SCHOOL OF DISTANCE EDUCATION

B. Sc. MATHEMATICS

MM5B06: ABSTRACT ALGEBRA

(Core Course)

FIFTH SEMESTER

STUDY NOTES

Prepared by:

Vinod Kumar P.
Assistant Professor
P. G.Department of Mathematics
T. M. Government College, Tirur

UNIVERSITY OF CALICUT

B.Sc. MATHEMATICS

MM5B06: ABSTRACT ALGEBRA

Study Notes

Prepared by:

Vinod Kumar P.
Assistant Professor
P. G.Department of Mathematics
T. M. Government College, Tirur
Email: vinodunical@gmail.com

Published by:

SCHOOL OF DISTANCE EDUCATION
UNIVERSITY OF CALICUT

June, 2013

The Jewel of Indian Mathematics

SRINIVASA RAMANUJAN

(December 22, 1887 to April 26, 1920)

"As are the crests on the heads of peacocks,

As are the gems on the hoods of cobras,

So is Mathematics, at the top of all sciences."

The Yajurveda, circa 600 B.C.

A Note to the Students

Mathematics is an abstract branch of human knowledge. Its language and style are precise and systematic. No one can learn this subject without capturing its language and the way of its thought processes. As Paul Halmos said, **the only way to learn Mathematics is to do Mathematics** and you cannot understand this subject by just reading some books, or by attending some lecture classes on Mathematics or just by watching someone doing it! So don't just read this notes, but try to ask your own questions, find out your own examples, and thereby try to internalize the concepts. While studying a theorem and its proof, try to convince yourself where the proof uses the hypothesis and how we arrive at the final conclusions. Each and every step of the proof requires a thorough analysis, sound reasoning, and explanations. Also, consider the following questions: Is the entire hypothesis necessary? Is there any other alternative ways to reach the conclusion? Can we connect the present result with any previous ideas? Is the converse true?... Such an analytic approach will help you for a better understanding of the concept and to enjoy the pleasure of doing Mathematics. Take special care to **do all the problems listed in these notes**, that will give you much confidence for future studies and to face the exams. Doing problems in an analytic and systematic way helps to internalize the abstract mathematical concepts more better. Always remember that **success is never an accident, it is the final out come of purposeful activities and hard work**.

Queries and suggestions are most welcome and that can be mailed to: *vinodunical@gmail.com*

C.U.Campus, Vinod Kumar. P

06 - 06- 2013.

Contents

Module-I

Module-II

Module-III

Module-IV

Chapter 1

Introduction to Groups

A **group** is one of the fundamental objects of study in the field of mathematics known as ***abstract algebra***. A group consists of a set of elements and an operation that takes any two elements of the set and forms another element of the set in such a way that certain conditions are met. The theory of groups is the subject of intense study within mathematics, and is used in many scientific fields. The branch of algebra that studies groups is called **group theory**. Group theory has extensive applications in mathematics, science, and engineering. Many algebraic structures such as fields and vector spaces may be defined concisely in terms of groups, and group theory provides an important tool for studying symmetry, since the symmetries of any object form a group. Groups are thus essential abstractions in branches of physics involving symmetry principles, such as relativity, quantum mechanics, and particle physics. Furthermore, their ability to represent geometric transformations finds applications in chemistry, computer graphics, and other fields.

As we noted above, group is an algebraic structure consisting of a set together with an operation that combines any two of its elements to form a third element.

To qualify as a group, the set and the operation must satisfy four conditions called the group axioms, namely closure, associativity, identity and invertibility. Many familiar mathematical structures such as number systems obey these axioms: for example, the integers endowed with the addition operation form a group. However, the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics. The concept of a group arose from the study of polynomial equations, starting with *Évariste Galois* in the 1830's. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870.

Many structures investigated in mathematics turn out to be groups. These include familiar number systems, such as the integers, the rational numbers, the real numbers, and the complex numbers under addition, as well as the non-zero rationals, reals, and complex numbers under multiplication. Other important examples are groups of non-singular matrices (with specified size and type of entries) under matrix multiplication, and permutation groups, which consist of invertible functions from a set to itself with composition as group operation. Group theory allows for the properties of such structures to be investigated in a general setting.

In what follows, we will discuss in detail the concept of groups with several illustrating examples. We begin with the definition of binary operations. Recall that a ***relation*** between the sets X and Y is any subset R of $X \times Y$. Also, a

function or ***mapping***, ϕ from X to Y is a relation between X and Y such that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ. If $\phi : X \to Y$ is a mapping, X is the ***domain*** of ϕ, Y is the ***codomain*** of ϕ, and the set $\{\phi(x) \mid x \in X\}$, denoted as $\phi[X]$, is the ***range*** of ϕ.
A function $\phi : X \to Y$ is ***one to one*** if $\phi(x_1) = \phi(x_2)$ only when $x_1 = x_2$. The function ϕ is ***onto*** Y if the range of ϕ is Y.

Notations.

$\mathbb{Z}^+, \mathbb{Q}^+$, and $\mathbb{R}^+$ denotes the sets of positive integers, positive rational numbers, and positive real numbers respectively. Also, $\mathbb{Q}^*, \mathbb{R}^*$, and $\mathbb{C}^*$ denotes the sets of non zero rational numbers, non zero real numbers, and non zero complex numbers respectively.

1.1 Binary Algebraic Structures

If m and n are any given integers, we know that the operations addition and multiplication gives us unique integers $m + n$ and mn respectively. In other words, addition and multiplication are mappings from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}$. Such mappings are called *binary operations*. More precisely, we have the following definition.

Definition 1.1.1.

A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. Thus, for each $(a, b) \in S \times S$, $*$ assigns a unique element of S, denoted as $a * b$.

We have observed that addition and multiplication are binary operations on $\mathbb{Z}$. It is clear that these operations defines binary operations on the sets $\mathbb{C}, \mathbb{R}, \mathbb{R}^+$, and $\mathbb{Z}^+$. Let $\mathbb{R}^*$ denotes the set of non zero real numbers. Then

addition is *not* a binary operation on $\mathbb{R}^*$ (Why?), where as multiplication defines a binary operation on $\mathbb{R}^*$ (Why?). Is *division* a binary operation on $\mathbb{Z}$? No, because the quotient of two integers need not be an integer always. Moreover, $\frac{a}{b}$ is not defined if $b = 0$. It may be noted that *a binary operation on a set S to be defined for every ordered pair (a, b) of elements of S.*

For an operation $*$ to be a binary operation on S, we require that (i) exactly one element is assigned to each possible pair of elements of S, and (ii) for each ordered pair of elements of S, the element assigned to it is again in S.

Definition 1.1.2.

Let $*$ be a binary operation on S and let H be a subset of S. The H is ***closed under*** $*$ if $a * b \in H$, for all $a, b \in H$. In this case, $*$ induces a binary operation on H.

For example, addition defines a binary operation on the subset of integers $\mathbb{Z}$ of $\mathbb{R}$. Consider $\mathbb{Z}$ with the binary operation subtraction. Clearly, the subset $\mathbb{Z}^+$ of positive integers is not closed under subtraction. As another example, consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, with the binary operation addition modulo 6. Clearly the subsets $\{0, 3\}$, and $\{0, 2, 4\}$ are closed under addition modulo 6. Is there any other subsets of $\mathbb{Z}_6$ which are closed under addition modulo 6?

Problem 1.

Let $H = \{n^2 \mid n \in \mathbb{Z}^+\} \subset \mathbb{Z}$. Show that H is closed under multiplication. Is H closed under addition?

Solution.

Let $x, y \in H$. Then $x = n_1^2, y = n_2^2$ for some $n_1, n_2 \in \mathbb{Z}^+$. Therefore, $xy = n_1^2.n_2^2 = (n_1.n_2)^2 \implies xy \in H$. Hence H is closed under multiplication,but H is not closed under addition. For instance, $1 = 1^2 \in H, 4 = 2^2 \in H$, but $1 + 4 = 5 \notin H$. ■

Definition 1.1.3.

A binary operation on $*$ on a set S is ***commutative*** if $a * b = b * a$ for all $a, b \in S$.

For example, addition and multiplication are commutative binary operations on $\mathbb{Z}$, whereas subtraction is a binary operation on $\mathbb{Z}$ which is not commutative. On the set $M_n(\mathbb{R})$ of all $n \times n$ matrices with entries from $\mathbb{R}$, matrix addition is a commutative binary operation, but matrix multiplication is not commutative.

Definition 1.1.4.

A binary operation on $*$ on a set S is ***associative*** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

Clearly, addition and multiplication are associative binary operations in $\mathbb{Z}$, but subtraction is not associative. Also, matrix addition and matrix multiplication are associative binary operations in $M_n(\mathbb{R})$.

Example 1.

Let S be any non empty set and let $\mathcal{P}(S)$ be its power set. It can be easily checked out that the operations intersection, union, and symmetric difference of sets are binary operations on $\mathcal{P}(S)$. Are they commutative? associative?

Problem 2.

Let F be the set of all functions from a set S into S. Show that composition of functions is an associative binary operation on F. Give an example to show that composition of functions need not be commutative.

Solution.

Let $f, g, h \in F$. Note that $f \circ g$ is defined as $(f \circ g)(x) = f(g(x)), \forall x \in S \implies (f \circ g) \in F$. We have, $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))), \forall x \in S$ and $(f \circ (g \circ h))(x) = (f(g \circ h)(x)) = f(g(h(x))), \forall x \in S$. Thus $((f \circ g) \circ h) = (f \circ (g \circ h)) \implies$ Composition of functions is an associative binary operation in F. Let $f, g : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = sin\ x$ and $g(x) = 2x$. Then $(f \circ g)(x) = f(2x) = Sin(2x)$ and $(g \circ f)(x) = g(sin\ x) = 2\ sin\ x \implies f \circ g \neq g \circ f$. Thus, composition of functions need not be commutative. ■

On a finite set, any given binary operation can be represented by means of a table in which the elements of the set are listed across the top as heads of columns and at the left side as heads of rows. Note that the elements are listed on both sides in the same order.
For example, consider the table

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

which defines a binary operation on the set $\{a, b, c\}$. The following table represents the binary operation addition modulo 5 on $\mathbb{Z}_5$.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

A binary operation defined by table is commutative if and only if the entries in the table are symmetric with respect to the diagonal that starts with the upper left corner of the table and ends at the lower right corner.

The associativity of a binary operation from its table, just by inspection will not be obvious.

Definition 1.1.5.

A **binary algebraic structure** $\langle S, * \rangle$ consists of a set S together with a binary operation $*$ on a set S.

Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be two binary algebraic structures. An **isomorphism** of S with S' is a *one to one* function ϕ mapping S *onto* S' such that $\phi(x * y) = \phi(x) *' \phi(y)$, for all $x, y \in S$.

The property that $\phi(x * y) = \phi(x) *' \phi(y)$, for all $x, y \in S$ is called **homomorphism property**.

If such a mapping ϕ exists, then S and S' are **isomorphic** binary algebraic structures, and we denote this as $S \simeq S'$.

A **structural property** of a binary algebraic structure is one that must be

shared any isomorphic structure.

For instance, the number of elements in the set S is a structural property of the binary algebraic structure $\langle S, * \rangle$, where as the name of the binary operation (or of the elements) is not a structural property.

Remark.

If $\phi : \langle S, * \rangle \to \langle S', *' \rangle$ is an isomorphism, then $\phi^{-1} : S' \to S$ exists and ϕ^{-1} is an isomorphism of $\langle S', *' \rangle$ onto $\langle S, * \rangle$.

Example 2.

Consider the binary algebraic structures $\langle \mathbb{R}, + \rangle$ with usual addition, and $\langle \mathbb{R}^+, . \rangle$ with usual multiplication. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ by $\phi(x) = e^x$. If $\phi(x) = \phi(y)$, then $e^x = e^y$. Taking natural logarithm on both sides we get $x = y$, showing that ϕ is one to one. To see that ϕ is onto, let $r \in \mathbb{R}^+$, then $lnr \in \mathbb{R}$ and $\phi(lnr) = e^{lnr} = r$. Finally, for $x, y \in \mathbb{R}$, we have $\phi(x + y) = e^{x+y} = e^x.e^y = \phi(x).\phi(y)$. Thus ϕ is indeed an isomorphism.

Example 3.

The binary structures $\langle \mathbb{C}, . \rangle$ and $\langle \mathbb{R}, . \rangle$ under usual multiplication are not isomorphic, since the equation $x.x = c$ has a solution in $\mathbb{C}$ for every $c \in \mathbb{C}$, but $x.x = -1$ has no solution in $\mathbb{R}$. The binary structure $\langle M_2(\mathbb{R}), . \rangle$ of 2×2 matrices of real numbers is not isomorphic to $\langle \mathbb{R}, . \rangle$, since multiplication of real numbers is commutative, but matrix multiplication is not commutative.

Problem 3.

Show that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under usual addition are not isomorphic.

Solution.

Note that the equation $x+x=c$ has a solution in $\mathbb{Q}$ for every $c \in \mathbb{Q}$, but this equation may not have solution in $\mathbb{Z}$ for every $c \in \mathbb{Z}$. For example, $x+x=3$ does not have a solution in $\mathbb{Z}$. This shows that these two binary structures are not isomorphic. ■

Definition 1.1.6.

Let $\langle S, * \rangle$ be a binary structure. An element $e \in S$ is an **identity element** for $*$ if $e * s = s * e = s, \forall s \in S$.

Remark.

A binary structure $\langle S, * \rangle$ has at most one identity element. i.e., if the identity element exists, it is unique.

To see this, let e and $\bar{e}$ be identity elements. Then by regarding $\bar{e}$ as identity element, we have $e * \bar{e} = e$. But by regarding e as the identity element, we get $e * \bar{e} = \bar{e}$. This shows that $e = \bar{e}$.

Example 4.

On $\mathbb{Z}$, define the binary operation $*$ as $a * b = max\{a, b\}$. Does this operation has an identity element in $\mathbb{Z}$? If e is the identity element, then $a * e = e * a = a, \forall a \in \mathbb{Z} \implies max\{a, e\} = a, \forall a \in \mathbb{Z} \implies e \leq a, \forall a \in \mathbb{Z}$. Since $\mathbb{Z}$ has no smallest element, such an e does not exists.
If we consider the above operation on the set $\mathbb{N}$, 1 is the identity element for $*$.

Problem 4.

On $\mathbb{Z} \times \mathbb{Z}$, define the binary operation $\circ$ by $(a, b) \circ (c, d) = (ac, bc + d)$.
Is $\circ$ commutative? associative? Find the identity element.

Solution.

We have $(1,2) \circ (3,4) = (3,10)$, and $(3,4) \circ (1,2) = (3,6)$. This shows that $\circ$ is not commutative. It is an easy exercise to verify that $((a,b) \circ (c,d)) \circ (e,f) = (a,b) \circ ((c,d) \circ (e,f))$. Let $e = (x,y)$ be the identity element for $\circ$. Then $(a,b) \circ (x,y) = (x,y) \circ (a,b) = (a,b) \implies (ax, bx+y) = (xa, ya+b) \implies ax = xa = a$ and $bx + y = ya + b = b \implies (x,y) = (1,0)$. Thus $(1,0)$ is the identity element for the binary operation $\circ$. ■

Theorem 1.1.7.

Suppose $\langle S, * \rangle$ has an identity element e for $*$. If $\phi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\phi(e)$ is an identity element for the binary operation $*'$ on S'.

Proof.

Let $s' \in S'$. We have to prove that $\phi(e) * s' = s' *' \phi(e) = s'$. Since ϕ is onto, there exists $s \in S$ such that $\phi(s) = s'$. Since e is the identity element for $*$, we have $s * e = e * s = s$. Since ϕ is a function, $\phi(s * e) = \phi(e * s) = \phi(e)$. Using homomorphism property, we get $\phi(s) *' \phi(e) = \phi(e) *' \phi(s) = \phi(e)$, which implies $\phi(e) *' s' = s' *' \phi(e) = s'$. Thus, $\phi(e)$ is an identity element for the binary operation $*'$ on S'. □

Problem 5.

The map $\phi : \mathbb{Z} \to \mathbb{Z}$, defined by $\phi(n) = n+1$ for $n \in \mathbb{Z}$ is one to one and onto $\mathbb{Z}$. Give the definition of a binary operation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphism mapping

(a) $\langle \mathbb{Z}, + \rangle$ onto $\langle \mathbb{Z}, * \rangle$,

(b) $\langle \mathbb{Z}, * \rangle$ onto $\langle \mathbb{Z}, + \rangle$,

(c) $\langle \mathbb{Z}, . \rangle$ onto $\langle \mathbb{Z}, * \rangle$,

(d) $\langle \mathbb{Z}, * \rangle$ onto $\langle \mathbb{Z}, . \rangle$.

In each case, find the identity element for $*$ on $\mathbb{Z}$.

Solution.

(a) For ϕ to be an isomorphism, we must have $m * n = \phi(m-1) * \phi(n-1) = \phi((m-1)+(n-1)) = \phi(m+n-2) = m+n-1$. The identity element is $\phi(0) = 1$.

(b) Using the fact that ϕ^{-1} must also be an isomorphism, we must have $m*n = \phi^{-1}(m+1) * \phi^{-1}(n+1) = \phi^{-1}((m+1)+(n+1)) = \phi^{-1}(m+n+2) = m+n+1$. The identity element is $\phi^{-1}(0) = -1$.

(c) For ϕ to be an isomorphism, we must have $m * n = \phi(m-1) * \phi(n-1) = \phi((m-1).(n-1)) = \phi(mn-m-n+1) = mn-m-n+2$. The identity element is $\phi(1) = 2$.

(d) Using the fact that ϕ^{-1} must also be an isomorphism, we must have $m*n = \phi^{-1}(m+1)*\phi^{-1}(n+1) = \phi^{-1}((m+1).(n+1)) = \phi^{-1}(mn+m+n+1) = mn+m+n$. The identity element is $\phi^{-1}(1) = 0$. ■

Exercises.

1. Determine whether the definition of $*$ give a binary operation on the given set. If so, check whether $*$ is (i) commutative (ii)associative? Also, examine $*$ for identity element.

   (a) On $\mathbb{Q}$, $a * b = ab + 1$.

   (b) On $\mathbb{Q}$, $a * b = \frac{ab}{2}$.

   (c) On $\mathbb{Z}^+$, $a * b = 2^{ab}$.

   (d) On $\mathbb{Z}^+$, $a * b = a^b$.

   (e) On $\mathbb{Z}^+$, $a * b = a - b$.

   (f) On $\mathbb{Z}$, $a * b = max\{a, b\}$.

(g) On $\mathbb{Z}$, $a * b = a + b - ab$.

(h) On $\mathbb{Z}^+$, $a * b = c$, where c is at least 5 more than $a + b$.

(i) On $\mathbb{Z}^+$, $a * b = c$, where c is the smallest integer greater than both a and b.

(j) On $\mathbb{Z}^+$, $a * b = c$, where c is the greatest integer less than ab.

(k) On M_nR, the set of $n \times n$ matrices with real entries under matrix addition.

(l) On M_nR, the set of $n \times n$ matrices with real entries under matrix multiplication.

2. Find the table representing the binary operation $A * B = A \cup B$ on the power set of the set $\{a, b\}$.

3. How many binary operations can be defined on a set S with exactly n elements? How many of them are commutative?

4. Show that every binary operation on a singleton set is both commutative and associative.

5. Show that every binary operation on a set having just two elements is associative.

6. Determine whether the given map is an isomorphism from the first binary structure to the second. Justify your answer. [For problems, (f) to (j), $\mathcal{F}$ stands for the set of all functions mapping $\mathbb{R}$ to $\mathbb{R}$ that have derivatives of all orders.]

(a) $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$, where $\phi(n) = -n$.

(b) $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$, where $\phi(n) = n + 1$.

(c) $\langle \mathbb{Q}, . \rangle$ with $\langle \mathbb{Q}, . \rangle$, where $\phi(x) = x^2$.

(d) $\langle \mathbb{Q}, . \rangle$ with $\langle \mathbb{Q}, . \rangle$, where $\phi(x) = x^3$.

(e) $\langle M_2(\mathbb{R}), . \rangle$ with $\langle \mathbb{R}, . \rangle$, where $\phi(A) =$ Determinant of A.

(f) $\langle \mathcal{F}, + \rangle$ with $\langle \mathcal{F}, + \rangle$, where $\phi(f) = f'$.

(g) $\langle \mathcal{F}, + \rangle$ with $\langle \mathcal{F}, + \rangle$, where $\phi(f)(x) = \int_0^x f(t)dt$.

(h) $\langle \mathcal{F}, + \rangle$ with $\langle \mathcal{F}, + \rangle$, where $\phi(f)(x) = \frac{d}{dx}[\int_0^x f(t)dt]$.

(i) $\langle \mathcal{F}, . \rangle$ with $\langle \mathcal{F}, . \rangle$, where $\phi(f)(x) = x.f(x)$.

(j) $\langle \mathcal{F}, + \rangle$ with $\langle \mathbb{R}, + \rangle$, where $\phi(f) = f'(0)$.

7. The map $\phi : \mathbb{Q} \to \mathbb{Q}$, defined by $\phi(x) = 3x - 1$ for $x \in \mathbb{Q}$ is one to one and onto $\mathbb{Q}$. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphism mapping

(a) $\langle \mathbb{Q}, + \rangle$ onto $\langle \mathbb{Q}, * \rangle$, **(b)** $\langle \mathbb{Q}, * \rangle$ onto $\langle \mathbb{Q}, + \rangle$,

(c) $\langle \mathbb{Q}, . \rangle$ onto $\langle \mathbb{Q}, * \rangle$, **(d)** $\langle \mathbb{Q}, * \rangle$ onto $\langle \mathbb{Q}, . \rangle$.

In each case, find the identity element for $*$ on $\mathbb{Q}$.

1.2 Groups: Definition and Elementary Properties

Definition 1.2.1.

A **group** $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied.

1. **Associativity**: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$

2. **Existence of identity element**: There is an element e in G such that $e * x = x * e = x$, $\forall x \in G$.

3. **Existence of inverse element**: For each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$.

   Here, a' is called the **inverse** of a.

Definition 1.2.2.

A group G is **abelian** if its binary operation is commutative.

A group that is not abelian is called **nonabelian**.

The word ***abelian*** derives from the name of the great Norwegian mathematician Niels Henrik Abel (1802-1829).

Remark.

In a group G , the identity element and inverse of each element are unique. (Prove this!). For each $a \in G$, the inverse of a is denoted by a^{-1}.

Example 5.

1. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups.

2. The sets $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*$, and $\mathbb{C}^*$ under multiplication are abelian groups.

3. The set $\mathbb{Z}^+$ under addition is *not* a group, since it has no identity element for $+$ in $\mathbb{Z}^+$.

4. The set $\mathbb{Z}^+ \cup \{0\}$ under addition is *not* a group, even if it has an identity element 0, but no inverse for 1.

5. The set $\mathbb{Z}^+$ under multiplication is *not* a group. It has an identity element 1, but no inverse for 2.

6. The set $M_n(\mathbb{R})$ under matrix addition is an abelian group. The zero matrix is the identity element.

7. The set $M_n(\mathbb{R})$ under matrix multiplication is *not* a group, since the zero matrix has no multiplicative inverse.

Problem 6.

Let $\langle G, * \rangle$ be a group. For $a, b \in G$, prove that $(a * b)^{-1} = b^{-1} * a^{-1}$

Solution.

We have $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. Since the inverse of any element in a group is unique, this shows that $(a * b)^{-1} = b^{-1} * a^{-1}$.

■

Problem 7.

Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = \dfrac{ab}{2}$. Prove that $\mathbb{Q}^+$ is an abelian group under $*$.

Solution.

It is clear that $\mathbb{Q}^+$ is closed under $*$. Also, $(a * b) * c = a * (b * c) = \dfrac{abc}{4}$, $\forall a, b, c \in \mathbb{Q}^+$, showing that $*$ is associative.
$*$ is commutative, since $a * b = b * a = \dfrac{ab}{2}$, $\forall a, b \in \mathbb{Q}^+$. If e is the identity for $*$, then $a * e = a \implies \dfrac{ae}{2} = a \implies e = 2$. Finally, computation shows that $a^{-1} = \dfrac{4}{a}$, $\forall a \in \mathbb{Q}^+$. ■

Theorem 1.2.3.

In a group G, with binary operation $*$, the left and right cancellation laws *holds. i.e., $a * b = a * c \implies b = c$ and $b * a = c * a \implies b = c$, $\forall a, b, c \in G$.*

Proof.

Suppose $a * b = a * c$. Multiplying from the left with a^{-1} on both sides, we get $a^{-1} * (a * b) = a^{-1} * (a * c)$. Using associativity, $(a^{-1} * a) * b = (a^{-1} * a) * c \implies e * b = e * c \implies b = c$. Similarly,from $b * a = c * a$, we get $b = c$. □

Theorem 1.2.4.

If G is a group with binary operation $*$, and if $a, b \in G$ the linear equations $a * x = b$ and $y * a = b$ have unique solutions , x, y in G.

Proof.

Try yourself! □

Remark.

A set together with an associative binary operation is called a **semigroup**. A **monoid** is a semigroup that has an identity element for the binary operation.

Note that a group is both a semigroup and a monoid.

Note that there is only one group of a single element, namely $\{e\}$ with binary operation $e * e = e$, up to isomorphism . By looking at the table representations, we can conclude that there is only one group of two elements (or three elements) up to isomorphism . In the next section, we will show that there exists two non isomorphic group structures on a set of four elements.

Problem 8.

Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ on S by $a * b = a + b + ab$.

(a) Show that $*$ is 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.

Solution.

(a) We must show that S is closed under $*$, that is, that $a+b+ab \neq -1$ for $a, b \in S$. Now $a+b+ab=-1$ if and only if $0=ab+a+b+1=(a+1)(b+1)$. This is the case if and only if either $a=-1$ or$b=-1$, which is not the case for $a, b \in S$.

(b) We have $a*(b*c)=a*(b+c+bc)=a+(b+c+bc)+a(b+c+bc)=a+b+c+ab+ac+bc+abc$ and $(a*b)*c=(a+b+ab)*c=(a+b+ab)+c+(a+b+ab)c=a+b+c+ab+ac+bc+abc$. Thus $*$ is associative. Note that 0 acts as identity element for $*$, since $0*a=a*0=a$.

Also, $\frac{-a}{a+1}$ acts as inverse of a, for $a*\dfrac{-a}{a+1}=a+\dfrac{-a}{a+1}+a\dfrac{-a}{a+1}+1=\dfrac{a(a+1)-a-a^2}{a+1}=\dfrac{0}{a+1}=0$. Thus $\langle S, *\rangle$ is a group.

(c) Because the operation is commutative, $2*x*3=2*3*x=11*x$. Now the inverse of 11 is $\dfrac{-11}{12}$, by Part(**b**). From, $11*x=7$, we obtain $x=\dfrac{-11}{12}*7=\dfrac{-11}{12}+7+\dfrac{-11}{12}7=\dfrac{-11+84-77}{12}=\dfrac{-4}{12}=\dfrac{-1}{3}$. ■

Problem 9.

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 $a*a=e$.

Solution.

Let $S=\{x \in G \mid x^{-1} \neq x\}$. Then S has an even number of elements, because its elements can be grouped in pairs x, x^{-1}. Because G has an even number of elements, the number of elements in G but not in S (the set $G-S$) must be even. The set $G-S$ is nonempty because it contains e. Thus there is at least one element of $G-S$ other than e, that is, at least one element other than e that is its own inverse. ■

Problem 10.

Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Solution.

Let G has m elements. Then the elements $e, a, a^2, a^3, ..., a^m$ are not all different, since G has only m elements. If one of $a, a^2, a^3, ..., a^m$ is e, then we are done. If not, then we must have $a^i = a^j$ where $i < j$. Repeated left cancellation of a yields $e = a^{j-i}$. ■

Problem 11.

Show that if $(a * b)^2 = a^2 * b^2$ for all a, b in a group G, then G is abelian.

Solution.

We have $(a * b) * (a * b) = (a * a) * (b * b)$, so $a * [b * (a * b)] = a * [a * (b * b)]$ and left cancellation yields $b * (a * b) = a * (b * b)$. Then $(b * a) * b = (a * b) * b$ and right cancellation yields $b * a = a * b$. Thus G is abelian. ■

Problem 12.

Let G be a group and let g be one fixed element of G. Show that the map i_g defined by $i_g(x) = gxg^{-1}$ for all x in G, is an isomorphism of G with itself.

Solution.

Let $a, b \in G$. If $g * a * g^{-1} = g * b * g^{-1}$, then $a = b$ by group cancellation, so i_g is a one-to-one map. Because $i_g(g^{-1} * a * g) = g * g^{-1} * a * g * g^{-1} = a$, we see that i_g maps G onto G. We have $i_g(a * b) = g * a * b * g^{-1} = g * a * (g^{-1} * g) * b * g^{-1} = (g * a * g^{-1}) * (g * b * g^{-1}) = i_g(a) * i_g(b)$, so i_g satisfies the homomorphism property also, and is thus an isomorphism. ■

Exercises.

1. Show that the subset S of $M_n(\mathbb{R})$ consisting of all invertible $n \times n$ matrices under multiplication is a group. [This group is called the **general linear group of degree n** and is denoted by $GL(n, \mathbb{R})$]

2. Determine whether the binary operation $*$ gives a group structure on the given set.

   (a) On $\mathbb{Z}$, let $*$ be defined by $a * b = ab$.

   (b) On $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$,let $*$ be defined by $a * b = a + b$.

   (c) On $\mathbb{C}$, let $*$ be defined by $a * b = |ab|$.

   (d) On $\mathbb{R}^*$, let $*$ be defined by $a * b = \frac{a}{b}$.

   (e) On $\mathbb{R}^+$, let $*$ be defined by $a * b = \sqrt{ab}$.

3. Let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$. Show that $\langle n\mathbb{Z}, + \rangle$ is a group and $\langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$.

4. Let G be a group and let $a, b \in G$. Show that $(a * b)^{-1} = a^{-1} * b^{-1}$ if and only if $a * b = b * a$.

5. If G is an abelian group, prove that $(a * b)^n = a^n * b^n$ for all integers n.

6. Let G be a group and suppose that $a * b * c = e$ for $a, b, c \in G$. Show that $b * c * a = e$ also.

7. If $*$ is a binary operation on a set S, an element $x \in S$ is an **idempotent** for $*$ if $x * x = x$. Prove that a group has exactly one idempotent.

8. Show that every group G with identity e and such that $x * x = e, \forall x \in G$ is abelian.

1.3 Subgroups

Let n be a positive integer. If a is an element of a group G, written multiplicatively, we denote the product $aaa....a$ for n factors a by a^n. We let a^0 be the identity element. Also, a^{-n} denotes the product $a^{-1}a^{-1}a^{-1}...a^{-1}$ for n factors.

Definition 1.3.1.

If G is a group, then the **order** $|G|$ of G is the number of elements in G.

Definition 1.3.2.

If a subset H of a group G is closed under the binary operation and if H with the induced operation from G is itself a group, then H is a **subgroup** of G. We denote this by $H \leq G$ or $G \geq H$. Also, $H < G$ or $G > H$ means that $H \leq G$ but $H \neq G$.

Example 6.

1. If G is any group, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups of G are **proper subgroups**. The subgroup $\{e\}$ is the **trivial** subgroup of G. All other subgroups are **non-trivial**.

2. $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$, but $\langle \mathbb{Q}^+, . \rangle$ is *not* a subgroup of $\langle \mathbb{R}, + \rangle$.

3. The n^{th} roots of unity in $\mathbb{C}$ form a subgroup U_n of the group $\mathbb{C}^*$ of non zero complex numbers under multiplication.

4. There are two different group structures of order 4. Consider the group table of $\mathbb{Z}_4$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

From the table, it is clear that the only proper subgroup of $\mathbb{Z}_4$is $\{0, 4\}$. Another group structure of order 4 is the group V, the **Klein 4-group**, which is described by the following table.

V :	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note that V has three proper nontrivial subgroups, $\{e, a\}, \{e, b\}$, and $\{e, c\}$.

Now we present a characterization of subgroups.

Theorem 1.3.3.

A subset H of a group G is a subgroup G if and only if (i). H is closed under the binary operation of G., (ii). the identity element e of G is in H, (iii). for all $a \in H$ it is true that $a^{-1} \in H$ also.

Theorem 1.3.4.

Let G be a group and let $a \in G$. Then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a, i.e., every subgroup containing a contains H.

Problem 13.

Show that a non empty subset H of a group G is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

Solution.

Let H be a subgroup of G. Then for $a, b \in H$, we have $b^{-1} \in H$ and $ab^{-1} \in H$ because H must be closed under the induced operation. Conversely, suppose that H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$. Let $a \in H$. Then taking $b = a$, we see that $aa^{-1} = e$ is in H. Taking $a = e$, and $b = a$, we see that $ea^{-1} = a^{-1} \in H$. Thus H contains the identity element and the inverse of each element. For closure, note that for $a, b \in H$, we also have $a, b^{-1} \in H$ and thus $a(b^{-1})^{-1} = ab \in H$. ■

Problem 14.

Let G be a group and let $H_G = \{x \in G \mid xa = ax, \forall a \in G\}$. Show that H_G is an abelian subgroup of G. (H_G is called the **center** of G.)

Solution.

Clearly H_G is closed under the operation and $e \in H_G$. From $xa = ax$, we obtain $xax^{-1} = a$ and then $ax^{-1} = x^{-1}a$, showing that $x^{-1} \in H_G$, which is thus a subgroup. Let $a \in H_G$. Then $ag = ga$ for all $g \in G$; in particular,$ab = ba$ for all $b \in H_G$ because H_G is a subset of G . This shows that H_G is abelian. ■

Definition 1.3.5.

Let G be a group and let $a \in G$. Then the subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ is called the **cyclic subgroup of** G **generated by** a, and is denoted by $\langle a \rangle$.

If the subgroup $\langle a \rangle$ of G is finite, then **order of** a is the order of $|\langle a \rangle|$ of this subgroup. Otherwise, we say that a is of **infinite order**.

Remark.

If a is of finite order m, then m is the smallest positive integer such that $a^m = e$.

Definition 1.3.6.

An element a of a group G **generates** G and is a **generator for** G if $\langle a \rangle = G$.

A group G is **cyclic** if there is some element $a \in G$ that generates G.

Example 7.

1. The group $\mathbb{Z}_4$ is and $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$. Also, $\langle 2 \rangle = \{0, 2\}$ and $\langle 0 \rangle = \{0\}$.

2. The Klein -4 group V is not cyclic, since $\langle e \rangle = \{e\}, \langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}$ and $\langle c \rangle = \{e, c\}$.

3. The group $\langle \mathbb{Z}, + \rangle$ is cyclic. Both 1 and -1 are generators for this group and they are the only generators. (Why?)

4. Consider the group $\langle \mathbb{Z}, + \rangle$. Note that the cyclic subgroup generated by $n \in \mathbb{Z}$ consists of all multiples of n. i.e., $\langle n \rangle = n\mathbb{Z}$.

Problem 15.

Show that every cyclic group is abelian.

Solution.

Let G be cyclic and let a be a generator for G. For $x, y \in G$, there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$. Then $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$, so G is abelian. ■

Problem 16.

Prove that a cyclic group with only one generator can have at most 2 elements.

Solution.

Let $B = \{e, a, a^2, a^3, ..., a^{n-1}\}$ be a cyclic group of n elements. Then $a^{-1} = a^{n-1}$ also generates G, because $(a^{-1})^i = (a^i)^{-1} = a^{n-i}$ for $i = 1, 2, ..., n-1$. Thus if G has only one generator, we must have $n - 1 = 1$ and $n = 2$. Of course, $G = \{e\}$ is also cyclic with one generator. ■

Problem 17.

Show that a group with no proper nontrivial subgroups is cyclic.

Solution.

Let G be a group with no proper nontrivial subgroups. If $G = \{e\}$, then G is of course cyclic. If $G \neq \{e\}$, then choose $a \in G$ such that $a \neq e$. We know that $\langle a \rangle$ is a subgroup of G and $\langle a \rangle \neq \{e\}$. Because G has no proper nontrivial subgroups, we must have $\langle a \rangle = G$. This shows that G is cyclic. ■

Problem 18.

Let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Then show that if G is cyclic, so is G'.

Solution.

Let a be a generator of G. We claim $\phi(a)$ is a generator of G'. Let $b' \in G'$. Because ϕ maps G onto G', there exists $b \in G$ such that $\phi(b) = b'$. Because a generates G, there exists $n \in \mathbb{Z}$ such that $b = a^n$. Because ϕ is an isomorphism, $b' = \phi(b) = \phi(a^n) = \phi(a)^n$. Thus G' is cyclic. ■

Problem 19.

Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

Solution.

We have to prove that $\sim$ is reflexive, symmetric and transitive. Let $a \in G$. Then $aa^{-1} = e$ and $e \in H$, since H is a subgroup. Thus $a \sim a \implies \sim$ is reflexive. Let $a, b \in G$ and $a \sim b$, so that $ab^{-1} \in H$. Since H is a subgroup, we have $(ab^{-1})^{-1} = ba^{-1} \in H$, so $b \sim a \implies \sim$ is symmetric. Now, let $a, b, c \in G$ and $a \sim b$ and $b \sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$ so $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, implies $a \sim c$. Thus $\sim$ is transitive. ■

Exercises.

1. If H and K are subgroups of a group G, then show that $H \cap K$ is a subgroup of G. Is $H \cup K$ a subgroup of G?

2. Determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$

   (a) The $n \times n$ matrices with determinant 2.

   (b) The $n \times n$ matrices with no zeros on the diagonal

   (c) The $n \times n$ matrices with determinant-1.

(d) The $n \times n$ matrices with determinant -1 or 1.

3. Find the order of the cyclic subgroup of $\mathbb{Z}_8$ generated by 2.

4. 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.

5. Let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. If H is a subgroup of G, then show that $\phi[H] = \{\phi(h) \mid h \in H\}$ is a subgroup of G'.

6. If G is an abelian group and if $H = \{a \in G \mid a^2 = e\}$, show that H is a subgroup of G.

Chapter 2

Groups of Permutations

Permutations are usually studied as combinatorial objects, we will see in this chapter that they have a natural group structure, and in fact, there is a deep connection between finite groups and permutations. Before, moving to permutation groups, we will discuss some more properties of cyclic groups.

2.1 Elementary Properties of Cyclic Groups

We recall the **Division Algorithm** for $\mathbb{Z}$. If m is a positive integer and n is any integer, then there exist unique integers q and r such that $n = mq + r$, and $0 \leq r < m$. Here, we regard q as the **quotient** and r as the non negative **remainder** when n is divided by m.

Theorem 2.1.1.

A subgroup of a cyclic group is cyclic.

Proof.

Let $G = \langle a \rangle$ and let $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \langle e \rangle$,

then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Choose m as the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$. We claim that $H = \langle a^m \rangle$. Let $b \in H$. Since $H \leq G$, we have $b = a^n$ for some $n \in \mathbb{Z}^+$. By division algorithm, there exists integers q and r such that $n = mq + r$ for $0 \leq r < m$. Then $a^n = a^{mq+r} = (a^m)^q a^r \implies a^r = (a^m)^{-q} a^n$. Since $a^n \in H, a^m \in H$, and H is a group, $(a^m)^{-q} \in H$, so that $(a^m)^{-q} a^n \in H \implies a^r \in H$. Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we have $r = 0$. Thus $n = qm$, so that $b = a^n = (a^m)^q \implies H = \langle a^m \rangle$. Hence a subgroup of a cyclic group is cyclic.

□

Corollary 2.1.2.

The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$

Let r and s be two positive integers. Then it is an easy exercise to show that $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\langle \mathbb{Z}, + \rangle$. By above corollary, H must be cyclic. The positive generator d of this cyclic subgroup is the **greatest common divisor** (gcd) of r and s. Since $d \in H$, $d = nr + ms$ for some integers n and m, so that every integer dividing both r and s, must also divide d. Hence d is indeed the largest number dividing both r and s.

We now describe all cyclic groups up to isomorphism.

Theorem 2.1.3.

Let G be a cyclic group with generator a. If the order of G is infinite , then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof.

Assume that the order of G is infinite. Then, for all positive integers m, $a^m \neq e$. We claim that $a^h \neq a^k$, whenever $h \neq k$. Let $h > k$. Then if $a^h = a^k \implies a^h a^{-k} = e \implies a^{h-k} = e$, which is a contradiction. Hence, every element of G can be expressed as a^m, for a unique $m \in \mathbb{Z}$. Define $\phi : G \to \mathbb{Z}$ as $\phi(a^i) = i$. Clearly, ϕ is well defined, one to one, and onto. Also, $\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$. Thus, ϕ is an isomorphism.

Now we assume that the order of G is finite, so that $a^m = e$ for some positive integer m. Choose the smallest positive integer n such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. Also, as above if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, which is a contradiction to the choice of n. Thus the elements $e, a, a^2, a^3, ..., a^{n-1}$ are all distinct and precisely these are the all elements of G. Define the map $\psi : G \to \mathbb{Z}_n$ as $\psi(a^i) = i$ for $i = 0, 1, 2, ..., n-1$.. Then ψ is well defined, one to one and onto. Since $a^n = e$, $a^i a^j = a^k$, where $k = i +_n j$. Thus $\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j)$, showing that ψ is an isomorphism. □

Now we present a basic theorem regarding generators of subgroups for the finite cyclic groups (Proof is left as an exercise to the student).

Theorem 2.1.4.

Let G be a cyclic group with n elements, and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing $\frac{n}{d}$ elements, where d is the gcd of n and s. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $gcd(s, n) = gcd(t, n)$.

Corollary 2.1.5.

If a is a generator of a finite cyclic group G of order n, then the other gener-

ators of G are the elements of the form a^r, where r is relatively prime to n. i.e., $gcd(r, n) = 1$.

Remark.

For every $n \in \mathbb{Z}^+$, we denote the number of positive integers $< n$ and relatively prime to n by $\phi(n)$ and is called the Euler function. Thus, if G is a cyclic group of order n, then there are $\phi(n)$ distinct elements in G, each of which generates G.

Example 8.

Consider $\langle \mathbb{Z}_7, +_7 \rangle$. Clearly 1 is a generator for this cyclic group. Since all integers $2, 3, ..., 6$ are relatively prime to 7, all of these elements are generators of $\langle \mathbb{Z}_7, +_7 \rangle$. But for the group $\langle \mathbb{Z}_8, +_8 \rangle$, the only generators are $1, 3, 5$, and 7. Since $\gcd(2, 8) = 2$, 2 generates a subgroup of order $8/2 = 4$, namely $\{0, 2, 4, 6\}$. Similarly, 4 generates a subgroup of order $8/4 = 2$, namely $\{0, 4\}$. Can you identify the subgroup generated by 6?

Example 9.

Let G be a cyclic group of order 12. Can you find the number of generators for G?. Here, the problem is that how many integers are there relatively prime to 12 and less than 12. We know that $1, 5, 7$, and 11 are the only integers smaller than 12 and relatively prime to 12. Hence a cyclic group of order 12 will have 4 generators.

Problem 20.

How many generators are there for a cyclic group of order 60?

Solution.

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53,and 59 are relatively prime to 60, so there are 16 generators for a cyclic group of order 60. ■

Problem 21.

How many elements are in the cyclic subgroup of **(a)** $\mathbb{Z}_{30}$ generated by 25? **(b)** $\mathbb{Z}_{42}$ generated by 30?

Solution.

We make use of theorem 2.1.4. **(a)** Since gcd $(25, 30) = 5$ and since $\frac{30}{5} = 6$, $\langle 25 \rangle$ has 6 elements.

(b) Since gcd $(30, 42) = 6$ and since $\frac{42}{6} = 7$, $\langle 30 \rangle$ has 7 elements. ■

Problem 22.

In the following, give an example of a group with the described property or explain why no example exists.

(a) A finite group that is not cyclic.

(b) An infinite group that is not cyclic.

(c) A cyclic group having only one generator.

(d) An infinite cyclic group having four generators.

(e) A cyclic group in which every element other than identity is a generator

(f) An finite cyclic group having four generators.

Solution.

(a) The Klein 4-group

(b) $\langle \mathbb{R}, + \rangle$

(c) $\mathbb{Z}_2$

(d) No such example exists. Every infinite cyclic group is isomorphic to $\langle \mathbb{Z}, + \rangle$ which has just two generators, 1 and -1.

(e) $\mathbb{Z}_p$, with p as a prime.

(f) $\mathbb{Z}_8$ has generators 1, 3, 5, and 7. ■

Problem 23.

Show that a group that has only a finite number of subgroups must be a finite group.

Solution.

Note that every group is the union of its cyclic subgroups, because every element of the group generates a cyclic subgroup that contains the element. Let G has only a finite number of subgroups, and hence only a finite number of cyclic subgroups. Now none of these cyclic subgroups can be infinite, for every infinite cyclic group is isomorphic to $\mathbb{Z}$ (by theorem 2.1.3) which has an infinite number of subgroups, namely $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, ...$ Such subgroups of an infinite cyclic subgroup of G would of course give an infinite number of subgroups of G, contrary to hypothesis. Thus G has only finite cyclic subgroups, and only a finite number of those. We see that the set G can be written as a finite union of finite sets, so G is itself a finite set. ■

Problem 24.

Show that $\mathbb{Z}_p$ has no proper non trivial subgroups if p is a prime number.

Solution.

All positive integers less than p are relatively prime to p because p is prime, and hence they all generate $\mathbb{Z}_p$. Thus $\mathbb{Z}_p$ has no proper cyclic subgroups, and

thus no proper subgroups, because as a cyclic group, $\mathbb{Z}_p$ has only cyclic subgroups (By theorem 2.1.1, a subgroup of a cyclic group is cyclic). ■

Exercises.

1. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

2. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the unique such element. Show that $ax = xa$ for all $x \in G$.

3. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

4. Let p be a prime number. Find the number of generators of the cyclic group $\mathbb{Z}_{p^r}$, where r is an integer ≥ 1.

5. Let G be a cyclic group of order n and H be a cyclic group of order m such that gcd $(m, n) = 1$. Then show that $G \times H$ is a cyclic group of order mn.

6. Show that a finite group of order n is cyclic if and only if the group contains an element of order n.

2.2 Groups of Permutations

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

Consider the operation function composition $\circ$ on the collection of all permutations of a set A (we call this operation as *permutation multiplication*). If σ and τ are any two permutations of a set A, we denote the composition of σ

and τ by $\sigma\tau$ instead of $\sigma \circ \tau$. Note that $\sigma\tau$ is clearly one to one and onto (Prove this!). Thus permutation multiplication is a binary operation on the collection of all permutations of a set A.

Remember that the action of $\sigma\tau$ on A is in right- to -left order; i.e., first apply τ, and then σ.

Theorem 2.2.1.

Let A be a nonempty set , and let S_A denotes the collection of all permutations of A. The S_A is a group under permutation multiplication.

The proof of the above theorem is left as an exercise.

Definition 2.2.2.

Let A be the finite set $\{1, 2, 3, ..., n\}$. The group of all permutations of the set A is the **symmetric group on n letters**, and is denoted by S_n.

Note that S_n has $n!$ elements.

Example 10.

Let $A = \{1, 2, 3\}$. Then we list below the $3! = 6$ elements of the symmetric group on three letters.

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

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

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

The multiplication table for S_3 is shown in the table given below.

	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

From the table, it is clear that this group is ***not*** abelian.

It is interesting to note that there is a natural correspondence between the elements of S_3 and the ways in which two copies of an equilateral triangle with vertices 1, 2, and 3 can be placed, one covering the other with vertices on top of vertices. Because of this fact, S_3 is also the ***group*** D_3 ***of symmetries of an equilateral triangle.***. D_3 is also called the third dihedral group.

In this context, the permutations ρ_i corresponds to rotations and μ_i corresponds to mirror images in bisectors of angles.

Remark.

Any group of at most 5 elements is abelian.

Lemma 2.2.3.

Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then the image of G under ϕ, $\phi[G] = \{\phi(g), g \in G\}$, is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Proof.

Let $x', y' \in \phi[G]$. Then there exists $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By assumption, $\phi(xy) = \phi(x)\phi(y) = x'y' \implies x'y' \in \phi[G]$. Thus $\phi[G]$ is closed under the operation of G'.

Let e' be the identity element in G'. Then, $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e) \implies e' = \phi(e)$ (by right cancellation in G') $\implies e' \in \phi[G]$.

Let $x' \in G'$. Choose $x \in G$ such that $\phi(x) = x'$. Note that $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1}) \implies x'^{-1} = \phi(x)^{-1} \in \phi[G]$. Thus $\phi[G]$ is a subgroup of G'.

Also, ϕ is an isomorphism of G onto $\phi[G]$, because ϕ is a one-to-one map of G onto $\phi[G]$ such that $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$. □

The following theorem due to the British mathematician, Arthur Cayley $(1821 - 1895)$ illustrates the importance of group of permutations.

Theorem 2.2.4. ***(Cayley's Theorem)***

Every group is isomorphic to a group of permutations.

Proof.

Let G be a group. We show that G is siomorphic to a subgroup of S_G. By above lemma, we need only to show that there exists a one-to-one function $\phi : G \to S_G$ such that $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$.

For $x \in G$, let $\lambda_x : G \to G$ be defined by $\lambda_x(g) = xg, \forall g \in G$. Then λ_x is one-to-one, because if $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$, so by left cancellation, $a = b$. Let $c \in G$. Then $x^{-1}c \in G$, and $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$, showing that λ_x maps G onto G. Thus λ_x is a permutation of G.

Define $\phi : G \to S_G$ as $\phi(x) = \lambda_x, \forall x \in G$. Suppose that $\phi(x) = \phi(y)$. Then

$\lambda_x = \lambda_y$ as functions mapping G into G. In particular $\lambda_x(e) = \lambda_y(e) \implies xe = ye \implies x = y$. Thus, ϕ is one-to-one. It remains only to show that $\phi(xy) = \phi(x)\phi(y)$, i.e. to show that $\lambda_{xy} = \lambda_x\lambda_y$. Let $g \in G$. Then, $\lambda_{xy}(g) = (xy)g$. Also, $(\lambda_x\lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$. Thus by associativity, $\lambda_{xy} = \lambda_x\lambda_y$. This completes the proof. □

Problem 25.

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$. Find **(a)** $|\langle\sigma\rangle|$ **(b)**σ^{100}.

Solution.

(a) Starting with 1 and applying σ repeatedly, we see that σ takes 1 to 3 to 4 to 5 to 6 to 2 to 1, so σ^6 is the smallest possible power of σ that is the identity permutation. It is easily checked that σ^6 carries 2, 3, 4, 5 and 6 to themselves also, so σ^6 is indeed the identity and $|\langle\sigma\rangle| = 6$.

(b) Since σ^6 is the identity permutation, we have

$$\sigma^{100} = (\sigma^6)^{16}\sigma^4 = \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

■

Problem 26.

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

Solution.

There are 4 possibilities for $\sigma(1)$, then 3 possibilities for $\sigma(3)$, then 2 possibilities for $\sigma(4)$, and then 1 possibility for $\sigma(5)$. Thus $4 \,.\, 3 \,.\, 2 \,.\, 1 = 24$ possibilities in all, showing that 24 elements will be in the set $\{\sigma \in S_5 | \sigma(2) = 5\}$. ■

Problem 27.

Give an example of a nonabelian group such that every proper subgroup is abelian.

Solution.

Consider the nonabelian group S_3. Its proper subgroups are

$$\{\rho_0, \rho_1, \rho_2\}, \{\rho_0, \mu_1\}, \{\rho_0, \mu_2\}, \{\rho_0, \mu_3\},$$

and $\{\rho_0\}$, and they are abelian. Thus, every proper subgroup of S_3 is abelian. ■

Problem 28.

Show that S_n is a nonabelian group for $n \geq 3$.

Solution.

Let $n \geq 3$, and let $\rho \in S_n$ be defined by $\rho(1) = 2, \rho(2) = 3, \rho(3) = 1$, and $\rho(m) = m$ for $3 < m \leq n$. Let $\mu \in S_n$ be defined by $\mu(1) = 1, \mu(2) = 3, \mu(3) = 2$, and $\mu(m) = m$ for $3 < m \leq n$. Then $\rho\mu \neq \mu\rho$ so S_n is not commutative. (Note that if $n = 3$, then $\rho = \rho_1$ and $\mu = \mu_1$ in S_3.) ■

Exercises.

1. Draw the multiplication table for the group D_4 of the symmetries of a square. (This group is also called the *octic group*). Identify the subgroups of this group. Is D_4 abelian?

2. Determine whether the following functions from $\mathbb{R}$ to $\mathbb{R}$ defines a permutation of $\mathbb{R}$.

   (a) $f_1(x) = x + 1$

(b) $f_2(x) = x^2$

(c) $f_3(x) = -x^3$

(d) $f_4(x) = e^x$

(e) $f_5(x) = x^3 - x^2 - 2x$.

3. Let G be a group. Prove that the permutations $\rho_a : G \to G$, where $\rho_a(x) = xa$ for $a \in G$ and $x \in G$ do form a group isomorphic to G.

4. Show that $H = \{\sigma \in S_n | \sigma(1) = 1\}$ is a subgroup of S_n.

5. Show that a function from a finite set S to itself is one-to-one if and only if it is onto. Is this true when S is infinite?

2.3 Orbits, Cycles, and the Alternating Groups

Let σ be a permutation of a set A. For $a, b \in A$, we let $a \sim b$ if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. Then $\sim$ defines an equivalence relation on A (Prove!). So, corresponding to σ, we obtain a partition of A into the equivalence classes determined by the above defined equivalence relation. These equivalence classes are called the **orbits of** σ.

For instance, the orbits of the identity permutation on A are the singleton subsets of A, since the identity permutation leaves each element of A fixed.

Example 11.

Find the orbits of

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}$ **(b)** $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$

(a) To find the orbit containing 1, we apply σ repeatedly, we see that $1 \to 5 \to 2 \to 1$, so the orbit containing 1 is $\{1, 2, 5\}$. Similarly, $3 \to 3$, and $4 \to 6 \to 4$, we see that the other orbits of σ are $\{3\}$ and $\{4, 6\}$.

(b) Proceeding as in **(a)**, we see that the orbits of μ are $\{1, 2, 3, 4, 5\}, \{6\}$, and $\{7, 8\}$.

We now identify a special type of permutations.

Definition 2.3.1.

A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element.

The **length** of a cycle is the number of elements in its largest orbit.

Two cycles are **disjoint** if any integer is moved by at most one of these cycles.

Clearly, identity permutation is a cycle of length 1.

We note that a cycle of length n has order n and the order of a permutation which is expressed as a product of disjoint cycles is the least common multiple of the lengths of the cycles.

Example 12.

Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 8 & 7 & 1 \end{pmatrix} \in S_8$. The only orbit of σ that contains more than one element is $\{1, 3, 6, 8\}$. Hence σ is a cycle of length 4. It can be represented as $(1, 3, 6, 8)$.

In this notation, $(1, 5, 4, 6, 8)$ represents the cycle $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 6 & 4 & 8 & 7 & 1 \end{pmatrix}$ in S_8.

Theorem 2.3.2.

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

Proof.

Let $B_1, B_2, ..., B_r$ be the orbits of σ, and let μ_i be the cycle defined by $\mu_i(x) = \sigma(x)$ for $x \in B_i$ and $\mu_i(x) = x$, otherwise. Then it is clear that $\sigma = \mu_1.\mu_2...\mu_r$. Since the orbits are disjoint, being distinct equivalence classes, the cycles $\mu_1, \mu_2, ..., \mu_r$ are also disjoint. □

Permutation multiplication is not commutative in general. But, multiplication of disjoint cycles is commutative. Since the orbits of a permutation are unique, the representation of a permutation as a product of disjoint cycles, none of which is the identity permutation is unique up to the order of factors.

Problem 29.

Compute the product of cycles (a) $(1,4,5)(7,8)(2,5,7)$(b) $(1,3,2,7)(4,8,6)$ in S_8.

Solution.

(a) Since the cycles are not disjoint, the order of the product can't be altered. We see that $1 \to 1 \to 1 \to 4$, $2 \to 5 \to 5 \to 1$. Proceeding like this, we get $(1,4,5)(7,8)(2,5,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 5 & 8 & 6 & 2 & 7 \end{pmatrix}$

(b) Here the cycles are disjoint, so the order of the product does not matters. As in **(a).**, we get $(1,3,2,7)(4,8,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 2 & 8 & 5 & 4 & 1 & 6 \end{pmatrix}$ ■

The following example illustrates that the product of two cycles need not be a cycle.

Example 13.

Consider the cycles $(1,4,5,6)$ and $(2,1,5)$ in S_6. We have $(1,4,5,6)(2,1,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$. The orbits of this product are $\{1,6\}, \{3\}$ and $\{2,4,5\}$, so it is not a cycle.

Here, $(2,1,5)(1,4,5,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$, which is also not a cycle.

A cycle of length 2 is called a ***transposition****. A transposition leaves all elements but two fixed, and maps each of these onto the other.*

Problem 30.

Show that any permutation of a finite set of at least two elements is a product of transpositions.

Solution.

Direct computations shows that

$$(a_1, a_2, ..., a_n) = (a_1, a_n)(a_1, a_{n-1})...(a_1, a_3)(a_1, a_2).$$

Thus any cycle is a product of transpositions. By theorem 2.3.2, we know that

every permutation of a finite set is a product of disjoint cycles. This shows that any permutation of a finite set of at least two elements is a product of transpositions. ■

We note that ***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.***

We classify a permutation of a finite set as **even** or **odd** according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions, respectively.

The identity permutation ι in S_n, where $n \geq 2$ is even, because $\iota = (1,2)(1,2)$.

Example 14.

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

so this is an even permutation.

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix} = (1,3,4)(2,6)(5,8,7) = (1,4)(1,3)(2,6)(5,7)(5.8),$

so this is an odd permutation.

Problem 31.

Show that every permutation in S_n , where $n \geq 3$ can be written as a product of at most $(n-1)$ transpositions.

Solution.

Note that $(1,2)(1,2)$ is the identity permutation in S_n, and $2 \leq n-1$ if $n > 2$. Because $(1,2,3,4,...,n) = (1,n)(1,n-1)...(1,3)(1,2)$, we see that a cycle of length n can be written as a product of $n-1$ transpositions.

Now a permutation in S_n can be written as a product of disjoint cycles, the sum of whose lengths is $\leq n$. If there are r disjoint cycles involved, we see the permutation can be written as a product of at most $n - r$ transpositions. Because $r \geq 1$, we can always write the permutation as a product of at most $n - 1$ transpositions. ■

We note that for $n \geq 2$, **the number of even permutation in S_n is the same as the number of odd permutation**; i.e., S_n has $n!/2$ even permutations and $n!/2$ odd permutations.

The following theorem shows that the collection of all even permutations of $\{1, 2, 3, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n, and this group is called the **alternating group** A_n on n letters.

Note that the set of all odd permutations is not a subgroup of S_n. (Why?)

Theorem 2.3.3.

If $n \geq 2$, then the collection of all even permutations of $\{1, 2, 3, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.

Proof.

Clearly the product of two even permutations is again an even permutation. Since $n \geq 2$, the identity permutation ι in S_n, is even, because $\iota = (1, 2)(1, 2)$. Also, note that if σ is expressed as a product of transpositions, the product of the same transpositions taken in the opposite order is σ^{-1}. Thus if σ is even, so is σ^{-1}. Thus the collection of all even permutations of $\{1, 2, 3, ..., n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n. □

Exercises.

1. Find all orbits of the permutation (a) $\sigma : \mathbb{Z} \to \mathbb{Z}$, where $\sigma(n) = n + 1$. (b) $\sigma : \mathbb{Z} \to \mathbb{Z}$, where $\sigma(n) = n + 2$

2. Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$ in S_8 as a product of transpositions.

3. Show that every permutation in S_n , where $n \geq 3$ that is not a cycle can be written as a product of at most $(n - 2)$ transpositions.

4. Find the order of the permutation
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 1 & 9 & 12 & 4 & 11 & 10 & 8 & 3 & 5 & 2 & 7 \end{pmatrix}$ in S_{12} .

5. Show that every odd permutation in S_n , where $n \geq 3$ can be written as a product of $(2n+3)$ transpositions and every even permutation as a product of $(2n + 8)$ transpositions .

6. Show that for every subgroup H of S_n for $n \geq 2$, either all the permutations in H are even or exactly half of them are even.

7. Show that the order of a permutation $\sigma \in S_n$ is the least common multiple (l.c.m.) of the lengths of its disjoint cycles.

Chapter 3

Cosets and the Theorem of Lagrange

Lagrange's theorem is about finite groups and their subgroups. The theorem is named after Joseph-Louis Lagrange (1736-1813), an Italian mathematician and astronomer, who made significant contributions to all fields of analysis, number theory, and classical and celestial mechanics

Before moving to the Lagrange's theorem and its consequences, we observe that every subgroup of a group G induces an important decomposition of G.

3.1 Cosets

Let H be a subgroup of a group G, which may be of finite or infinite order. We exhibit two partitions of G by defining two equivalence relations $\sim_L$ and $\sim_R$ on G as follows: $a \sim_L b$ if and only if $a^{-1}b \in H$ and $a \sim_R b$ if and only if $ab^{-1} \in H$. It is easy to see that these relations are reflexive, symmetric and transitive and hence they are equivalence relations on G. Now, let $a \in G$. Then

the equivalence class (corresponding to $\sim_L$) containing a consists of all $x \in G$ such that $a^{-1}x \in H$. $\implies$ $a^{-1}x = h$ for some $h \in H$. $\implies$ $x = ah$ for some $h \in H$. Thus the equivalence class of a under the equivalence relation $\sim_L$ is the set $\{ah|h \in H\}$ which we denote by aH. Similarly, we find that the equivalence class of a under the equivalence relation $\sim_R$ is the set $\{ha|h \in H\}$ and we denote this set by Ha.

We call aH, the **left coset** of H containing a, and Ha, the **right coset** of H containing a.

For example, consider the subset $3\mathbb{Z}$ of $\mathbb{Z}$. Here we use additive notation, so the left coset containing the integer n is $n + \mathbb{Z}$. When $n = 0$, $0 + 3\mathbb{Z} = 3\mathbb{Z} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$. Similarly, the left coset containing the integer 1 is $1 + 3\mathbb{Z} = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$ and the left coset containing 2 is $2 + 3\mathbb{Z} = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$. We note that these three left cosets constitute a partition of $\mathbb{Z}$. Since the group $\mathbb{Z}$ is abelian, the left coset $n + 3\mathbb{Z}$ is the same as the right coset $3\mathbb{Z} + n$, thus the partition of $\mathbb{Z}$ into right cosets is the same. (Generally, the left and the right coset of a subgroup determined by the same element need not be equal.)

From above example, we have the following observation.

For a subgroup H of an abelian group G, the partition of G into left cosets of H is the same as the partition of G into right cosets of H.

Let H be a subgroup of G. Now we show that every left coset and right coset of H have the same number of elements as H. We show this by exhibiting a one

to one map of H onto a left coset gH of H for a fixed element g of G. Define $\phi : H \to gH$ by $\phi(h) = gh, \forall h \in H$. Since $gH = \{gh|h \in H\}$, it is clear that ϕ is onto. Now let $\phi(h_1) = \phi(h_2)$ for some $h_1, h_2 \in H$. $\implies$ $gh_1 = gh_2$. By left cancellation, we get $h_1 = h_2$. Thus ϕ is one to one. This shows that every left coset of H have the same number of elements as H. In a similar way, we can get a one to one map of H onto the right coset Hg. Thus, ***every coset(left or right) of a subgroup H of a group G has the same number of elements as H.***

Problem 32.

Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.

Solution.

Since $2\mathbb{Z}$ is abelian, the left cosets and the right cosets are the same. The left coset containing the integer 0 is $0 + 4\mathbb{Z} = \{..., -8, -4, 0, 4, 8, ...\}$ and left coset containing the integer 2 is $2 + 4\mathbb{Z} = \{..., -6, -2, 2, 6, 10, ...\}$. Since these two left cosets exhausts $2\mathbb{Z}$, they form a partition of $2\mathbb{Z}$. ■

Problem 33.

Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

Solution.

The cosets are $0+\langle 4 \rangle = \langle 4 \rangle = \{0, 4, 8\}$, $1+\langle 4 \rangle = \{1, 5, 9\}$, $2+\langle 4 \rangle = \{2, 6, 10\}$, and $3 + \langle 4 \rangle = \{3, 7, 11\}$. ■

Problem 34.

Let H be a subgroup of a group G such that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. Show that every left coset gH is the same as the right coset Hg.

Solution.

We show that $gH = Hg$ by showing that each coset is a subset of the other. Let $gh \in gH$ where $g \in G$ and $h \in H$. Then $gh = ghg^{-1}g = [(g^{-1})^{-1}hg^{-1}]g$ is in Hg because $(g^{-1})^{-1}hg^{-1}$ is in H by hypothesis. Thus gH is a subset of Hg. Now let $hg \in Hg$ where $g \in G$ and $h \in H$. Then $hg = gg^{-1}hg = g(g^{-1}hg)$ is in gH because $g^{-1}hg \in H$ by hypothesis. Thus Hg is a subset of gH also, which shows that $gH = Hg$. ■

Problem 35.

Let H be a subgroup of a group G. Show that the number of left cosets of H is the same as the number of right cosets of H.

Solution. We prove this by exhibiting a one-to-one map between the collection of left cosets of H and the collection of right cosets of H. For any $a \in G$, we claim that Ha^{-1} consists of all inverses of elements in aH . For proving this, note that since H is a subgroup, we have $\{h^{-1}|h \in H\} = H$. Therefore, $Ha^{-1} = \{ha^{-1}|h \in H\} = \{h^{-1}a^{-1}|h \in H\} = \{(ah)^{-1}|h \in H\}$. This proves that Ha^{-1} consists of all inverses of elements in aH . Define a map ϕ from the collection of left cosets of H into the collection of right cosets of H by $\phi(aH) = Ha^{-1}$. Then ϕ is well defined for if $aH = bH$, then $\{(ah)^{-1}|h \in H\} = \{(bh)^{-1}|h \in H\}$. Because Ha^{-1} may be any right coset of H, the map is onto the collection of right cosets. Because elements in disjoint sets have disjoint inverses, we see that ϕ is one to one. Thus there are the same number of left as right cosets of a subgroup H of a group G.

■

Exercises.

1. Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.
2. Find all cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.
3. Let H be the subgroup $\{\rho_0, \mu_1\}$ of S_3. Find the partitions of S_3 into left cosets and right cosets of H.
4. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.
5. Give an example of a subgroup of a group G of order 6 whose left cosets give a partition of G into just one cell.
6. Give an example of a subgroup of a group G of order 6 whose left cosets give a partition of G into 6 cells.

3.2 Theorem of Lagrange

From the examples of groups that we have considered so far, we may observe that the order of a subgroup H of a finite group G is a divisor of the order of G. This is known as the theorem of Lagrange, and we have the precise statement as given below.

Theorem 3.2.1.

Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof.

Let G be a group of order n and the subgroup H have order m. Then every coset of H also has m elements. Let r be the number of cells in the partition of G into left cosets of H. Then $n = rm$, so m is a divisor of n. □

Corollary 3.2.2.

Every group of prime order is cyclic.

Proof.

Let G be of prime order p, and let $a \in G$ and $a \neq e$. Then the cyclic subgroup generated by a, $\langle a \rangle$ must contain at least two elements a and e, so that order of $\langle a \rangle \geq 2$. But by Lagrange's theorem, order of H must divide the order of G. This shows that order of $\langle a \rangle$ must be p, so that G is a cyclic group. □

We know that the order of an element is the same as the order of the cyclic subgroup generated by that element. Thus from Lagrange's theorem, it follows that ***the order of an element of a finite group divides the order of the group***.

Definition 3.2.3.

Let H be a subgroup of a group G. The number of left cosets of H in G is the **index** $(G : H)$ **of** H **in** G.

The index $(G : H)$ of a subgroup H of G may be finite or infinite. If G is a finite group, then $(G : H)$ is finite and $(G : H) = |G|/|H|$, since every coset of H contains $|H|$ elements. But, there are the same number of left as right cosets of a subgroup H of a group G (See Problem 35), so the index $(G : H)$ could be equally well defined as the number of right cosets of H in G.

Example 15.

Consider the group $\mathbb{Z}_{24}$ and its cyclic subgroup $\langle 3\rangle$ generated by 3. Since $\langle 3\rangle = \{1, 3, 6, 9, 12, 15, 18, 21\}$ has 8 elements, its index (the number of cosets) is $24/8 = 3$.

Problem 36.

Let $\sigma = (1, 2, 5, 4)(2, 3)$ in S_5. Find the index of $\langle\sigma\rangle$ in S_5.

Solution.

We have, $\sigma = (1, 2, 5, 4)(2, 3) = (1, 2, 3, 5, 4)$ generates a cyclic subgroup of S_5 of order 5, so its index (the number of left cosets) is $5!/5 = 4! = 24$.

■

Theorem 3.2.4.

Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose that $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite, and $(G : K) = (G : H)(H : K)$.

Proof.

Let $\{a_iH \mid i = 1, 2, ..., r\}$ be the collection of distinct left cosets of H in G and $\{b_jK \mid j = 1, 2, ..., s\}$ be the collection of distinct left cosets of K in H. Then it suffices to prove $\{(a_ib_j)K \mid i = 1, 2, ..., r, j = 1, 2, ..., s\}$ is the collection of distinct left cosets of K in G. Let $g \in G$ and let g be in the left coset a_iH of H. Then $g = a_ih$ for some $h \in H$. Let h be in the left coset b_jK of K in H. Then $h = b_jk$ for some $k \in K$, so $g = a_ib_jk$ and $g \in a_ib_jK$. This shows that the collection $\{(a_ib_j)K \mid i = 1, 2, ..., r, j = 1, 2, ..., s\}$ includes all left cosets of K in G. It remains to show the cosets in the collection are distinct. Suppose

that $a_ib_jK = a_pb_qK$, so that $a_ib_jk_1 = a_pb_qk_2$ for some $k_1, k_2 \in K$. Now $b_jk_1 \in H$ and $b_qk_2 \in H$. Thus a_i and a_p are in the same left coset of H, and therefore $i = p$ and $a_i = a_p$. Using group cancellation, we deduce that $b_jk_1 = b_qk_2$. But this means that b_j and b_q are in the same left coset of K, so $j = q$. Thus, $\{(a_ib_j)K \mid i = 1, 2, ..., r, j = 1, 2, ..., s\}$ is the collection of distinct left cosets of K in G. □

By Lagrange's theorem, if there is a subgroup H of a finite group G, then the order of H divides the order of G.

In general, the converse of this result is not true. It can be shown that if G is an abelian group of order n and m divides n, then there is always a subgroup of order m of G. However, by looking at the subgroups of the non abelian group A_4 (which has order 12) one can see that it has no subgroup of order 6, even though 6 divides 12.

Problem 37.

Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

Solution.

By Lagrange's theorem, the possible orders for a proper subgroup are p, q, and 1. Now p and q are primes and every group of prime order is cyclic, and of course every group of order 1 is cyclic. Thus every proper subgroup of a group of order pq must be cyclic. ■

Problem 38.

Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order.

Solution.

Let G be of order ≥ 2 but with no proper nontrivial subgroups. Let $a \in G, a \neq e$. Then $\langle a \rangle$ is a nontrivial subgroup of G, and thus must be G itself. Because every cyclic group not of prime order has proper subgroups, we see that G must be finite of prime order. ■

Problem 39.

Show that if H is a subgroup of index 2 in a finite group G, then every left coset of H is also a right coset of H.

Solution.

Since H is a subgroup of index 2, the partition of G into left cosets of H must be H and $G - H$, the compliment of H in G, because G has finite order and H must have half as many elements as G. For the same reason, this must be the partition into right cosets of H. Thus every left coset is also a right coset. ■

Exercises.

1. Find the index of the subgroup $\langle \mu_1 \rangle$ in the group S_3.
2. Let $\mu = (1, 2, 4, 5)(3, 6)$ in S_6. Find the index of $\langle \mu \rangle$ in S_6.
3. Show that if a group G has finite order n, then $a^n = e$, $\forall a \in G$.
4. Find the index of the subgroup $\langle 18 \rangle$ of the group $\mathbb{Z}_{36}$.
5. Show that every left coset of the subgroup $\mathbb{Z}$ of the additive group of real numbers contains exactly one element x such that $0 \leq x < 1$.
6. Show that a finite cyclic group of order n has exactly one subgroup of each order d dividing n, and that these are all the subgroups it has.

Chapter 4

Homomorphisms

In this chapter, we will discuss maps from a group G to the group G' which preserves the group structure.

4.1 Definition and Examples

Definition 4.1.1.

A map ϕ of a group G into a group G' is a **homomorphism** if the homomorphism property $\phi(ab) = \phi(a)\phi(b)$ holds for all $a, b \in G$.

Remark.

For any groups G and G', there is always at least one homomorphism $\phi : g \to G'$ namely the *trivial homomorphism* defined by $\phi(g) = e'$ for all $g \in G$, where e' is the identity element of G'.

Example 16.

Let $\phi : G \to G'$ be a group homomorphism of G onto G'. Then G' will be abelian if G is abelian. To see this, let $a', b' \in G'$. Since ϕ is onto, there

exists $a, b \in G$ such that $\phi(a) = a'$ and $\phi(b) = b'$. Then $a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'$, where the third equality is due to the fact that G is abelian. This shows that G' is abelian. Thus, this example illustrates how one can get information about G' from a given information about G via a homomorphism $\phi : G \to G'$.

Example 17.

Let F be the additive group of all functions from $\mathbb{R}$ into $\mathbb{R}$ and let R be the additive group of real numbers and c be any fixed real number. Define $\phi_c : F \to \mathbb{R}$ by $\phi_c(f) = f(c)$ for $f \in F$. Since the sum of two functions f and g is the function $f + g$ whose value at x is $f(x) + g(x)$, we see that $\phi_c(f+g) = (f+g)(c) = f(c)+g(c) = \phi_c(f)+\phi_c(g)$. Thus ϕ is a homomorphism of F into $\mathbb{R}$, and is called the ***evaluation homomorphism***.

Example 18.

Let $GL(n, \mathbb{R})$ be the multiplicative group of all invertible $n \times n$ matrices. Then $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ defined by $\phi(A) = detA$, the *determinant* of A, for all $A \in GL(n, \mathbb{R})$ is a homomorphism, since $det(AB) = det(A)det(B)$ and since $det(A) \neq 0$ for any invertible $n \times n$ matrix A.

Example 19.

Consider the additive group $\mathbb{Z}$ of integers. For $r \in \mathbb{Z}$, define $\phi_r(n) = rn$ for all $n \in \mathbb{Z}$. Then $\phi_r(n + m) = r(n + m) = rn + rm = \phi_r(n) + \phi_r(m)$, so ϕ_r is a homomorphism of Z into itself. When $r = 0$, we get ϕ_0, which is the trivial homomorphism. Similarly, ϕ_1 is the identity map and ϕ_{-1} maps $\mathbb{Z}$ onto $\mathbb{Z}$.

Problem 40.

Determine whether the given map ϕ is a homomorphism.

(a) Let $\phi : \mathbb{Z} \to \mathbb{R}$ under addition be given by $\phi(n) = n$.

(b) Let $\phi : \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) =$ the greatest integer $\leq x$.

(c) Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ under multiplication be given by $\phi(x) = |x|$.

(d) Let $\phi : \mathbb{R} \to \mathbb{R}^*$ where $\mathbb{R}$ is additive and $\mathbb{R}^*$ is multiplicative, be given by $\phi(x) = 2^x$.

Solution.

(a) It is a homomorphism, because $\phi(m+n) = m+n = \phi(m) + \phi(n)$.

(b) It is not a homomorphism, because $\phi(2.6 + 1.6) = \phi(4.2) = 4$ but $\phi(2.6) + \phi(1.6) = 2 + 1 = 3$.

(c) It is a homomorphism, because $\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y)$ for $x, y \in \mathbb{R}^*$

(d) It is a homomorphism, because $\phi(x+y) = 2^{x+y} = 2^x 2^y = \phi(x)\phi(y)$ for $x, y \in \mathbb{R}^*$. ■

Problem 41.

Let $M_n(\mathbb{R})$ be the additive group of all $n \times n$ matrices with real entries, and let $\mathbb{R}$ be the additive group of real numbers. Determine whether the given map ϕ is a homomorphism.

(a) Let $\phi : M_n(\mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = det(A)$, the determinant of $A \in M_n(\mathbb{R})$.

(b) Let $\phi : M_n(\mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = tr(A)$, the trace of $A \in M_n(\mathbb{R})$. (*The* ***trace*** *of A, $tr(A)$ is the sum of the elements on the main diagonal of A.*)

Solution.

(a) No, it is not a homomorphism. Let $n = 2$ and $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, so that $A + B = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. We see that $\phi(A+B) = det(A+B) = 4 - 1 = 3$, but $\phi(A) + \phi(B) = det(A) + det(B) = 1 + 0 = 1$.

(b) Yes, it is a homomorphism. Let $A = (a_{ij})$ and $B = (b_{ij})$ where the element with subscript ij is in the i^{th} row and j^{th} column. Then $\phi(A+B) = tr(A+B) = \sum_{i=1}^{n}(a_{ii} + b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = tr(A) + tr(B) = \phi(A) + \phi(B)$. ■

Exercises.

1. Let S_n be the symmetric group on n letters, and let $\phi : S_n \to \mathbb{Z}_2$ be defined by $\phi(\sigma) = 0$ if σ is an even permutation and $\phi(\sigma) = 1$ if σ is an odd permutation . Show that ϕ is a homomorphism.

2. Let F be the additive group of continuous functions from $[0, 1]$ into $\mathbb{R}$ and let R be the additive group of real numbers . Show that the map $\phi : F \to \mathbb{R}$ defined by $\phi(f) = \int_0^1 f(x)dx$ for $f \in F$, is a homomorphism.

3. Show that the map $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\gamma(m) = r$, where r is the remainder given by the division algorithm when m is divided by n, is a homomorphism..

4. Let $GL(n, \mathbb{R})$ be the multiplicative group of invertible $n \times n$ matrices with real entries, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi : GL(n, \mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = tr(A)$, the trace of A. Is ϕ a homomorphism? Justify your answer.

4.2 Properties of Homomorphisms

In this section, we will look into some structural features of G and G' that are preserved under a homomorphism $\phi : G \to G'$. We begin with the following definition.

Definition 4.2.1.

Let ϕ be a mapping of as set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The **image** $\phi[A]$ **of** A **in** Y **under** ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the **range of** ϕ. The **inverse image** $\phi^{-1}[B]$ **of** B **in** X is $\{x \in X \mid \phi(x) \in B\}$.

The next theorem shows that a homomorphism $\phi : G \to G'$ preserves the identity element, inverses, and subgroups.

Theorem 4.2.2.

Let ϕ be a homomorphism of a group G into a group G'.

(a) *If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.*

(b) *If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.*

(c) *If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.*

(d) *If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.*

Proof.

Let ϕ be a homomorphism of a group G into a group G'.

(a) We have $\phi(a) = \phi(ae) = \phi(a)\phi(e)$. Multiplying on the left by $\phi(a)^{-1}$, we see that $e' = \phi(e)$. Thus $\phi(e)$ must be the identity element e' in G'.

(b) We have $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. This shows that $\phi(a^{-1}) = \phi(a)^{-1}$.

(c) Let H be a subgroup of G and let $\phi(a)$ and $\phi(b)$ be any two elements in $\phi[H]$. Then $\phi(a)\phi(b) = \phi(ab)$, so that $\phi(ab) \in \phi[H]$. Thus $\phi[H]$ is closed under the operation of G'. Also, $e' = \phi(e) \in \phi[H]$ and $\phi(a)^{-1} = \phi(a^{-1}) \in \phi[H]$. Thus $\phi[H]$ is a subgroup of G'.

(d) Similar to **(c)**, try yourself! □

Definition 4.2.3.

Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[e'] = \{x \in G \mid \phi(x) = e'\}$ is the **kernel of** ϕ, denoted by Ker(ϕ).

Theorem 4.2.4.

Let $\phi : G \to G'$ be a group homomorphism, and let $H = Ker(\phi)$. Let $a \in G$. Then, the set $\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\}$ is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

Proof.

We have to show that $\{x \in G \mid \phi(x) = \phi(a)\} = aH$. Suppose that $\phi(x) = \phi(a)$. Then $\phi(a)^{-1}\phi(x) = e'$, where e' is the identity element of G'. But by above theorem, $\phi(a)^{-1} = \phi(a^{-1})$, so that $\phi(a^{-1})\phi(x) = e'$. Since ϕ is a homomorphism, this implies that $\phi(a^{-1})\phi(x) = \phi(a^{-1}x)$, so we get $\phi(a^{-1}x) = e'$. But, this means that $a^{-1}x$ is in $H = \text{Ker } (\phi)$, so $a^{-1}x = h$ for some $h \in H \implies x = ah \in aH$. This shows that $\{x \in G \mid \phi(x) = \phi(a)\} \subseteq aH$.

To prove the reverse inclusion, let $y \in aH$, so that $y = ah$ for some h in H. Then, $\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a) \implies y \in \{x \in G \mid \phi(x) = \phi(a)\}$. Thus, $aH \subseteq \{x \in G \mid \phi(x) = \phi(a)\}$, so that $\{x \in G \mid \phi(x) = \phi(a)\} = aH$.

In a similar way, we can show that $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$. □

Corollary 4.2.5.

A group homomorphism $\phi : G \to G'$ is a one- to- one map if and only if Ker $(\phi) = \{e\}$.

Proof.

Assume that Ker $(\phi) = \{e\}$. Then for every $a \in G$, the elements mapped into $\phi(a)$ are precisely the elements of the left coset $a\{e\} = \{a\}$, which shows that ϕ is one-to-one.

Conversely, assume that ϕ is one-to-one. Since a homomorphism preserves the identity element, we have $\phi(e) = e'$. Since ϕ is one-to-one, we see that e is the only element mapped into e' by ϕ, so Ker$(\phi) = \{e\}$. □

Problem 42.

Find Ker(ϕ) and $\phi(25)$ for the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_7$ such that $\phi(1) = 4$.

Solution.

Note that Ker$(\phi) = 7\mathbb{Z}$, because 4 has order 7 in $\mathbb{Z}_7$. We have $\phi(25) = \phi(21 + 4) = \phi(21) +_7 \phi(4) = 0 +_7 \phi(4) = \phi(1) +_7 \phi(1) +_7 \phi(1) +_7 \phi(1) = 4 +_7 4 +_7 4 +_7 4 = 1 +_7 1 = 2$. ■

Problem 43.

Find Ker(ϕ) and $\phi(18)$ for the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_{10}$ with $\phi(1) = 6$.

Solution.

Note that Ker$(\phi) = 5\mathbb{Z}$, because 6 has order 5 in $\mathbb{Z}_{10}$. We have $\phi(18) = \phi(15+3) = \phi(15) +_{10} \phi(3) = 0 +_{10} \phi(3) = \phi(1) +_{10} \phi(1) +_{10} \phi(1) = 6 +_{10} 6 +_{10} 6 = 2 +_{10} 6 = 8$. ■

Problem 44.

How many homomorphisms are there of $\mathbb{Z}$ onto $\mathbb{Z}$?

Solution.

Because the homomorphism ϕ must be onto $\mathbb{Z}$, $\phi(1)$ must be a generator of $\mathbb{Z}$. Thus there are only two such homomorphisms ϕ, one where $\phi(1) = 1$ so $\phi(n) = n$ for all $n \in \mathbb{Z}$, and one where $\phi(1) = -1$ so $\phi(n) = -n$ for all $n \in \mathbb{Z}$. ■

Problem 45.

How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}$?

Solution.

There are an infinite number of homomorphisms from $\mathbb{Z}$ into $\mathbb{Z}$. For any nonzero $n \in \mathbb{Z}$, we know that $\langle n \rangle$ is isomorphic to $\mathbb{Z}$, and that $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(m) = mn$ is an isomorphism, and hence a homomorphism. Of course ϕ defined by $\phi(m) = 0$ for all $m \in \mathbb{Z}$ is also a homomorphism. ■

Definition 4.2.6.

A subgroup H of a group G is **normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$.

Remark.

Clearly, all subgroups of abelian groups are normal.

The following corollary is immediate from the theorem 4.2.4.

Corollary 4.2.7.

If $\phi : G \to G'$ is a group homomorphism, then $Ker(\phi)$ is a normal subgroup of G.

Problem 46.

Show that any group homomorphism $\phi : G \to G'$ where $|G|$ is a prime must either be the trivial homomorphism or a one-to-one map.

Solution.

By theorem 4.2.2, Ker(ϕ)= $\phi^{-1}[\{e'\}]$ is a subgroup of G. By the Lagrange's theorem, either Ker(ϕ)= $\{e\}$ or Ker(ϕ)= G because $|G|$ is a prime number. If Ker(ϕ)= $\{e\}$, then ϕ is one-to-one by corollary 4.2.5. If Ker(ϕ)= G, then ϕ is the trivial homomorphism, mapping everything into the identity element.

■

Problem 47.

Let G be a group. Let $h, k \in G$ and let $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ be defined by $\phi(m, n) = h^m k^n$. Show that ϕ is a homomorphism if and only if $hk = kh$.

Solution.

We have $\phi(1, 0) = h^1 k^0 = h$ and $\phi(0, 1) = h^0 k^1 = k$. Assume that ϕ is a homomorphism. Using addition notation in $\mathbb{Z} \times \mathbb{Z}$ as usual, we have $\phi(1, 1) = \phi((1, 0)+(0, 1)) = \phi(1, 0)\, \phi(0, 1) = hk$, $\phi(1, 1) = \phi((0, 1)+(1, 0)) = \phi(0, 1)\, \phi(1, 0) = kh$. Thus if ϕ is a homomorphism, we must have $hk = kh$.

Conversely, assume that $hk = kh$. Then for any (i, j) and (m, n) in $\mathbb{Z} \times \mathbb{Z}$, we have $\phi((i, j) + (m, n)) = \phi(i + m, j + n) = h^{i+m} k^{j+n} = h^i h^m k^j k^n = h^i k^j h^m k^n = \phi(i, j)\phi(m, n)$, where the first equality in the second line follows from the commutativity of h and k. Thus ϕ is a homomorphism if and only if $hk = kh$ ■

Exercises.

1. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}_2$?

2. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G'$ be defined by $\phi_g(x) = gx$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

3. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G'$ be defined by $\phi_g(x) = gxg^{-1}$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

4. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if for all $x, y \in G$, we have $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$.

5. Show that if G, G' and G'' are groups and if $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\phi : G \to G''$ is a homomorphism.

6. Show that a homomorphism of a cyclic group is completely determined by its value on a generator of the group.

7. Let G be any group and let a be any element of G. Let $\phi : \mathbb{Z} \to G$ be defined by $\phi(n) = a^n$. show that ϕ is a homomorphism. Describe the image and the possibilities for the kernel of ϕ.

Chapter 5

Rings, Integral Domains and Fields

A **ring** is an algebraic structure consisting of a set together with two binary operations usually called addition and multiplication, where the set is an abelian group under addition and a semi group under multiplication such that multiplication distributes over addition. One of the most common examples of a ring is the set of integers endowed with its natural operations of addition and multiplication. The branch of mathematics that studies rings is known as **ring theory**. Ring theorists study properties common to both familiar mathematical structures such as integers and polynomials, and to the many less well-known mathematical structures that also satisfy the axioms of ring theory. The ubiquity of rings makes them a central organizing principle of contemporary mathematics. Ring theory may be used to understand fundamental physical laws, such as those underlying special relativity and symmetry phenomena in molecular chemistry.

The study of rings originated from the theory of polynomial rings and the theory of algebraic integers. In the 1880's Richard Dedekind introduced the con-

cept of a ring, and the term ring was coined by David Hilbert in 1892. After contributions from other fields, mainly number theory, the ring notion was generalized and firmly established during the 1920's by Emmy Noether and Wolfgang Krull. Modern ring theory-a very active mathematical discipline-studies rings in their own right. To explore rings, mathematicians have devised various notions to break rings into smaller, better-understandable pieces, such as ideals, quotient rings and simple rings. In addition to these abstract properties, ring theorists also make various distinctions between the theory of commutative rings and non commutative rings-the former belonging to algebraic number theory and algebraic geometry. A particularly rich theory has been developed for a certain special class of commutative rings, known as **fields**, which lies within the realm of field theory. Likewise, the corresponding theory for noncommutative rings, that of noncommutative division rings, constitutes an active research interest for noncommutative ring theorists. Since the discovery of a mysterious connection between noncommutative ring theory and geometry during the 1980's by Alain Connes, noncommutative geometry has become a particularly active discipline in ring theory.

5.1 Rings and Fields

Definition 5.1.1.

A **ring** $\langle R, +, . \rangle$ is a set R together with two binary operations $+$ and $.$, called *addition* and *multiplication*, defined on R such that the following axioms are satisfied:

(i) $\langle R, + \rangle$ is an **abelian group**.

(ii) Multiplication is **associative**.

(iii) For all $a, b, c \in R$, the **left distributive law**, $a.(b + c) = a.b + a.c$ and the **right distributive law** $(a + b).c = a.c + b.c$ hold.

Notations.

We denote the multiplication in a ring by juxtaposition. i.e., we use ab to denote $a.b$

Example 20.

Let R be any ring, and let $M_n(R)$ be the set of all $n \times n$ matrices with entries from R. The addition and multiplication in R allows us to define matrix addition and multiplication in the usual way. Then it can be shown that $M_n(R)$ is a ring with these operations. In particular, we can have the rings $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R})$ and $M_n(\mathbb{C})$. Note that multiplication is not a commutative operation in any of these rings for $n \geq 2$.

Example 21.

Let F be the set of all functions from a set $\mathbb{R}$ into $\mathbb{R}$. Then F is a ring under the usual function addition and point wise multiplication defined by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for $x \in \mathbb{R}$ and for all $f, g \in F$.

The following theorem shows that our usual rule of signs are valid in any ring and its proof is straight forward and we leave it as an exercise to the student.

Theorem 5.1.2.

If R is a ring with additive identity 0, then for any $a, b \in R$ we have

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

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

Definition 5.1.3.

A map ϕ from a ring R to a ring R' is a **homomorphism** if (i) $\phi(a+b) = \phi(a) + \phi(b)$ (ii) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

A homomorphism $\phi : R \to R'$ from a ring R to a ring R' is a **isomorphism** if it is both one to one and onto .

The rings R and R' are then **isomorphic**.

Example 22.

Consider the rings $\langle \mathbb{Z}, +, . \rangle$ and $\langle 2\mathbb{Z}, +, . \rangle$. We know that as abelian groups, $\langle \mathbb{Z}, + \rangle$ and $\langle 2\mathbb{Z}, + \rangle$ are isomorphic under the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$ defined by $\phi(x) = 2x, \forall x \in \mathbb{Z}$. But ϕ is not a ring isomorphism, for $\phi(xy) = 2xy$, while $\phi(x)\phi(y) = 2x2y = 4xy$.

Definition 5.1.4.

A ring in which the multiplication is commutative is a **commutative ring**. A ring with a multiplicative identity element is a **ring with unity**; the multiplicative identity element 1 is called **unity**.

A **multiplicative inverse** of an element a in a ring R with unity $1 \neq 0$ is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a **divison ring** (or **skew field**).

A **field** is a commutative division ring. A noncommutative division ring is called a **strictly skew field**.

Example 23.

Note that $\langle \mathbb{Z}, +, . \rangle$ is a commutative ring with unity. The only units in it are -1 and 1. Thus $\mathbb{Z}$ is not a field. However, $\langle \mathbb{Q}, +, . \rangle$, $\langle \mathbb{R}, +, . \rangle$ and $\langle \mathbb{C}, +, . \rangle$ are fields.

Example 24.

Consider $n\mathbb{Z}$,where $n \in \mathbb{Z}^+$ with usual addition and multiplication. Then it is a commutative ring, but without unity unless $n = 1$, and is not a field.

Example 25.

$\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components is a commutative ring with unit $(1, 1)$, but is not a field because $(2, 0)$ has no multiplicative inverse. The only units in $\mathbb{Z} \times \mathbb{Z}$ are $(1, 1), (1, -1), (-1, 1)$, and $(-1, -1)$.

Example 26.

Consider $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ with addition and multiplication by components . This is a commutative ring with unity, but is not a field. The units of this ring are $(1, q, 1), (-1, q, 1), (1, q, -1)$ and $(-1, q, -1)$ for any nonzero $q \in \mathbb{Q}$.

Problem 48.

Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$.

Solution.

Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be a ring homomorphism. Because $1^2 = 1$, we see that $\phi(1)$ must be an integer whose square is itself, namely either 0 or 1. If $\phi(1) = 1$, then $\phi(n) = \phi(n1) = n$, so ϕ is the identity map of $\mathbb{Z}$ onto itself which is a homomorphism. If $\phi(1) = 0$, then $\phi(n) = \phi(n1) = 0$, so ϕ maps everything onto 0, which also yields a homomorphism. ■

We list below some important points to be remembered about rings and fields.

- *A multiplicative inverse of an element a in a ring R with unity is unique, if it exists.*
- *The set of nonzero elements of a field is an abelian group under multiplication.*
- *A* ***subring*** *of a ring is a subset of the ring that is a ring under induced operations from the whole ring.*
- *A* ***subfield*** *of a field is a subset of the field that is a field under induced operations from the whole field.*
- *Unity is the multiplicative identity element, while a unit is an element having a multiplicative inverse.*
- *Unity is a unit, but not every unit is a unity.*
- *The units in $\mathbb{Z}_n$ are precisely those $m \in \mathbb{Z}_n$ such that $gcd(m, n) = 1$.*

Problem 49.

Consider the map *det* of $M_n(\mathbb{R})$ into $\mathbb{R}$ where $det(A)$ is the determinant of the matrix A for $A \in M_n(\mathbb{R})$. Is *det* a ring homomorphism? Justify your answer.

Solution.

Because $det(A + B)$ need not equal $det(A) + det(B)$, we see that *det* is not a ring homomorphism. For example, $det(I_n + I_n) = 2^n$ but $det(I_n) + det(I_n) = 1 + 1 = 2$. ■

Problem 50.

If U is the collection of all units in a ring $\langle \mathbb{R}, +, . \rangle$ with unity, show that $\langle U, . \rangle$

is a group.

Solution.

Let $u, v \in U$. Then there exists $s, t \in R$ such that $us = su = 1$ and $vt = tv = 1$. These equations show that s and t are also units in U. Then $(ts)(uv) = t(su)v = t1v = tv = 1$ and $(uv)(ts) = u(vt)s = u1s = 1$, so uv is again a unit $\implies U$ is closed under multiplication. Of course multiplication in U is associative because multiplication in R is associative. The equation $(1)(1) = 1$ shows that 1 is a unit. Since any unit $u \in U$ has a multiplicative inverse s in U, we see that U is a group under multiplication. ■

Exercises.

1. Show that $\langle n\mathbb{Z}, +, . \rangle$ is a ring.
2. Show that $\mathbb{Z}_n$ is a ring under the operations of addition modulo n and multiplication modulo n.
3. Describe all units in the ring (a) $\mathbb{Q}$ (b) $\mathbb{Z}_5$.
4. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$.
5. Describe all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$.
6. Let F be the ring of all functions from $\mathbb{R}$ into $\mathbb{R}$. For each $a \in \mathbb{R}$, define $\phi_a : F \to \mathbb{R}$ by $\phi_a(f) = f(a), \forall f \in F$. Show that ϕ_a is a ring homomorphism. (This map is called the **evaluation homomorphism**) .
7. Show that an intersection of subrings of a ring R is again a subring of R.
8. Show that an intersection of subfields of a field F is again a subfield of F.

9. Let R be a ring, and let a be a fixed element of R. Let $I_a = \{x \in R \mid ax = 0\}$. Show that I_a is a subring of R.

5.2 Integral Domains

We know that the product of any two nonzero integers is always nonzero. But this may not be the case of arbitrary rings. For example, consider the ring $\langle \mathbb{Z}_6, +, . \rangle$. Note that product of two nonzero elements may be zero in this ring, for instance, $2.3 = 0$ in $\mathbb{Z}_6$. We call these type of elements as 0 divisors.

Definition 5.2.1.

If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are **divisors of 0**(or **0 divisors**)

The following theorem illustrates the importance of the concept of 0 divisors in rings.

Theorem 5.2.2.

The cancellation laws hold in a ring R if and only if R has no divisors of 0.

Proof.

Assume that R is a ring in which the cancellation laws hold, and let $ab = 0$ for some $a, b \in R$. If $a \neq 0$, we have $ab = a0 \implies b = 0$, by left cancellation law. Similarly, if $b \neq 0$, $ab = 0b \implies a = 0$, by right cancellation law. Thus R has no divisors of 0, if the cancellation laws hold in R.

Conversely, suppose that R has no divisors of 0, and suppose that $ab = ac$, with $a \neq 0$. Since $a \neq 0$ and since R has no divisors of 0, we have $0 = ab - ac = a(b -$

$c) \implies b - c = 0 \implies b = c$. In a similar way, $ba = ca$ with $a \neq 0 \implies b = c$. Thus, if R has no divisors of 0, the cancellation laws hold in R. □

Definition 5.2.3.

An **integral domain** D is a commutative ring with unity $1 \neq 0$ and containing no divisors of 0.

Example 27.

The rings $\mathbb{Z}$ and $\mathbb{Z}_p$ for any prime p are integral domains, but $\mathbb{Z}_n$ is not an integral domain if n is not a prime. The direct product of two integral domains D_1 and D_2 is not an integral domain, because the product of two nonzero elements may be zero, for instance $(d, 0)(0, d') = (0, 0)$.

We now show that a field has no divisors of 0.

Theorem 5.2.4.

Every field F is an integral domain.

Proof.

Let $a, b \in F$ with $a \neq 0$. Assume that $ab = 0$. Since $a \neq 0$, the multiplicative inverse a^{-1} of a exists, multiplying the above equation on both sides by a^{-1}, we get $a^{-1}(ab) = a^{-1}0 = 0$. This implies, $0 = a^{-1}(ab) = (a^{-1}a)b = eb = b$, which shows that F has no divisors of 0. Since F is a field, in particular F is a commutative ring with unity, and we showed that F has no divisors of 0. Hence F is an integral domain. □

We know that $\mathbb{Z}$ is an integral domain, but not a field. We next prove that finite integral domains are fields.

Theorem 5.2.5.

Every finite integral domain is a field.

Proof.

Let D be a finite integral domain, and let $0, 1, a_1, a_2, ..., a_n$ be all the distinct elements of D. To show D is a field, we need to prove that if $a \in D$ with $a \neq 0$, then the multiplicative inverse a^{-1} of a exists in D. Now, consider $a1, aa_1, aa_2, ..., aa_n$. All these are distinct elements of D, for if $aa_i = aa_j \implies a(a_i - a_j) = 0 \implies a_i = a_j$ which is a contradiction to our assumption . Also, since D has no divisors of 0, none of these elements is 0. Thus the elements $a1, aa_1, aa_2, ..., aa_n$ are the elements $1, a_1, a_2, ..., a_n$ in some order, so that either $a1 = 1$ or $aa_i = 1$ for some i. Thus a has a multiplicative inverse. □

Since $\mathbb{Z}_p$ is an integral domain, if p is a prime, from the above theorem, it follows that $\mathbb{Z}_p$ is a field if p is a prime.

Definition 5.2.6.

If for a ring R a positive integer n exists such that $a + a + ... + a = n.a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R.

If no such positive integer exists, then R is of **characteristic** 0.

For example, the ring $\mathbb{Z}_n$ is of characteristic n, while $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ all have characteristic 0.

Theorem 5.2.7.

Let R be a ring with unity. If $n.1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0. If $n.1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such positive integer is the

characteristic of R.

Proof.

If $n.1 \neq 0$ for all $n \in \mathbb{Z}^+$, then surely we cannot have $n.a = 0, \forall a \in R$ for some $n \in \mathbb{Z}^+$. Therefore, R has characteristic 0.
If there is an $n \in \mathbb{Z}^+$ such that $n.1 = 0$, then $n.a = a + a + ... + a = a(1 + 1 + ... + 1) = a(n.1) = a.0 = 0$. Thus, the smallest $n \in \mathbb{Z}^+$ such that $n.1 = 0$ is the characteristic of R. □

Example 28.

The ring $\mathbb{Z}_3 \times \mathbb{Z}_3$ has characteristic 3 and $\mathbb{Z}_3 \times \mathbb{Z}_4$ has characteristic 12. Can you find the characteristic of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$?

Problem 51.

Find all solutions in $\mathbb{Z}_6$ of (a) $x^2 + 2x + 4 = 0$, and (b) $x^2 + 2x + 2 = 0$.

Solution.

(a) Trying all possibilities $-2, -1, 0, 1, 2$, and 3, we find that $x = 2$ is the only solution in $\mathbb{Z}_6$.
(b) Trying all possibilities -2, -1, 0, 1, 2, and 3, we find that the given equation has no solutions in $\mathbb{Z}_6$. ■

Problem 52.

Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^9$ for $a, b \in R$.

Solution.

Since R has characteristic 3, $3.a = 0$ for all $a \in R$, we get

$(a+b)^9 = [(a+b)^3]^3 = [a^3 + 3.a^2b + 3.ab^2 + b^3]^3 = (a^3 + b^3)^3 = a^9 + 3.a^6b^3 + 3.a^3b^6 + b^9 = a^9 + b^9$. ■

Problem 53.

Show that the characteristic of an integral domain D must be either 0 or a prime p.

Solution.

Suppose that the characteristic of D is mn for $m > 1$ and $n > 1$.
Then we have $(m.1)(n.1) = (mn).1 = 0$. Since an integral domain have no divisors of 0, we must have either $m.1 = 0$ or $n.1 = 0$. But if $m.1 = 0$, then Theorem 5.2.7 shows that the characteristic of D is at most m. If $n.1 = 0$, then characteristic of D is at most n. Thus the characteristic of D cant be a composite positive integer, so it must either be 0 or a prime p. ■

Problem 54.

An element a of a ring R is **idempotent** if $a^2 = a$. Show that a division ring contains exactly two idempotents.

Solution.

If $a^2 = a$, then $a^2 - a = a(a-1) = 0$. If $a \neq 0$, then a^{-1} exists in R and we have $a - 1 = (a^{-1}a)(a-1) = a^{-1}[a(a-1)] = a^{-1}0 = 0$, so $a - 1 = 0 \implies a = 1$. Thus 0 and 1 are the only two idempotent elements in a division ring. ■

Exercises.

1. A **subdomain** of an integral domain D is a subset of D that is an integral domain under induced operations from D. Show that the intersection of subdomains of an integral domain D is again a subdomain of D.

2. Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$.

3. Solve the equation $3x = 2$ in $\mathbb{Z}_7$.

4. Find the characteristic of $\mathbb{Z}_3 \times \mathbb{Z}$.

5. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^6$ for $a, b \in R$.

6. Show that a finite ring R with unity $1 \neq 0$ and no divisors of 0, is a division ring.

7. Show that the characteristic of a subdomain of an integral domain D is equal to the characteristic of D.

Chapter 6

Introduction to Vector Spaces

Linear Algebra is that branch of Mathematics which treats the common properties of algebraic systems that consists of a set, together with a notion of linear combination of elements in the set.

In this chapter, we study an important algebraic system namely, **vector spaces**. Vector spaces are a central theme in modern mathematics and has extensive applications in the natural sciences and the social sciences. The ideas behind the abstract notion of a vector space occurred in many concrete examples during the nineteenth century and earlier. It was Descartes and Fermat who first discussed the vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$ in much the way that are presented today.

In the study of vector spaces, we generalize the geometric concept of a vector as a line segment of given length and direction advantageously in an abstract way. The modern definition of a vector space seems to be due to the Italian mathematician Giuseppe Peano (1858-1932). Theory of vector spaces is a fundamental tool in pure and applied Mathematics and is becoming increasingly important in the Physical, Biological and Social Sciences.

6.1 Definition and Examples

Definition 6.1.1.

Let a non empty set V of elements be given and a rule of addition of any two elements of V, denoted by $+$ and another rule of multiplication of elements of V by real numbers (or complex numbers) also be defined, then the set V is called a ***vector space*** and elements of V are called ***vectors*** of V, provided the following conditions are satisfied.

1. For any $u, v \in V$, addition $+$ is defined and $u + v \in V$. i.e., V is closed under addition. Further,

(a) Addition is commutative, $u + v = v + u$ for all $u, v \in V$;

(b) Addition is associative, $u + (v + w) = (u + v) + w$ for all $u, v, w \in V$;

(c) There is a unique element $0 \in V$, called the zero vector, such that $u + 0 = u$ for all $u \in V$ (Existence of additive identity);

(d) For each vector $u \in V$, there is a unique vector $-u \in V$, called the additive inverse of u such that $u + (-u) = 0$;

2. Multiplication of vectors by scalars (real or complex numbers), satisfies $\alpha u \in V$ for each $u \in V$ and each scalar α. i.e., V is closed under scalar multiplication. Further,

(e) If α is a scalar, then $\alpha(u + v) = \alpha u + \alpha v$, for all $u, v \in V$

(f) If α, β are two scalars, then $(\alpha + \beta)u = \alpha u + \beta u$ for all $u \in V$;

(g) If α, β are two scalars, then $\alpha(\beta)u = (\alpha\beta)u = \beta(\alpha u)$ for all $u \in V$;

(h) For all elements u of V, we have $1.u = u$. Here, 1 is called the unit scalar.

Remark.

Note that the conditions on the operation addition, in the above definition of a vector space, says simply that V is an abelian group with respect to addition. If

u, v are elements of V, then $u+(-v)$ is usually written as $u-v$. Note that for any vector $v \in V$, we have $0.v = 0$, here the 0 on the left side is the scalar zero, and the zero on the right side is the zero vector. ($0.v = (0+0).v = 0.v+0.v \implies 0.v = 0$). Similarly, $\alpha 0 = 0$, for any scalar α.

Definition 6.1.2.

A nonempty subset S of a vector space V is called a ***subspace*** of V, if S itself is a vector space with the operations of addition and scalar multiplication on V.

To check whether S is a subspace or not, we need only to check that S is closed under addition and scalar multiplication and that $0 \in S$.

Clearly, if V is any vector space, then V itself is a subspace of V. Also, the subset consisting of the zero vector alone is a subspace of V, called the ***zero subspace*** of V, and it is the smallest subspace of any vector space V.

The following theorem gives a characterization of subspaces of a vector space.

Theorem 6.1.3.

A non empty subset S of a vector space V is a subspace of V if and only if
(a) If $u, v \in S$, then $u + v \in S$ for all $u, v \in S$.
(b) If $u \in S$, then $\alpha u \in S$ for each $u \in S$ and every scalar α.

Proof.

Assume that (a) and (b) are true. Then commutativity and associativity of addition follows because elements of S are in particular elements of the vector space V. Choosing $\alpha = -1$, from (b), we get $-1u \in S$, for all $u \in S$. Also, by taking $\alpha = 0$ in (b), we see that $0u = 0 \in S$. Therefore, S is a vector space, hence a subspace of V.

Conversely, if S is a subspace of V, then S itself is a vector space, and in particular, S is closed under vector addition and scalar multiplication. Hence S satisfies the conditions (a) and (b). □

The above characterization of subspaces can be modified in the following way.

A non empty subset S of a vector space V is a subspace of V if and only if for each pair of vectors $u, v \in S$ and for each scalar α, the vector $\alpha u + v$ is again in S.

Now we look at some examples of vector spaces.

Example 29.

Let V be the set of all n-tuples, $u = (x_1, x_2, ..., x_n)$ of real numbers. For any $u = (x_1, x_2, ..., x_n), v = (y_1, y_2, ..., y_n)$ in V and for any real number α, we define addition and scalar multiplication as follows: $u + v = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$, $\alpha u = (\alpha x_1, \alpha x_2, ..., \alpha x_n)$. It is easy to see that these definitions of vector addition and scalar multiplication makes V a vector space. **This vector space is denoted by** $\mathbb{R}^n$. Now let W be the subset of V consisting of all $u = (x_1, x_2, ..., x_n)$ with $x_1 = 0$. Then W is a subspace of V (Prove this!).

Example 30.

Let V be the set of all functions from the set $\mathbb{R}$ into $\mathbb{R}$. Define sum of two elements f, g of V as the function $f + g$, defined by $(f + g)(x) = f(x) + g(x)$. The product of the scalar α and the function f is defined as the function αf , where $(\alpha f)(x) = \alpha f(x)$. It is an easy exercise to verify these operations make V a vector space. Let W be the subset of V consisting of all continuous functions on $\mathbb{R}$ and U be the subset of V consisting of all differentiable functions on $\mathbb{R}$.

Then W and U are subspaces of V. This is because if f and g are continuous (resp. differentiable) functions on $\mathbb{R}$ and α is a real number, then $f+g$ and αf are continuous(resp. differentiable) functions on $\mathbb{R}$. Also, the zero function is both continuous and differentiable. In fact, U is a subspace of W, because every differentiable function is continuous. The space P of polynomial functions on $\mathbb{R}$ is a subspace of the vector space V of all functions from $\mathbb{R}$ into $\mathbb{R}$. (Furthermore, P is a subspace of U, and consequently, a subspace of W as well.)

Example 31.

Let P_n be the set of all polynomials in the variable x of degree $\leq n$. Then under usual addition and scalar multiplication of polynomials, the set P_n is a vector space. (Verify!). Let $V = \{p(x) \in P_n \mid p(1) = 0\}$ be the set of all polynomials in the variable x of degree $\leq n$ and vanishes at 1. Then V is a subspace of P_n, since if $p_1(x), p_2(x) \in V$, then $(p_1 + p_2)(1) = p_1(1) + p_2(1) = 0 + 0 = 0$, and $(\alpha p_1)(1) = \alpha P_1(1) = \alpha 0 = 0$, for all scalar α. But, the set $W = \{p(x) \in P_n \mid p(x) \text{ is of degree } n\}$ is not a vector space as the zero polynomial (the additive identity) $\notin W$, and hence not a subspace of P_n.

Problem 55.

Let V be a vector space. If U and W be subspaces of V, then show that $U \cap W$ is a subspace of V. Is $U \cup W$ a subspace of V?

Solution.

Clearly, $U \cap W$ is a subset of V. Let $u, v \in U \cap W$. Then $u, v \in U$ and $u, v \in W$. Since U and W are subspaces of V, $u + v \in U$, $u + v \in W$, $\alpha u \in U$ and $\alpha u \in W$, for any scalar α. Therefore $u + v \in U \cap W$ and $\alpha u \in U \cap W$. Hence $U \cap W$ is a subspace of V. Note that the union of subspaces of a vector space V need not be a subspace of V. For example, consider the vector space

$V = \{(x, y, z)|x, y, z \in \mathbb{R}\}$. Then $W_1 = \{(0, 0, z)|z \in \mathbb{R}\}$ and $W_2 = \{(0, y, 0)|y \in \mathbb{R}\}$ are subspaces of V. Now $(0, 0, 3)$ and $(0, 5, 0)$ are two elements of $W_1 \cup W_2$. But their sum, $(0, 5, 3) \notin W_1 \cup W_2$. Thus $W_1 \cup W_2$ is not a subspace of V. ■

Problem 56.

Let $V = \{(x, y, z)|x, y, z \in \mathbb{R}\}$ and let W be subset of V consisting of all $(x, y, z) \in V$ such that $x = 1 + y$. Is W a subspace of V?

Solution.

Clearly, V is a vector space with identity element $(0, 0, 0)$. Since $(0, 0, 0) \notin W$, it can not be a vector space with respect to the operations in V, and hence not a subspace of V. ■

Exercises.

1. If W_1 and W_2 are subspaces of a vector space V, then show that their union is a subspace of V if and only if one of the spaces W_i is contained in the other.

2. Let V be a vector space. Show that
   (a) $\alpha 0 = 0$, for all scalar α.
   (b) $0v = 0$, for all v in V.
   (c) $(-1)v = -v$, for all v in V.
   (d) If α is a non zero scalar and v is a vector such that $\alpha v = 0$, then $v = 0$
   (e) If u, v are in V, and $u + v = 0$, then $u = -v$

3. Show that a non empty subset W of V is a subspace of V if and only if for each pair of vectors u, v in W, and each scalar α, the vector $\alpha u + v$ is again in W.

4. Let $V = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ and let W be the subset of V consisting of all $(x, y, z) \in V$ such that $x + y + z = 0$. Show that W is a subspace of V.

5. If W_1, W_2 are subspaces of a vector space V, then show that their sum, $W = W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$ is a subspace of V.

6. Let $S = \{p(x) \in P_5 \mid p(1) = 0 \text{ and } p(3) = 0\}$, where P_5 is the space of all polynomials in the variable x of degree ≤ 5. Show that S is a subspace of P_5.

7. Let $S = \{p(x) \in P_n \mid p(x) = xp'(x)\}$, where P_n is the space of all polynomials in the variable x of degree $\leq n$ and $p'(x)$ is the derivative of $p(x)$. Is S a subspace of P_n?.

8. Let V be the set of all $m \times n$ matrices with real entries . For $A = [a_{ij}]$ and $B = [b_{ij}]$ in V , and for a scalar α, define : $A + B = [a_{ij} + b_{ij}]$ and $\alpha A = [\alpha a_{ij}]$. Show that, under this rules of addition and scalar multiplication V is a vector space.

6.2 Linear Dependence and Independence

Definition 6.2.1.

Let V be any vector space. A vector $u \in V$ is said to be a ***linear combination*** of the vectors $u_1, u_2, ..., u_n$ in V if there exist scalars $\alpha_1, \alpha_2, ..., \alpha_n$ such that $u = \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n$.

For example, consider $\mathbb{R}^3$, the space of all 3- tuples of real numbers. Note that $(3, 1, 5) = 3(1, 0, 0) + 1(0, 1, 0) + 5(0, 0, 1)$. Thus, we can say the vector $(3, 1, 5)$ in $\mathbb{R}^3$ is a linear combination of $(1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)$.

Remark.

If all scalars $\alpha_1, \alpha_2, ..., \alpha_n$ are zeros, then the linear combination is called ***trivial*** linear combination.

If at least one of $\alpha_i's$ is non zero, then it is called a ***non-trivial*** linear combination.

Definition 6.2.2.

Let V be a vector space , and let $S = \{u_1, u_2, ..., u_n\}$ be a subset of V. Then S is said to be ***linearly dependent***(in short, LD) if there exist scalars $\alpha_1, \alpha_2, ..., \alpha_n$, not all of which are zero, such that $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0$.

If $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$ is the only solution for the equation $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0$, then $S = \{u_1, u_2, ..., u_n\}$ is ***linearly independent*** (in short, LI).

Remark.

Any set which contains the zero vector is always linearly dependent (Why?).

Example 32.

Consider the vector space $\mathbb{R}^3$. Then the set $S = \{v_1 = (3, 0, -3), v_2 = (-1, 1, 2), v_3 = (4, 2, -2), v_4 = (2, 1, 1)\} \subset \mathbb{R}^3$ is linearly dependent, since $2v_1 + 2v_2 - v_3 + 0.v_4 = 0$. The vectors $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$ are linearly independent, since $\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = 0 \implies \alpha_1 = 0, \alpha_2 = 0$, and $\alpha_3 = 0$.

Remark.

An infinite subset S of a vector space V is said to be linearly dependent (resp. independent) if every finite subset of S is linearly dependent (resp. independent).

Let $S = \{u_1, u_2, ..., u_n\}$ be a subset of a vector space V. Now we will show that the set of all linear combinations of vectors in S is a subspace of V. Let W

denotes the set of all linear combinations of vectors $u_1, u_2, ..., u_n$. Then $W \subset V$. Clearly, $0 = 0u_1 + 0u_2 + ... + 0u_n \in W \implies W$ is nonempty. Let $u, v \in W$. Then u and v are linear combinations of $u_1, u_2, ..., u_n$. So, we can write $u = \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n$, $v = \beta_1 u_1 + \beta_2 u_2 + ... + \beta_n u_n$ where α_i, β_j are scalars. We have $u + v = (\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n) + (\beta_1 u_1 + \beta_2 u_2 + ... + \beta_n u_n) = (\alpha_1 + \beta_1)u_1 + (\alpha_2 + \beta_2)u_2 + ... + (\alpha_n + \beta_n)u_n \in W$. For any scalar α, $\alpha u = \alpha(\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n) = (\alpha\alpha_1)u_1 + (\alpha\alpha_2)u_2 + ... + (\alpha\alpha_n)u_n \in W$. Hence by theorem 6.1.3, W is a subspace of V. This subspace W is called the ***span*** of S, and is denoted by $[S]$.

Theorem 6.2.3.

(a) If a set $S = \{u_1, u_2, ..., u_n\}$ of a vector space V is linearly independent, then every subset of S is also linearly independent.

(b) If a set $S = \{u_1, u_2, ..., u_n\}$ of a vector space V is linearly dependent, then every superset of S is also linearly dependent.

Proof.

(a) Let $S_1 = \{u_1, u_2, ..., u_k\} \subset S$, where $k \leq n$. Suppose that $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_k u_k = 0$. Then, we have $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_k u_k + 0u_{k+1} + ... + 0u_n = 0$. Since S is linearly independent, we get $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$. Thus, S_1 is linearly independent.

(b) Given that $S = \{u_1, u_2, ..., u_n\}$ is linearly dependent. Therefore, there are scalars $\alpha_1, \alpha_2, ..., \alpha_n$, not all of which are zero, such that $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n = 0$. Now let $S_1 = \{u_1, u_2, ..., u_n, u_{n+1}, ..., u_m\}$ be any superset of S. Then we have $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n + 0u_{n+1} + ... + 0u_m = 0$, with not all $\alpha_1, \alpha_2, ..., \alpha_n$ are zero, showing that S_1 is linearly dependent. □

Theorem 6.2.4.

If $S = \{u_1, u_2, ..., u_k\}$ is an ordered subset of nonzero elements of a vector space V, then S is linearly dependent if and only if one of the vectors of $\{u_1, u_2, ..., u_k\}$ belongs to the span of the remaining vectors in S.

Proof.

Without loss of generality, assume that u_k is a linear combination of $\{u_1, u_2, ..., u_{k-1}\}$. Then, there exists scalars $\alpha_1, \alpha_2, ..., \alpha_{k-1}$ such that $u_k = \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_{k-1} u_{k-1}$. This implies, $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_{k-1} u_{k-1} - u_k = 0$. This shows that S is linearly dependent.

Conversely, assume that $S = \{u_1, u_2, ..., u_k\}$ is linearly dependent . Then there are scalars $\alpha_1, \alpha_2, ..., \alpha_k$, not all of which are zero, such that $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_k u_k = 0$. Let $\alpha_k \neq 0$. Then, $\alpha_k u_k = -\alpha_1 u_1 - \alpha_2 u_2 - ... - \alpha_{k-1} u_{k-1}$, which implies $u_k = -\frac{\alpha_1}{\alpha_k} u_1 - \frac{\alpha_2}{\alpha_k} u_2 - ... - \frac{\alpha_{k-1}}{\alpha_k} u_{k-1}$. Thus, u_k is a linear combination of $\{u_1, u_2, ..., u_{k-1}\}$. Therefore, $u_k \in [u_1, u_2, ..., u_{k-1}]$. □

Problem 57.

Given that $\{u, v, w\}$ is linearly independent, check whether $\{u-v, v-w, w-u\}$ is linearly independent or not.

Solution.

Let $\alpha(u - v) + \beta(v - w) + \gamma(w - u) = 0$. This implies, $(\alpha - \gamma)u + (\beta - \alpha)v + (\gamma - \beta)w = 0$. Since, $\{u, v, w\}$ is linearly independent, we get $\alpha - \gamma = \beta - \alpha = \gamma - \beta = 0 \implies \alpha = \beta = \gamma$, which may be other than zero. Therefore the set $\{u - v, v - w, w - u\}$ is linearly dependent. ■

Exercises.

1. Find the value of m such that $(m, 7, -4)$ is a linear combination of the vectors $(-2, 2, 1)$ and $(2, 1, -2)$.

2. Determine whether the set $S = \{1 + x, x + x^2, x^2 + 1\} \subset P_2$, the space of all polynomials of degree ≤ 2 is linearly dependent or independent.

3. Find three vectors in $\mathbb{R}^3$ which are linearly dependent and are such that any two of them are linearly independent .

4. Show that the vectors $v_1 = (1, 0, -1), v_2 = (1, 2, 1)$, and $v_3 = (0, 2, 2)$ in $\mathbb{R}^3$ are linearly dependent.

5. Prove that if two vectors in a vector space V are linearly dependent , one of them is a scalar multiple of the other.

6. Are the vectors $u_1 = (1, 1, 2, 4), u_2 = (2, -1, -5, 2), u_3 = (1, -1, -4, 0)$ and $u_4 = (2, 1, 1, 6)$ linearly dependent in $\mathbb{R}^4$?

7. Let V be a vector space and suppose α, β, γ are linearly independent vectors in V. Prove that $(\alpha + \beta), (\beta + \gamma), (\gamma + \alpha)$ are linearly independent.

6.3 Basis and Dimension

Definition 6.3.1.

Let V be a vector space. A subset B of V is called a ***basis*** of V, if (a) B is linearly independent, and (b) $[B] = V$.

Remark.

A vector space V may have different bases, but it can be shown that if one basis of V has n elements , then any other basis of V also has n elements.

Definition 6.3.2.

Let B be a basis of a vector space V. If the number of vectors in B is n, then the vector space V is called n-***dimensional*** and we write $dim(V) = n$. If V consists of zero vector alone, then V does not have a basis, and we shall say that V has dimension 0. A vector space V which has a basis consisting of a finite number of elements, or the zero vector space, is called ***finite dimensional***. Other vector spaces are called ***infinite dimensional***.

It can be proved that if V is a vector space, and if $\{v_1, v_2, ..., v_n\}$ is a basis of V, then any elements $w_1, w_2, ..., w_m$, with $m > n$ of V, are linearly dependent. In particular, if V is n-dimensional, any set of $n + 1$ vectors in V is linearly dependent.

Example 33.

Consider the vector space $\mathbb{R}^n$ and consider the vectors $e_1 = (1, 0, ..., 0), ..., e_n = (0, 0, ..., 1)$. Then, $e_1, ..., e_n$ are linearly independent vectors in $\mathbb{R}^n$. For, note that $\alpha_1 e_1 + ... + \alpha_n e_n = 0$ if and only if $\alpha_i = 0$, for every $i = 1, ..., n$. Also, any $(x_1, x_2, ..., x_n) \in \mathbb{R}^n$ can be written as: $(x1, x2, ..., x_n) = x_1 e_1 + x_2 e_2 + ... + x_n e_n$. Thus $e_1, ..., e_n$ are linearly independent vectors in $\mathbb{R}^n$ and also $[e_1, ..., e_n] = \mathbb{R}^n$. Thus, $e_1, ..., e_n$ is a basis for $\mathbb{R}^n$ and hence $\mathbb{R}^n$ is an n-dimensional vector space.

Definition 6.3.3.

If U, W are subspaces of a vector space V, then the set of all sums, $u + w$ of vectors, where $u \in U$ and $w \in W$ is called the ***sum*** of the subspaces U and W

and is denoted by $U+W$. Clearly, $U+W$ is a subspace of V which contain each of the subspaces U and W. Also, it can be proved that $[U \cup W] = U + W$.

Now, we state a theorem about the dimension of a sum of two subspaces of a vector space.

Theorem 6.3.4.

If U and W are subspaces of an N-dimensional vector space V, then $dim(U+W) = dim(U) + dim(W) - dim(U \cap W)$.

Proof. Let $dim(U) = m$, $dim(W) = n$, where $m, n \leq N$. Since $U \cap W$ is a subspace of both U and W, if $dim(U \cap W) = r$, then $r \leq$ both m and n.
Let $B = \{u_1, u_2, ..., u_r\}$ be a basis for $U \cap W$.
Extend B to a basis for U, by adjoining $(m-r)$ linearly independent vectors $v_1, v_2, ..., v_{m-r}$ to B, so that $B_1 = \{u_1, u_2, ..., u_r, v_1, v_2, ..., v_{m-r}\}$ is a basis for U. (*See 8^{th} question in the following exercise.*)
Similarly, extend B to a basis for V, by adjoining $(n-r)$ linearly independent vectors $w_1, w_2, ..., w_{n-r}$ to B, so that $B_2 = \{u_1, u_2, ..., u_r, w_1, w_2, ..., w_{n-r}\}$ is a basis for W.
Now, consider $U + W = \{u + w \mid u \in U, w \in W\}$.
Clearly, the vectors $\{u_1, u_2, ..., u_r, v_1, v_2, ..., v_{m-r}, w_1, w_2, ..., w_{n-r}\}$ spans the subspace $U + W$.
We claim that

$$\{u_1, u_2, ..., u_r, v_1, v_2, ..., v_{m-r}, w_1, w_2, ..., w_{n-r}\}$$

is linearly independent.
Assume that $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_r u_r + \beta_1 v_1 + \beta_2 v_2 + ... + \beta_{m-r} v_{m-r} + \gamma_1 w_1 +$

$\gamma_2 w_2 + ... + \gamma_{n-r} w_{n-r} = 0$

$\implies \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_r u_r + \beta_1 v_1 + \beta_2 v_2 + ... + \beta_{m-r} v_{m-r} = -\gamma_1 w_1 - \gamma_2 w_2 - ... - \gamma_{n-r} w_{n-r}$ ..... (1)

$\implies -\gamma_1 w_1 - \gamma_2 w_2 - ... - \gamma_{n-r} w_{n-r} \in U.$

Also, $-\gamma_1 w_1 - \gamma_2 w_2 - ... - \gamma_{n-r} w_{n-r} \in W.$

Thus, $-\gamma_1 w_1 - \gamma_2 w_2 - ... - \gamma_{n-r} w_{n-r} \in U \cap W$, so that we can write

$-\gamma_1 w_1 - \gamma_2 w_2 - ... - \gamma_{n-r} w_{n-r} = \delta_1 u_1 + \delta_2 u_2 + ... + \delta_r u_r$ for some scalars $\delta_1, \delta_2, ..., \delta_r$.

Therefore, $\gamma_1 w_1 + \gamma_2 w_2 + ... + \gamma_{n-r} w_{n-r} + \delta_1 u_1 + \delta_2 u_2 + ... + \delta_r u_r = 0$.

Since, $\{u_1, u_2, ..., u_r, w_1, w_2, ..., w_{n-r}\}$ is linearly independent, we see that $\gamma_i = 0$ and $\delta_j = 0$, $\forall i$ and $\forall j$.

Therefore, equation (1) becomes, $\alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_r u_r + \beta_1 v_1 + \beta_2 v_2 + ... + \beta_{m-r} v_{m-r} = 0$.

Since, $\{u_1, u_2, ..., u_r, v_1, v_2, ..., v_{m-r}\}$ is linearly independent, we get $\alpha_i = 0$ and $\beta_j = 0$, $\forall i, \forall j$..

This shows that $\{u_1, u_2, ..., u_r, v_1, v_2, ..., v_{m-r}, w_1, w_2, ..., w_{n-r}\}$ is linearly independent and so it is a basis for $U + W$.

Hence $dim(U + W) = r + (m - r) + (n - r) = m + n - r = dim(U) + dim(W) - dim\ (U \cap W)$. □

Definition 6.3.5.

If V is a finite dimensional vector space, an ***ordered basis*** for V is a finite sequence of vectors which is linearly independent and spans V. Suppose V is n- dimensional vector space and $B = \{u_1, ..., u_n\}$ is an ordered basis for V, then given $v \in V$, there exists a unique scalars $(\alpha_1, \alpha_2, ..., \alpha_n)$ such that $v = \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n$. Then $(\alpha_1, \alpha_2, ..., \alpha_n)$ is called the ***coordinate vector*** of v relative to the ordered basis B.

Problem 58.

Find the coordinates of $(3, 4, 5) \in \mathbb{R}^3$ relative to the ordered basis $B = \{(1, 0, 1), (1, 1, 0), (0, 1, 1)\}$ of $\mathbb{R}^3$.

Solution.

Let $(3, 4, 5) = \alpha(1, 0, 1) + \beta(1, 1, 0) + \gamma(0, 1, 1)$. This implies, $(3, 4, 5) = (\alpha + \beta, \beta + \gamma, \alpha + \gamma)$. Equating both sides, we get $\alpha + \beta = 3, \beta + \gamma = 4$, and $\alpha + \gamma = 5$. On solving, we get $\alpha = 2, \beta = 1$, and $\gamma = 3$. Thus, the coordinates of the vector $(3, 4, 5)$ with respect to the given basis B is $(2, 1, 3)$. ■

Exercises.

1. Show that $S = \{1, x, x^2\}$ is a basis for P_2, the space of all polynomials of degree ≤ 2.

2. Show that $S = \{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ is a basis for $\mathbb{R}^3$.

3. Let V be a vector space of dimension n, and let $v_1, v_2, .., v_n$ be linearly independent elements of V. Then show that $v_1, v_2, ..., v_n$ constitutes a basis for V.

4. Consider the subspace $U = \{(x, y, z)|x - y + z = 0\}$ of $\mathbb{R}^3$. Find a basis of U. What is dim U?

5. Let V be an n-dimensional vector space. Then show that

   (a) Any subset of V which contains more than n vectors is linearly dependent;

   (b) No subset of V which contains less than n vectors can span V.

6. Let S be a linearly independent subset of a vector space V. Suppose β is a vector in V which is not in $[S]$. Then show that the set obtained by adjoining β to S is linearly independent.

7. If W is a subspace of a finite dimensional vector space V, then show that every linearly independent subset of W is finite and is a part of a basis for W.

8. Let V be a vector space of dimension n. Let r be a positive integer with $r < n$, and let $v_1, v_2, ..., v_r$ be linearly independent elements of V. Then show that there exists elements $v_{r+1}, v_{r+2}, ..., v_{n-r}$ such that $\{v_1, v_2, ..., v_n\}$ is a basis of V.

9. Find the coordinates of $(-1, 2, 3)$ relative to the ordered basis $B = \{(1, 1, 1), (2, 0, 1), (2, 3, 5)\}$ of $\mathbb{R}^3$.

10. Find the coordinates of $x^2 + 2x - 1$ relative to the ordered basis $B = \{x + 1, x^2 + x - 1, x^2 - x + 1\}$ of P_2.

Text Books (As per Syllabus)

1. John B. Fraleigh: A First Course in Abstract Algebra, 7^{th} Ed., Pearson Education Inc.

2. D. Prasad: Linear Algebra, Narosa Pub. House

Further Reading

1. Joseph A. Gallian: Contemporary Abstract Algebra, Narosa Pub. House.

2. I. N. Herstein: Topics in Algebra, 2^{nd} Edition, John Wiley and Sons.

3. Kenneth Hoffman, and Ray Kunze: Linear Algebra ,2^{nd} Edition, Prentice Hall of India Private Ltd.

4. Artin: Algebra, Prentice Hall of India Private Ltd.