader will soon see, many examples are given in each chapter. In addition to that, exercises are given after each chapter. The purpose of these problems is to allow students to test their assimilation of the material, to challenge their mathematical integrity, and to be a means of developing mathematical insight, intuition, and techniques.

However, the author feels that having these lecture notes only are not enough. Every student should have or should refer to at least one text book of Graduate Text in Group Theory.

Finally, the author wishes all readers a joyful voyage on the mathematical journey they are about to embark into a beautiful realm of group theory.

Nor Haniza Sarmin
Hidayat Ullah Khan
October 2020

CONTENTS

LIST OF SYMBOLS

$\mathbb{Z}$ - integer

$\mathbb{N}$ - natural number

$\mathbb{Q}$ - rational number

$\mathbb{R}$ - real number

W - whole number

$Z(G)$ - center of a group G

$C_G(a)$ - centralizer of a in G

$cl(a)$ - conjugacy class of a

$\langle a \rangle$ - cyclic subgroup generated by a

$\in$ - element of

ϕ or $\{\ \}$ - empty set

$=$ - equal

$p \Rightarrow q$ - if p then q

$\cap$ - intersection

$\cong$ - isomorphic

aH - left coset of H

$\not\subset$ - not a subset

$\notin$ - not element of

$\neq$ - not equal

$|G|$ - order of a group G

$|g|$ - order of an element g

Ha - right coset of H

$\subseteq$ - subset

$\{e\}$ - trivial subgroup

$\cup$ - union

$H \lhd G$ - H normal subgroup of G

$H \leq G$ - H subgroup of G

$H < G$ - H proper subgroup of G

$p \Leftrightarrow q$ - p if and only if q

$t|s$ - t divides s

CHAPTER 1

GROUPS

1.1 Introduction

Definition 1.1 (Binary Operation)

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

A binary operation on a set G is simply a method (or formula) by which two members of G is combined to yield a new member of G. The most familiar binary operations are ordinary addition, subtraction, and multiplication of integers. Division of integers is not a binary operation on the integers. This is because an integer divided by an integer might not be an integer.

Definition 1.2 (Group)

Let G be a nonempty set with a binary operation that assigns to each ordered pair (a,b) of elements of G an element ab in G. We say G is a group under this operation if the following three properties are satisfied:

1. ***Associativity***

   The operation is associative, that is

   $(ab)c = a(bc)$ for all $a,b,c \in G$.

2. ***Identity***

   There is an element e (called the identity) in G, such that $ea = ae = a$ for all $a \in G$.

3. ***Inverse***

   For each element $a \in G$, there is an element a^{-1} in G such that $aa^{-1} = a^{-1}a = e$.

If all elements in a group G is commutative, then we call the group G to be an **Abelian Group**.

Definition 1.3 (Abelian Group)

A group G is **abelian** if its binary operation * is commutative $(ab = ba \quad \forall a,b \in G)$.

Example 1.1

1. The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are all groups under ordinary addition. In each case the identity is 0 and the inverse of a is $-a$. □

2. The set of integers under multiplication is not a group. Property (3) fails. For example, there is no integer b such that $5b=1$ where 1 is identity. □

3. The set Q^+ of positive rational numbers is a group under ordinary multiplication. The inverse of any a is $\frac{1}{a}$. □

4. The subset $\{1,-1,i,-i\}$ of the complex numbers is a group under complex multiplication. Note that –1 is its own inverse, while the inverse of i is $-i$. □

5. The set $\mathbb{Z}_n=\{0,1,2,\ldots,n-1\}$ for $n\geq 1$ is a group under addition modulo n for any i in $\mathbb{Z}_n$, the inverse of i is n-i. This group is usually referred to as the group of integers modulo n. □

6. The determinant of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the number $ad-bc$. The set

$GL(2,\mathbb{R})=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d\in\mathbb{R}, ad-bc\neq 0\right\}$, of 2×2

matrices with real entries and nonzero determinant is a non-Abelian group under the operation

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}=\begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}.$$

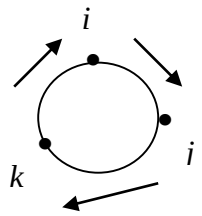
Associativity can be verified by direct (but cumbersome) calculations. The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$, (explaining the requirement that $ad-bc\neq 0$). This very important group is called the general linear group of 2×2 matrices over $\mathbb{R}$. □

7. The set of all 2×2 matrices with determinant 1 with entries from $\mathbb{Q},\mathbb{R},\mathbb{C}$ or $\mathbb{Z}_p$ (p a prime) is a non-Abelian group under matrix multiplication. This group is called the ***special linear group*** of 2×2 matrices over $\mathbb{Q},\mathbb{R},\mathbb{C}$ or $\mathbb{Z}_p$ respectively. If the entries are from F, where F is any of the above, we denote this group by $SL(2,F)$. □

8. The set $\{1,2,\ldots,n-1\}$ is a group under multiplication modulo n if and only if n is prime. □

9. For each $n>1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n. For $n=10$, we have $U(10)=\{1,3,7,9\}$. For $n=7$, we have $U(7)=\{1,2,3,4,5,6\}$.

10. The set $\{\pm 1,\pm i,\pm j,\pm k\}$ is a quaternion group where $i^2=j^2=k^2=-1$, and $i\cdot j=k,\ j\cdot k=i,$ $k\cdot i=j,\ j\cdot i=-k,\ i\cdot k=-j, k\cdot j=-i.$ Figure 2.1 is a nice way to visualize the multiplication of those elements.



11. Consider a regular $n-sided$ polygon centered at the origin. The symmetries of this polygon (i.e., length- and angle-preserving transformations of the plane that map this polygon onto itself) are rotations about the origin through an integer multiple of $\frac{2\pi}{n}$ radians, and reflections in the n axes of symmetry of the polygon. The symmetries of the polygon constitute a group of order

$2n$. This group is referred to as the dihedral group of order $2n$.

12. The symmetries of a rectangle that is not a square constitute a group of order 4. This group consists of the identity transformation, reflection in the axis of symmetry joining the midpoints of the two shorter sides, reflection in the axis of symmetry joining the two longer sides, and rotation though an angle of π radians (180^o). If I denotes the identity transformation, A and B denote the reflections in the two axes of symmetry, and C denotes the rotation through π radians then $A^2 = B^2 = C^2 = I, \quad AB = BA = C, \quad AC = CA = B$ and $BC = CB = A$. This group is Abelian: it is often referred to as the Klein $4-group$ (or, in German, Kleinsche Viergruppe).

Definition 1.4 (Power of an Element in *G*)

The power of an element in G, g^n, is defined as

$$g^n = \begin{cases} g \cdot g \cdot \ldots \cdot g, & n > 0 \\ \left(g^{-1}\right)^{-n}, & n < 0 \end{cases}, \quad \text{and } g^0 = e.$$

For any $g \in G$ and $m, n \in \mathbb{Z}$, we have $g^m g^n = g^{m+n}$ and $\left(g^m\right)^n = g^{mn}$, but for $a, b \in G$, $(ab)^n \neq a^n b^n$. On the other hand, if G is Abelian, $(ab)^n = a^n b^n$.

Note:

If the operation in G is addition, then $g^n = ng$ and $g^{-1} = -g$.

Definition 1.5 (Cyclic Group)

Let $a \in G$. Then

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{..., a^{-2}, a^{-1}, e, a, a^2, a^3, ...\}.$$

If $G = \langle a \rangle$, then we define G as a cyclic group generated by a.

Note:

All cyclic groups are Abelian groups since

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i.$$

For example, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is a cyclic group under addition.

Example 1.2

The following are not examples of groups.

1. The set of integers, $\mathbb{Z}$ under ordinary multiplication is not a group. Property (3) fails. For examples, there is no integer b such that $5b = 1$.
2. The set of integers, $\mathbb{Z}$ under ordinary subtraction is not a group. This is because the operation is not associative. For example, $(4-3)-2 \neq 4-(3-2)$.

3. The set S of positive irrationals numbers is not a group under ordinary multiplication since the product of two irrationals can be rational $\left(\sqrt{2}\cdot\sqrt{2}=2\right)$, thus multiplication does not define a function from $S\times S$ into S. Also, there is no identity element in S.
4. The set $H=\{0,1,2,3\}$ is not a group under multiplication modulo 4, since 0 and 2 do not have an inverse.

Groups have certain elementary properties and we state them in the following section.

1.2 Elementary Properties of Groups

Theorem 1.1 Uniqueness of the Identity

In a group G, there is only one identity element.

Lemma

A group G has exactly one identity element e satisfying $ex=x=xe$ for all $x\in G$.

Proof

Let $a\in G$ with the property that $ax=x$ for all $x\in G$, in particular $a=ae=e$. Similarly one can show that e is the only element of G satisfying $xe=x$ for all $x\in G$.

Theorem 1.2 Cancellation Law

In a group *G*, the right and left cancellation law hold; that is, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Theorem 1.3 Uniqueness of Inverse

For each element *a* in a group *G*, there is a unique element *b* in *G* such that $ab = ba = e$.

Lemma

An element x of a group G has exactly one inverse x^{-1}.

Proof

We know that the group G contains at least one element x^{-1} which satisfies $xx^{-1} = e$ and $x^{-1}x = e$. If $z \in G$ which satisfies $xz = e$ then,

$$z = ez = (x^{-1}x)z = x^{-1}(xz) = x^{-1}e = x^{-1}.$$

Similarly, if $w \in G$ which satisfies $wx = e$ then $w = x^{-1}$. In particular we conclude that the inverse x^{-1} of x is uniquely determined, as required.

Lemma

Let x and y be elements of a group G. Then $(xy)^{-1} = y^{-1}x^{-1}$.

Proof

It follows from the group axioms that

$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e$
Similarly, $(y^{-1}x^{-1})(xy) = e$, and thus $y^{-1}x^{-1}$ is the inverse of xy, as required.

Remark:

Note in particular that $(x^{-1})^{-1} = x$ *for all elements* x *of a group* G, *since* x *has the properties that characterize the inverse of the inverse* x^{-1} *of* x.

1.3 Multiplication Table

Let n be the order of a group. Then, we can list $n \times n$ multiplication in a multiplication table.

Example 1.3

1. Consider the set $S = \{a, b, c, d, e\}$ together with the following Cayley table:

.	*a*	*b*	*c*	*d*	*e*
a	*a*	*b*	*c*	*d*	*e*
b	*b*	*a*	*d*	*e*	*c*
c	*c*	*e*	*a*	*b*	*d*
d	*d*	*c*	*e*	*a*	*b*
e	*e*	*d*	*b*	*c*	*a*

First, note that the Cayley table does define a binary operation on *S* since every entry in the table belongs to *S*. Clearly, *a* is the identity element, since the first row and first column match the corresponding row and column labels. Every element has an inverse, since the identity appears in each row. The only troublesome axiom is the associative law and this is always the case when one is dealing with an operation defined by a table.

2. Consider $\mathbb{Z}_4 = \{0,1,2,3\}$. The Cayley table for $\mathbb{Z}_4$ is given as follows:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

From the Cayley table, we can conclude that;

i) $\mathbb{Z}_4$ is closed; since all elements in the table are in $\mathbb{Z}_4$.

ii) the set is associative.

iii) there exists an identity; which is 0.

iv) inverse; a unique inverse means that only an element, e in each row and column. The inverse of the elements are

$$0^{-1}=0,\quad 1^{-1}=3,\quad 2^{-1}=2 \quad \text{and} \quad 3^{-1}=1.$$

3. $U(n)=\{$ All positive integers greater than or equal to 1, relatively prime to n and less than n $\}$

Example 1.4

$$U(5)=\{1,2,3,4\}$$

.	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$U(8)=\{1,3,5,7\}$$

.	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition 1.6 (Order of a Group)

The number of elements in a group (finite or infinite) is called its **order**. We will use $|G|$ to denote the order of *G*.

Definition 1.7 (Order of an Element)

The order of an element *g* in a group *G* is the smallest positive integer *n* such that $g^n = e$. If no such integer exists, we say *g* has infinite order. The order of an element *g* is denoted by $|g|$.

Note : **The order of the identity is always 1 since** $e^1 = e$.

Example 1.5

1) Let $G = U(5) = \{1, 2, 3, 4\}$ with multiplication modulo 5. Then $|U(5)| = 4$. The order of each element in *G* is stated below:

$|1| = 1$

$|2| = 4$; since $2 \times 2 \times 2 \times 2 = 1$.

$|3| = 4$; since $3 \times 3 \times 3 \times 3 = 1$.

$|4| = 2$; since $4 \times 4 = 1$.

2) Consider the group $\mathbb{Z}_{10}$ under addition modulo 10. Since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, we

have $|2| = 5$. Similar computations give $|0| = 1$, $|7| = 10$, $|5| = 2$ and $|6| = 5$.

3) Consider the group $\mathbb{Z}$ under addition. Here every nonzero element has infinite order since the series a, $2a$, $3a$, … never becomes 0 when $a \neq 0$.

Exercises 1: (Groups)

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

Table 1.1

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

Table 1.2

Exercises 1 through 4 concern the binary operation $*$ defined on $S = \{a, b, c, d, e\}$ by means of Table 1.1.

1. Compute $b*d$, $c*c$, and $[(a*c)*e]*a$.
2. Compute $(a*b)*c$ and $a*(b*c)$. Can you say on the basis of this computation whether $*$ is associative?
3. Compute $(b*d)*c$ and $b*(d*c)$. Can you say on the basis of this computation whether $*$ is associative?
4. Is $*$ commutative? Why?

5. Complete Table 1.2 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d, e\}$.
6. Table 1.3 can be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries.

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

Table 1.3

In Exercises 7 through 11, determine whether the binary operation $*$ defined is commutative and whether $*$ is associative.

7. $*$ defined on $\mathbb{Z}$ by $a*b = a-b$.
8. $*$ defined on $\mathbb{Q}$ by $a*b = ab+1$.
9. $*$ defined on $\mathbb{Q}$ by $a*b = ab/2$.
10. $*$ defined on $\mathbb{Z}^+$ by $a*b = 2^{ab}$.
11. $*$ defined on $\mathbb{Z}^+$ by $a*b = a^b$.

12. Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.
13. How many different commutative binary operations can be defined on a set of 2 elements? On a set of 3 elements? On a set of n elements?

In Exercises 14 through 16, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

14. A binary operation $*$ is *commutative* if and only if $a*b=b*a$.
15. A binary operation $*$ on a set *S* is *associative* if and only if, for all $a,b,c\in S$, we have $(b*c)*a=b*(c*a)$.
16. A subset *H* of a set *S* is *closed* under a binary operation $*$ on *S* if and only if $(a*b)\in H$ for all $a,b\in S$.

In Exercises 17 through 22, determine whether the definition of $*$ does give a binary operation on the set. In the event that $*$ is not a binary operation, state whether Condition 1, Condition 2, or both of these conditions in the following are violated.

In an attempt to define a binary operation $*$ on a set *S* we must be sure that 1. exactly one element is assigned to each possible ordered pair of elements of *S*. 2. for each ordered pair of elements of *S*, the element assigned to it is again in *S*.

17. On $\mathbb{Z}^+$, define $*$ by $a*b=a-b$.
18. On $\mathbb{Z}^+$, define $*$ by $a*b=a^b$.
19. On $\mathbb{R}$, define $*$ by $a*b=a-b$.
20. On $\mathbb{Z}^+$, define $*$ by $a*b=c$, where *c* is the smallest integer greater than both *a* and *b*.
21. On $\mathbb{Z}^+$, define $*$ by $a*b=c$, where *c* is at least 5 more than $a+b$.
22. On $\mathbb{Z}^+$, define $*$ by $a*b=c$, where *c* is the largest integer less than the product of *a* and *b*.
23. Let *H* be the subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a,b\in\mathbb{R}$. Is *H* closed under
    a. matrix addition? b. matrix multiplication
24. Mark each of the following true or false.
    ___ a. If $*$ is any binary operation on any set S then $a*a=a$ for all $a\in S$.
    ___ b. If $*$ is any commutative binary operation on any set *S*, then $a*(b*c)=(b*c)*a$ for all $a,b,c\in S$.
    ___ c. If $*$ is any associative binary operation on any set S, then $a*(b*c)=(b*c)*a$ for all $a,b,c\in S$.
    ___ d. The only binary operations of any importance are those defined on sets of numbers.
    ___ e. A binary operation $*$ on a set S is commutative if there exist $a,b\in S$ such that $a*b=b*a$.

___ f. Every binary operation defined on a set having exactly one element is both commutative and associative.
___ g. A binary operation on a set *S* assigns at least one element of *S* to each ordered pair of elements of *S*.
___ h. A binary operation on a set *S* assigns at most one element of *S* to each ordered pair of elements of *S*.
___ i. A binary operation on a set *S* assigns exactly one element of *S* to each ordered pair of elements of *S*.
___ j. A binary operation on a set *S* may assign more than one element of *S* to some ordered pair of elements of *S*.

In Exercises 25 through 30, determine whether the binary operation $*$ gives a group structure on the given set. If no group results, which property/properties in the definition of a group does/do not hold?

25. Let $*$ be defined on $\mathbb{Z}$ by $a*b=ab$.
26. Let $*$ be defined on $2\mathbb{Z}=\{2n \mid n\in\mathbb{Z}\}$ by $a*b=a+b$.
27. Let $*$ be defined on $\mathbb{R}^+$ by $a*b=\sqrt{ab}$.
28. Let $*$ be defined on $\mathbb{Q}$ by $a*b=ab$.
29. Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by $a*b=a/b$.
30. Let $*$ be defined on $\mathbb{C}$ by $a*b=|ab|$.

In Exercises 31 through 38, determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group. Recall that a **diagonal matrix** is a square matrix whose only nonzero entries lie on the **main diagonal**, from the upper left to the lower right corner. An **upper-triangular matrix** is a square matrix with only zero entries below the main diagonal. Associated with each $n\times n$ matrix *A* is a number called the determinant of *A*, denoted by det(*A*). If *A* and *B* are both $n\times n$ matrices, then det(*AB*) = det(*A*)det(*B*). Also, $\det(I_n)=1$ and *A* is invertible if and only if $\det(A)\neq 0$.

31. All $n\times n$ diagonal matrices under matrix addition.
32. All $n\times n$ diagonal matrices under matrix multiplication.
33. All $n\times n$ diagonal matrices with no zero diagonal entry under matrix multiplication.
34. All $n\times n$ diagonal matrices with all diagonal entries 1 or -1 under matrix multiplication.
35. All $n\times n$ upper-triangular matrices under matrix multiplication.
36. All $n\times n$ upper-triangular matrices under matrix addition.
37. All $n\times n$ upper-triangular matrices with determinant 1 under matrix multiplication.
38. All $n\times n$ matrices with determinant either 1 or -1 under matrix multiplication.
39. Let *S* be the set of all real numbers except -1. Define $*$ on *S* by
$$a*b=a+b+ab.$$
    a. Show that $*$ gives a binary operation on S.
    b. Show that $\langle S,\ *\rangle$ is a group.

c. Find the solution of the equation $2 * x * 3 = 7$ in *S*.

40. Show that if *G* is a finite group with identity *e* and with an even number of elements, then there is $a \neq e$ in *G* such that $a * a = e$.
41. Show that every group *G* with identity *e* and such that $x * x = e$ for all $x \in G$ is abelian. [*Hint*: Consider $(a * b) * (a * b)$.]
42. Show that if $(a * b)^2 = a^2 * b^2$ for *a* and *b* in a group *G*, then $a * b = b * a$.
43. Give two reasons why the set of odd integers under addition is not a group.
44. Show that $\begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix}$ does not have a multiplicative inverse in $GL(2, \mathbb{R})$.
45. For any elements *a* and *b* from a group and any integer *n*, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.
46. Is the binary operation defined by the following table associative? Is it commutative?

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

47. Show that {1, 2, 3} under multiplication modulo 4 is not a group but that {1, 2, 3, 4} under multiplication modulo 5 is a group.
48. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, \mathbb{Z}_{11})$.
49. Prove that the set of all 2×2 matrices with entries from $\mathbb{R}$ and determinant +1 is a group under matrix multiplication.
50. Let *G* be a group with the following property: If *a*, *b*, and *c* belong to *G* and *ab* = *ca*, then *b* = *c*. Prove that *G* is Abelian.
51. (Law of Exponents for Abelian groups) Let *a* and *b* be elements of an Abelian group and let *n* be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?
52. Prove that a group *G* is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all *a* and *b* in *G*.
53. Construct a Cayley table for *U*(12).
54. Let *G* be a group and let $g \in G$. Define a function ϕ_g from *G* to *G* by $\phi_g(x) = gxg^{-1}$ for all *x* in *G*. Show that ϕ_g is one-to-one and onto.
55. Let *G* be a group and $g, h \in G$. Define ϕ_g, ϕ_h, ϕ_{gh} as in the previous problem (that is, $\phi_h(x) = hxh^{-1}$ and $\phi_{gh}(x) = (gh)x(gh)^{-1}$). Show that $\phi_g \circ \phi_h = \phi_{gh}$.
56. Prove that if *G* is a group with the property that the square of every element is the identity, then *G* is Abelian.

57. Let $\Omega = \{ (a,b) \mid a,b \in \mathbb{Z} \}$ with the operation defined as

$$(a,b)\cdot(c,d) = \left(a+c,(-1)^c b + d\right).$$

(i) Show that Ω is a group with the operation defined above.
(ii) Show that Ω is not abelian.
(iii) Determine $Z(\Omega)$, the center of Ω.

58. Let *G* be a group of matrices under multiplication. Show that:

(a) If one element of *G* is singular, then all elements of *G* are singular.

(b) If one element of *G* is nonsingular, then all elements of *G* are nonsingular.

CHAPTER 2

SUBGROUPS

2.1 Definitions and Subgroup Test

Definition 2.1 (Subgroup)

If a subset H of a group G is itself a group under the same operation as in G, we say H is a subgroup of G.

Or

Definition 2.1 (Subgroup)

Let H be a subset of a group G. We say that H is a subgroup of G if the following conditions are satisfied:

i. The identity element of G is an element of H,

ii. The product of any two elements of H is itself an element of H,

iii. The inverse of any element of H is itself an element of H.

We use the notation $H \leq G$ to mean H is a subgroup of G. If we want to indicate that H is a subgroup of G, but not equal to G itself, we write $H < G$. Such a subgroup is called a **proper subgroup**. The subgroup $\{e\}$ is called the **trivial subgroup** of

G; a subgroup that is not $\{e\}$ is called a **nontrivial subgroup** of G.

Theorem 2.1 One-Step Subgroup Test

Let G be a group and H a nonempty subset of G. Then, H is a subgroup of G if H is closed under multiplication; that is, if ab^{-1} is in H whenever a and b are in H.

Theorem 2.2

Let H be a subset of a group $(G,*)$. Then H is a subgroup of G if and only if $h_1 * h_2^{-1} \in H$ for all $h_1, h_2 \in H$.

Proof

Suppose H is a subgroup of a group G and $h_1, h_2 \in H$, then $h_1^{-1}, h_2^{-1} \in H$ (by condition (iii) definition of subgroup). Now since $h_1, h_2^{-1} \in H$ implies $h_1 * h_2^{-1} \in H$ (by condition (ii) of definition of subgroup).

Conversely: Let H be a subset of a group $(G,*)$ and $h_1 * h_2^{-1} \in H$ for all $h_1, h_2 \in H$. Need to show that H is a subgroup of G.

i. Since $h_1 \in H$, then by given hypothesis $e = h_1 * h_1^{-1} \in H$.

ii. Since $e \in H$ and $h_1 \in H$, then by given hypothesis $h_1^{-1} = e * h_1^{-1} \in H$.

iii. Let $h_1, h_2^{-1} \in H$ then by given hypothesis,

$$h_1 * h_2 = h_1 * (h_2^{-1})^{-1} \in H .$$

All the conditions of subgroups are satisfied and hence H is a subgroup of G.

Example 2.1

Let G be an Abelian group with the identity e. Then $H = \{x \in G | x^2 = e\}$ is a subgroup of G.

Theorem 2.3 Two-Step Subgroup Test

Let G be a group and H a nonempty subset of G. Then, H is a subgroup of G if

1. $ab \in H$ whenever $a, b \in H$ (H is closed under multiplication).
2. $a^{-1} \in H$ whenever $a \in H$ (each element in H has an inverse).

Theorem 2.4 Finite Subgroup Test

Let H be a nonempty finite subset of a group G. Then, H is a subgroup of G if H is closed under the operation of G.

2.2 Examples of Subgroups

1. The group of integers is a subgroup of the groups of rational numbers, real numbers and complex numbers under addition.

2. The group of non-zero rational numbers is a subgroup of the groups of non-zero real numbers and non-zero complex numbers under multiplication.

Definition 2.2 (Cyclic Subgroups)

Let $a \in G$. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{e, a, a^2, a^3, \ ...\}$ is called a cyclic subgroup of *G* generated by *a*.

Example 2.2

Let $G = U(5) = \{1,2,3,4\}$. All cyclic subgroups of *G* and their orders are listed as follows:

$$\langle 1 \rangle = \{1\} \quad ; \quad \text{then } |\langle 1 \rangle| = 1,$$
$$\langle 2 \rangle = \{1,2,3,4\} \quad ; \quad \text{then } |\langle 2 \rangle| = 4,$$
$$\langle 3 \rangle = \{1,2,3,4\} \quad ; \quad \text{then } |\langle 3 \rangle| = 4,$$
$$\langle 4 \rangle = \{1,4\} \quad ; \quad \text{then } |\langle 4 \rangle| = 2.$$

Thus, $G = U(5)$ is cyclic since $G = \langle 2 \rangle = \langle 3 \rangle$.

Theorem 2.5 $\langle a \rangle$ ***is a subgroup***

Let *G* be a group, and let *a* be any element of *G*. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of *G*.

Lemma 2.1

Let g be an element of a group G. Then the set of all elements of G that are of the form g^n for some integer n is a subgroup of G.

Proof

Let $H = \{g^n : n \in Z\}$.Then the identity element belongs to H, since it is equal to g^0. The product of two elements of H is itself an element of H, since $g^m g^n = g^{m+n}$ for all integers m and n. Also the inverse of an element of H is itself an element of H since $(g^n)^{-1} = g^{-n}$ for all integers n. Thus H is a subgroup of G, as required.

Definition 2.3 (Center of a Group)

The center $Z(G)$ of a group *G* is the set of elements in *G* that commute with every element of *G*. In symbols,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}.$$

The notation $Z(G)$ comes from the fact that German word for center is *Zentrum*.

Examples 2.3

1. Consider the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ji = -k$, $ik = -j$. Then find the centre of Q_8.

Solution: Since 1 is the identity of Q_8, therefore 1 commute with every element of Q_8, hence $1 \in Z(Q_8)$. Also $(-1)\cdot 1 = -1 = 1\cdot(-1)$, $(-1)\cdot i = i^2 \cdot i = i^3$ and $i\cdot(-1) = i\cdot i^2 = i^3$ that is $(-1)\cdot i = i^3 = i\cdot(-1)$, $(-1)\cdot(-i) = i^2\cdot(-i) = -i^3$ and $(-i)\cdot(-1) = (-i)\cdot i^2 = -i^3$ that is $(-1)\cdot(-i) = -i^3 = (-i)\cdot(-1)$. Similarly $(-1)\cdot(\pm j) = (\pm j)\cdot(-1)$ and $(-1)\cdot(\pm k) = (\pm k)\cdot(-1)$ hence $-1 \in Z(Q_8)$. However, $i\cdot j = k$ and $j\cdot i = -k$ this implies $i, j \notin Z(Q_8)$. Similarly $j\cdot k = i$ and $k\cdot j = -i$ that is $k \notin Z(Q_8)$. Hence $Z(Q_8) = \{\pm 1\}$.

2. Consider the dihedral group of order 6 i.e. $D_3 = \{e, a, a^2, b, ab, a^2b\}$ where $a^3 = b^2 = (ab)^2 = e$, and the groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ of integers, rationals, reals and complex numbers under their usual addition. Then $Z(D_3) = \{e\}$, $Z(\mathbb{Z}) = \mathbb{Z}$, $Z(\mathbb{Q}) = \mathbb{Q}$, $Z(\mathbb{R}) = \mathbb{R}$, and $Z(\mathbb{C}) = \mathbb{C}$.

Theorem 2.6 Center is a subgroup

The center for a group *G* is a subgroup of *G*.

Theorem 2.7

Prove that the center $Z(g)=\{x\in G\ :\ xg=gx\}$ of a group G is a subgroup of G.

Proof

Since $eg=g=ge$ for all $g\in G$, this implies $e\in Z(G)$. If x and y are elements of $Z(g)$, then $gy=yg$ and $gx=xg$ for all $g\in G$. Consider,

$$(xy)g=x(yg)=x(gy)=(xg)y=(gx)y=g(xy),$$

therefore xy is an element of $Z(g)$. Also x^{-1} is an element of $Z(g)$ for all elements x of $Z(g)$, since

$$x^{-1}g=x^{-1}(gx)x^{-1}=x^{-1}(xg)x^{-1}=gx^{-1}.$$

Thus $Z(g)$ is a subgroup of the group G.

Definition 2.4 (Centralizer of *a* in *G*)

Let *a* be a fixed element of a group *G*. The **centralizer of *a* in *G***, $C_G(a)$ is the set of all elements in *G* that commute with *a*.

In symbols, $C_G(a)=\{g\in G\,|\,ga=ag\}$.

Theorem 2.8 $C_G(a)$ ***is a subgroup***

For each *a* in a group *G*, the centralizer of *a* is a subgroup of *G*.

Theorem 2.9 $Z(G) = \bigcap_{a \in G} C_G(a)$

Theorem 2.10 If H is a subgroup of a group G then the order of H divides the order of G.

Exercises 2: (Subgroups)

In Exercises 1 through 2, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. The set $i\mathbb{R}$ of pure imaginary numbers including 0
2. The set $\pi\mathbb{Q}$ of rational multiples of π

In Exercises 3 through 5, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

3. The $n \times n$ matrices with determinant 2
4. The upper-triangular $n \times n$ matrices with no zeros on the diagonal
5. The $n \times n$ matrices with determinant -1 or 1

Let F be the set of all real-valued functions with domain $\mathbb{R}$ and let $\tilde{F}$ be the subset of F consisting of those functions that have a nonzero value at every point in $\mathbb{R}$. In Exercises 6 through 7, determine whether the given subset of F with the induced operation is (a) a subgroup of the F under addition, (b) a subgroup of the group $\tilde{F}$ under multiplication.

6. The subset of all $f \in \tilde{F}$ such that $f(1)=1$
7. Nine groups are given below. Give a *complete* list of all subgroup relations, of the form $G_i \leq G_j$, that exist between these given groups $G_1, G_2, ..., G_9$.

   $G_1 = \mathbb{Z}$ under addition

   $G_2 = 12\mathbb{Z}$ under addition

   $G_3 = \mathbb{Q}^+$ under multiplication

   $G_4 = \mathbb{R}$ under addition

   $G_5 = \mathbb{R}^+$ under multiplication

   $G_6 = \{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication

   $G_7 = 3\mathbb{Z}$ under addition

   $G_8 =$ the set of all integral multiples of 6 under addition

   $G_9 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication

Describe all the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by the given 2×2 matrix.

8. $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

9. Which of the following groups are cyclic? For each cyclic group, list all the generators of the group.

   $G_1 = \langle \mathbb{Z}, + \rangle$ $G_2 = \langle \mathbb{Q}, + \rangle$ $G_3 = \langle \mathbb{Q}^+, \cdot \rangle$

   $G_4 = \langle 6\mathbb{Z}, + \rangle$

   $G_5 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication

$G_6 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ under addition

10. Find the order of the subgroup of the multiplicative group *G* of invertible 4×4 matrices generated by

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

11. Study the structure of the table for the group $\mathbb{Z}_4$ in the following.

$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

a. By analogy, complete Table 4.1 to give a cyclic group $\mathbb{Z}_6$ of 6 elements. (You need not prove the associative law.)

b. Compute the subgroups $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, and $\langle 5 \rangle$ of the group $\mathbb{Z}_6$ given in part (a).

c. Which elements are generators for the group $\mathbb{Z}_6$ of part (a)?

d. Give the lattice diagram for the part (b) subgroups of $\mathbb{Z}_6$. (We will see later that these are all the subgroups of $\mathbb{Z}_6$.)

$\mathbb{Z}_6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2					
3	3					
4	4					
5	5					

Table 4.1

12. Show that if *H* and *K* are subgroups of an abelian group *G*, then

$$\{hk \mid h \in H \text{ and } k \in K\}$$

is a subgroup of *G*.

13. Prove that if *G* is an abelian group with identity *e*, then all elements *x* of *G* satisfying the equation $x^2 = e$ form a subgroup *H* of *G*.

14. Let *G* be a group and let *a* be one fixed element of *G*. Show that

$$H_a = \{x \in G \mid xa = ax\}$$

is a subgroup of G.

15. For sets H and K, we define the **intersection** $H \cap K$ by
$$H \cap K = \{x \mid x \in H \text{ and } x \in K\}.$$
Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.

16. Prove that every cyclic group is Abelian.

17 For each group in the following list, find the order of the group and the order of each element in the group. In each case, how are the orders of the elements of the group related to the order of the group?
$\mathbb{Z}_{12}$, $U(10)$, $U(12)$, $U(20)$, D_4.

18. Prove that in any group, an element and its inverse have the same order.

19. Without actually computing the orders, explain why the two elements in each of the following pairs of elements from $\mathbb{Z}_{30}$ must have the same order: {2, 28}, {8, 22}. Do the same for the following pairs of elements from $U(15)$: {2, 8}, {7, 13}.

20. Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

21. Show that $U(14) = \langle 3 \rangle = \langle 5 \rangle$. [Hence, $U(14)$ is cyclic.] Is $U(14) = \langle 11 \rangle$?

22. Show that $\mathbb{Z}_{10} = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$. Is $\mathbb{Z}_{10} = \langle 2 \rangle$?

23. Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

24. Suppose G is the group defined by the following Cayley table.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

a. Find the centralizer of each member of G.
b. Find $Z(G)$.
c. Find the order of each element of G. How are these orders arithmetically related to the order of the group?

25. If H is a subgroup of G, then by the *centralizer* $C(H)$ of H we mean that the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

26. Let G be an Abelian group with identity e and let n be some integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G. Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G.

27. Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find $|A|$, $|B|$, and $|AB|$. Does your answer surprise you?

28. U(15) has six cyclic subgroups. List them.

29. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a + b + c + d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

30. Let $G = GL(2, \mathbb{R})$. Let $H = \{A \in G \mid \det A \text{ is a power of 2}\}$. Show that H is a subgroup of G.

31. Let $G = GL(2, \mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \text{ and } b \text{ are nonzero integers} \right\}$. Prove or disprove that H is a subgroup of G.

32. Let $G = GL(2, \mathbb{R})$.

    a. Find $C\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right)$.

    b. Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)$.

    c. Find $Z(G)$.

CHAPTER 3

CYCLIC GROUPS

3.1 Definition and Some Examples of Cyclic Groups

Definition 3.1 (Cyclic Group)

A group G is called cyclic if there is an element a in G such that $G = \langle a^n \mid n \in \mathbb{Z} \rangle$. Such an element a is called a *generator* of G.

Example 3.1

Some examples of cyclic and noncyclic groups.

i) $\langle e \rangle = \{e\}$.

ii) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

iii) $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle = \{0,1,2,3\}$.

iv) $U(10) = \langle 3 \rangle = \langle 7 \rangle = \{1,3,7,9\}$.

v) $U(8) = \{1,3,5,7\}$ is not a cyclic group since it has no generator.

vi) $U(12) = \{1,5,7,11\}$ is not a cyclic group since it has no generator.

vii) $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.

3.2 Elementary Properties of Cyclic Groups

Theorem 3.1

Let *G* be a group and let *a* be an element of *G*. If *a* has infinite order, then all distinct powers of *a* are distinct group elements. If *a* has finite order, say *n*, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if *n* divides *i-j*.

Corollary 3.1 If $a^k = e$, then $|a| \mid k$.

Corollary 3.2 If $g \in G$, then $|g| \mid |G|$.

Example 3.2

We know $|\mathbb{Z}_4| = 4$. List all its elements orders:

$|0| = 1$

$|2| = 2$

$|3| = 4$

1 and 3 are the generators of $\mathbb{Z}_4$ since $|1| = |3| = |\mathbb{Z}_4| = 4$.

Note that all of the elements orders are divisors of $|\mathbb{Z}_4| = 4$.

Theorem 3.2

Let $G = \langle a \rangle$ be a cyclic group of order *n*. Then $G = \langle a^k \rangle$ if and only if the $\gcd(k, n) = 1$.

Note : $\gcd(k,n)=1$ which means *k* and *n* are relatively prime or *k* and *n* have no common factors. In other words, $k \in U(n)$.

Corollary 3.3

An integer *k* is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k,n)=1$.

Theorem 3.3

Every cyclic group is Abelian.

Theorem 3.4

Prove that every cyclic group is commutative. But the converse is not true.

Proof

Let G is a cyclic group generated by g and $a,b \in G$. Then $a = g^m$ and $b = g^n$ for some $m,n \in Z$. Consider $ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba$. This shows that G is commutative group as required.

Further consider the *Klein* $4-group$ i.e. $V_4 = \{e,a,b,c\}$, this group is commutative however it is not cyclic.

3.3 Classification of Subgroups of a Cyclic Group

Theorem 3.5

If $|\langle a \rangle| = n$, then the order of any subgroup of the group is a divisor of *n*; and, for each divisor *k* of *n*, the group has exactly one subgroup of order *k*, namely, $\langle a^{n/k} \rangle$.

Corollary 3.4

If *a* is a generator of a finite cyclic group *G* of order *k*, then the other generator of *G* are the elements of the term a^r, where *r* is relatively prime to *k*.

Theorem 3.6

A subgroup of a cyclic group is cyclic.

Example 3.3

Let $G = \langle g \rangle$ and $|G| = 24$. Then for every $k|24$, there exists $H \leq G$ such that $H = \langle g^k \rangle$. List of all subgroups are listed as below:

Subgroups of G	***k***	$\left\|\langle g^k \rangle\right\| = \frac{24}{k}$
$G = \langle g \rangle = \{e, g, g^2, \ldots, g^{23}\}$	1	24
$\langle g^2 \rangle = \{e, g^2, g^4, \ldots, g^{22}\}$	2	12
$\langle g^3 \rangle = \{e, g^3, g^6, \ldots, g^{21}\}$	3	8
$\langle g^4 \rangle = \{e, g^4, g^8, \ldots, g^{20}\}$	4	6
$\langle g^6 \rangle = \{e, g^6, g^{12}, g^{18}\}$	6	4
$\langle g^8 \rangle = \{e, g^8, g^{16}\}$	8	3
$\langle g^{12} \rangle = \{e, g^{12}\}$	12	2
$\langle g^{24} \rangle = \langle e \rangle = \{e\}$	24	1

In specific, if $G = \mathbb{Z}_n$, Theorem 3.7 can be restated as in the following.

Corollary 3.5

For each divisor *k* of *n*, the set $\langle n/k \rangle$ is a unique subgroup of $\mathbb{Z}_n$ of order *k*. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

Example 3.4

Let $G = \mathbb{Z}_{24}$. All cyclic subgroups of *G* are stated below:

$\langle 1 \rangle = \{0,1,2, \ldots ,23\}$ with order 24,

$\langle 2 \rangle = \{0,2,4, \ldots ,22\}$ with order 12,

$\langle 3 \rangle = \{0,3,6, \ldots ,21\}$ with order 8,

$\langle 4 \rangle = \{0,4,8, \ldots ,20\}$ with order 6,

$\langle 6 \rangle = \{0,6,12,18\}$ with order 4,

$\langle 8 \rangle = \{0,8,16\}$ with order 3,

$\langle 12 \rangle = \{0,12\}$ with order 2,

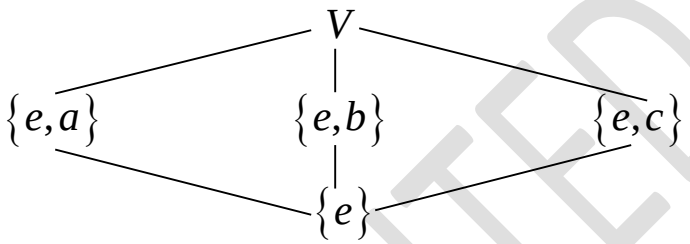
$\langle 0 \rangle = \{0\}$ with order 1.

3.4 Lattice Diagram

It is often useful to draw a lattice diagram of the subgroups of a group. In such a diagram, a line running downward from a group *G* to a group *H* means that *H* is a subgroup of *G*. Thus the larger group is placed nearer to the top of the diagram.

Example 3.5 (Klien-4-group)

Let $V = \{e, a, b, c\}$. There are four subgroups of V which are $\{e\}$, $\{e, a\}$, $\{e, b\}$ and $\{e, c\}$. Thus, we can draw the Lattice Diagram for V:



Example 3.6 ($\mathbb{Z}_{12}$)

Let $G = \mathbb{Z}_{12}$. The cyclic subgroups and orders of elements of G are listed below:

$\langle 0 \rangle = \{0\}$, thus $|\langle 0 \rangle| = 1$,

$\langle 1 \rangle = \{0,1,2, \ldots ,11\}$, so $|\langle 1 \rangle| = 12$,

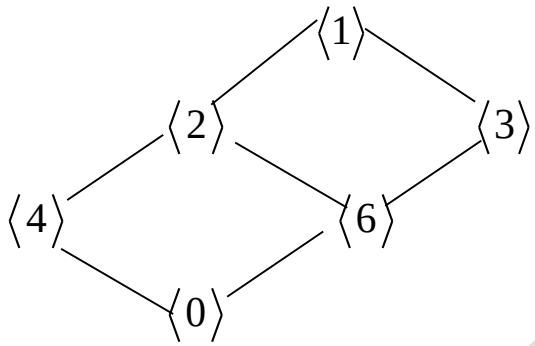
$\langle 2 \rangle = \{0,2,4, \ldots ,10\}$, so $|\langle 2 \rangle| = 6$,

$\langle 3 \rangle = \{0,3,6,9\}$, so $|\langle 3 \rangle| = 4$,

$\langle 4 \rangle = \{0,4,8\}$, so $|\langle 4 \rangle| = 3$,

$\langle 6 \rangle = \{0,6\}$, so $|\langle 6 \rangle| = 2$.

The lattice diagram of G is given as below:



Exercises 3: (Cyclic Groups)

In Exercise 1 through 4, find the number of generators of a cyclic group having the given order.

1. 5 2. 8 3. 12 4. 60

In Exercises 5 through 9, find the number of elements in the indicated cyclic group.

5. The cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25
6. The cyclic subgroup of $\mathbb{Z}_{42}$ generated by 30
7. The cyclic subgroup $\langle i \rangle$ of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication
8. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 7 generated by $(1+i)/\sqrt{2}$
9. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 7 generated by $1+i$

In Exercise 10 through 12, find all subgroups of the given group, and draw the lattice diagram for the subgroups.

10. $\mathbb{Z}_{12}$ 11. $\mathbb{Z}_{36}$ 12. $\mathbb{Z}_8$

In Exercise 13 through 17, find all orders of subgroups of the given group.

13. $\mathbb{Z}_6$ 14. $\mathbb{Z}_8$ 15. $\mathbb{Z}_{12}$ 16. $\mathbb{Z}_{20}$ 17. $\mathbb{Z}_{17}$

In Exercises 18 through 21, either give an example of a group with the property described, or explain why no example exists.

18. A finite group that is not cyclic
19. An infinite group that is not cyclic
20. A cyclic group having only one generator
21. A finite cyclic group having four generators

22. Let *r* and *s* be positive integers. Show that $\{nr+ms \mid n,m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.
23. Show by a counterexample that the following "converse" of the theorem below is not a theorem: "If a group *G* is such that every proper subgroup is cyclic, then *G* is cyclic."

Theorem: A subgroup of a cyclic group is cyclic.

24. Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if *p* is a prime number.
25. Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.
26. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$.
27. Let *a* be an element of a group and let $|a| = 15$. Compute the orders of the following elements of *G*.
    a. a^3, a^6, a^9, a^{12};
    b. a^5, a^{10};

c. $a^2,\ a^4,\ a^8,\ a^{14}$.

28. Let G be a group and let $a \in G$. Prove that $\langle a^{-1} \rangle = \langle a \rangle$.
29. Suppose that $|a| = 24$. Find a generator for $\langle a^{21} \rangle \cap \langle a^{10} \rangle$. In general, what is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?
30. If a cyclic group has an element of infinite order, how many elements of finite order does it have?
31. Let G be a group and let a be an element of G.
    a. If $a^{12} = e$, what can we say about the order of a?
    b. If $a^m = e$, what can we say about the order of a?
    c. Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a \rangle = G$.
32. Prove that a group of order 3 must be cyclic.
33. Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? Why? Describe all the subgroups of Z.
34. Determine the subgroup lattice for $\mathbb{Z}_{p^2q}$, where p and q are distinct primes.
35. Determine the subgroup lattice for $\mathbb{Z}_8$.
36. Show that the group of positive rational numbers under multiplication is not cyclic.
37. Consider the set $\{7, 35, 49, 77\}$. Show that this set is a group under multiplication modulo 84 by constructing its Cayley table. What is the identity element? Is the group cyclic?
38. Let m and n be elements of the group $\mathbb{Z}$. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.
39. Let p be a prime. If a group has more than $p-1$ elements of order p, why can't the group be cyclic?
40. Let $|x| = 40$. List all the elements of $\langle x \rangle$ that have order 10.
41. Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show $\langle a \rangle \cap \langle b \rangle = \{e\}$.
42. Let a and b belong to a group. If $|a| = 24$ and $|b| = 10$, what are the possibilities for $\langle a \rangle \cap \langle b \rangle$?

CHAPTER 4

PERMUTATION GROUPS

4.1 Definitions and Some Examples of Permutation Groups

Definition 4.1 (Permutation)

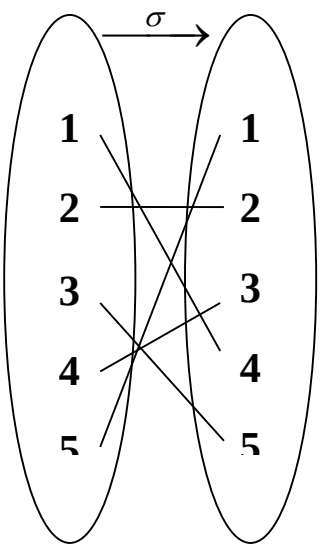
A permutation of a set A is a function $\phi : A \to A$ that is both one to one and onto.

Definition 4.2 (Permutation Group)

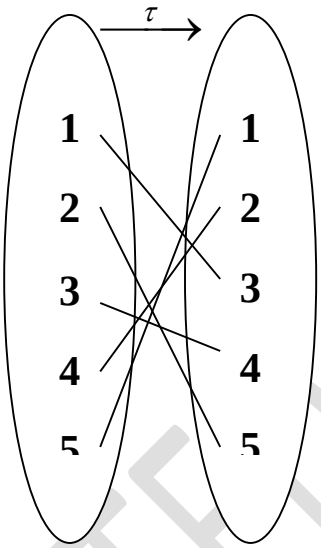
Given a set A. Then a permutation group is a set consists of all permutations on A that forms a group under the composition operations.

Example 4.1

Suppose that $A = \{1,2,3,4,5\}$ and σ and τ are permutations defined as below:



σ
$1 \to 4$
$2 \to 2$
$3 \to 5$
$4 \to 3$
$5 \to 1$



τ
$1 \to 3$
$2 \to 5$
$3 \to 4$
$4 \to 2$
$5 \to 1$

Both permutations can be written in a matrix form as:

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

Then,

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

For example, multiplying in right-to-left order gives $(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5$.

Definition 4.3 (Permutation Group)

Let *A* be a finite set $\{1, 2, \ldots, n\}$. The group of all permutations of *A* is the symmetric group on *n* letters and is denoted by S_n.

Note:

The order of permutation group denoted by $|S_n|$ is $|S_n| = n!$

Example 4.2

An interesting example is the group S_3 of $3! = 6$ elements. Let the set A be $\{1,2,3\}$. All permutations of A are listed below:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ and } \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

S_3 is the same as the group D_3 of symmetries of an equilateral triangle. Naively, we used ρ_i for rotations and μ_i for mirror images. The nth **dihedral group** D_n is the group of symmetries of regular n-gon. The multiplication table for S_3 is shown in Table 4.1:

Table 4.1 Multiplication Table for S_3

$\cdot$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

4.2 Cycle Notation

Example 4.3

Given $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_8$. Then σ can be written in a cycle notation as $\sigma = (136)(28)(475)$.

Figure 4.1 is a nice way to visualize the structure of the permutation σ.

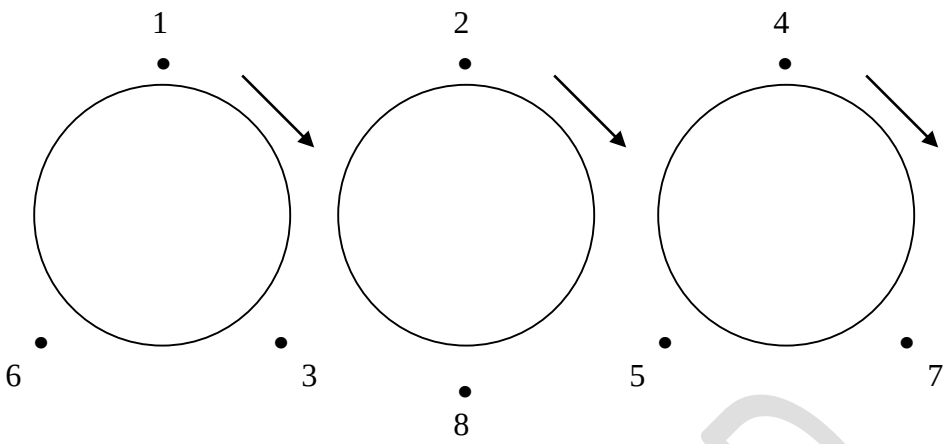


Figure 4.1 $\sigma = (136)(28)(475)$

Definition 4.4 (Cycle)

A permutation $(a_1 a_2 \ ... \ a_m)$ is a cycle if it contains more than one element and *m* the length of a cycle.

Example 4.4

Working within S_8, we see that

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 8 & 7 & 2 & 1 & 5 & 3 \end{pmatrix} = (16)(2475)(38),$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 2 & 8 & 3 & 4 & 7 \end{pmatrix} = (163)(25874), \text{ thus}$$

$$\alpha\beta = (16)(2475)(38)\ (163)(25874) = (1)(2)(3685)(4)(7) = (3685)$$

Definition 4.5 (Disjoint Cycles)

Any integer is moved by at most one of these cycles, thus no one number appears in the notation of two different cycles.

Example 4.5

Disjoint cycles:

$$(136)(28)(475), \quad (16)(2475)(38)$$

Joint cycles:

$$(12)(32)(157), \quad (1356)(246)$$

4.3 Properties of Permutations

Theorem 4.1

Every permutation of a finite set is a product of disjoint cycles.

Theorem 4.2

Multiplication of disjoint cycles is commutative.

Example 4.6

Consider the cycle (1456) and (23) in S_6:

$$(23)(1456) = (1456)(23).$$

Definition 4.6 (Order of a Permutation)

The order of a permutation, α is the smallest positive integer, n such that $\alpha^n = \varepsilon$. The order of a permutation α is denoted by $|\alpha|$.

Theorem 4.3

A permutation of a cycle with length n has order n.

Example 4.7

$|(a_1\ a_2)| = 2$ and $|(a_1\ a_2\ a_3)| = 3$.

Let $\gamma = (146)$. Then

$|\gamma| = |(146)| = 3, \quad |\gamma^2| = |(146)(146)| = |(164)| = 3,$

$|\gamma^3| = |\gamma^2\gamma| = |(164)(146)| = |(1)(4)(6)| = |\varepsilon| = 1.$

Theorem 4.4

The order of a permutation written in disjoint cycles is the least common multiple (*lcm*) of the length of each cycle.

Example 4.8

$|(123)(45)| = lcm(3,2) = 6,$

$|(12)(3456)| = lcm(2,4) = 4,$

$|(12)(352)| = |(2351)| = 4$.

Definition 4.7 (Transposition)

A transposition is a cycle of length two (or a 2-cycle).

Theorem 4.5

Any permutation of a finite set of at least two elements is a product of transpositions.

(In other words, any permutation of S_n, $n > 1$ can be written as a product of transpositions.)

Proof For identity permutation $\varepsilon = (12)(12)$. Then for every permutation with length *k*,

$$(a_1 a_2 \ldots a_{k-1} a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2).$$

Example 4.9

We can write $(86543217) = (87)(81)(82)(83)(84)(85)(86)$, a product of 7 transpositions.

Note that : $|(86543217)| = 8$.

Corollary 4.1

If $\varepsilon = \beta_1\beta_2\beta_3 \ldots \beta_r$ where β_i is a transposition, then *r* is an even number.

Definition 4.8 (Even or Odd Permutation)

An even/odd permutation is a permutation that can be written as a product of an even/odd number of transpositions.

For, an *n*-cycle, where *n* is odd, it can be written as a product of *n*-1 (even) number of transpositions, thus it is an even permutation.

For, an *n*-cycle, where *n* is even, it can be written as a product of *n*-1 (odd) number of transpositions, thus it is an odd permutation.

Example 4.10

Permutation, α	Product of Transpositions	**No. of transpositions**	**Type**
(12345)	$(15)(14)(13)(12)$	4	*even*
$(123)(45)$	$(13)(12)(45)$	*3*	*odd*
$(123)(54)(876)$	$(13)(12)(54)(86)(87)$	*5*	*odd*
(2)	$(12)(12)$	*2*	*even*

Theorem 4.6

The set of even permutations in S_n forms a subgroup of S_n.

Definition 4.9 (Alternating Group, A_n)

The subgroup of S_n consisting of even permutations of n letters is the alternating group, A_n on n letters.

We can prove that $|A_n| = n!/2$ when $n > 1$. This means half of the elements in S_n are even permutations and another half are odd permutations.

Example 4.11

$$S_4 = \{(1),(12),(13),(14),(23),(24),(34),$$
$$(123),(124),(134),(132),(142),(143),(234),(243),$$
$$(1234),(1243),(1324),(1342),(1423),(1432),$$
$$(12)(34),(13)(24),(14)(23)\}$$

$|S_4| = 4! = 24.$

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

$|A_4| = 4!/2 = 12.$

For $S_3 = \{(1),(12),(13),(23),(123),(132)\}$, then

$A_3 = \{(1),(123),(132)\}.$

Now we look at the Cayley Table of A_3 :

Let $\gamma_1 = (1)$, $\gamma_2 = (123)$ and $\gamma_3 = (132)$. Thus the Cayley

Table for A_3 is:

	γ_1	γ_2	γ_3
γ_1	γ_1	γ_2	γ_3
γ_2	γ_2	γ_3	γ_1
γ_3	γ_3	γ_1	γ_2

Exercises 4: (Permutation Groups)

In Exercises 1 through 5, compute the indicated product involving the following permutations in S_6 :

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

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix},$$

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

1. $\tau\sigma$ 2. $\tau^2\sigma$ 3. $\mu\sigma^2$ 4. $\sigma^{-2}\tau$ 5. $\sigma^{-1}\tau\sigma$

In Exercises 6 through 9, compute the expressions shown for the permutations σ, τ, and μ defined prior to Exercise 1.

6. $|\langle\sigma\rangle|$ 7. $|\langle\tau^2\rangle|$ 8. σ^{100} 9. μ^{100}

10. Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

is the **orbit** of a **under** σ. Find the orbit of 1, 2, 3, 4, 5 and 6 under the permutation τ defined prior to Exercise 1.

11. Find the number of elements in the set $\{\sigma \in S_4 \mid \sigma(3) = 3\}$.

12. Find the number of elements in the set $\{\sigma \in S_5 \mid \sigma(2) = 5\}$.

13. Consider the group S_3 of the following:

Let the set A be $\{1, 2, 3\}$. We list the permutations of A and assign to each a subscripted Greek letter for a name.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

a. Find all cyclic subgroups $\langle \rho_1 \rangle$, $\langle \rho_2 \rangle$, and $\langle \mu_1 \rangle$ of S_3.

b. Find *all* subgroups, proper and improper, of S_3 and give the lattice diagram for them.

14. Show by an example that every proper subgroup of a nonabelian group may be abelian.

In Exercise 15 through 17, compute the indicated product of cycles that are permutations of {1, 2, 3, 4, 5, 6, 7, 8}.

15. (1, 4, 5)(7, 8)(2, 5, 7)

16. (1, 3, 2, 7)(4, 8, 6)

17. (1, 2)(4, 7, 8)(2, 1)(7, 2, 8, 1, 5)

In Exercises 18 through 20, express the permutation of {1, 2, 3, 4, 5, 6, 7, 8} as a product of disjoint cycles, and then as a product of transpositions.

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

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

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

21. Recall that element *a* of a group *G* with identity *e* has order $r > 0$ if $a^r = e$ and no smaller positive power of *a* is the identity. Consider the group S_8.

a. What is the order of the cycle (1, 4, 5, 7)?

b. State a theorem suggested by part (a).

c. What is the order of $\sigma = (4,\ 5)(2,\ 3,\ 7)$? of $\tau = (1,\ 4)(3,\ 5,\ 7,\ 8)$?

d. Find the order of each of the permutations given in Exercises 18 through 20 by looking at its decomposition into a product of disjoint cycles.

e. State a theorem suggested by parts (c) and (d). [*Hint*: The important words you are looking for are *least common multiple*.]

In Exercises 22 through 26, find the maximum possible order for an element of S_n for the given value of *n*.

22. $n = 5$ 23. $n = 6$ 24. $n = 7$ 25. $n = 10$ 26. $n = 15$

27. Mark each of the following true or false.

___ a. Every permutation is a cycle.

___ b. Every cycle is a permutation.

___ c. The definition of even and odd permutations could have been given equally well before the following theorem.

Theorem: No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

___ d. Every nontrivial subgroup H of S_9 containing some odd permutation contains a transposition.

___ e. A_5 has 120 elements.

___ f. S_n is not cyclic for any $n \geq 1$.

___ g. A_3 is a commutative group.

___ h. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 8 fixed.

___ i. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 5 fixed.

___ j. The odd permutations in S_8 form a subgroup of S_8.

28. Show that if σ is a cycle of odd length, then σ^2 is a cycle.

29. Find the order of each of the following permutations.

    a. (14) b. (147) c. (14762)

30. What is the order of each of the following permutations?

    a. (124)(357) b. (124)(356)

    c. (124)(35) d. (124)(3578)

31. What is the order of each of the following permutations?

    a. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$ b. $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$

32. What are the possible orders for the elements of S_6 and A_6? What about S_7 and A_7?

33. Show that A_8 contains an element of order 15.

34. Determine whether the following permutations are even or odd.

    a. (135) b. (1356) c. (13567)

    d. (12)(134)(152) e. (1243)(3521)

35. If α is even, prove that α^{-1} is even. If α is odd, prove that α^{-1} is odd.

36. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.$$

    Compute each of the following.

    a. α^{-1}

    b. $\beta\alpha$

    c. $\alpha\beta$

37. Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 5 & 4 & 7 & 6 & 8 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

    Write α and β as

    a. products of disjoint cycles,

    b. products of 2-cycles.

38. Do the odd permutations in S_n form a group? Why?

39. Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

40. Use Table 4.2 to compute the following.

    a. The centralizer of $\alpha_3 = (13)(24)$.

    b. The centralizer of $\alpha_{12} = (124)$.

(In this table, the permutations of A_4 are designated as α_1, α_2, ..., α_{12} and an entry *k* inside the table represents α_k. For example, $\alpha_3\alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

Table 4.2 The Alternating Group A_4 of Even Permutations of {1, 2, 3, 4}

41. What cycle is $(\alpha_1\alpha_2...\alpha_n)^{-1}$?

42. Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that *H* is a subgroup of S_5.

43. In S_4, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.

44. In S_3, find elements α and β so that $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

45. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

46. Let G be a group. For elements $a, b \in G$, define a mapping $f_{a,b}: G \to G$ by $f_{a,b}(x) = axb$ for all $x \in G$.

    (i) Show that each $f_{a,b}$ is a permutation of the set G.

    (ii) Decide if the set $H = \{ f_{a,b} \mid a, b \in G \}$ is a subgroup of the group S_G of all permutations of the set G.

47. How many elements of order 2 are in S_6?

48. If α commutes with β and β commutes with γ. Show that α may not commute with γ.

CHAPTER 5

HOMOMORPHISMS AND ISOMORPHISMS

5.1 Introduction

It turns out that permutation groups can serve as models for all groups. In order to describe the relation of permutation groups with groups in general, we need the concept of isomorphism.

5.2 Definition and Some Examples

We define formally the concept of homomorphism and isomorphism below.

Definition 5.1 (Homomorphism)
If $(G_1,*_1)$ and $(G_2,*_2)$ be any groups. A mapping $f:(G_1,*_1)\xrightarrow{\text{into}}(G_2,*_2)$ is said to be a homomorphism or homomorphic mapping of G_1 into G_2 if

$$f(a*_1 b)=f(a)*_2 f(b) \text{ for all } a,b\in G_1.$$

Note:

If f is homomorphic mapping of G_1 onto G_2 so that $f(G_1)=G_2$, then the group G_2 is called the homomorphic image of a group G_1.

Examples 5.1

1. Let Z be the group of integers (with the operation of addition). The function $f : Z \to Z$ that sends each integer n to $2n$ i.e. $f(n) = 2n$ is a homomorphism. This follows from the fact that $2(m+n) = 2m+2n$ for all integers m and n. More generally, given any integer q, the function that sends each integer n to qn is a homomorphism.

2. There is an obvious homomorphism from the group of integers to the group of real numbers (where the binary operation for both the groups is addition). This is the homomorphism that sends each integer to itself.

3. Let a be a positive real number. The function that sends each integer n to the real number a^n is a homomorphism from the group of integers (with the operation of addition) to the group of non-zero real numbers (with the operation of multiplication). This follows from the fact that $a^{m+n} = a^m a^n$ for all integers m and n.

4. Let g be an element of a group G, and let $f : Z \to G$ be defined by $f(n) = g^n$ for all integers n. The fact that $g^{m+n} = g^m g^n$ for all integers m and n ensures that the function $f : Z \to G$ is a homomorphism from the group of integers (with the operation of addition) to the given group G.

***Theorem* 5.1**

Let $f : G_1 \xrightarrow{\text{into}} G_2$ be a homomorphism. Then $f(G_1)$ is a group. In other words, the homomorphic image $f(G)$ of a group G is a group.

Proof Let $f : G_1 \xrightarrow{\text{into}} G_2$ be a homomorphism. To show that $f(G_1)$ is a group we check all the four properties of a group for $f(G_1)$.

i. Closure property: Let $f(g_1),\ f(g_2) \in f(G_1)$ for all $g_1, g_2 \in G_1$ and consider, $f(g_1)\cdot f(g_2) = f(g_1 \cdot g_2)$ (f being a homomorphism) that is,
$f(g_1)\cdot f(g_2) = f(g_1 \cdot g_2) \in f(G_1)$ (because $g_1 \cdot g_2 \in G_1$).

ii. Associative property: Let $f(g_1),\ f(g_2),\ f(g_3) \in f(G_1)$ for all $g_1, g_2, g_3 \in G_1$ and consider,

$$\begin{aligned}(f(g_1)\cdot f(g_2))\cdot f(g_3) &= f(g_1 \cdot g_2)\cdot f(g_3)\\ &= f((g_1 \cdot g_2)\cdot g_3)\\ &= f(g_1 \cdot (g_2.g_3))\\ &= f(g_1)\cdot f(g_2.g_3)\\ &= f(g_1)\cdot(f(g_2)\cdot f(g_3))\end{aligned}$$

iii. Existence of the identity: If e_1 is the identity of G_1, then $f(e_1)$ is the identity of G_2, because for any $f(g_1) \in f(G_1)$, we have,

$$f(g_1)\cdot f(e_1) = f(g_1 \cdot e_1) = f(g_1)$$

and

$$f(e_1)\cdot f(g_1) = f(e_1 \cdot g_1) = f(g_1).$$

iv. Existence of the inverse: For each $f(g_1) \in f(G_1)$, there exists $f(g_1^{-1}) \in f(G_1)$ such that,

$$f(g_1) \cdot f(g_1^{-1}) = f(g_1 \cdot g_1^{-1}) = f(e_1)$$

and

$$f(g_1^{-1}) \cdot f(g_1) = f(g_1^{-1} \cdot g_1) = f(e_1).$$

Hence $f(G_1)$ is a group. □

***Theorem* 5.2**

The homomorphic image of an Abelian group is Abelian.

Proof Let $f : G \to G^*$ be a homomorphism of an abelian group G into a group G^*. Let $f(x), f(y) \in f(G)$, where $x, y \in G$ and consider, $f(x) \cdot f(y) = f(xy) = f(yx) = f(y) \cdot f(x)$.

This shows that $f(x) \cdot f(y) = f(y) \cdot f(x)$ for all $f(x), f(y) \in f(G)$ and hence $f(G)$ is Abelian. □

Theorem 5.3

The homomorphic image of a cyclic group is cyclic.

Proof Let $f : G \to G^*$ be a homomorphism of a cyclic group G into a group G^*. Let G be generated by a. Since $a \in G$, therefore $f(a) \in f(G)$. Let $x \in f(G)$, then $x = f(g)$ for some $g \in G$, but $g = a^k$, hence,

$$\begin{aligned} x &= f(a^k) \text{(for some integer } k\text{)} \\ &= f(a \cdot a \cdot \ldots k\text{-times}) \\ &= f(a) \cdot f(a) \ldots k\text{-times} \\ &= \left(f(a)\right)^k \end{aligned}$$

This shows that every element of $f(G)$ is of the form $\left(f(a)\right)^k$. Hence $f(G)$ is cyclic. □

Theorem 5.4

If $f : G \xrightarrow{\text{into}} G^*$ is a homomorphism and H is any subgroup of a group G, then $f(H)$ is a subgroup of G^*.

Proof Since H is a subgroup therefore $e \in H$ and hence $f(e) \in f(H)$ that is $f(H)$ is non-empty. Let $f(x), f(y) \in f(H)$, where $x, y \in H$. Consider,

$$\begin{aligned} f(x) \cdot \left(f(y)\right)^{-1} &= f(x) \cdot f(y^{-1}) \\ &= f(xy^{-1}) \in f(H) \text{ (because } xy^{-1} \in H\text{)}, \end{aligned}$$

implies, $f(x) \cdot \left(f(y)\right)^{-1} \in f(H)$. Hence $f(H)$ is a subgroup of G^*. □

Definition 5.2 (Isomorphism)

An isomorphism ϕ from a group G to a group H is a one-to-one and onto function that preserves the group operation, i.e.

$$\phi(gh) = \phi(g)\phi(h) \ \forall g, h \in G.$$

Note that a mapping that satisfies operation preserving is called a *homomorphism*. A homomorphism from a group G to itself is called an *endomorphism*.

If there exists an isomorphism that maps a group to another group, we say that those two groups are isomorphic.

Definition 5.3 (Isomorphic)
If there exists an isomorphism from G to H, then we say G and H are isomorphic or G is isomorphic to H. In symbols, we write $G \cong H$ or $H \cong G$.

5.3 Operation Preserving

There are four types of operation preserving, depending on the operations on G and H, listed in the table below:

Operation on G	Operation on H	Operation Preserving
#	#	$\phi(g\#h)=\phi(g)\#\phi(h)$
#	*	$\phi(g\#h)=\phi(g)*\phi(h)$
*	#	$\phi(g*h)=\phi(g)\#\phi(h)$
*	*	$\phi(g*h)=\phi(g)*\phi(h)$

5.4 How to show two groups are isomorphic.

There are four normal steps to show that $\langle S, * \rangle$ and $\langle S', \# \rangle$ are isomorphic:

Step 1: Define the function ϕ that gives the isomorphism of S with S'. This means that we have to describe, in some fashion, what $\phi(s)$ is so that $\phi(s)$ is closed for every $s \in S$.

Step 2: Show that ϕ is a one-to-one function. This means we suppose that $\phi(x) = \phi(y)$ in S' and deduce from this that $x = y$ in S.

Step 3: Show that ϕ is onto S'. That is, suppose that $s' \in S'$ is given. Then we show that there exists $s \in S$ such that $\phi(s) = s'$.

Step 4: Prove that ϕ is operation preserving. That is, to show that $\phi(x * y) = \phi(x) \# \phi(y) \quad \forall x, y \in S$. This is just a question of computation. Compute both sides of the equation and see whether they are the same.

Example 5.2

Let $2\mathbb{Z} = \{2n \mid n \in Z\}$. Thus $2\mathbb{Z}$ is the set of all even integers. We claim that $\langle \mathbb{Z}, + \rangle$ is isomorphic to $\langle 2\mathbb{Z}, + \rangle$, where + is the usual addition.

Step 1: The obvious function $\phi : \mathbb{Z} \to 2\mathbb{Z}$ is given by $\phi(n) = 2n$ for $n \in \mathbb{Z}$.

Step 2: If $\phi(m) = \phi(n)$, then $2m = 2n$ so $m = n$. Thus ϕ is one-to-one.

Step 3: If $n \in 2\mathbb{Z}$, then n is even so $n = 2m$ for $m = \frac{n}{2}$.

Hence $\phi(m) = 2\left(\frac{n}{2}\right) = n$, so ϕ is onto $2\mathbb{Z}$.

Step 4: Let $m, n \in \mathbb{Z}$. We have

$$\phi(m+n) = 2(m+n) = 2m + 2n = \phi(m) + \phi(n).$$

Thus, ϕ is an isomorphism.

Example 5.3

Let us show that the binary structure $\langle \mathbb{R}, + \rangle$ with the usual addition operation is isomorphic to the structure $\langle \mathbb{R}^+, \cdot \rangle$ where "$\cdot$" is the usual multiplication.

Step 1: We have to somehow convert an operation of addition to multiplication. Recall from $a^{b+c} = \left(a^b\right)\left(a^c\right)$ that addition of exponents corresponds to multiplication of two quantities. Thus we try defining $\phi : \mathbb{R} \to \mathbb{R}^+$ by $\phi\left(x\right) = e^x$ for $x \in \mathbb{R}$. Note that $e^x > 0$ for all $x \in \mathbb{R}$. So indeed $\phi\left(x\right) \in \mathbb{R}^+$.

Step 2: If $\phi\left(x\right) = \phi\left(y\right)$, then $e^x = e^y$. Taking the natural logarithm, we see that, $x = y$ so ϕ is indeed one-to-one.

Step 3: If $r \in \mathbb{R}^+$, then $\ln\left(r\right) \in \mathbb{R}$ and $\phi\left(\ln r\right) = e^{\ln r} = r$. Thus ϕ is onto $\mathbb{R}^+$.

Step 4: For $x, y \in \mathbb{R}$, we have $\phi\left(x + y\right) = e^{x+y} = e^x \cdot e^y$
$= \phi\left(x\right) \cdot \phi\left(y\right)$.

Thus we conclude that ϕ is an isomorphism.

Example 5.4

Let $G = SL\left(2, \mathbb{R}\right)$, the group of 2×2 real matrices with determinant 1. Let *M* be any 2×2 real matrix with nonzero determinant. Then we can define an isomorphism from *G* to *G* itself by $\phi_m\left(A\right) = M^{-1}AM, \forall A \in G$.

Step 1: ϕ_m is a function from G to G. Here, we must show that $\phi_m(A)$ is indeed an element of G whenever A is. This follows from properties of determinants:

$$\begin{aligned}\det\left(M^{-1}AM\right) &= \left(\det\left(M\right)\right)^{-1}\left(\det A\right)\left(\det M\right)\\ &= \det\left(A\right) = 1.\end{aligned}$$

Thus, $M^{-1}AM$ is in G.

Step 2: We show that ϕ_m is one-to-one. Suppose $\phi_m(A) = \phi_m(B)$. Then by the left and right cancellation, $M^{-1}AM = M^{-1}BM$ gives $A = B$.

Step 3: Next, show ϕ_m is onto. Let B belongs to G. We must find a matrix A in G such that $\phi_m(A) = B$. If such a matrix A is to exist, it must have the property that $M^{-1}AM = B$. But this tells us exactly what A must be. We may solve for A to obtain $A = M^{-1}BM$.

Step 4: Lastly, we show that ϕ_m is operation preserving. Let A and B belong to G. Then,

$$\begin{aligned}\phi_m(AB) &= M^{-1}\left(AB\right)M\\ &= M^{-1}A\left(MM^{-1}\right)BM\\ &= \left(M^{-1}AM\right)\left(M^{-1}BM\right)\\ &= \phi_m(A)\cdot\phi_m(B).\end{aligned}$$

Thus we conclude that ϕ is an isomorphism.

Example 5.5

Any finite cyclic group of order *n* is isomorphic to $\mathbb{Z}_n$. In general, any infinite cyclic group is isomorphic to $\mathbb{Z}$. Indeed, in either case, if *a* is a generator of the cyclic group, then the mapping $\phi\left(a^k\right)=k$ is an isomorphism.

Step 1: The mapping is $\phi:\langle a\rangle\to\mathbb{Z}$ with $\phi\left(a^k\right)=k$.

Step 2: ϕ is one-to-one. Let $\phi\left(a^k\right)=\phi\left(a^l\right)$, then $k=l$.

This gives $a^k=a^l$.

Step 3: ϕ is onto. We must find $k\in\mathbb{Z}$ such that any $a^l\in\langle a\rangle, \phi\left(a^l\right)=k$. This gives $l=k$.

Step 4: ϕ is operation preserving, which means that,

$$\phi\left(a^k\cdot a^l\right)=\phi\left(a^k\right)+\phi\left(a^l\right), \forall a^k, a^l\in\langle a\rangle.$$

Then, $\phi\left(a^k\cdot a^l\right)=\phi\left(a^{k+l}\right)=k+l=\phi\left(a^k\right)+\phi\left(a^l\right).$

Since ϕ is an isomorphism, we conclude that any cyclic group with order *n* is isomorphic to $\mathbb{Z}_n$.

Example 5.6

$U(10)\approx\mathbb{Z}_4\approx U(5)$. To verify this, one need only observe that both $U(10)$ and $U(5)$ are cyclic of order 4. Then, use Example 5.5.

Example 5.7

Decide whether ϕ is an isomorphism.

i) $\phi : \langle \mathbb{Z}, + \rangle \to \langle \mathbb{Z}, + \rangle$ with $\phi(n) = -n$.

ii) $\phi : \langle GL(2, \mathbb{R}), \cdot \rangle \to \langle \mathbb{R}, \cdot \rangle$ with $\phi(A) = |A|$.

iii) $\phi : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^*, \cdot \rangle$ with $\phi(x) = 2^x$.

(Note that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$).

iv) $\phi : \langle M_2(\mathbb{R}), + \rangle \to \langle \mathbb{R}, + \rangle$ with $\phi(A) = tr(A)$, where $tr(A)$ is the trace of A.

v) $\phi : f \to \mathbb{R}^*$ where $\phi(f) = \int_0^1 f(x)dx$.

Here, we denote $\mathbb{R}^* = \langle \mathbb{R} \setminus \{0\}, \times \rangle$ and f is a continuous function.

5.4 Some Properties of Isomorphism

In this section we list some important properties for isomorphism.

Let ϕ be an isomorphism from a group G to a group H. Then

1. $\phi(e_G) = e_H$, where e_G denotes the identity element in G and e_H denotes the identity element in H.

2. $\phi\left(a^{-1}\right)=\left(\phi(a)\right)^{-1}$ for all a in G.

3. $\phi\left(a^{n}\right)=\left(\phi(a)\right)^{n}$ for all a in G.

4. $ab=ba \leftrightarrow \phi(a)\phi(b)=\phi(b)\phi(a)$ for all a,b in G, in other words, G Abelian $\leftrightarrow$ H Abelian.

5. G cyclic $\leftrightarrow$ H cyclic.

6. $|a|=|\phi(a)|$ for all a in G.

7. ϕ^{-1} is an isomorphism from H onto G.

8. $K \leq G \rightarrow \phi(K) \leq H$ where $\phi(K)=\{\phi(k) \mid k \in K\}$.

Theorem 5.5

Let $f:(G_1,*_1) \overset{\text{into}}{\rightarrow} (G_2,*_2)$ be a homomorphism (or an isomorphism). If e_1 is the identity of G_1, then $f(e_1)$ is the identity of G_2.

Proof Let e_1 and e_2 be the identities of G_1 and G_2 respectively. If $a \in G_1$, then $f(a) \in G_2$. Now consider,

$$e_2 *_2 f(a) = f(a) = f(e_1 *_1 a) = f(e_1) *_2 f(a),$$

that is,

$$e_2 *_2 f(a) = f(e_1) *_2 f(a),$$

hence $e_2 = f(e_1)$. This shows that $f(e_1)$ is the identity of G_2. □

Theorem 5.6

Let $f:(G_1,*_1)\overset{\text{into}}{\to}(G_2,*_2)$ be a homomorphism (or an isomorphism). Then $f(g^{-1})=\big(f(g)\big)^{-1}$.

Proof Let g be an element of G_1. Let e_1 and e_2 be the identities of G_1 and G_2, respectively. Then $f(e_1)=e_2$. Consider, $e_2 = f(e_1) = f(g *_1 g^{-1}) = f(g) *_2 f(g^{-1})$ that is, $e_2 = f(g) *_2 f(g^{-1})$. This shows that $f(g^{-1})$ is the inverse of $f(g)$ in G_2, consequently $f(g^{-1})=\big(f(g)\big)^{-1}$. □

Theorem 5.7

If $|G|<\infty$ and $|H|<\infty$. Then $G\cong H\to|G|=|H|$. Conversely, if $|G|\neq|H|\to G\ncong H$.

Theorem 5.8

Any finite cyclic group of order *n* is isomorphic to $\mathbb{Z}_n$

Definition 5.4 (Automorphism)

An automorphism on *G* is an isomorphism ϕ from a group *G* onto itself , i.e. $\phi:G\to G$, and ϕ is an isomorphism.

Examples 5.8

Decide whether *G* and *H* are isomorphic. Give your reasons.

1. Given $G=U(10)$ and $H=U(5)$.

$G = U(10) = \{1,3,7,9\}$, $H = U(5) = \{1,2,3,4\}$ and let

$g \in G$ and $h \in H$.

The mapping can be given as follows:

$g \in G$	$h \in H$
1	1
3	2
7	3
9	4

- the mapping is one to one
- the mapping is onto
- we can check the preserving operation is satisfied

We conclude that $U(10) \cong U(5)$.

2. $G = U(10)$ and $H = \mathbb{Z}_4$

$G = U(10) = \{1,3,7,9\}$, $H = \mathbb{Z}_4 = \{0,1,2,3\}$ and let

$g \in G$ and $h \in H$.

The mapping can be given as follows:

$g \in G$	$h \in H$
1	0
3	1
7	2
9	3

- the mapping is one to one
- the mapping is onto
- we can check for preserving operation

So $U(10) \cong \mathbb{Z}_4$.

3. $G = U(10)$ and $H = U(12)$

$G = U(10) = \{1,3,7,9\}$, $H = U(12) = \{1,5,7,11\}$ and let $g \in G$ and $h \in H$.

Since *G* is cyclic but *H* is not cyclic, then *G* is not isomorphic to *H*.

4. $G = \mathbb{Z}_4$ and $H = \mathbb{Z}_6$

$G = \mathbb{Z}_4 = \{0,1,2,3\}$ and $H = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$.

Since the order of the groups are not the same, there does not exist a mapping that is both one to one and onto. Therefore, *G* is not isomorphic to *H*.

5. $G = D_3$ and $H = \mathbb{Z}_6$.

$G = D_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$, $H = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$.

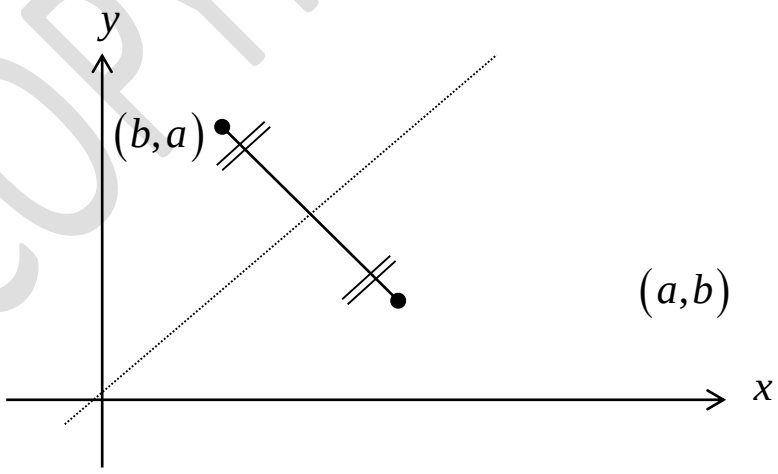
\# Since $\mathbb{Z}_6$ is cyclic but D_3 is not cyclic, then the mapping is not an isomorphism OR

Since $\mathbb{Z}_6$ is an abelian but D_3 is not abelian group, then the mapping is not an isomorphism OR

Since the order of elements in D_3 are not the same with the order of elements in $\mathbb{Z}_6$, thus D_3 is not isomorphic to $\mathbb{Z}_6$.

6. $\phi : \mathbb{C} \to \mathbb{C}$ where $\phi(a+bi) = a-bi$ is an automorphism.

7. Let $\mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$. Then $\phi(a,b) = (b,a)$ is an automorphism. We can see ϕ as a mirror on the axis $y = x$.



■

Note:

Any group G is always isomorphic to itself (identity mapping).

Definition 5.5 (Kernel of Homomorphism)
Let $f : G_1 \to G_2$ be a homomorphism of a group G_1 onto a group G_2. Then the kernel of f is denoted and define as $\ker f = \{a \in G : f(a) = 0\}$.

Theorem 5.9
A homomorphism $f : G \to G^*$ is one-one if and only if $\ker f = \{e\}$, where e is the identity of G.

Proof Let $f : G \to G^*$ be one-one homomorphism. If $x \in \ker f$, then $f(x) = e^*$ (identity of G^*), also $f(e) = e^*$ that is $f(x) = f(e)$. But f is one-one, therefore $x = e$ and hence $\ker f = \{e\}$.

Conversely: Let $\ker f = \{e\}$ and $x, y \in G$ such that,
$f(x) = f(y)$, then
$\Rightarrow f(x) \cdot (f(y))^{-1} = e$
$\Rightarrow f(x) \cdot f(y^{-1}) = e^*$
$\Rightarrow f(xy^{-1}) = e^*$
$\Rightarrow xy^{-1} \in \ker f = \{e\}$
$\Rightarrow xy^{-1}y = ey$
$\Rightarrow x = y$. This shows that f is one-one. □

Exercises 5: (Isomorphisms)

In Exercises 1 through 6, determine whether the given map ϕ is a homomorphism.

1. Let $\phi: \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) =$ the greatest integer $\leq x$.
2. Let $\phi: \mathbb{R}^* \to \mathbb{R}^*$ under multiplication be given by $\phi(x) = |x|$.
3. Let $\phi: \mathbb{Z}_6 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder of x when divided by 2, as in the division algorithm.
4. Let G be any group and let $\phi: G \to G$ be given by $\phi(g) = g^{-1}$ for $g \in G$.
5. Let F be the additive group of all continuous functions mapping $\mathbb{R}$ into $\mathbb{R}$. Let $\mathbb{R}$ be the additive group of real numbers, and let $\phi: F \to \mathbb{R}$ be given by
$$\phi(f) = \int_0^4 f(x)\, dx.$$
6. Let $GL(n, \mathbb{R})$ be the multiplicative group of invertible $n \times n$ matrices, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi: GL(n, \mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = tr(A)$, where $tr(A)$ is defined as the sum of the elements on the main diagonal of A, from the upper-left to the lower-right corner.

In Exercises 7 through 14, determine whether the given map ϕ is an isomorphism of the first binary structure with the second. If it is not an isomorphism, why not?

7. $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\phi(n) = -n$ for $n \in \mathbb{Z}$
8. $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\phi(n) = n + 1$ for $n \in \mathbb{Z}$
9. $\langle \mathbb{Q}, + \rangle$ with $\langle \mathbb{Q}, + \rangle$ where $\phi(x) = x/2$ for $x \in \mathbb{Q}$
10. $\langle \mathbb{Q}, \cdot \rangle$ with $\langle \mathbb{Q}, \cdot \rangle$ where $\phi(x) = x^2$ for $x \in \mathbb{Q}$
11. $\langle \mathbb{R}, \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(x) = x^3$ for $x \in \mathbb{R}$
12. $\langle M_2(\mathbb{R}), \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(A)$ is the determinant of matrix A
13. $\langle M_1(\mathbb{R}), \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(A)$ is the determinant of matrix A
14. $\langle \mathbb{R}, + \rangle$ with $\langle \mathbb{R}^+, \cdot \rangle$ where $\phi(r) = 0.5^r$ for $r \in \mathbb{R}$

Let F be the set of all functions f mapping $\mathbb{R}$ into $\mathbb{R}$ such that $f(0) = 0$ and f has derivatives of all orders. Follow the instructions for Exercise 7 through 14.

15. $\langle F, + \rangle$ with $\langle \mathbb{R}, + \rangle$ where $\phi(f) = f'(0)$
16. Let H be a subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$, where H is closed under both matrix addition and matrix multiplication.
    a. Show that $\langle \mathbb{C}, + \rangle$ is isomorphic to $\langle H, + \rangle$.

b. Show that $\langle \mathbb{C}, \cdot \rangle$ is isomorphic to $\langle H, \cdot \rangle$.

(We say that *H* is a matrix representation of the complex numbers $\mathbb{C}$.)

17. Find an isomorphism from the group of integers under addition to the group of even integers under addition.
18. Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.
19. Show that $U(8)$ is not isomorphic to $U(10)$.
20. Show that $U(8)$ is isomorphic to $U(12)$.
21. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.
22. Let G be a group and let a belong to G. Prove that the mapping of ϕ_a defined by $\phi_a(x) = axa^{-1}$ is an automorphism of G.
23. Show that the mapping $\phi(a+bi) = a-bi$ is an automorphism of the group of complex numbers under addition. Show that ϕ preserves complex multiplication as well – that is, $\phi(xy) = \phi(x)\phi(y)$ for all x and y in $\mathbb{C}$.
24. Explain why S_n $(n \geq 3)$ contains a subgroup isomorphic to D_n.
25. Let $G = \{(a, b, c) \mid a, b, c \in \mathbb{R}\}$ with multiplication defined by
$$(a_1, b_1, c_1)(a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2 + a_2b_1).$$
and let $0 \neq t \in \mathbb{R}$. Prove that the map $f_t : G \to G$ defined by
$$f_t((a, b, c)) = (ta, tb, t^2c)$$
is an automorphism of G.
26. Let G be a finite Abelian group and n a positive integer that is relatively prime to $|G|$. Show that the mapping $a \to a^n$ is an automorphism of G.

CHAPTER 6

DIRECT PRODUCTS

6.1 Introduction

Two or more groups can be combined to produce a larger group. This is called an external direct product of groups. In this chapter, we first define the external direct product formally. Then we include some properties of external direct products in the next section.

The concept of a direct product can be used for factorization of a group into a product of smaller groups.

Definition 6.1 (External Direct Product)

Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$ is defined as

$$G_1 \oplus G_2 \oplus \ldots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}.$$

Example 6.1

1. $U(6) \oplus U(12)$

$$= \{1,5\} \oplus \{1,5,7,11\}$$
$$= \{(1,1),(1,5),(1,7),(1,11),(5,1),(5,5),(5,7),(5,11)\}.$$

2. $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R} = \{(x, y) | x, y \in \mathbb{R}\}$ where

$(x, y) \cdot (x', y') = (x + x', y + y')$

3. $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{0,1\} \oplus \{0,1,2\}$

$= \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

$= \langle (1,1) \rangle$

4. $U(8) \oplus U(10)$

$= \{1,3,5,7\} \oplus \{1,3,7,9\}$

$= \{(1,1),(1,3),(1,7),(1,9),(3,1),(3,3),(3,7),(3,9)$

$(5,1),(5,3),(5,7),(5,9),(7,1),(7,3),(7,7),(7,9)\}.$

5. $\mathbb{Z}_2 \oplus U(4) = \{0,1\} \oplus \{1,3\} = \{(0,1),(0,3),(1,1),(1,3)\}.$

6.2 Properties of External Direct Product

In this section, we list some important properties of external direct product.

Assuming that all groups are finite, the first property states that the order of an external direct product is just the product of the orders of each group listed as a component in the external direct product.

Property 1

$$\begin{aligned}\left|G_1 \oplus G_2 \oplus \ \ldots \ \oplus G_n\right| &= \left|\bigoplus_{i=1}^{n} G_i\right| \\ &= \left|G_1\right| \times \left|G_2\right| \times \ \ldots \ \times \left|G_2\right| \\ &= \prod_{i=1}^{n} \left|G_i\right|.\end{aligned}$$

Example 6.2

i. $\left|U(6) \oplus U(12)\right| = \left|U(6)\right| \times \left|U(12)\right|$

$$= 2 \times 4 = 8.$$

ii. $\mathbb{Z}_3 \oplus D_3$

$$\begin{aligned}&= \{0,1,2\} \oplus \{\rho_0, \rho_{120}, \rho_{240}, \mu_1, \mu_2, \mu_3\} \\ &= \{(0,\rho_0),(0,\rho_{120}),(0,\rho_{240}),(0,\mu_1),(0,\mu_2),(0,\mu_3), \\ &\quad (1,\rho_0),(1,\rho_{120}),(1,\rho_{240}),(1,\mu_1),(1,\mu_2),(1,\mu_3), \\ &\quad (2,\rho_0),(2,\rho_{120}),(2,\rho_{240}),(2,\mu_1),(2,\mu_2),(2,\mu_3)\}\end{aligned}$$

$$\left|\mathbb{Z}_3 \oplus D_3\right| = \left|\mathbb{Z}_3\right| \times \left|D_3\right| = 3 \times 6 = 18.$$

Thus, there are 18 elements in $\mathbb{Z}_3 \oplus D_3$.

The second property states that the multiplication of two elements in the external direct product preserves the operations in the groups involved.

Property 2

Let $(G_1,*)$ and $(G_2,\#)$ are two structures, where * and # are the binary operations of G_1 and G_2, consecutively. Then $(g_1,g_2)\cdot(g_3,g_4)=(g_1 * g_3, g_2 \# g_4)$ where $g_1,g_3 \in G_1$ and $g_2,g_4 \in G_2$.

Example 6.3

i. Refer to Example 6.1, calculate $(5,7)\cdot(5,5)$:

$$\begin{aligned}(5,7)\cdot(5,5) &= (5\times 5, 7\times 5)\\ &= (25 \bmod 6, 35 \bmod 12)\\ &= (1,11).\end{aligned}$$

ii. Refer to Example 6.2, calculate $(2,\rho_{120})\cdot(2,\mu_2)$:

$$\begin{aligned}(2,\rho_{120})\cdot(2,\mu_2) &= (2+2, \rho_{120}\cdot\mu_2)\\ &= (1,\mu_3)\end{aligned}$$

The third property states that the identity element in the direct product is formed componentwise from the identity elements from each group involved.

Property 3

$$e_{G_1 \oplus G_2 \oplus \ldots \oplus G_n} = \left(e_{G_1}, e_{G_2}, \ldots, e_{G_n} \right)$$

Example 6.4

i. Let $G = U(6) \oplus U(12)$. Then $e_G = (1,1)$.

ii. Let $G = D_4 \oplus \mathbb{Z}_7$. Then $e_G = (\rho_0, 0)$.

iii. Let $G = U(7) \oplus Q \oplus SL(2, \mathbb{R})$. Then

$e_G = \left(1,1, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$, where Q is the quaternion.

Theorem 6.1 Order of an Element in a Direct Product

The order of an element in a direct product of finite groups is the least common multiple of the orders of the components of the elements. In symbol:

$$\left| (g_1, g_2, \ldots, g_n) \right| = lcm\left(|g_1|, |g_2|, \ldots, |g_n| \right).$$

We write this in short as Property 4.

Property 4

$$\left| (g_1, g_2, \ldots, g_n) \right| = lcm\left(|g_1|, |g_2|, \ldots, |g_n| \right)$$

Example 6.5

i. Let $(1,5) \in U(6) \oplus U(12)$

By definition, $(1,5)^2 = (1,5)\cdot(1,5)$

$$= (1 \bmod 6, 25 \bmod 12)$$
$$= (1,1) = e.$$

Thus $|(1,5)| = 2.$

OR

Using Property 4,

$$|(1,5)| = lcm(|1|,|5|) = lcm(1,2) = 2.$$

ii. Let $(1, \rho_{120}) \in U(8) \oplus D_4.$

By definition,

$$(1, \rho_{120})\cdot(1, \rho_{120})\cdot(1, \rho_{120}) = (1, \rho_{240})\cdot(1, \rho_{120})$$
$$= (1, \rho_0) = e.$$

Thus $|(1, \rho_{120})| = 3.$

OR

Using Property 4,

$$|(1, \rho_{120})| = lcm(|1|, |\rho_{120}|) = lcm(1,3) = 3.$$

iii. Let $\left(2,-j,\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)\in U(7)\oplus Q\oplus SL(2,\mathbb{R})$, where Q is the quaternion. Thus

$$\left|\left(2,-j,\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)\right| = lcm\left(|2|,|-j|,\left|\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right|\right)$$
$$= lcm(3,4,1)$$
$$= 12.$$

iv. If $y=\left(2,-j,\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}\right)\in U(7)\oplus Q\oplus SL(2,\mathbb{R})$, then

$$|y| = \left|\left(2,-j,\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}\right)\right| = lcm\left(|2|,|-j|,\left|\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}\right|\right)$$
$$= lcm(3,4,\infty)=\infty$$

since $\left|\begin{pmatrix}2 & 1\\ 3 & 2\end{pmatrix}\right| = \infty.$

We list some other properties of a direct product in the following. Property 4 states that the inverse of an element in the direct product is formed from the inverse of each element from the components.

Property 5

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$
$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$$

Example 6.6

i. Let $(1,5) \in U(6) \oplus U(12)$. Then

$$(1,5)^{-1} = (1^{-1}, 5^{-1}) = (1,5).$$

ii. Let $(1, \rho_{120}) \in U(8) \oplus D_4$. Then

$$(1, \rho_{120})^{-1} = (1^{-1}, \rho_{120}^{-1}) = (1, \rho_{240}).$$

iii. Let $\left(2, -j, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \in U(7) \oplus Q \oplus SL(2, \mathbb{R})$, where Q is the quaternion. Thus

$$\left(2, -j, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)^{-1} = \left(2^{-1}, (-j)^{-1}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{-1}\right) = \left(4, j, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Property 4 is used in the following example.

Example 6.7

We will determine the number of elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$. By Property 4, we must count the number of elements (a,b) in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ so that $5 = |(a,b)| = lcm\{|a|, |b|\}$. Clearly, this

requires that either $|a| = 5$ and $|b| = 1$ or 5, or $|b| = 5$ and $|a| = 1$ or 5. We consider three mutually exclusive cases:

Case I: $|a| = 5$ and $|b| = 5$.

Here, there are four choices for *a* and four choices for *b*. This gives sixteen elements of order 5.

Case II: $|a| = 5$ and $|b| = 1$.

Here, there are four choices for *a* and only one for *b*. This gives four more elements of order 5.

Case III: $|a| = 1$ and $|b| = 5$.

This time there is one choice for *a* and four choices for *b* so that we obtain four more elements of order 5.

Thus $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ has 24 elements of order 5.

Example 6.8

Find all subgroups of order 15 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$.

Let $G = \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ and $H \leq G$. We have $H = H_1 \oplus H_2$ where $H_1 \leq \mathbb{Z}_{25}$ and $H_2 \leq \mathbb{Z}_5$. This gives $|H_1| \| 25$, which implies $|H_1| \in \{1, 5, 25\}$ and $|H_2| \| 5$ gives $|H_2| \in \{1, 5\}$. Since $15 \neq |H| = |H_1| \times |H_2|$ we conclude that there is no such H_1 and H_2 exists. Furthermore, there is no element of order 15 in G (verify this).

Theorem 6.1

Let G and H be two finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $\gcd(|G|, |H|) = 1$.

Example 6.9

1. $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$
2. $\mathbb{Z}_3 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{21}$
3. $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_4$
   $\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$

Corollary 6.1

For $G_1 \oplus G_2 \oplus ... \oplus G_n, n < \infty, G_i$ is cyclic, $|G_i| < \infty$, then $G_1 \oplus G_2 \oplus ... \oplus G_n$ is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ for $i \neq j$.

Corollary 6.2

Let $m = n_1 n_2 ... n_k$. Then $\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ... \oplus \mathbb{Z}_{n_k}$ if and only if $(n_i, n_j) = 1$ for $i \neq j$.

Example 6.10

i) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

Note that $\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \ncong \mathbb{Z}_{60}$.

ii) $$\begin{aligned} \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 &\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_7 \\ &\cong \mathbb{Z}_5 \oplus \mathbb{Z}_{21} \\ &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{35} \\ &\cong \mathbb{Z}_{105} \end{aligned}$$

iii) $$\begin{aligned} \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{15} \\ &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{10} \\ &\cong \mathbb{Z}_6 \oplus \mathbb{Z}_{15} \\ &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{30} \\ &\cong \mathbb{Z}_6 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5. \end{aligned}$$

Example 6.11

Find all abelian groups up to isomorphism, of the given order:

i) 12 ii) 20 iii) 14

6.3 Groups of Units Modulo *n* as an External Direct Product

In this section, we will see that groups of units modulo *n*, written earlier as $U(n)$, can be written as an external direct product of cyclic groups under addition, $Z(n)$.

Theorem 6.2

Let $m = n_1 n_2 ... n_k$, and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then

$$U(m) \cong U(n_1) \oplus U(n_2) \oplus ... \oplus U(n_k).$$

Example 6.12

$$\begin{aligned} U(105) &\cong U(3) \oplus U(5) \oplus U(7) \\ &\cong U(15) \oplus U(7) \\ &\cong U(3) \oplus U(35) \\ &\cong U(21) \oplus U(15). \end{aligned}$$

Theorem 6.3

$U(2) \cong \mathbb{Z}_1 \cong \{1\}$,

$U(2^n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$, $n \geq 2$,

$U(p) \cong \mathbb{Z}_{p-1}$, where p is an odd prime,

$U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$.

Example 6.13

1. $U(105) \cong U(3) \oplus U(5) \oplus U(7)$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6.$$

2. $U(27) = U\left(3^3\right) \cong \mathbb{Z}_{3^3 - 3^2} = \mathbb{Z}_{18}$.

Exercises 6: (Direct Product)

1. List the elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. Find the order of each of the elements. Is this group cyclic?
2. Repeat Exercise 1 for the group $\mathbb{Z}_3 \oplus \mathbb{Z}_4$.

In Exercise 3 through 4, find the order of the given element of the direct product.

3. $(2, 3)$ in $\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$
4. (3, 10, 9) in $\mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$

5. What is the largest order among the orders of all the cyclic subgroups of $\mathbb{Z}_6 \oplus \mathbb{Z}_8$? of $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$?
6. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
7. Fill in the blanks.
   a. The cyclic subgroup of $\mathbb{Z}_{24}$ generated by 18 has order _____.
   b. $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ is of order _____.
   c. The element (4, 2) of $\mathbb{Z}_{12} \oplus \mathbb{Z}_8$ has order _____.
   d. The Klein 4-group is isomorphic to $\mathbb{Z}$ ___ $\oplus \mathbb{Z}$ ___.
   e. $\mathbb{Z}_2 \oplus \mathbb{Z} \oplus \mathbb{Z}_4$ has _____ elements of finite order.
8. Calculate the number of elements of order 4 in each $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, and $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
9. Prove that any Abelian group of order 45 has an element of order 15. Does every Abelian group of order 45 have an element of order 9?
10. Find all Abelian groups (up to isomorphism) of order 360.

In Exercises 11 through 12, find all abelian groups up to isomorphism, of the given order.

11. Order 16
12. Order 720

13. Mark each of the following true or false.
   ___ a. If G_1 and G_2 are any groups, then $G_1 \oplus G_2$ is always isomorphic to $G_2 \oplus G_1$.
   ___ b. Computation in an external direct product of groups is easy of you know how to compute in each component group.
   ___ c. Groups of finite order must be used to form an external direct product.
   ___ d. A group of prime order could not be the internal direct product of two proper nontrivial subgroups.
   ___ e. $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_8$.
   ___ f. $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is isomorphic to S_8.
   ___ g. $\mathbb{Z}_3 \oplus \mathbb{Z}_8$ is isomorphic to S_4.

___ h. Every element in $\mathbb{Z}_4 \oplus \mathbb{Z}_8$ has order 8.

___ i. The order of $\mathbb{Z}_{12} \oplus \mathbb{Z}_{15}$ is 60.

___ j. $\mathbb{Z}_m \oplus \mathbb{Z}_n$ has *mn* elements whether *m* and *n* are relatively prime or not.

14. Let *G* be an abelian group of order 72.
    a. Can you say how many subgroups of order 8 *G* has? Why?
    b. Can you say how many subgroups of order 4 *G* has? Why?
15. Prove that a direct product of abelian groups is abelian.
16. Let *G* be an abelian group. Let *H* be the subset of *G* consisting of the identity *e* together with all elements of *G* of order 2. Show that *H* is a subgroup of *G*.
17. Find the order of each element in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.
18. Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.
19. Determine the subgroup lattice of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
20. Prove or disprove that $\mathbb{Z} \oplus \mathbb{Z}$ is a cyclic group.
21. Prove, by comparing orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.
22. Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$? Why?
23. How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have? (Do not do this exercise by brute force.)
24. Suppose $G_1 \approx G_2$ and $H_1 \approx H_2$. Prove that $G_1 \oplus H_1 \approx G_2 \oplus H_2$.
25. Construct a Cayley table for $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.
26. What is the largest order of any element in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$?
27. Let $G = \{3^m 6^n \mid m, n \in \mathbb{Z}\}$ under multiplication. Prove that *G* is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.
28. Determine the number of elements of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$. Hence give two cyclic subgroups of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$.
29. Without doing any calculating in *U*(27), decide how many subgroups *U*(27) has.
30. What is the largest order of any element in *U*(900)?
31. Use the results presented in this chapter to prove that *U*(55) is isomorphic to *U*(75).
32. Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{15}$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.
33. Find the numbers of elements of order 9 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$.
34. Find all subgroups of order 16 in $\mathbb{Z}_{20} \oplus \mathbb{Z}_{16}$. Are they cyclic or not cyclic?
35. Given $G = U(10) \oplus \mathbb{Z}_3$.
    (a) Find the order of *G*.
    (b) List all elements of *G* and find their orders.

(c) Is G Abelian? Is G cyclic?

(d) Find

(i) $(3, 2)\cdot(7, 1)$

(ii) $(9, 2)\cdot(3, 2)$

36. Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Z}_2 \right\}$ under addition and $H = S_3$.

i. List all elements of G and all elements of H.

ii. List all elements of $G \oplus H$.

iii. Find the order of each element in $G \oplus H$.

iv. Is $G \oplus H$ Abelian? Cyclic? Why or why not?

v. Find a group that $G \oplus H$ is isomorphic to and give your reasons.

CHAPTER 7

COSETS AND LAGRANGE THEOREM

7.1 Introduction

The binary operation in a given group can be used in a natural way to define a product between subsets of the group. This leads to the definition of cosets. The notion of subgroups will later lead to *factor* or *quotient groups* that will be discussed in the next chapter.

We define cosets of a subgroup in a group formally as follows.

Definition 7.1 (Cosets of *H* in *G*)

Let G be a group and $H \leq G$. Then for $a \in G$,

$aH = \{ah \mid h \in H\}$ is called the left coset of H in G.

$Ha = \{ha \mid h \in H\}$ is called the right coset of H in G.

The element a is called the coset's representative.

Example 7.1

Let $G = \mathbb{Z}_8$ and $H = \langle 2 \rangle = \{0, 2, 4, 6\}$. In this case, the group operation is addition, so we use the notation $a + H$ instead of aH to find all left and right cosets of H in G.

The left cosets of H in G are:

$0 + H = \{0, 2, 4, 6\} = H$, $4 + H = \{4, 6, 0, 2\}$

$1 + H = \{1, 3, 5, 7\}$, $5 + H = \{5, 7, 1, 3\}$

$2 + H = \{2, 4, 6, 0\}$, $6 + H = \{6, 0, 2, 4\}$

$3 + H = \{3, 5, 7, 1\}$, $7 + H = \{7, 1, 3, 5\}$.

The cosets of H in G can be seen as a partition of the group G. In other words, they separate the elements of G into mutually disjoint subsets. This is illustrated in the following figure.

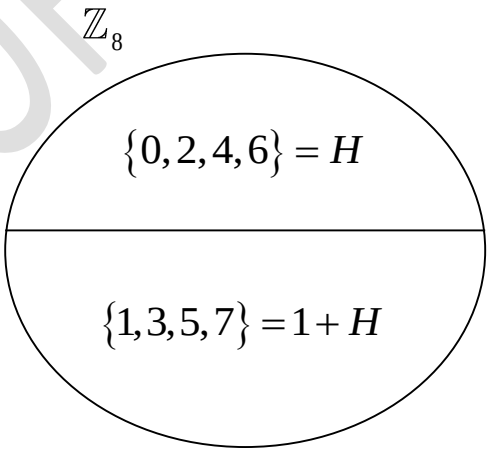


Figure 7.1 Cosets of $\mathbb{Z}_8$

The right cosets of H in G are:

$H+0=\{0,2,4,6\}=H$, $H+4=\{4,6,0,2\}$

$H+1=\{1,3,5,7\}$, $H+5=\{5,7,1,3\}$

$H+2=\{2,4,6,0\}$, $H+6=\{6,0,2,4\}$

$H+3=\{3,5,7,1\}$, $H+7=\{7,1,3,5\}$.

In this example, the right cosets and the left cosets turn out to be the same.

Note that the coset's representative is not unique. In the example above, the elements 0, 2, 4 and 6 are all representatives for the coset H. Likewise, the elements 1, 3, 5 and 7 are representatives for the coset $1+H$.

Example 7.2

Let $H=\{0,3,6\}$ in $\mathbb{Z}_9$ under addition. Thus the left cosets of H in $\mathbb{Z}_9$ are:

$$0+H=\{0,3,6\}=3+H=6+H$$
$$1+H=\{1,4,7\}=4+H=7+H$$
$$2+H=\{2,5,8\}=5+H=8+H.$$

Example 7.3

Let $G = S_3 = \{(1),(12),(13),(23),(123),(132)\}$ and

$H = \{(1),(13)\}$.

The left cosets of H in G are:

$$(1)H = \{(1)(1),(1)(13)\} = H.$$
$$(12)H = \{(12)(1),(12)(13)\} = \{(12),(132)\} = (132)H.$$
$$(13)H = \{(13)(1),(13)(13)\} = \{(13),(1)\} = H.$$
$$(23)H = \{(23)(1),(23)(13)\} = \{(23),(123)\} = (123)H.$$

Straightforward computations show that the right cosets of H in G are:

$$H(1) = H(13) = H.$$
$$H(12) = \{(23),(132)\} = H(123).$$
$$H(23) = \{(23),(132)\} = H(132).$$

In this example, the right cosets and the left cosets turn out to be different.

Example 7.4

Consider the Klein 4-group i.e. $V_4 = \{e, a, b, c\}$ and $H = \{e, a\}$ a subgroup of V_4. Then the right cosets of H in G are, $He = \{e.e, a.e\} = \{e, a\}$, $Ha = \{e.a, a.a\} = \{a, a^2\} = \{a, e\}$, $Hb = \{e.b, a.b\} = \{b, ab\} = \{b, c\}$ and

$Hc = \{e.c, a.c\} = \{c, ac\} = \{c, b\}$. This shows that there are two distinct right cosets of H in V_4 and that are $He = \{e, a\}$ and $Hb = \{b, c\}$.

Meanwhile, the left cosets of H in V_4 are $eH = \{e.e, e.a\} = \{e, a\}$, $aH = \{a.e, a.a\} = \{a, a^2\} = \{a, e\}$, $bH = \{b.e, b.a\} = \{b, ba\} = \{b, c\}$ and $cH = \{c.e, c.a\} = \{c, ca\} = \{c, b\}$. The distinct left cosets of H in V_4 are $eH = \{e, a\}$ and $bH = \{b, c\}$.

As $eH = He$, $aH = Ha$, $bH = Hb$ and $cH = Hc$ i.e. left cosets and right cosets coincide and hence V_4 is a commutative group.

7.2 Properties of Cosets

In this section we list some main properties that involve cosets.

Let H be a subgroup of G, and let $a, b \in G$. Then,

1. $a \in aH$.
2. $aH = H \leftrightarrow a \in H$.
3. $aH = bH$ or $aH \cap bH = \phi$.
4. $aH = bH \leftrightarrow a^{-1}b \in H$.
5. $|aH| = |bH|$.
6. $aH = Ha \leftrightarrow H = a^{-1}Ha$
7. $aH \leq G \leftrightarrow a \in H$.

Refer to Examples 7.1, 7.2 and 7.3.

Proposition 7.1

Let H be a subgroup of a group G. Then the left cosets of H in G have the following properties:
(i) $a \in aH$ for all $a \in G$.
(ii) If x and y are elements of G, and if $y = xa$ for some $a \in H$, then $xH = yH$.
(iii) If x and y are elements of G, and if $xH \cap yH$ is non-empty then $xH = yH$.

Proof

(i) Let $x \in G$. Then $x = xe$, where e is the identity element of G. But $e \in H$. It follows that $x \in xH$. This proves (i).

(ii) Let x and y be elements of G, where $y = xa$ for some $a \in H$. Then $yh = x(ah)$ and $xh = y(a^{-1}h)$ for all $h \in H$. Moreover $ah \in H$ and $a^{-1}h \in H$ for all $h \in H$, since H is a subgroup of G. It follows that $yH \subset xH$ and $xH \subset yH$, and hence $xH = yH$. This proves (ii).

(iii) Finally suppose that $xH \cap yH$ is non-empty for some elements x and y of G. Let z be an element of $xH \cap yH$. Then $z = xa$ for some $a \in H$, and $z = yb$ for some $b \in H$. It follows from (ii) that $zH = xH$ and $zH = yH$. Therefore $xH = yH$. This proves (iii). □

Proposition 7.2

Let H be a finite subgroup of a group G. Then each left coset of H in G has the same number of elements as H.

Proof Let $H = \{h_1, h_2, ..., h_m\}$, where $h_1, h_2, ..., h_m$ are distinct, and let x be an element of G. Then the left coset xH consists of the elements xh_j for $j = 1, 2, ..., m$. Suppose that j and k are integers between 1 and m for which $xh_j = xh_k$. Then $h_j = x^{-1}(xh_j) = x^{-1}(xh_k) = h_k$, implies $h_j = h_k$ and thus $j = k$, since $h_1, h_2, ..., h_m$ are distinct. It follows that the elements $xh_1, xh_2, ..., xh_m$ are distinct. We conclude that the subgroup H and the left coset xH both have m elements, as required.

Similarly each right coset of H in G has the same number of elements as H. Consequently there is a one-one correspondence between any two right (or left) cosets of H in G. □

Proposition 7.3

Any two right (left) cosets of H in G are either identical or disjoint.

Proof Let aH and bH be two distinct left cosets of H in G. Suppose $aH \cap bH \neq \phi$, let $x \in aH \cap bH$, implies $x \in aH$ and $x \in bH$, implies there exists $h_1, h_2 \in H$ such that $x = ah_1$ and $x = bh_2$, implies $ah_1 = bh_2$, implies $ah_1h_1^{-1} = bh_2h_1^{-1}$, implies

$a = bh_2h_1^{-1}$. Now consider $y \in aH$. This implies $y = ah_3$ for some $h_3 \in H$, which implies $y = bh_2h_1^{-1}h_3$ (using $a = bh_2h_1^{-1}$). This then implies $y = b(h_2h_1^{-1}h_3) \in bH$ (because $h_2h_1^{-1}h_3 \in H$) and therefore $y \in bH$, implies $aH \subset bH$. Similarly we can show that $bH \subset aH$ and hence $aH = bH$. □

7.3 Lagrange's Theorem

Lagrange's Theorem states that if a group G is finite, then the order of any subgroup of G must divide the order of G. We state this formally in the following theorem.

Theorem 7.1 Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Proof Each element of G belongs to at least one left coset of H in G, and no element can belong to two distinct left cosets of H in G. Therefore every element of G belongs to exactly one left coset of H. Moreover each left coset of H contains $|H|$ elements. Therefore $|G| = n|H|$, where n is the number of left cosets of H in G. The result follows. □

Corollary 7.1 $|G|/|H|$ ***is the number of cosets***

If H is a subgroup of a finite group G, then the number of distinct left (right) cosets of H in G is $|G|/|H|$.

We also call the number of distinct left (right) cosets of H in G as **the index of *H* in *G***, denoted by $[G:H]=\frac{|G|}{|H|}$.

Lagrange's Theorem is of great value if we are interested in finding all the subgroups of a finite group. In connection with this, it is important to include the following corollary.

Corollary 7.2 $|a|$ ***divides*** $|G|$

In a finite group G, the order of each element in the group divides the order of the group. In symbols, we write

$$|a|\,||G| \quad \forall a \in G.$$

Using Corollary 7.2 and Lagrange's Theorem, we can prove the following.

Theorem 7.2 ***Groups of Prime Order are Cyclic***

A group of prime order is cyclic.

Another important property in a group is that any element raised by the order of the group will produce the identity.

Theorem 7.3 $\left(a^{|G|} = e\right)$

Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.

Lagrange's Theorem can be used to prove Fermat's Little Theorem stated in the following.

Theorem 7.4 ***Fermat's Little Theorem***

For every integer a and every prime p, $a^p \bmod p = a \bmod p$.

An example of Fermat's Little Theorem is given as below:

Example 7.5

$$10^3 \bmod 3 \equiv 10 \bmod 3 \equiv 1.$$

7.4 An Application of Cosets to Permutation Groups

The theory of cosets can be applied to permutation groups. In this section we define the stabilizer and orbit of a point in a set $\{1, 2, \ldots, n\}$.

Definition 7.2 (Stabilizer of a Point)

Let G be a group of permutation on the set $\{1,2,\ ...\ ,n\}$. For any $1 \le i \le n$, let $G_i = \{\phi \in G \mid \phi(i) = i\}$. The set G_i is called the **stabilizer of *i* in *G*** or **the set of permutation that fixes *i*.**

Definition 7.3 (Orbit of a Point)

Let G be a group of permutation on the set $\{1,2,\ ...\ ,n\}$. For each $1 \le i \le n$, let $i^G = \{\phi(i) \mid \phi \in G\}$. The set i^G is subset of $\{1,2,\ ...\ ,n\}$ called the **orbit of *i* under *G*** or **the sets of images of *i***.

Example 7.5

Let $G = \{(1),(132)(465)(78),(132)(465),(123)(456),$
$(123)(456)(78),(78)\} \le S_8$.

Then,

$1^G = \{1,3,2\}$, $G_1 = \{(1),(78)\}$

$2^G = \{2,1,3\}$, $G_2 = \{(1),(78)\}$

$3^G = \{3,2,1\}$, $G_3 = \{(1),(78)\}$

$4^G = \{4,6,5\}$, $G_4 = \{(1),(78)\}$

$$5^G = \{5,4,6\}, \quad G_5 = \{(1),(78)\}$$

$$6^G = \{6,5,4\}, \quad G_6 = \{(1),(78)\}$$

$$7^G = \{7,8\}, \quad G_7 = \{(1),(132)(465),(123)(456)\}$$

$$8^G = \{8,7\}, \quad G_8 = \{(1),(132)(465),(123)(456)\}$$

From the example, we can see that an orbit can be viewed as a mapping for set *S* or the partition of the set *S*, such that

1. $i^G \neq \varnothing \ \ \forall i \in S$,
2. $i^G \cap j^G = \varnothing$ for $i \neq j$ and
3. $\bigcup_{i \in S} i^G = S$.

It turns out that the set G_i is a subgroup of the group.

Theorem 7.5

Let *G* be group then $G_i \leq G$.

Definition 7.4 (Index of a Group)

Let *H* be a subgroup of a group *G*. If the number of left cosets of *H* in *G* is finite then the number of such cosets is referred to as the index of *H* in *G*, denoted by $[G : H]$.

Conclusion: *The proof of Lagrange's Theorem shows that the index* $[G : H]$ *of a subgroup* H *of a finite group* G *is given by* $[G : H] = \frac{|G|}{|H|}$.

7.5 Normalizer and Centralizer

Definition 7.5 (Normalizer)
Let H be a subgroup of a group G. Then the normalizer of H in G is the set of all those elements G which commute with H, symbolically we write, $N_G(H) = \{g \in G : gH = Hg\}$.

Theorem 7.6

Verify that $N(H)$ is a subgroup of G.

Proof Since $eH = He$ implies $e \in N_G(H)$, hence $N_G(H) \neq \phi$.

Let $a,b \in N_G(H)$, then $aH = Ha$ and $bH = Hb$. Since $bH = Hb$, then

$b^{-1}bHb^{-1} = b^{-1}Hbb^{-1} \Rightarrow eHb^{-1} = b^{-1}He \Rightarrow Hb^{-1} = b^{-1}H$.

this implies $b^{-1} \in N_G(H)$. Now consider,

$(ab^{-1})H = a(b^{-1}H) = a(Hb^{-1}) = (aH)b^{-1} = (Ha)b^{-1}) = H(ab^{-1})$

That is $(ab^{-1})H = H(ab^{-1})$. This implies $ab^{-1} \in N_G(H)$ and hence $N_G(H)$ is a subgroup of G. □

Example 7.6

Let $G = < a, b : a^3 = b^2 = (ab)^2 = e >$ i.e. $G = \{e, a, a^2, b, ab, a^2b\}$ and $H = \{e, b\}$.

For $a \in G$ consider $aH = \{a.e, a.b\} = \{a, ab\}$ and $Ha = \{e.a, b.a\} = \{a, ba\}$ as $ab \neq ba$, implies $aH \neq Ha$ and hence $a \notin N_G(H)$.

For $b \in G$ consider $bH = \{b.e, b.b\} = \{b, b^2\} = \{b, e\}$ (as $b^2 = e$ in G) and $Hb = \{e.b, b.b\} = \{b, b^2\} = \{b, e\}$ that is $bH = Hb$ and hence $b \in N_G(H)$.

For $a^2 \in G$ consider $a^2H = \{a^2.e, a^2.b\} = \{a^2, a^2b\}$ and $Ha^2 = \{e.a^2, b.a^2\} = \{a^2, ba^2\} = \{a^2, ab\}$

(as $ba^2 = baa = a^2ba = a^2a^2b = a^4b = a^3ab = ab$) but $a^2b \neq ab$, therefore $a^2H \neq Ha^2$ this implies $a^2 \notin N_G(H)$.

For $ab \in G$ consider, $abH = \{ab.e, ab.b\} = \{ab, ab^2\}$ and $Hab = \{e.ab, b.ab\} = \{ab, ba.b\} = \{ab, a^2b.b\} = \{ab, a^2b^2\} = \{ab, a^2\}$ (as $b^2 = e$) but $a^2 \neq ab^2$, therefore, $abH \neq Hba$ this shows that $ab \notin N_G(H)$.

For $a^2b \in G$ consider, $a^2bH = \{a^2b.e, a^2b.b\} = \{a^2b, a^2b^2\}$ $= \{a^2b, a^2\}$ (as $b^2 = e$)

and $Ha^2b = \{e.a^2b, b.a^2b\} = \{a^2b, ba^2.b\} = \{a^2b, ab.b\} = \{a^2b, ab^2\}$ $= \{a^2b, a\}$ (as $b^2 = e$) but $a^2 \neq a$, therefore $a^2bH \neq Ha^2b$ this implies $a^2b \notin N_G(H)$. Hence $N_G(H) = \{e, b\}$. □

Definition 7.6 (Centralizer)
Let H be a subgroup of a group G. Then the centralizer of H in G is the set of all those elements G which commute with every element H, symbolically we write,

$$C_G(H) = \{g \in G \ : \ gh = hg \text{ for all } h \in H\}.$$

Note:
If $H = \{x\}$, then the normalizer and centralizer of H are identical. However, if H contains more than one element, then the normalizer and centralizer may be different.

Example 7.7
Consider the subgroup $H = \{e, a, a^2, a^3\}$ of the dihedral group of order 8 i.e. $D_4 = < a, b \ : \ a^4 = b^2 = (ab)^2 = e >$. Then find the centralizer of H in D_4.

Solution
The dihedral group of order 8 is given as $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, as $(ab)^2 = e$ implies $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^3$ (since $b^{-1} = b$ and $a^{-1} = a^3$) i.e. $ab = ba^3$. Moreover, $a^2b = a \cdot ab = a \cdot ba^3 = ab \cdot a^3 = ba^3 \cdot a^3$ $= ba^2 \cdot a^4 = ba^2 \cdot e = ba^2$. i.e. $a^2b = ba^2$.
For $b \in D_4$: As $ba \neq ab \Rightarrow b \notin C_{D_4}(H)$.

For $ab \in D_4$: As $(ab)a^3 = ba^3.a^3 = b.a^4.a^2 = ba^2$ i.e. $a^3(ab) = ba^2$ and $a^3(ab) = a^4b = b$, this implies $a^3(ab) \neq (ab)a^3$ and hence $ab \notin C_{D_4}(H)$.

For $a^2b \in D_4$: As $(a^2b)a = ba^2.a = ba^3 = ab$ i.e. $(a^2b)a = ab$ and $a(a^2b) = a(ba^2) = ab.a^2 = ba^3.a^2 = ba.a^4 = ba.e = ba$ i.e. $a(a^2b) = ba$ but $ab \neq ba$, implies $(a^2b)a \neq a(a^2b)$ hence $a^2b \notin C_{D_4}(H)$.

For $a^3b \in D_4$: As $(a^3b)a^3 = a^3.ba^3 = a^3.ab = a^4b = b$ i.e. $(a^3b)a^3 = b$ and $a^3(a^3b) = a^4.a^2b = e.a^2b = a^2b$ i.e. $a^3(a^3b) = a^2b$ but $a^2b \neq b$, hence $(a^3b)a^3 \neq a^3(a^3b)$, implies $a^3b \notin C_{D_4}(H)$. Hence $N_{D_4}(H) = H$.

Exercises 7: (Cosets and Lagrange Theorem)

1. Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.
2. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.
3. Find all cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.
4. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.
5. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.
6. Find all left cosets of the subgroup $\{\rho_0, \mu_2\}$ of the group D_4 given by Table 7.1 below.

	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Table 7.1

7. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left cosets?
8. Rewrite Table 7.1 in the order exhibited by the left cosets in Exercise 6. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group *V*?
9. Repeat Exercise 6 for the subgroup $\{\rho_0, \rho_2\}$ of D_4.
10. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left coset?
11. Rewrite Table 7.1 in the order exhibited by the left cosets in Exercise 37. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group *V*?
12. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.
13. Find the index of $\langle \mu_1 \rangle$ in the group S_3.
14. Find the index of $\langle \rho_3 \rangle$ in the group D_4 given in Table 8.1.
15. Let $\sigma = (1254)(23)$ in S_5. Find the index of $\langle \sigma \rangle$ in S_5.
16. Let $\mu = (1245)(36)$ in S_6. Find the index of $\langle \mu \rangle$ in S_6.

17. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4.
18. Let $H = \{0, \pm 3, \pm 6, \pm 9, ...\}$. Find all the left cosets of H in $\mathbb{Z}$.
19. Let H be as in exercise 18. Decide whether or not the following cosets of H are the same.
    a. $11 + H$ and $17 + H$
    b. $-1 + H$ and $5 + H$
    c. $7 + H$ and $23 + H$
20. Find all of the left cosets of $\{1, 11\}$ in $U(30)$.
21. Exercise Cosider a subgroup $H = \{e, b\}$ of a group D_4. Then evaluate right and left cosets of H in D_4 and show that $xH \neq Hx$ for all $x \in D_4$.
22. Cosider a subgroup $H = \{e, a, a^2, a^3\}$ of a group D_4. Then evaluate right and left cosets of H in D_4 and show that $xH = Hx$ for all $x \in D_4$.
23. Suppose that a has order 15. Find all the left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$.
24. Let G be a group and let H be a subgroup of G. Let $a \in G$. Prove that $aH = H$ if and only if $a \in H$.
25. Let G be the group of nonzero complex numbers under multiplication, and let $H = \{x \in G \mid |x| = 1\}$. (Recall that $|a + bi| = \sqrt{a^2 + b^2}$.) Give a geometric description of the cosets of H.
26. Let G be a group of order 60. What are the possible orders for the subgroups of G?
27. Suppose that K is a proper subgroup of H, and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?
28. Suppose that $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.
29. Use Corollary 1 of Lagrange's Theorem to prove that the order of $U(n)$ is even when $n > 2$.
30. Find all the left cosets of $\{(0, 1), (1, 2), (2, 4), (3, 3)\}$ in $\mathbb{Z}_4 \oplus U(5)$.
31. Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.
32. Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G.
33. Let $|G| = 8$. Show that G must have an element of order 2. Show by example that G need not have an element of order 4.
34 Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.
    a. Find the stabilizer of 1 and the orbit of 1.
    b. Find the stabilizer of 3 and the orbit of 3.
    c. Find the stabilizer of 5 and the orbit of 5.

35. Consider the subgroup $H = \{e, a, a^2\}$ of the group $G = \{e, a, a^2, b, ab, a^2b\}$. Then prove that $N_G(H) = G$.

36. Consider the subgroup $H = \{e, a, a^2, a^3\}$ of the dihedral group of order 8 i.e. $D_4 = < a, b \ : \ a^4 = b^2 = (ab)^2 = e >$. Then find the normalizer of H in G.

CHAPTER 8

NORMAL SUBGROUPS AND FACTOR GROUPS

8.1 Introduction

A special case of a set of cosets of a group where the left cosets coincide with the right cosets is called a ***normal subgroup***.

Definition 8.1 (Normal Subgroups)

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \lhd G$.

In other words, a subgroup is normal if all its left and right cosets are the same.

Note:

Every group G has at least two normal subgroups, namely the identity subgroup $E = \{e\}$ and the group G itself. Normal subgroups of G different from these two are called proper normal subgroups.

Note:

Groups having no proper normal subgroups are called Simple Groups.

There are several equivalent formulations of the definition of normality. We have chosen the one that is the easiest to use in applications. However, to verify that a subgroup is normal, it is usually much easier to use the following theorem.

Theorem 8.1 ***Normal Subgroup Test***

A subgroup H of G is normal in G if and only if $x^{-1}Hx \subseteq H$ for all x in G.

In other words, a subgroup H of a group G is said to be a normal subgroup of G if $xhx^{-1} \in H$ for all $h \in H$ and $x \in G$.

(In symbols, we write $H \lhd G \leftrightarrow x^{-1}Hx \subseteq H \quad \forall x \in G$).

Many students make the mistake of thinking that H is normal in G means $ha = ah$ for each $a \in G$ and $h \in H$. This is not what normality of H means; rather it means that if $a \in G$ and $h \in H$, then there exists some $h' \in H$ such that $ah = h'a$.

Example 8.1

Consider a subgroup $H = \{e, b\}$ of a group D_4. Since $a \in D_4$ and $aba^{-1} = aba^3 = a(ba)a^2 = a(a^3b)a^2 = a^4ba^2 = ba^2 \notin H$ i.e. $aba^{-1} \notin H$. This shows that H is not a normal subgroup of D_4.

Theorem 8.2

Every subgroup of an Abelian group is normal.

Proof Let N be a subgroup of an Abelian group G and consider

$xnx^{-1} = (xn)x^{-1}$ for all $n \in N$ and $x \in G$,

$= (nx)x^{-1}$ G being an Abelian group,

$= n(xx^{-1}) = ne = n \in N$ where e is the identity element of G.

i.e. $xnx^{-1} \in N$. The result follows. □

The converse of this is not true, because every subgroup of Q_8 (quaternian group of order 8) is normal but Q_8 is not an abelian group.

Theorem 8.3

The center, $Z(G)$, of a group is always normal.

Proof Consider $a \in Z(G)$ and $g \in G$, then $ag = ga$, implies $gag^{-1} = a \in Z(G)$ for all $g \in G$ i.e. $gag^{-1} \in Z(G)$ for all $g \in G$. This shows $Z(G)$ is normal subgroup of G. □

Theorem 8.4

The alternating group, A_n , of even permutations is a normal subgroup of S_n.

Proposition 8.1

The intersection of two normal subgroups of a group is also a normal subgroup of that group.

Proof Let N_1 and N_2 be normal subgroups of a group G. Then since the intersection of two subgroups is a subgroup therefore $N_1 \cap N_2$ is a subgroup of G.

Next we consider $n \in N_1 \cap N_2$, implies $n \in N_1$ and $n \in N_2$. Then $gng^{-1} \in N_1$ and $gng^{-1} \in N_2$ for all $g \in G$ (since N_1 and N_2 are normal subgroups of *G*). This implies $gng^{-1} \in N_1 \cap N_2$ for all $n \in N_1 \cap N_2$ and $g \in G$. This shows that $N_1 \cap N_2$ is normal in *G*. □

Theorem 8.5

A subgroup of index 2 in a group G is normal.

Proof If *H* is a subgroup of index 2 in *G* then $G = \{H, Hg\}$ and $G = \{H, gH\}$ for all $g \in G$ such that $g \notin H$ and therefore $\{H, Hg\} = \{H, gH\}$, implies $Hg = gH$ for all $g \in G$ such that $g \notin H$. However if $g \in H$ then obviously $Hg = gH$. This shows that *H* is normal in *G*.

Theorem 8.6

Let a be an element of order 2 in a group G. Then the subgroup $H = \{e, a\}$ is normal in G if and only if $a \in C(G)$ (centralizer of G).

Proof For $g \in G$, H is normal in G if and only if $Hg = gH$ if and only if $\{e, a\}g = g\{e, a\}$ if and only if $\{g, ga\} = \{g, ag\}$ if and only if $ag = ga$ if and only if $a \in C(G)$ as required. □

Theorem 8.7

A sub group N of a group G is a normal subgroup of G if and only if product of any two right cosets of N in G is right coset of N in G.

Proof If N is a normal subgroup of G and let x and y be elements of G then $Nx = xN$, and therefore $(Nx)(Ny) = N(xN)y = N(Nx)y = (NN)(xy)$. But $NN = N$ (since N is a subgroup of G). Therefore $(Nx)(Ny) = N(xy)$. Thus the product of two right cosets of N in G, i.e. the product of Nx and Ny is Nxy ($xy \in G$) which is a right coset of N in G.

Conversely; Let N be a group of G such that the product of right cosets of N in G is right coset of N in G. Let x be an elements of G, then x^{-1} is also an element of G. Therefore Nx and Nx^{-1} are right cosets of N in G. Consequently, by hypothesis $NxNx^{-1}$

is also a right coset of N in G. Since $e \in N$, so we can write $e = exex^{-1} \in NxNx^{-1}$. Thus N and $NxNx^{-1}$ are two right cosets of N in G with one common element e and hence $NxNx^{-1} = N$, therefore for $n_1, n_2 \in N$, we can write $n_1 x n_2 x^{-1} \in N$, implies $n_1^{-1}(n_1 x n_2 x^{-1}) \in n_1^{-1}N = N$, implies $xn_2x^{-1} \in N$. This shows that N is a normal subgroup of G. □

Example 8.2

The subgroup of rotation in D_n is normal in D_n.

Example 8.3

The group $SL(2,\mathbb{R})$ of 2×2 matrices with determinant 1 is a normal subgroup of $GL(2,\mathbb{R})$, the group of 2×2 matrices with nonzero determinant.

A special class of group where its only normal subgroups are the trivial subgroup and itself is called a simple group.

Definition 8.2 (Simple Group)

A group is **simple** if its only normal subgroups are the identity subgroup and the group itself.

In other words, we say that a group is simple if it has no proper normal subgroups.

There is another easy way to determine whether a subgroup of a group is normal or not by checking its index. If the index is two, then we can say that the subgroup is normal in the group. However, the converse is not necessarily true.

Theorem 8.8

If the index of H in G is 2, then H is a normal subgroup.

In other words, we say that if H has only two left or right cosets in G, then H is normal in G.

8.2 Factor Groups

If H is a normal subgroup of G, then $aH = Ha$ for all a in G, so there is no distinction between left and right cosets of H in G. In this case we refer simply to the cosets of H in G.

If H is a normal subgroup of G, then the set of all cosets of H in G forms a group, and is called the ***factor group***.

Proposition 8.2

Let G be a group, and let N be a normal subgroup of G. Then the set of all cosets of N in G is a group under the operation of multiplication. The identity element of this group is N itself, and the inverse of a coset xN is the coset $x^{-1}N$ for any element x of G.

Proof Since N is normal subgroup of G, therefore each right coset is a left coset. Hence there is no distinction between right and left cosets, so we simply write a coset here.

Let G/N be the collection of all cosets of N in G i.e. $G/N = \{xN \ : \ x \in G\}$.

- Closure property: Let $x, y \in G$ then,

$$(xN)(yN) = x(Ny)N = x(yN)N \text{ (because } N \text{ is normal in } G)$$
$$= (xy)NN = xyN \text{ (using } NN = N)$$

since $xy \in G$ therefore xyN is a coset of N in G i.e. $xyN \in G/N$. This implies G/N is closed with respect to coset multiplication.

- Associative property: Let x, y and z be any elements of G, then xN, yN and zN. Consider

$$\left[(xN)(yN)\right](zN) = (xy)N(zN) = (xy)zN = x(yz)N$$
$$((xy)z = x(yz) \text{ for all } x, y, z \in G)$$
$$= xN\left[yzN\right] = xN\left[yNzN\right].$$

This implies G/N satisfies associative property with respect to coset multiplication.

- Existence of identity: The subgroup N is itself a coset of N in G, since $N = eN$. Moreover, $(xN)N = (xN)(eN) = (xe)N$

$= xN$ and $N(xN) = (eN)(xN) = (ex)N = xN$, this implies N is the identity element of G/N.

- Existence of inverse: Since $(xN)(x^{-1}N) = (xx^{-1})N = N$ and $(x^{-1}N)(xN) = (x^{-1}x)N = N$. This shows that $x^{-1}N$ is the inverse of xN for all elements x of *G*.

Thus the group axioms are satisfied.

Definition 8.3 (Factor Groups)

Let *G* be a group and $H \lhd G$. Then a subgroup consisting of all cosets, aH or Ha, is called a **factor group** for *G* of *H*.

or

Let *N* be a normal subgroup of a group *G*. The quotient group (or factor group) G/N is defined to be the group of cosets of *N* in *G* under the operation of coset multiplication.

Example 8.4

If N_1 and N_2 are normal subgroups of a group *G*. Then $G/N_1 = G/N_2$ if and only if $N_1 = N_2$.

Solution

Let $G/N_1 = G/N_2$, then as $N_1 \in G/N_1 = G/N_2$, implies $N_1 \in G/N_2$ i.e. N_1 is equal to some coset of N_2 in *G*. But we know that two cosets are either identical or disjoint, and here N_1 and N_2 are not disjoint because $e \in N_1 \cap N_2$ and hence $N_1 = N_2$.

Conversely; If $N_1 = N_2$, then obviously $G/N_1 = G/N_2$.

Theorem 8.9

Let G be a group and H a normal subgroup of G. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation

$$(aH)(bH) = abH .$$

Theorem 8.10

If $G/Z(G)$ is cyclic then G is abelian, where $Z(G)$ denotes the center of a group G.

Proof Let $Z(G) = C$ and let Cg be a generator of G/C, where $g \in G$. Let $a, b \in G$ then $Ca, Cb \in G/C$, then $Ca = (Cg)^m$ and $Cb = (Cg)^n$ for some $m, n \in Z^+$, this implies $Ca = Cg \cdot Cg \cdot Cg \cdots Cg$ (m-times), implies $Ca = Cg^m$ similarly $Cb = Cg^n$. As $a \in Ca = Cg^m$, then $a = c_1 g^m$, for some $c_1 \in C$. Similarly $b = c_2 g^n$, for some $c_2 \in C$. Consider,

$$ab = (c_1 g^m)(c_2 g^n) = c_1 (g^m c_2) g^n = c_1 (c_2 g^m) g^n ,$$

(because $c_2 \in C$, implies $g^m c_2 = c_2 g^m$)

$= c_1 c_2 g^{m+n} = c_2 c_1 g^{n+m}$ (because $c_1, c_2 \in C$, implies $c_1 c_2 = c_2 c_1$),

$= c_2 c_1 g^n g^m = c_2 (c_1 g^n) g^m = c_2 (g^n c_1) g^m = (c_2 g^n)(c_1 g^m) = ba,$

i.e. $ab = ba$ for all $a, b \in G$ and hence G is abelian.

Example 8.5

Let $G = \mathbb{Z}_{18}$ and $H = \langle 6 \rangle = \{0,6,12\}$. Then,

$$G/H = \{0+H, 1+H, 2+H, 3+H, 4+H, 5+H\}.$$

Example 8.6

Let $G = S_3$ and $H = \{(1),(123),(132)\}$. We can prove that $H \lhd G$ using Theorem 8.2 because the index of H in G is 2. Then, $G/H = \{H,(12)H\}$ with

$$H = \{(1),(123),(132)\} \text{ and}$$
$$(12)H = \{(12),(23),(13)\}.$$

The Cayley table for the factor group is given as follows :

$\cdot$	H	$(12)H$
H	H	$(12)H$
$(12)H$	$(12)H$	H

Example 8.7

Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$. To construct $\mathbb{Z}/4\mathbb{Z}$, we must first determine the left cosets of $4\mathbb{Z}$ in G. Consider the following four cosets:

$$0+4\mathbb{Z}=4\mathbb{Z}=\{\ldots,-8,-4,0,4,8,\ \ldots\},$$
$$1+4\mathbb{Z}=\{\ldots,-11,-7,-3,\ 1,5,9,\ \ldots\},$$
$$2+4\mathbb{Z}=\{\ldots,-10,-6,-2,2,6,10,\ \ldots\ \},$$
$$3+4\mathbb{Z}=\{\ldots,-9,-5,-1,3,7,11,\ \ \ldots\}.$$

Now we claim that there are no other cosets. If $k\in\mathbb{Z}$, then $k=4q+r$ where $0\le r<4$; and, therefore,

$$k+4\mathbb{Z}=r+4q+4\mathbb{Z}=r+4\mathbb{Z}.$$

Now that we know the elements of the factor group, our next job is to determine the structure of $\mathbb{Z}/4\mathbb{Z}$. Its Cayley table is given in the following:

$\cdot$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

We can show that $\mathbb{Z}/4\mathbb{Z}\cong\mathbb{Z}_4$. More generally, if for any $n>0$ we let $n\mathbb{Z}=\{0,\pm n,\pm 2n,\pm 3n,\ \ldots\}$, then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

8.3 Internal Direct Product

Another application that is related to normal subgroups is internal direct product. However, internal direct product differs from external direct product in the sense that internal direct product involves subgroups of the same group.

We first define a product of two subgroups of a group in the following.

Definition 8.4 (Product of Subgroups)

Suppose H and K are subgroups of some group G, then we define the set $HK = \{hk \mid h \in H, k \in K\}$ as a product of subgroups H and K.

Example 8.8

Given $U(24) = \{1,5,7,11,13,17,19,23\}$. Let $H = \{1,17\}$ and $K = \{1,13\}$. Then, $HK = \{1,5,13,17\}$, since $5 = 17 \cdot 13 \bmod 24$.

Example 8.9

In S_3, let $H = \{(1),(12)\}$ and $K = \{(1),(13)\}$. Then $HK = \{(1),(13),(12),(12)(13)\} = \{(1),(13),(12),(132)\}$.

We should be careful not to assume the set HK is a subgroup of G; in Example 9.6 it is, but in Example 9.7 it is not.

We are now ready to define internal direct product of two subgroups, given in the following.

Definition 8.5 (Internal Direct Product of H and K)

Let H and K be two normal subgroups of a group G. We say that G is the internal direct product of H and K and write $G = H \times K$ if

1. $G = HK$,
2. $hk = kh \quad \forall h \in H, k \in K$,
3. $H \cap K = \{e\}$.

Example 8.10

Let $G = \mathbb{R}$. Then, for $E =$ set of even numbers and $D =$ set of odd numbers, $E \times D = E \oplus D$.

Example 8.11

Let $G = C_2 \times C_2 = \{(1,1),(1,a),(1,b),(a,b)\}$, then $G = \{1,a\} \times \{1,b\}$.

Example 8.12

In D_6, the dihedral group of order 12, let F denote some reflections and let R_k denote a rotation of k degrees. Then,

$$D_6 = \{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\} \times \{R_0, R_{180}\}.$$

Exercises 8: (Normal Subgroups and Factor Groups)

In Exercises 1 through 8, find the order of the given factor group.

1. $\mathbb{Z}_6/\langle 3\rangle$
2. $(\mathbb{Z}_4 \oplus \mathbb{Z}_{12})/\langle (2,2)\rangle$
3. $(\mathbb{Z}_4 \oplus \mathbb{Z}_2)/\langle (2,\ 1)\rangle$
4. $(\mathbb{Z}_3 \oplus \mathbb{Z}_5)/\langle (0,3)\rangle$
5. $(\mathbb{Z}_2 \oplus \mathbb{Z}_4)/\langle (1,\ 1)\rangle$
6. $(\mathbb{Z}_{12} \oplus \mathbb{Z}_{18})/\langle (4,\ 3)\rangle$
7. $(\mathbb{Z}_2 \oplus S_3)/\langle (1,\ \rho_1)\rangle$
8. $(\mathbb{Z}_{11} \oplus \mathbb{Z}_{15})/\langle (1,\ 1)\rangle$

In Exercises 9 through 15, give the order of the element in the factor group.

9. $5+\langle 4\rangle$ in $\mathbb{Z}_{12}/\langle 4\rangle$
10. $26+\langle 12\rangle$ in $\mathbb{Z}_{60}/\langle 12\rangle$
11. $(2,\ 1)+\langle (1,\ 1)\rangle$ in $(\mathbb{Z}_3 \oplus \mathbb{Z}_6)/\langle (1,\ 1)\rangle$
12. $(3,\ 1)+\langle (1,\ 1)\rangle$ in $(\mathbb{Z}_4 \oplus \mathbb{Z}_4)/\langle (1,\ 1)\rangle$
13. $(3,\ 1)+\langle (0,\ 2)\rangle$ in $(\mathbb{Z}_4 \oplus \mathbb{Z}_8)/\langle (0,\ 2)\rangle$
14. $(3,\ 3)+\langle (1,\ 2)\rangle$ in $(\mathbb{Z}_4 \oplus \mathbb{Z}_8)/\langle (1,\ 2)\rangle$
15. $(2,\ 0)+\langle (4,\ 4)\rangle$ in $(\mathbb{Z}_6 \oplus \mathbb{Z}_8)/\langle (4,\ 4)\rangle$

16. A student is asked to show that if *H* is a normal subgroup of an abelian group *G*, then *G*/*H* is abelian. The student's proof starts as follows:

    We must show that *G*/*H* is abelian. Let *a* and *b* be two elements of *G*/*H*.

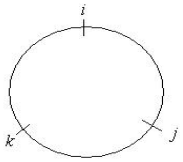
    a. Why does the instructor reading this proof expect to find nonsense from here on in the student's paper?
    b. What should the student have written?
    c. Complete the proof.

17. Show that the intersection of two normal subgroups of *G* is a normal subgroup of *G*.
18. Show that an intersection of normal subgroups of a group *G* is again a normal subgroup of *G*.
19. Let $H = \{(1), (12)\}$. Is *H* normal in S_3?
20. Prove that A_n is normal in S_n.
21. Let $H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a,\ b,\ d \in \mathbb{R} \right\}$. Is *H* a normal subgroup of $GL(2,\ \mathbb{R})$.
22. Prove that $SL(2,\ \mathbb{R})$ is a normal subgroup of $GL(2,\ \mathbb{R})$.

23. Viewing $\langle 3\rangle$ and $\langle 12\rangle$ as subgroups of $\mathbb{Z}$, prove that $\langle 3\rangle/\langle 12\rangle$ is isomorphic to $\mathbb{Z}_4$. Similarly, prove that $\langle 8\rangle/\langle 48\rangle$ is isomorphic to $\mathbb{Z}_6$. Generalize to arbitrary integers *k* and *n*.
24. Prove that if *H* has index 2 in *G*, then *H* is normal in *G*.
25. Let $H = \{(1), (12)(34)\}$ in A_4.
    a. Show that *H* is not normal in A_4.
    b. Referring to the multiplication table for A_4, show that, although $\alpha_6 H = \alpha_7 H$ and $\alpha_9 H = \alpha_{11} H$, it is not true that $\alpha_6\alpha_9 H = \alpha_7\alpha_{11} H$. Explain why this proves that the left cosets of *H* do not form a group under coset multiplication.
26. Prove that a factor group of a cyclic group is cyclic.
27. What is the order of elements $5+\langle 6\rangle$ in the factor group $\mathbb{Z}_{18}/\langle 6\rangle$?
28. Let $G = \mathbb{Z}/\langle 20\rangle$ and $H = \langle 4\rangle/\langle 20\rangle$. List the elements of *H* and G/H.
29. What is the order of the factor group $\mathbb{Z}_{60}/\langle 15\rangle$?
30. What is the order of the factor group $(\mathbb{Z}_{10} \oplus U(10))/\langle (2,9)\rangle$?
31. Let $G = U(16)$, $H = \{1, 15\}$, and $K = \{1, 9\}$. Are *H* and *K* isomorphic? Are G/H and G/K isomorphic?
32. Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4$, $H = \{(0, 0), (2, 0), (0, 2), (2, 2)\}$, and $K = \langle (1,2)\rangle$. Is G/H isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? Is G/K isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$?
33. Let $G = GL(2, \mathbb{R})$ and $H = \{A \in G \mid \det A = 3^k,\ k \in \mathbb{Z}\}$. Prove that *H* is a normal subgroup of *G*.
34. Express $U(165)$ as an internal direct product of proper subgroups in three different ways.
35. Let $\mathbb{Z}$, let $H = \langle 5\rangle$ and $K = \langle 7\rangle$. Prove that $\mathbb{Z} = HK$. Does $\mathbb{Z} = H \oplus K$?
36. Let $G = \{3^a 6^b 10^c \mid a, b, c \in \mathbb{Z}\}$ under multiplication. Prove that $G = \langle 3\rangle \oplus \langle 6\rangle \oplus \langle 10\rangle$, whereas $H \neq \langle 3\rangle \oplus \langle 6\rangle \oplus \langle 12\rangle$.
37. Show, by example, that in a factor group G/H it can happen that $aH = bH$ but $|a| \neq |b|$.
38. Prove that a factor group of an Abelian group is Abelian.
39. If $|G| = pq$, where *p* and *q* are not necessarily distinct primes, prove that $|\mathbb{Z}(G)| = 1$ or pq.
40. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1$, $-i = (-1)i$, $1^2 = (-1)^2 = 1$, $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$.
    a. Construct the Cayley table for *G*.
    b. Show that $H = \{1, -1\} \triangleleft G$.

c. Construct the Cayley table for G/H.

(The rules involving *i*, *j*, and *k* can be remembered by using the circle below.



Going clockwise, the product of two consecutive elements is the third one. The same is true for going counterclockwise, except that we obtain the negative of the third element.) This group is called the *quaternions* and was invented by William Hamilton in 1843. The quaternions are used to describe rotations in three-dimensional space, and they are used in physics. The quaternions can be used to extend the complex numbers in a natural way.

41. If *N* is a normal subgroup of *G* and *H* is any subgroup of *G*, prove that *NH* is a subgroup of *G*.
42. If *N* and *M* are normal subgroups of *G*, prove that *NM* is also a normal subgroup of *G*.
43. Let *N* be a normal subgroup of a group *G*. If *N* is cyclic, prove that every subgroup of *N* is also normal in *G*.
44. Let *H* be a normal subgroup of a finite group *G*. If $\gcd(|x|, |G/H|) = 1$, show that $x \in H$.
45. If *H* is a normal subgroup of *G*, and $|H| = 2$, prove that *H* is contained in the center of *G*.

CHAPTER 9

SERIES OF GROUPS, NILPOTENT GROUPS AND SOLVABLE GROUPS

9.1 Series of Groups

We restate the definition of normal subgroups from the previous chapter below.

Definition 9.1 (Normal Subgroups)

A subgroup H of a group G is **normal** in G, denoted by $H \triangleleft G$, if $Hx = xH$ for every x in G.

Next, we introduce a special sequence of subgroups of a group called subnormal series.

Definition 9.2 (Subnormal Series)

A **subnormal** (or **subinvariant) series of a group *G*** is a finite sequence $H_0, H_1, ..., H_n$ of subgroups of G such that $H_i < H_{i+1}$, and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = G$.

A special case where all subgroups are normal is called a normal series of a group.

Definition 9.3 (Normal Series)

A **normal** (or **invariant) series of *G*** is a finite sequence $H_0, H_1, ..., H_n$ of normal subgroups of G such that $H_i < H_{i+1}$, $H_0 = \{e\}$, and $H_n = G$.

We observe that a normal series always exists for an arbitrary group.

Definition 9.4 (Composition Series)

A **composition series of *G*** is a finite sequence $H_0, H_1, ..., H_n$ of subgroups of G such that $H_i < H_{i+1}$, and H_i is maximal normal subgroup of H_{i+1} with $H_0 = \{e\}$, and $H_n = G$.

Example 9.1

The symmetric group S_4 has the following normal series, among others:

$\langle(1)\rangle < C_2 < V_4 < A_4 < S_4,$

$\langle(1)\rangle < V_4 < A_4 < S_4,$

$\langle(1)\rangle < C_2 < V_4 < S_4,$

$\langle(1)\rangle < V_4 < S_4,$

$\langle(1)\rangle < S_4,$

where V_4 is the Klein 4-group and, as usual, C_n denotes a cyclic group of order n, here, e.g., take $C_n = \langle(1\ 2)(3\ 4)\rangle$.

Example 9.2

Consider the group $(\mathbb{Z}_{12}, +_{12})$. All subgroups of $\mathbb{Z}_{12}$ are normal because it is abelian. Hence, the following chains are normal:

i. $\langle 0\rangle \subset \langle 6\rangle \subset \mathbb{Z}_{12}$,

ii. $\langle 0\rangle \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{12}$,

iii. $\langle 0\rangle \subset \langle 4\rangle \subset \langle 2\rangle \subset \mathbb{Z}_{12}$,

iv. $\langle 0\rangle \subset \langle 6\rangle \subset \langle 2\rangle \subset \mathbb{Z}_{12}$.

In the above chains, ii-iv are composition series.

In mathematics, especially in the fields of group theory and Lie theory, a central series is a kind of normal series of subgroups or Lie subalgebras, expressing the idea that the commutator is nearly trivial. For groups, this is an explicit

expression that the group is a nilpotent group, and for matrix rings, this is an explicit expression that in some basis the matrix ring consists entirely of upper triangular matrices with constant diagonal.

Definition 9.5 (A Central Series)

A **central series** is a sequence of subgroups of a group G

$$\{1\} = H_0 \leq H_1 \leq \ldots \leq H_n = G$$

such that the successive quotients are central, in the sense that $[G, H_{i+1}] \leq H_i$, where $[G, H]$ denotes the commutator subgroup generated by $g^{-1}h^{-1}gh$ for g in G and h in H.

Note that the subgroups in a central series are always normal subgroups of G.

The lower central series and upper central series (also called the descending central series and ascending central series, respectively), are characteristic series, which, despite the names, are central series if and only if a group is nilpotent as we shall define later.

Here we define the upper (or ascending) central series. The lower central series can be defined accordingly.

Definition 9.6 (Upper Central Series)

A series $\{1\} = H_0 \leq H_1 \leq \ldots$ of subgroups of a group G is called the **upper central series** of G with $H_0 = \{1\}$, $H_1 = Z(G)$ is the center of G, and $H_{i+1}/H_i = Z\left(G/H_i\right)$.

9.2 Nilpotent Groups

Nilpotent groups arise in Galois theory, as well as in the classification of groups. They also appear prominently in the classification of Lie groups.

Definition 9.7 (Nilpotent Groups)

A group G is **nilpotent** if its upper central series ascend to G in a finite number of steps. A group G is nilpotent of class k if and only if in its upper central series $H_k = G$ and $H_{k-1} \neq G$.

Example 9.3

Every abelian group is nilpotent.

Example 9.4

All finite p-groups are nilpotent.

Example 9.5

Other nilpotent groups include the dihedral and quaternion groups of order 8.

9.3 Solvable Groups

In the field of group theory, a solvable group (or is sometimes called soluble group) is a group that can be constructed from abelian groups using extensions. That is, a solvable group is a group whose derived series terminates in the trivial subgroup.

Historically, the word "solvable" arose from Galois theory and the proof of the general unsolvability of quintic equation. Specifically, a polynomial equation is solvable by radicals if and only if the corresponding Galois group is solvable.

Definition 9.8 (Solvable Groups)

A group G is called **solvable** if it has a subnormal series whose factor groups are all abelian, that is, if there are subgroups $\{1\} = G_0 \leq G_1 \leq ... \leq G_k = G$ such that G_{j-1} is normal in G_j, and G_j / G_{j-1} is an abelian group for $j = 1, 2, ..., k$.

For finite groups, an equivalent definition is that a solvable group is a group with a composition series all of whose factors are cyclic groups of prime order. This is equivalent because a finite abelian group has finite composition length, and every finite simple abelian group is cyclic of prime order.

Example 9.6

All abelian groups are solvable.

Example 9.7

A small example of a solvable, non-nilpotent group is the symmetric group S_3.

Example 9.8

The group S_5 is not solvable since it has a composition series $\{E, A_5, S_5\}$ giving factor groups isomorphic to A_5 and C_2; and A_5 is not Abelian. While S_4 **and** A_4 are solvable.

Example 9.9

All nilpotent groups are solvable.

Exercises 9: (Series of Groups, Nilpotent Groups and Solvable Groups)

1. Find the upper central series and the class for groups in Example 9.2 – 9.4.
2. Find the subnormal series for groups in Example 9.5 – 9.6.
3. Show that all nilpotent groups are solvable.
4. Find all composition series of the group $\mathbb{Z}/\langle 42\rangle$. Verify that they are equivalent.

CHAPTER 10

THE SYLOW THEOREMS

10.1 Introduction

The aim of this chapter is to sample the flavor of more advanced work in groups while maintaining an acceptable level of rigor in the presentation. We first start with a section of conjugacy classes.

10.2 Conjugacy Classes

The elements of any group may be partitioned into conjugacy classes, where members of the same conjugacy class share many properties. The study of conjugacy classes of non-abelian groups reveals many important features of their structure.

We define the conjugacy class formally as follows.

Definition 10.1 (Conjugacy Class of *a*)

Let $a,b \in G$. We say *a* and *b* are conjugate in *G* (and call *b* a conjugate of *a*) if $x^{-1}ax = b$ for some *x* in *G*. The conjugacy class of *a* is the set $\mathrm{cl}(a) = \{x^{-1}ax \mid x \in G\}$.

Next, we state some properties of conjugacy classes. The first one states that the identity element is always in its own class.

Theorem 10.1 $\mathrm{cl}(e)=\{e\}$.

Proof From the definition,

$$\mathrm{cl}(e)=\{x^{-1}ex \mid x\in G\}=\{e\}. \ \square$$

Next, we prove that an element is always contained in its own conjugacy class.

Theorem 10.2 $a\in \mathrm{cl}(a)$.

Proof All groups contain an identity element, e. This gives $a=eae^{-1}$, thus the theorem is proven. $\square$

Note that if G is abelian, then $\mathrm{cl}(a)=\{a\}, \forall a\in G$.

Example 10.1

Find the conjugacy class of each element in S_3.

(i) For (12) :

$(1)(12)(1)=(12),(12)(12)(21)=(12),\ (13)(12)(31)=(23),$
$(23)(12)(32)=(13),(123)(12)(132)=(23),(132)(12)(123)=(13).$
Thus $cl((12))=\{(12),(23),(13)\}$.

(ii) $cl((1)) = \{(1)\}$, since $x(1)x^{-1} = xx^{-1}(1) = (1)$.

(iii) $cl((123)) = \{(123),(132)\}$ since

$(123)(123)(132) = (123), (132)(123)(123) = (132)$.

The complete list will be:

$cl((1)) = \{(1)\}$,

$cl((12)) = \{(12),(23),(13)\} = cl((13)) = cl((23))$,

$cl((123)) = \{(123),(132)\} = cl((132))$.

Theorem 10.3 If $|cl(a)| = 1$, then $a \in Z(G)$.

We can also rewrite Theorem 10.3 as $cl(a) = \{a\}$.

Theorem 10.4

The number of elements in a conjugacy C_a of an element a in a group G is equal to the the index of its normalizer in G i.e. $|C_a| = [G : N_G(a)]$.

Proof Let Ω be the collection of all right cosets of $N_G(a) = N$, where a is an element of a group G. We have to show that the number of elements in Ω being the index of $N_G(a)$ is equal to the number of elements in C_a. To do this we define a function $f : \Omega \to C_a$ by $f(Ng) = g^{-1}ag$, where $g \in G$

that is to each right coset N_g associate the conjugate element $g^{-1}ag$ of $a \in C_a$ under *f*.

First of all we show that f is well defined, let

$$Ng_1 = Ng_2 \Rightarrow Ng_1g_1^{-1} = Ng_2g_1^{-1} \Rightarrow Ne = Ng_2g_1^{-1} \Rightarrow N = Ng_2g_1^{-1} \Rightarrow g_2g_1^{-1} \in N$$

this implies there exist $n \in N$ such that $g_2g_1^{-1} = n \Rightarrow g_2 = ng_1$.

Consider $g_2^{-1}ag_2 = (ng_1)^{-1}a(ng_1) = g_1^{-1}(n^{-1}an)g_1 = g_1^{-1}(a)g_1$ (because $n \in N \Rightarrow na = an \Rightarrow a = n^{-1}an$), this impllies $g_2^{-1}ag_2 = g_1^{-1}ag_1$ and hence $f(Ng_2) = f(Ng_1)$. This shows that *f* is well defined.

Next we have to show that f is bijective. Since each $g^{-1}ag \in C_a$ is the image of $Ng \in \Omega$, therefore *f* is clearly onto (surjective).

Next consider, $f(Ng_2) = f(Ng_1)$, implies $f(Ng_2) = f(Ng_1)$, implies $g_2^{-1}ag_2 = g_1^{-1}ag_1$, implies $g_1g_2^{-1}ag_2g_1^{-1} = g_1g_1^{-1}ag_1g_1^{-1}$, implies $(g_1g_2^{-1})a(g_1(g_2)^{-1})^{-1} = a$, implies $g_1g_2{}^{-1} \in N$, implies $g_1 \in Ng_2$ but $g_1 \in Ng_1$, implies $Ng_1 = Ng_2$. This implies *f* is bijective. And hence Ω and C_a have same number of elements i.e. $|C_a| = [G : N_G(a)]$.

Corollary 10.1

Let a be an element of a finite group *G*. Then the number of elements in the conjugacy class C_a of a divides the order of *G*.

Proof Since $N_G(a)$ is a subgroup of *G*, hence by Lagrange's theorem, the order and index of $N_G(a)$ will divide the order of *G*. Also we know that the index of $N_G(a)$ is equal to the number of elements in C_a. Hence, from the above discussion we

conclude that the number of elements in the conjugacy class C_a of a divides the order of G. □

10.3 The Sylow Theorems

The ***Sylow theorems***, named after Ludwig Sylow, form a partial converse to Lagrange's theorem, which states that if H is a subgroup of a finite group G, then the order of H divides the order of G. The Sylow theorems guarantee, for certain divisors of the order of G, the existence of corresponding subgroups, and give information about the number of those subgroups.

The following theorem was first proposed and proven by Norwegian mathematician Ludwig Sylow in 1872, and published in *Mathematische Annalen*.

Theorem 10.5 First Sylow Theorem

Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$.
2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i \leq n$.

Example 10.2

Let $|G| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7$. Using First Sylow Theorem, *G* has at least a proper nontrivial subgroup of order

$$2, 4, 8, 3, 9, 5, 25, 125, 625 \text{ and } 7.$$

Example 10.3

Let $|G| = 2^2 \cdot 3^3 \cdot 5^3$. Thus, *G* has a subgroup of order 2, 4, 3, 9, 27, 5, 25 and 125.

Let $|H_1| = 3, |H_2| = 9, |H_3| = 27, |H_4| = 2, |H_5| = 4, |H_6| = 5,$ $|H_7| = 25$ and $|H_8| = 125$. Then, by First Sylow Theorem,

$$H_1 \lhd H_2 \lhd H_3, \quad H_4 \lhd H_5 \text{ and } \quad H_6 \lhd H_7 \lhd H_8.$$

Definition 10.2 (Sylow *p*-Subgroup)

Let *G* be finite group and let *p* be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of *G* of order p^k is called a **Sylow *p*-subgroup** of *G*.

Example 10.4

Let *G* be a group with $|G| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7$. Then we call any subgroup of order 8 a Sylow 2-subgroup of *G*, any subgroup of order 9 a Sylow 3-subgroup of *G*, any subgroup of order 625 a

Sylow 5-subgroup of *G*, and any subgroup of order 7 a Sylow 7-subgroup of *G*.

Any subgroup of *G* of order p^k is called a **Sylow *p*-subgroup** of *G* and we denote it by Syl_pG.

Example 10.5

(i) Let $|G| = 20 = 2^2 \times 5$. Then

$|Syl_2G| = 2^2 = 4$, $|Syl_5G| = 5$.

(ii) Let $|G| = 2^2 \times 3^3 \times 5^3$. Then

$|Syl_2G| = 2^2 = 4$, $|Syl_3G| = 3^3 = 27$, $|Syl_5G| = 5^3 = 125$.

The following less general version of Theorem 10.4 was first proved by Cauchy.

Corollary 10.2 Cauchy's Theorem

Let *G* be a finite group and *p* a prime that divides the order of *G*. Then *G* has an element of order *p*.

Therefore, we can conclude that the converse of Lagrange Theorem is true for two cases, that is for finite Abelian groups and groups with prime number order.

Definition 10.3 (Conjugate Subgroups)

If H and K are both subgroups of a finite group G, then we say H is a conjugate of K if there exists an element x of G such that $H = x^{-1}Kx$.

Theorem 10.6 Second Sylow Theorem

Let P_1 and P_2 be Sylow p-subgroups of G. Then P_1 and P_2 are conjugate subgroups of G.

Example 10.6

Let $G = S_3 = \{(1),(12),(13),(23),(123),(132)\}$. Since $|G| = |S_3| = 2 \cdot 3$, then we have $|Syl_2G| = 2$ and $|Syl_3G| = 3$.

P_1 P_2 P_3

$|Syl_2G| = 2 \Rightarrow Syl_2G$ are $\{(1),(12)\},\{(1),(13)\},$ and $\{(1),(23)\}$.

$|Syl_3G| = 3 \Rightarrow Syl_3G$ is $\{(1),(123),(132)\}$.

We know P_i and P_j are conjugates if $\exists x \in G \ni xP_ix^{-1} = P_j$. We have

$$(23)P_1(23)^{-1} = \{(23)(1)(32),(23)(12)(32)\}$$
$$= \{(1),(13)\}$$
$$= P_2.$$

Theorem 10.7 Third Sylow Theorem

If G is finite and p divides $|G|$, then the number of Sylow p-subgroups of G is one modulo p and divides the order of G.

We will use the notation $n\left(Syl_p G\right)$ for the number of Sylow p-subgroups of G.

Recall from before the following definition.

Definition 10.4 (A Simple Group)

A simple group is a group with no proper normal subgroup.

A very important consequence of Theorem 10.6 is that the condition $n\left(Syl_p G\right)=1$ is equivalent to saying that the Sylow p-subgroup of G is a normal subgroup.

Corollary 10.3 A Unique Sylow p-Subgroup Is Normal

A Sylow p-subgroup of a finite group G is normal subgroup of G if and only if it is the only Sylow p-subgroup of G.

In symbols, we write:

$$n\left(Syl_p G\right)=1 \leftrightarrow Syl_p \lhd G.$$

Example 10.7

$Syl_2S_3 = \{(1),(12)\}$, $\{(1),(13)\}$ and $\{(1),(23)\}$. Using Sylow's Third Theorem,

$n(Syl_2S_3) = k$, where $k \equiv 1 \bmod 2$ and $k \mid |S_3| = 6$. Thus we have $k = 3$.

Example 10.8

Find the number of all Syl_pS_4:

Since $|S_4| = 4! = 24 = 2^3 \cdot 3$, thus we have

$$|Syl_2S_4| = 8 \text{ and } |Syl_3S_4| = 3.$$

For Syl_2S_4:

$$\left.\begin{array}{l} n(Syl_2S_4) = 1(2) \\ n(Syl_2S_4) \mid 24 \end{array}\right\} 1, \cancel{2}, 3, \cancel{4}, \cancel{6}, \cancel{8}, \cancel{12}, \cancel{24}$$

$\therefore n(Syl_2S_4) = 1$ or 3.

For Syl_3S_4:

$$\left.\begin{array}{l} n(Syl_3S_4) = 1(3) \\ n(Syl_3S_4) \mid 24 \end{array}\right\} 1, \cancel{2}, \cancel{3}, 4, \cancel{6}, \cancel{8}, \cancel{12}, \cancel{24}$$

$\therefore n(Syl_3S_4) = 1$ or 4.

There are actually three Syl_2S_4, namely $\langle(1234),(12)(34)\rangle$, $\langle(1243),(12)(43)\rangle$, $\langle(1324),(13)(24)\rangle$ and four Sylow-3 subgroups of S_4, namely $\langle(123)\rangle,\langle(124)\rangle,\langle(134)\rangle,\langle(234)\rangle$.

10.4 Applications of Sylow Theorems

In this section, we give two examples on how Sylow Theorems can be applied to solve certain problem.

Example 10.9

Given a group with order 40. Decide whether the group is simple.

***Solution*:**

Let G be the group and $|G| = 40$. We can write $|G| = 40 = 2^3 \cdot 5$. Thus $|Syl_2G| = 8$ and $|Syl_5G| = 5$. Since $n(Syl_5G) \mid 40$ and $n(Syl_5G) \equiv 1 \mod 5$, this gives $n(Syl_5G) = 1$.

Let $K = Syl_5G$. Thus G has only a subgroup of order 5 and it is normal $(\text{i.e } K \lhd G)$. Therefore, G is not simple.

However, the Sylow-2 subgroup of G is not necessarily normal. There are 2 cases to consider:

Case I: $n(Syl_2G)=1.$

Let $H=Syl_2G$. Then $H \lhd G$ in this case.

Case II: $n(Syl_2G)=5.$

Then $H \not\lhd G$ in this case.

Example 10.10

Let G be a group with order 99. Show that G has a normal subgroup of order 9 and 11, respectively.

***Solution*:**

Let H be Syl_3G and K be $Syl_{11}G$. Since $|G|=99=3^2\cdot 11$, then $|H|=9,\ |K|=11.$

Furthermore,

$$n(H)\,|\,99 \text{ and } n(H)\equiv 1(3),$$

which gives $n(H)=1$. Therefore $H \lhd G$.

We conclude that a group of order 99 has a normal subgroup of order 9.

Similarly,

$$n(K)\,|\,99 \text{ and } n(K)\equiv 1(11),$$

gives $n(K)=1$. Thus, $K \lhd G$.

We conclude that a group of order 99 also has a normal subgroup of order 11.

Exercises 10: (The Sylow Theorems)

In Exercises 1 through 2, fill in the blanks.

1. A Sylow 3-subgroup of a group of order 54 has order _____.
2. Using the Third Sylow Theorem, we can show that the group of order 255 = (3)(5)(17) must have either ____ or ____ Sylow 3-subgroups and ____ or ____ Sylow 5-subgroups.
3. Find two Sylow 2-subgroups of S_4 and show that they are conjugate.
4. Find the conjugacy class of each element of D_3.
5. Let *H* be a subgroup of a group *G*. Show that $G_H = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of *G*.
6. Show that every group of order 45 has a normal subgroup of order 9.
7. Show that there are no simple groups of order 255 = (3)(5)(17).
8. Calculate all conjugacy classes for the quaternions.
9. Describe the conjugacy classes of an Abelian group.
10. Find all the Sylow 3-subgroups of A_4.
11. Show that every group of order 56 has a proper nontrivial normal subgroup.
12. How many Sylow 5-subgroups of S_5 are there? Exhibit two.
13. Prove that a group of order 595 has a normal Sylow 17-subgroup.

CHAPTER 11

RINGS AND INTEGRAL DOMAINS

11.1 Rings

A ring is an algebraic structure consisting of a set together with two binary operations (usually called addition and multiplication) where each operation combines two elements to form a third element. To qualify as a ring, the set together with its two operations must satisfy certain conditions — namely, the set must be an abelian group under addition and a monoid under multiplication such that multiplication distributes over addition.

The concept of a ring first arose from attempts to prove Fermat's last theorem, starting with Richard Dedekind in the 1880s. After contributions from other fields, mainly number theory, the ring notion was generalized and firmly established during the 1920s by Emmy Noether and Wolfgang Krull.

We define a ring formally as follows:

Definition 11.1 (Ring)

A ring $<R,+,\cdot>$ is a set R together with two binary operations + and $\cdot$, defined on R such that

1. $<R,+>$ **is an Abelian group.**
2. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ for $a,b,c\in R$.
3. $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ and $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ for $a,b,c\in R$.

Example 11.1 Some examples of a ring

1. $<\mathbb{Z},+,\cdot>$, $<\mathbb{Q},+,\cdot>$, $<\mathbb{R},+,\cdot>$ and $<\mathbb{C},+,\cdot>$.
2. $<M_2(\mathbb{R}),+,\cdot>$ and $<M_n(\mathbb{Z}),+,\cdot>$.
3. $<F,+,\cdot>$ where F is a set of all continuous function.
4. $<n\mathbb{Z},+,\cdot>$.
5. $<\mathbb{Z}_n,+,\cdot>$.

11.2 Types of Rings

Definition 11.2 (Commutative Ring)

A ring $<R,+,\cdot>$ is called a commutative ring if $a\cdot b=b\cdot a$ $\forall\, a,b\in R$.

Example 11.2

The rings $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{Z}_n$ and $R[x]$ are all commutative rings.

Definition 11.3 (Ring with Unity)

Identity under multiplication of a ring R is called a unity denoted by I. A ring with unity is **a ring with multiplicative identity**.

Example 11.3

The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ and $R[x]$ are rings with unity(identity), while the ring $\left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \right\}$ is not a ring with unity.

Definition 11.4 (Unit, Division Ring & Field)

Let R be a ring with unity $I \neq 0$. An element $r \in R$ is a unit if it has a multiplicative inverse in R. If every non zero element is a unit, then R is called a division ring. A field is a commutative division ring.

Note:

An element $r \in R$ is a unit if exist $r^{-1} \in R$ such that $r \cdot r^{-1} = r^{-1} \cdot r = I \in R$ and r^{-1} is called the multiplicative inverse of r.

***Note*:**

A ring R is a division ring if and only if $(R \setminus \{0\}, \cdot)$ is a group. Therefore if R is a division ring, then for all $a \in R$, $a \neq 0$ there exists a unique element denoted by $a^{-1} \in R$ such that

$aa^{-1} = 1 = a^{-1}a$. We call the element a^{-1} the multiplicative inverse of a.

Similarly, a ring R is a field if and only if $(R \setminus \{0\}, \cdot)$ is a commutative group.

Example 11.4

1. Units in $\mathbb{Z}_{14}$ are $1,3,5,9,11,13$. These are also elements in $U(14)$.

2. $\mathbb{Z}$ is not a field.

3. $\mathbb{Q}$ and $\mathbb{R}$ are fields.

11.3 Integral Domains

Definition 11.5 (Zero Divisor)

A non-zero element a in a ring R is called a zero divisor, if there exist $b \in R$ such that $b \neq 0$ and either $ab = 0$ or $ba = 0$. We do not call 0 a zero divisor.

or

Definition 11.6 (Divisors of 0)

If a and b are non-zero elements such that $a \cdot b = 0$, then we called a and b as divisors of 0.

Definition 11.7 (Integral Domain)

A commutative ring with unity $1 \neq 0$ and containing no divisors of 0 is called an integral domain.

or

Definition 11.8 (Integral Domain)

A commutative ring R with identity is called an integral domain if R has no zero divisors.

Example 11.5

1. $\mathbb{Z}_p$, p prime, is an integral domain.
2. $\mathbb{Z}_n$ is not an integral domain.

Example 11.6

Decide whether $M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z}_2 \right\}$ is an integral domain or not.

Theorem 11.1 Every finite integral domain is a field.

Corollary 11.1

Let R be a ring with 1. Then $R \neq \{0\}$ if and only if $0 \neq 1$.

Proof Suppose $R \neq \{0\}$ and $0 \neq a \in R$, consider,

$$\begin{aligned} & 1 = 0 \\ \Rightarrow\ & a \cdot 1 = a \cdot 0 \\ \Rightarrow\ & a = 0 \end{aligned}$$

a contradiction, thus $0 \neq 1$.
Conversely; Let $0 \neq 1$ i.e. 0 and 1 are distinct elements of a ring R. And hence $R \neq \{0\}$. □

Theorem 11.2

Let R be a ring with 1 (identity) and T the set of all units of R. Then,
(i) $T \neq \phi$ (ii) $0 \notin T$ (iii) $ab \in T$ for all $a, b \in T$.

Proof

(i). Since $1 \cdot 1 = 1 = 1 \cdot 1$, implies $1 \in T$ and hence $T \neq \phi$.

(ii). Let us suppose on contrary that $0 \in T$, then there exists $v \in R$ such that $0v = 1 = v0$. However $0v = 0$, implies $0 = 1$, a contradiction. Hence $0 \notin T$.

(iii). $a, b \in T$ then there exists $c, d \in R$ such that $ac = 1 = ca$ and $bd = 1 = db$. Consider, $(ab)(dc) = a(bd)c = a \cdot 1 \cdot c = ac = 1$ and $(dc)(ab) = d(ca)b = d \cdot 1 \cdot b = db = 1$. This shows that $ab \in T$ for all $a, b \in T$. □

Theorem 11.3

Let R be a ring with 1 (identity) and $u \in R$ is a unit in R. Then show that u is non-zero divisor in R.

Proof Let $r \in R$ such that $r \cdot u = 0$, but it is given that u is a unit in R, implies u^{-1} exists, therefore,

$$\begin{aligned} r \cdot u = 0 &\Rightarrow (r \cdot u)u^{-1} = 0u^{-1} = 0 \\ &\Rightarrow r(uu^{-1}) = 0 \\ &\Rightarrow r(1) = 0 \\ &\Rightarrow r = 0 \end{aligned}$$

Also,

$$\begin{aligned} ur = 0 &\Rightarrow u^{-1}(ur) = u^{-1}0 = 0 \\ &\Rightarrow (u^{-1}u)r = 0 \\ &\Rightarrow 1 \cdot r = 0 \\ &\Rightarrow r = 0 \end{aligned}$$

This implies u is not a zero divisor in R. □

Theorem 11.4

If a ring R has no zero divisors, then $ab = ac$ implies $b = c$ (Left cancellation Law)for all $a,b,c \in R$, with $a \neq 0$ and $ba = ca$ implies $b = c$ (Right cancellation Law). If either cancellation law holds then R has no zero divisors.

Proof Suppose R has no zero divisors. Let $a,b,c \in R$ with $a \neq 0$ such that $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$. Since R has no zero divisors and $a \neq 0$, then $(b-c) = 0$ or $b = c$. Hence the left cancellation law holds. Similarly, the right cancellation law holds.

Conversely; Suppose one of the cancellation law holds, say, the left cancellation law holds that is for all $a,b,c \in R$, with $a \neq 0$, $ab = ac$ implies $b = c$.
Consider,

$$ab = 0 \Rightarrow ab = a \cdot 0$$
$$\Rightarrow b = 0 \text{ (by canceling } a\text{)}$$

Again consider,

$$ba = 0 \text{ and } b \neq 0$$
$$\Rightarrow ba = b \cdot 0$$
$$\Rightarrow a = 0 \text{ (by canceling } b\text{)}$$

a contradiction. Therefore $b = 0$. Hence R has no zero divisors. □

Theorem 11.5

A finite commutative ring R with more than one element and without zero divisor is a field.

Proof Let $a_1, a_2, a_3, ..., a_n$ be distinct elements of R. Let $0 \neq a \in R$ then $aa_i \in R$ for all $i = 1, 2, 3, ..., n$ and hence the set $\{aa_1, aa_2, aa_3, ..., aa_n\} \subset R$. If $aa_i = aa_j$, then $a_i = a_j$ (by cancellation law) therefore the elements $aa_1, aa_2, aa_3, ..., aa_n$ must be distinct and hence $R = \{aa_1, aa_2, aa_3, ..., aa_n\}$. Since $a \in R$, therefore $a = aa_i$ (say). Similarly if $b \in R$ then there

exists $a_j \in R$ such that $b = aa_j$. But it is given that R is commutative, so we can write

$$\begin{aligned} ba_i &= a_i b \\ &= a_i(aa_j) \text{ (putting for } b) \\ &= (a_i a)a_j \\ &= (aa_i)a_j \ (R \text{ being commutative}) \\ &= (a)a_j \\ &= b \end{aligned}$$

From this we see that $ba_i = b$.

This implies a_i is the identity of R and we denote the identity of R by 1. From the above we conclude that $1 \in R = \{aa_1, aa_2, aa_3, ..., aa_n\}$ implies $1 = aa_j$ for some j, hence $aa_j = 1 = a_j a$. Implies every non-zero element of R is a unit. And hence R is a commutative division ring with 1 consequently R is a field. □

Theorem 11.6

If R is a commutative ring with 1. Then R is an integral domain if and only if $ab = ac \Rightarrow b = c$, where $a, b, c \in R$ with $a \neq 0$.

Proof Let R be an integral domain, $a, b, c \in R$ with $a \neq 0$ and consider $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0.$ Since $a \neq 0$ and R is an integral domain, therefore R has no zero divisor. Hence $a(b-c) = 0$ implies $(b-c) = 0$ consequently $b = c$.

Conversely; Let $ab = ac \Rightarrow b = c$ for all $a, b, c \in R$ with $a \neq 0$. Consider R is not an integral domain, then R has some zero divisor. Let a be a zero divisor of R. Let $0 \neq b \in R$ such that $ab = 0$ implies $ab = a0$ implies $b = 0$ (by hypothesis) a contradiction as $b \neq 0$. Hence, R is an integral domain. □

Theorem 11.7

A division ring has no zero divisor.

Proof Let R be division ring and $0 \neq a \in R$, then a must be a unit that is a^{-1} exists. Consider

$$\begin{aligned} & ab = 0 \text{ for some } b \in R, \\ & \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0 = 0, \\ & \Rightarrow (a^{-1}a)b = 0, \\ & \Rightarrow b = 0. \end{aligned}$$

11.4 Characteristic of a Ring

If $\exists n \in \mathbb{Z}^+$ such that $n \cdot a = 0 \ \forall a \in R$ then the least n is called a **characteristic of a ring *R***. If not, the characteristic is 0. We denote the characteristic of a ring R as char(R).

Example 11.7

1. Let $R = \mathbb{Z}_n$. Then char(R) = n.

2. Let $R = \mathbb{Z}$. Then char(R) = 0.

3. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have characteristic zero. The ring $\mathbb{Z}_n$ ($n = 1,2,3,...$) has characteristic n.

Note:

In $\mathbb{Z}_6$, $3[2] = [6] = [0]$ and $2[3] = [6] = [0]$. However 6, is the smallest positive integer such that $6[a] = [0]$ for all $[a] \in \mathbb{Z}_6$. In particular, [1] has additive order 6.

Theorem 11.8

A ring R has characteristic $n > 0$ if and only if n is the smallest positive integer such that $n \cdot 1 = 0$.

Proof Let R has characteristic $n > 0$, then $na = 0$ for all $a \in R$ and hence in particular $n \cdot 1 = 0$. If $m \cdot 1 = 0$ for $0 < m < n$, then $ma = m(1 \cdot a) = (m \cdot 1)a = 0 \cdot a = 0$. However, this contradicts the minimility of n. Hence n is the smallest positive integer such that $n \cdot 1 = 0$.

Conversely; Suppose n is the smallest positive integer such that $n \cdot 1 = 0$. Then for all $a \in R$, $na = n(1 \cdot a) = (n \cdot 1)a = 0 \cdot a = 0$. By the minimility of n for 1 , n must be the characteristic of R. □

Theorem 11.9

The characteristic of an integral domain R is either zero or a prime.

Proof If there does not exist a positive integer n such that $na = 0$ for all $a \in R$, then R is of characteristic zero. Suppose there exist a positive integer n such that $na = 0$ for all $a \in R$, and let m be the smallest positive integer such that $ma = 0$ for all $a \in R$. Then $m \cdot 1 = 0$. If m is not a prime number, then there exist integers m_1, m_2 such that $m = m_1 \cdot m_2$ where $0 < m_1, m_2 < m$. Hence,

$$\begin{aligned} 0 &= m \cdot 1 \\ &= (m_1 m_2) \cdot 1 \\ &= (m_1 \cdot 1)(m_2 \cdot 1), \end{aligned}$$

$\Rightarrow (m_1 \cdot 1)(m_2 \cdot 1) = 0.$

Since R is an integral domain therefore R has no zero divisors, consequently, $(m_1 \cdot 1)(m_2 \cdot 1) = 0$ implies, $m_1 \cdot 1 = 0$ or $m_2 \cdot 1 = 0$. This contradicts the minimility of m, thus m is a prime. □

Definition 11.9 (Subrings)
Let $(R, +, \cdot)$ be a ring and S be a subset of R. Then $(S, +, \cdot)$ is called a subring of $(R, +, \cdot)$ if $(S, +)$ is a sub-group of $(R, +)$ and $xy \in S$ for all $x, y \in S$.

Examples 11.8

1. The ring E of even integers is a subring of $\mathbb{Z}$. We note that $1 \in \mathbb{Z}$ but $1 \notin E$.

2. Consider the sub-set $E_8 = \{[0],[2],[4],[6]\}$ of $\mathbb{Z}_8$. Then E_8 is a subring of $\mathbb{Z}_8$. Hence E_8 is commutative. However, E_8 has no identity and does have zero divisor, namely, [2],[4],[6].

Theorem 11.10

A non-empty subset S of a ring R is a subring of R if and only if $x-y \in S$ and $xy \in S$ for all $x, y \in S$.

Proof Let S is a subring of of a ring R. Then S is a ring and hence $x-y \in S$ and $xy \in S$ for all $x, y \in S$.

Conversely; Suppose $x-y \in S$ and $xy \in S$ for all $x, y \in S$. Since $x-y \in S$ for all $x, y \in S$ implies $(S,+)$ is a sub-group of $(R,+)$. Also by hypothesis $xy \in S$ for all $x, y \in S$. Hence $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$. □

Theorem 11.11

Let $\{S_i : i \in \Omega\}$ be a non-empty family of subrings of a ring R. Then $\underset{i\in\Omega}{\cap} S_i$ is also a subring of R.

Proof Since $0 \in S_i$ for all $i \in \Omega$, implies $0 \in \underset{i\in\Omega}{\cap} S_i$ and hence $\underset{i\in\Omega}{\cap} S_i \neq \phi$. Let $x, y \in \underset{i\in\Omega}{\cap} S_i$, implies $x, y \in S_i$ for all $i \in \Omega$.

Since each S_i is a subring of R, therefore $x-y \in S_i$, $x, y \in S_i$

for all $i \in \Omega$. Hence $x - y \in \bigcap_{i\in\Omega} S_i$ and $x, y \in \bigcap_{i\in\Omega} S_i$. Hence $\bigcap_{i\in\Omega} S_i$ is also a subring of R. □

Definition 11.10 (Left ideal)
A non-empty sub-set I of a ring R is called a *left Ideal of* R if $a-b \in I$ and $ra \in I$ for all $a,b \in I$ and $r \in R$.

Definition 11.11 (Right ideal)
A non-empty sub-set I of a ring R is called a *right Ideal of* R if $a-b \in I$ and $ar \in I$ for all $a,b \in I$ and $r \in R$.

Definition 11.12 (Ideal)
A non-empty sub-set I of a ring R is called a *(two-sided) Ideal of* R if I is both left and right ideal of R.

Note:
From the definition of a left (right) ideal, it follows that if I is a left (right) ideal of a ring R, then I is a subring of R. Also, if R is commutative ring then every left ideal is a right ideal and every right ideal is a left ideal. Thus for commutative rings every left or right ideal is an ideal.

Examples 11.9

The sub-sets $\{0\}$ and R of a ring R are (left, right) ideals of R. Theses ideals are called trivial ideals and all other (left, Right) ideals are called non-trivial ideals.

Definition 11.13 (Proper ideal)
An ideal I of a ring R is called a proper ideal if $I \neq R$.

Next, we give an example of a ring in which there exist a left ideal which is not a right ideal, a right ideal which is not a left ideal and a subring which is not a left (right) ideal.

Example 11.10 Consider the ring $M_2(\mathbb{Z})$ and let,

$$I_1 = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a,b \in \mathbb{Z} \right\},\ I_2 = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a,b \in \mathbb{Z} \right\},$$

$$I_3 = \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} : a,b,c,d \text{ are even integers} \right\},$$

$$I_4 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{Z} \right\}.$$

Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I_1$, implies $I_1 \neq \phi$. Let $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in I_1$ and $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(\mathbb{Z})$.

Then, $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in I_1$ and

$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} xa+yb & 0 \\ za+wb & 0 \end{bmatrix} \in I_1$.

This shows that I_1 is a left ideal of $M_2(\mathbb{Z})$ But

$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax & ay \\ bx & by \end{bmatrix} \notin I_1$. Hence I_1 is not a right ideal of $M_2(\mathbb{Z})$.

Similarly, I_2 is not a right ideal of $M_2(\mathbb{Z})$ but is a left ideal. I_3 is an ideal of $M_2(\mathbb{Z})$. And I_4 is a subring but not an ideal of $M_2(\mathbb{Z})$.

Theorem 11.12

Let $\{I_i : i \in \Omega\}$ be a non-empty collection of left (right) ideals of a ring R. Then $\underset{i\in\Omega}{\cap} I_i$ is a left (right) ideal of R.

Proof Suppose $\{I_i : i \in \Omega\}$ is a non-empty collection of left ideals of a ring R. Since $0 \in I_i$ for all $i \in \Omega$, implies $0 \in \underset{i\in\Omega}{\cap} I_i$. Hence $\underset{i\in\Omega}{\cap} I_i \neq \phi$. Let $a,b \in \underset{i\in\Omega}{\cap} I_i$,

$\Rightarrow a,b \in I_i$ for all $i \in \Omega$,

$\Rightarrow a-b \in I_i$ for all $i \in \Omega$ (because each I_i is left ideal),

$\Rightarrow a-b \in \underset{i\in\Omega}{\cap} I_i$.

Let $r \in R$, then

$ra \in I_i$ for all $i \in \Omega$ (since each I_i is a left ideal of R)

$\Rightarrow ra \in \underset{i\in\Omega}{\cap} I_i$. This shows that $\underset{i\in\Omega}{\cap} I_i$ is a left ideal of R.

Similarly if $\{I_i : i \in \Omega\}$ is a non-empty collection of right ideals of a ring R then $\underset{i\in\Omega}{\cap} I_i$ is a right ideal of R.

11.5 Quotient Ring

We now give the analogue of quotient groups for rings. Let I be an ideal of a ring R. Then since $(I,+)$ is a sub-group of $(R,+)$ and $(R,+)$ is commutative, therefore $(I,+)$ is normal in $(R,+)$. Hence, if R/I denotes the set of all cosets,

$$r+I = \{r+a : a \in I \text{ for all } r \in R\}$$

Then $(R/I,+)$ is commutative group, where addition and multiplication is defined on R/I by,

$$(r+I)+(r'+I) = (r+r')+I \text{ for all } (r+I),(r'+I) \in R/I$$

$(r+I)\cdot(r'+I)=rr'+I$ for all $(r+I),(r'+I)\in R/I$

Then $(R/I,+,\cdot)$ is a ring.

Definition 11.14 (Quotient Ring)

I is an ideal of a ring R, then the ring $(R/I,+,\cdot)$ is called the quotient ring of R by I.

Definition 11.15 (Ring Homomorphism)

Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be given rings, the a function $f : R \xrightarrow{\text{into}} R'$ is called a homomorphism of R into R' if,

$f(a+b)=f(a)+f(b)$, $f(a\cdot b)=f(a)\cdot f(b)$ for all $a,b\in R$.

Definition 11.16

A homomorphism $f : R \xrightarrow{\text{into}} R'$ of a ring R into a ring R' is called,

(i) Monomorphism if $f : R \xrightarrow{\text{into}} R'$ is one-one,

(ii) Epimorphism if $f : R \xrightarrow{\text{into}} R'$ is into R',

(iii) Isomorphism if $f : R \xrightarrow{\text{into}} R'$ is bijective.

Theorem 11.13

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring R into a ring R'. Then

(i) $f(0)=0'$, where $0'$ is the zero of R'.

(ii) $f(-a)=-f(a)$ for all $a\in R$.

Proof

(i) Let $x\in R$ and consider,

$f(x) = f(x+0)$

$= f(x) + f(0)$ (f being homomorphism),

$\Rightarrow f(x) - f(x) = f(x) + f(0) - f(x)$,

$\Rightarrow 0' = 0' + f(0)$,

$\Rightarrow 0' = f(0)$.

This is the required result.

(ii) Let $a \in R$, and consider $a + (-a) = 0$,

$\Rightarrow f(a + (-a)) = f(0)$

$\Rightarrow f(a) + f(-a) = f(0)$ (f being homomorphism)

$\Rightarrow -f(a) + f(a) + f(-a) = -f(a) + f(0)$

$\Rightarrow 0' + f(-a) = -f(a) + 0'$

$\Rightarrow f(-a) = -f(a)$. Hence proved.

Theorem 11.14

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring R into a ring R'. Then the following assertion holds.

(i) $f(R) = \{f(a) : a \in R\}$ is a subring of R'.

(ii) If R is commutative, then $f(R)$ is commutative.

Proof

(i). Let $f(a), f(b) \in f(R) \subset R'$. Consider

$f(a) - f(b) = f(a) + (-f(b))$

$= f(a) + f(-b)$

$= f(a - b) \in R$ (f being homomorphism),

$\Rightarrow f(a) - f(b) \in R$. Also

$f(a) \cdot f(b) = f(ab) \in R \Rightarrow f(a) \cdot f(b) \in R$, hence

$f(R) = \{f(a) : a \in R\}$ is a subring of R'.

(ii) Let R is commutative and $x, y \in f(R)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in R$. Consider,

$$\begin{aligned} xy &= f(a) \cdot f(b) \\ &= f(ab) \ (f \text{ being homomorphism}) \\ &= f(ba) \ (R \text{ being commutative}) \\ &= f(b) \cdot f(a) \ (f \text{ being homomorphism}) \\ &= yx. \end{aligned}$$

This implies $f(R)$ is commutative.

Theorem 11.15

Let $f : R \xrightarrow{onto} R'$ be a ring homomorphism of a ring R onto a ring R', where R has an identity. Then prove that,

(i) $f(1)$ is the identity of R'.

(ii) If $a \in R$ is a unit in R then $f(a)$ is a unit of R' and $(f(a))^{-1} = f(a^{-1})$.

Proof

(i) Since it is given that $1 \in R$ this implies $f(1) \in f(R)$ but since f is onto therefore $f(1) \in f(R) = R'$ that is $f(1) \in R'$. Let $f(a) \in R'$, where $a \in R$ and consider,

$f(1) \cdot f(a) = f(1 \cdot a)$ (f being homomorphism) $= f(a)$,

$\Rightarrow f(1) \cdot f(a) = f(a)$ for all $a \in R$.

Similarly,

$f(a) \cdot f(1) = f(a \cdot 1)$ (f being homomorphism) $= f(a)$,

$\Rightarrow f(a) \cdot f(1) = f(a)$ for all $a \in R$.

Showing that $f(1)$ is an identity of R'.

(ii) Let $a \in R$ is a unit in R therefore a^{-1} exist and $aa^{-1} = 1 = a^{-1}a$. Now consider,

$f(1) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$,
$\Rightarrow f(1) = f(a) \cdot f(a^{-1})$ similarly $f(1) = f(a^{-1}) \cdot f(a)$.
Hence $f(a)$ is a unit in R'.
Next consider,
$f(a) \cdot f(a^{-1}) = f(1)$,
$\Rightarrow (f(a))^{-1} f(a) \cdot f(a^{-1}) = (f(a))^{-1} f(1)$,
$\Rightarrow f(a^{-1}) = (f(a))^{-1}$.

Definition 11.17 (Kernel)

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring R onto a ring R'. Then the kernel of f is denoted and define as $\ker f = \{a \in R : f(a) = 0\}$.

Theorem 11.16

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring R onto a ring R', then show that $\ker f$ is an ideal of R.

Proof Since $0 \in R$ and $f(0) = 0$, implies $0 \in \ker f$ that is $\ker f \neq \phi$. Let $a, b \in \ker f$ and $r \in R$. Consider,

$$f(a-b) = f(a+(-b)) = f(a) + f(-b)$$
$$= f(a) - f(b) = 0 - 0 \text{ (since } a, b \in \ker f) = 0,$$
$\Rightarrow a - b \in \ker f$.

Also consider,
$$f(ra) = f(r) f(a)$$
$$= f(r) \cdot 0 \text{ (since } a \in \ker f) = 0,$$

$\Rightarrow ra \in \ker f$. Hence $\ker f$ is an ideal of R. □

Theorem 11.17

Let I be an ideal of a ring R, then the mapping $g : R \to R/I$ defined by $g(a) = a + I$ for all $a \in R$, is a homomorphism, called the natural homomorphism of R onto R/I. Furthermore, $\ker g = I$.

Proof Let $a, b \in R$, then

$$g(a+b) = (a+b) + I = (a+I) + (b+I)$$
$$= g(a) + g(b),$$

and

$$g(a \cdot b) = (a \cdot b) + I = (a+I) \cdot (b+I)$$
$$= g(a) \cdot g(b).$$

Hence $g : R \to R/I$ is a homomorphism.

Next as,

$$\ker g = \{a \in R : g(a) = I\} = \{a \in R : a + I = I\}$$
$$= \{a \in R : a \in I\} = R \cap I = I$$

Hence, $\ker g = I$.

11.6 Isomorphism Theorems

Theorem 11.18 (First Isomorphism Theorem)

Let f be a homomorphism of a ring R into a ring R'. Then $f(R)$ is an ideal of R' and $R/\ker f \cong f(R)$.

Proof

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring R onto a ring R'. To show that $f(R)$ is an ideal of R', we let $f(a)$, $f(b) \in f(R)$, where $a, b \in R$ and consider,

$$\begin{aligned} f(a) - f(b) &= f(a) + \big(-f(b)\big) \\ &= f(a) + f(-b) \text{ (because } -f(b) = f(-b)) \\ &= f\big(a + (-b)\big) \text{ (f being a homomorphism)} \\ &= f(a-b) \in f(R) \text{ (as } a - b \in R) \end{aligned}$$

$\Rightarrow f(a) - f(b) \in f(R)$.

Now let $r' \in R'$, then $r' = f(r)$ for some $r \in R$. Consider,

$$\begin{aligned} r' f(a) &= f(r) \cdot f(a) \\ &= f(ra) \in f(R) \text{ (f being a homomorphism and } ra \in R) \end{aligned}$$

$\Rightarrow r' f(a) \in f(R)$

Similarly,

$f(a) r' \in f(R)$

Hence $f(R)$ is an ideal of R'.

Next we suppose $\ker f = I$ and define

$h : R/I \to f(R)$ by $h(r + I) = f(r)$ for all $r + I \in R/I$

Now to show that this mapping is well defined, we consider,

$$r+I=r'+I$$
$$\Leftrightarrow -r'+r+I=-r'+r'+I$$
$$\Leftrightarrow -r'+r+I=0+I$$
$$\Leftrightarrow -r'+r+I=I$$
$$\Leftrightarrow -r'+r\in I=\ker f$$
$$\Leftrightarrow f(-r'+r)=0$$
$$\Leftrightarrow f(-r')+f(r)=0 \ (f \text{ being a homomorphism})$$
$$\Leftrightarrow -f(r')+f(r)=0 \ (\text{because } f(-b)=-f(b))$$
$$\Leftrightarrow f(r)=f(r')$$
$$\Leftrightarrow h(r+I)=h(r'+I) \ (\text{by definition of } h:\ R/I\to f(R))$$

This shows that h is well defined and one-one.

To show that h is onto, let $x\in f(R)$, then $x=f(r)$ for some $r\in R$ and hence $h(r+I)=f(r)=x$, this shows that h is onto.

Finally we have to show that h is homomorphism, to do this we consider,

$$h[(r+I)+(r'+I)]=h[(r+r')+I],$$
$$=f(r+r') \ (\text{by definition}),$$
$$=f(r)+f(r') \ (f \text{ being homomorphism}),$$
$$=h(r+I)+h(r'+I) \ (\text{by definition}),$$
$$\Rightarrow h[(r+I)+(r'+I)]=h(r+I)+h(r'+I).$$

Also consider,

$$h[(r+I)\cdot(r'+I)]=h[(r\cdot r')+I]=f(r\cdot r') \ (\text{by definition}),$$
$$=f(r)\cdot f(r') \ (f \text{ being homomorphism}),$$
$$=h(r+I)\cdot h(r'+I) \ (\text{by definition}),$$
$$\Rightarrow h[(r+I)\cdot(r'+I)]=h(r+I)\cdot h(r'+I).$$

This shows that h is homomorphism and hence $R/\ker f\cong f(R)$. $\square$

Theorem 11.19 (Second Isomorphism Theorem)

If I and J are ideals of a ring R, then $I / I \cap J \cong (I + J) / J$.

Proof Let us define a mapping $f : I \to (I + J) / J$ by $f(i) = i + J$ for all $i \in I$ and $i + j + J \in (I + J) / J$, then $j + J = J$ (since $j \in J$). Thus $i + j + J = i + J = f(i)$. This implies $(i + j + J)$ is the image of some $i \in I$ under f and hence f is onto.

Next we consider,

$$\begin{aligned} f(i_1 + i_2) &= (i_1 + i_2) + J \text{ for all } i_1, i_2 \in I, \\ &= (i_1 + J) + (i_2 + J), \\ &= f(i_1) + f(i_2). \end{aligned}$$

Also

$$\begin{aligned} f(i_1 \cdot i_2) &= (i_1 \cdot i_2) + J \text{ for all } i_1, i_2 \in I, \\ &= (i_1 + J) \cdot (i_2 + J), \\ &= f(i_1) \cdot f(i_2). \end{aligned}$$

This shows that f is homomorphism and hence by *First Isomorphism Theorem,* $I / \ker f \cong (I + J) / J$

Finally we need to show that $\ker f = I \cap J$ consider,

$$\begin{aligned} \ker f &= \{i \in I \ : \ f(i) = J\}, \\ &= \{i \in I \ : \ i + J = J\}, \\ &= \{i \in I \ : \ i \in J\}, \\ &= I \cap J. \end{aligned}$$

Consequently, $I / I \cap J \cong (I + J) / J$. □

Theorem 11.20 (Third Isomorphism Theorem)

If I and J are ideals of a ring R, such that $I \subseteq J$ then $(R/I)/(J/I) \cong R/J$.

Proof Define a mapping, $f : R/I \to R/J$ by $f(r+I) = r+J$ for all $r \in R$.

To show that f is well defined, let $r_1+I, r_2+I \in R/I$ such that $r_1+I = r_2+I$,

$$\Rightarrow -r_2+r_1+I = -r_2+r_2+I,$$
$$\Rightarrow -r_2+r_1+I = 0+I,$$
$$\Rightarrow -r_2+r_1+I = I,$$
$$\Rightarrow -r_2+r_1 \in I \subseteq J,$$
$$\Rightarrow -r_2+r_1 \in J,$$
$$\Rightarrow -r_2+r_1+J = J,$$
$$\Rightarrow r_1+J = r_2+J,$$
$$\Rightarrow f(r_1+I) = f(r_2+I).$$

This shows that f is well defined.

Next to show that f is homomorphism, let $r_1+I, r_2+I \in R/I$ and consider

$$\begin{aligned} f[(r_1+I)+(r_2+I)] &= f[(r_1+r_2)+I)], \\ &= (r_1+r_2)+J, \\ &= (r_1+J)+(r_2+J), \\ &= f(r_1+I)+f(r_2+I), \end{aligned}$$

$$\Rightarrow f\big((r_1+I)+(r_2+I)\big) = f(r_1+I)+f(r_2+I).$$

Also,

$$\begin{aligned} f[(r_1+I)\cdot(r_2+I)] &= f[(r_1\cdot r_2)+I)], \\ &= (r_1\cdot r_2)+J, \\ &= (r_1+J)\cdot(r_2+J), \\ &= f(r_1+I)\cdot f(r_2+I). \end{aligned}$$

Shows that f is homomorphism.

If $x \in R/J$, then $x = r+J$ for some $r \in R$ follows that $x = r+J = f(r+I)$. This implies f is onto. Hence by the *First Isomorphism Theorem,* $(R/I)/\ker f \cong R/J$.

Finally we need to show that $\ker f = J/I$, consider

$$\begin{aligned} \ker f &= \{x \in R/I \ : \ f(x) = J\}, \\ &= \{x = r+I \ : \ f(r+I) = J\}, \\ &= \{r+I \ : \ r+J = J\}, \\ &= \{r+I \ : \ r \in J\}, \\ &= J/I. \end{aligned}$$

Hence $(R/I)/(J/I) \cong R/J$.

Exercises 11: (Rings and Integral Domains)

1. The set $\{0, 2, 4\}$ under addition and multiplication modulo 6 has a unity. Find it.

In Exercise 2 through 4, find the characteristic of the given ring.

2. $\mathbb{Z} \oplus \mathbb{Z}$ 3. $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ 4. $\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$

5. Let *R* be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^9$ for $a, b \in R$.
6. Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.
7. Verify a through g below are as claimed.
   a. The ring of integers is an integral domain.
   b. The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is an integral domain.
   c. The ring $Z[x]$ of polynomials with integer coefficients is an integral domain.
   d. The ring $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ is an integral domain.
   e. The ring $\mathbb{Z}_p$ of integers modulo a prime *p* is an integral domain.
   f. The ring $\mathbb{Z}_n$ of integers modulo *n* is *not* an integral domain when *n* is not prime.
   g. The ring $M_2(\mathbb{Z})$ of 2×2 matrices over the integers is not an integral domain.
8. Which of a through e in Exercise 7 are fields?
9. List all zero-divisors in $\mathbb{Z}_{20}$. Can you see a relationship between the zero-divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?
10. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.
11. Prove that every field is an integral domain.
12. Prove that a ring R is commutative if and only if $(a+b)^2 = a^2 + b^2 + 2ab$ for all $a, b \in R$.
13. Give an example of a commutative ring without zero-divisors that is not an integral domain.
14. If $x^2 = x$ for all x belonging to a ring R. Then prove the following,

    (i) $2x = 0$ for all $x \in R$.
    (ii) R is commutative.

15. Is $\mathbb{Z} \oplus \mathbb{Z}$ an integral domain? Explain.
16. If R is a ring with 1 such that $(xy)^2 = x^2 y^2$ for all $x \in R$. Then R is commutative.

17. Prove that the set of matrices $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a,b,c \in R \right\}$ forms a subring of the ring $M_2(R)$.

18. Prove that the set of matrices $S = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} : a,b,c \in R \right\}$ is not a subring of the ring $M_2(R)$.

19. If I_1 and I_2 are tow left (right) ideals of a ring R. Then prove that $I_1 \cap I_2$ is also a left (right) ideal of R.

20. Prove or disprove that union of two ideals of ring R is also and ideal of R.

21. Let I be an ideal of a ring R. Then show that $(R/I, +, .)$ is also a ring under addition and multiplication defined as

$$(r+I)+(r'+I) = (r+r')+I \text{ for all } (r+I),(r'+I) \in R/I$$
$$(r+I).(r'+I) = rr'+I \text{ for all } (r+I),(r'+I) \in R/I .$$

22. Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism, then show that,

(i) $f(na) = nf(a)$ for all $a \in R$ and $n \in Z$.

(ii) $f(na) = (f(a))^n$ for all $a \in R$ and $n \in Z$.

23. Prove that the composition of two ring homomorphism is a ring homomorphism.

CHAPTER 12

GROUPS PRESENTATIONS

12.1 Introduction

A group can be formed by giving (i) a set of generators for the group and (ii) certain equations or relations that the generators satisfy. We write

$$G = < g_1, g_2, ..., g_n | r_1 = r_2 = ... = r_t = e >,$$

where g_i generators and r_j relations.

12.2 Examples of Groups Presentation

1. $C_n = < x \mid x^n = e >$, the cyclic group of order *n*.

2. $D_4 = < a, b | a^4 = b^2 = (ab)^2 = e >$, the dihedral group of order eight.

2. $\mathbb{Z}_4 \oplus \mathbb{Z}_2 = < a, b | a^4 = b^2 = e,\ ab = ba >$

3. $Q = < a, b | a^2 = b^2 = (ab)^2 >$, the quaternion group of order eight.

Note that $b^2 = (ab)^2 = abab$ implies $b = aba$

and $a^2 = b^2 = (aba)(aba) = aba^2ba = abb^2ba = ab^4a$ implies $b^4 = e.$

Exercises 12: (Groups Presentations)

1. Show that $\langle a,b \mid a^5 = b^2 = e, ba = a^2b \rangle$ is isomorphic to $\mathbb{Z}_2$.
2. In any group, show that $\langle a,b \rangle = \langle a, ab \rangle$.
3. Let $M = \frac{1}{3}\begin{bmatrix} 0 & -2 & 1 \\ 2 & 0 & -2 \\ -1 & 2 & 0 \end{bmatrix}$ and $N = \frac{1}{3}\begin{bmatrix} 1 & -2 & 0 \\ -2 & 0 & 2 \\ 0 & 2 & -1 \end{bmatrix}$. Show that the group generated by *M* and *N* is isomorphic to D_4.
4. What is the minimum number of generators needed for $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$? Find a set of generators and relations for this group.
5. Let $\langle a,b \mid a^2 = b^4 = e, ab = b^3a \rangle$.
   a. Express $a^3b^2abab^3$ in the form $b^i a^j$.
   b. Express b^3abab^3a in the form $b^i a^j$.
6. Give a presentation of $\mathbb{Z}_4$ involving
   a. one generator.
   b. two generators.
   c. three generators.
7. Give a presentation of S_3 involving three generators.
8. Gives the tables for both the octic group $\langle a,b \mid a^4 = 1, b^2 = 1, ba = a^3b \rangle$ and the quaternion group $\langle a,b \mid a^5 = b^2 = e, ba = a^2b \rangle$. In both cases, write the elements in the order 1, a, a^2, a^3, b, ab, a^2b, a^3b. (Note that we do not have to compute *every* product. We know that these presentations give groups of order 8, and once we have computed enough products, the rest are forced so that each row and each column of the table has each element exactly once.)
9. Determine all groups of order 21 up to isomorphism.
10. Show that the presentation $\langle a,b \mid a^3 = 1, b^2 = 1, ba = a^2b \rangle$ gives a group of order 6. Show that also it is nonabelian.

References

Fraleigh, J.B. (2003), *A First Course in Abstract Algebra*, 7th Edition, Reading, Massachusetts: Addision-Wesley Publishing Company, Inc.

Gallian, J.A. (2010), *Contemporary Abstract Algebra*, 7th Edition, Cengage Learning, Belmont, C.A: Brooks/ Cole.

Gilbert, J. and Gilbert, L. (2005), *Elements of Modern Algebra*, 6th Edition, Belmont, California: Thomson Brooks/ Cole.

Gilbert, W. J. and Nicholson, W.K. (2004), *Modern Algebra with Applications*, 3rd Edition, New Jersey: John Wiley & Sons.

Robinson, D.J.S. (1996*), A Course in the Theory of Groups* (*Graduate Texts in Mathematics*), 2nd Edition, Springer-Verlag.