Contents

Chapter 1

UNIT I: Group

1.1 Relations

Definition 1.1.1. A *binary relation* or simply a *relation* ρ from a set A into a set B is a subset of $A \times B$.

If an ordered pair $(a, b) \in \rho$ we say that a is related to b in the given relation and we write $a\rho b$. If $(a, b) \notin \rho$ we say that a is not related to b in the given relation.

Examples 1.1.2. Let ρ be the set of all ordered pairs (m, n) of integers such that $m < n$, i.e.,

$$\rho = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m < n\}.$$

Then ρ is a binary relation on $\mathbb{Z}$.

Examples 1.1.3. Let $\rho = \{(x, y) : x, y \in \mathbb{R},\ x^2 + y^2 = 1,\ y > 0\}$. Then ρ is a binary relation on $\mathbb{R}$. S is the set of points in the Euclidean plane constituting the semicircle lying above the x-axis with center $(0, 0)$ and radius 1.

Definition 1.1.4. Let ρ be a binary relation on a set A. Then ρ is called

(i) *reflexive* if for all $x \in A$, $x\rho x$,

(ii) *symmetric* if for all $x, y \in A$, $x\rho y$ implies $y\rho x$,

(iii) *transitive* if for all $x, y, z \in A$, $x\rho y$ and $y\rho z$ imply $x\rho z$.

Definition 1.1.5. A binary relation ρ on a set A is called an *equivalence relation* on A if ρ is reflexive, symmetric, and transitive.

Examples 1.1.6. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $\rho = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (2, 3), (3, 2)\}$. Then ρ is an equivalence relation on A.

Examples 1.1.7. (i) Let L denote the set of all straight lines in the Euclidean plane and ρ_1 be the relation on L defined by for all $l_1, l_2 \in L$, $(l_1, l_2) \in \rho_1$ if and only if l_1 and l_2 are parallel. Then ρ_1 is an equivalence relation on L.

(ii) Let L be defined as in (i) and ρ_2 be the relation defined on L by for all $l_1, l_2 \in L$, $(l_1, l_2) \in \rho_2$ if and only if l_1 and l_2 are perpendicular. Let l be a line in L. Since l cannot be perpendicular to itself, $(l, l) \in \rho_2$. Hence, ρ_2 is not reflexive and so ρ_2 is not an equivalence relation on L. Also, ρ_2 is not transitive.

Examples 1.1.8. Let n be a fixed positive integer in $\mathbb{Z}$. Define the relation $\equiv_n$ on $\mathbb{Z}$ by for all $x, y \in \mathbb{Z}$, $x \equiv_n y$ if and only if $n|(x - y)$, i.e., $x - y = nk$ for some $k \in \mathbb{Z}$. We now show that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

(i) For all $x \in \mathbb{Z}$, $x - x = 0 = 0n$. Hence, for all $x \in \mathbb{Z}$, $x \equiv_n x$. Thus, $\equiv_n$ is reflexive.

(ii) Let $x, y \in \mathbb{Z}$. Suppose $x \equiv_n y$. Then there exists $q \in \mathbb{Z}$ such that $qn = x - y$. Thus, $(-q)n = y - x$ and so $n|(y - x)$. Hence, $\equiv_n$ is symmetric.

(iii) Let $x, y, z \in \mathbb{Z}$. Suppose $x \equiv_n y$ and $y \equiv_n z$. Then there exist $q, r \in \mathbb{Z}$ such that $qn = x - y$ and $rn = y - z$. Thus, $(q + r)n = x - z$ and $q + r \in \mathbb{Z}$. This implies that $x \equiv_n z$. Hence, $\equiv_n$ is transitive. Consequently, $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

Definition 1.1.9. Let ρ be an equivalence relation defined on a set S. Let $x \in S$. The equivalence class $[x]$ determined by the element x is defined by

$$[x] = \{y \in S : \ x\rho y\}$$

Since $x\rho x$, $x \in [x]$ so that any equivalence class is non-empty.

Examples 1.1.10. Consider the relation ρ defined on $\mathbb{Z}$ by $x\rho y \Leftrightarrow x - y$ is a multiple of 3. Then ρ is an equivalence relation on $\mathbb{Z}$ and so

$$\begin{aligned}
[0] &= \{y \in \mathbb{Z} : \ y - 0 = 3k \text{ where } k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \cdots\} \\
[1] &= \{3k+1 : \ k \in \mathbb{Z}\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\} \\
[2] &= \{3k+2 : \ k \in \mathbb{Z}\} = \{\cdots, -4, -1, 2, 5, 8, \cdots\} \\
[3] &= \{3k+3 : \ k \in \mathbb{Z}\} = [0] = [6] = [9] = \cdots.
\end{aligned}$$

In fact, it is easy to see that $[0], [1], [2]$ are the only three distinct equivalence classes. Any two distinct equivalence classes are disjoint and the union of all these equivalence classes is equal to $\mathbb{Z}$.

Definition 1.1.11. Let ρ be an equivalence relation defined on a set S. Then the set of all equivalence classes is called the *quotient set* of S and is denoted by S/ρ.

Definition 1.1.12. Let S be any set. A collection of pairwise disjoint non-empty subsets of S whose union is S is called a *partition* of S.

Examples 1.1.13. Let $S = \{1, 2, 3, 4, 5\}$. Then the subsets $\{1\}, \{2\}, \{3, 4\}, \{5\}$ form a partition of S. Hence the set of all singleton's of a non-empty set S forms a partition of S.

Theorem 1.1.14. *Let ρ be an equivalence relation deefined on a set S. Then*

(i) $a\rho b \Leftrightarrow [a] = [b]$.

(ii) *Any two distinct equivalence classes are disjoint.*

(iii) *S is the union of all the equivalence classes.*

Proof. (i) Let $a\rho b$. Suppose $x \in [a]$. Then $x\rho a$. Since $a\rho b$, by transitivity, we get $x\rho b$ and so $x \in [b]$. Hence $[a] \subseteq [b]$. Similarly $[b] \subseteq [a]$. Hence $[b] = [a]$.

Conversely, let $[a] = [b]$. Then a and b belong to the same equivalence class. Hence $a\rho b$.

(ii) It is enough if we prove that $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$.

Suppose $[a] \cap [b] \neq \emptyset$. Then there exists $c \in S$ such that $c \in [a] \cap [b]$. Clearly $c \in [a]$ and $c \in [b]$. From this, we have $c\rho a$ and $c\rho b$. This implies that $a\rho b$ and hence $[a] = [b]$.

(iii) Since each element a of S is in $[a]$, the union of all equivalence classes is S. □

By Theorem 1.1.14, shows that every equivalence relation defined on a set S gives rise to a partition of S. The following theorem deals with the converse situation.

Theorem 1.1.15. *Any partition of a set S determines an equivalence relation ρ such that the members of the partition are precisely the equivalence class determined by ρ.*

Proof. If $a, b \in S$, we define $a\rho b \Leftrightarrow a$ and b belongs to the same member of the partition. Obviously ρ is reflexive and symmetric. Now let $a\rho b$ and $b\rho c$.

$a\rho b \Leftrightarrow a$ and b belongs to the same partition set A.

$b\rho c \Leftrightarrow b$ and c belongs to the same partition set B.

Suppose $A \neq B$. Since $b \in A$ and $b \in B$, $A \cap B \neq \emptyset$. This is a contradiction since any two partition sets are disjoint. Hence $A = B$. Thus a and $c \in A$ and so that $a\rho c$. Hence ρ is transitive and so ρ is an equivalence relation.

Now let $a \in S$. Let A be the unique member of the partition such that $a \in A$. Then $[a] = A$ (by definition of ρ). □

The equivalence relation ρ defined in Theorem 1.1.15 is called the equivalence relation induced by the given partition .

Problem 1.1.16. Find the equivalence relation induced by the partition $\{\{1\}, \{2, 3\}, \{4\}\}$ of $S = \{1, 2, 3, 4\}$.

Solution. The equivalence relation ρ induced by the given partition is given by the following subset of $S \times S$, $\{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2), (4, 4)\}$.

Problem 1.1.17. Find the equivalence relation induced by the partition $\{A, B\}$ of $\mathbb{Z}$ where $A = \{0, 1, 2, \ldots\}, B = \{-1, -2, -3, \ldots\}$.

Solution. Let $x, y \in \mathbb{Z}$. Then $x\rho y \Leftrightarrow x, y \in A$ or $x, y \in B$. Therefore $x\rho y \Leftrightarrow x, y \leq 0$ or $x, y < 0$.

Problem 1.1.18. If ρ and σ are equivalence relations on defined on a set S, prove that $\rho \cap \sigma$ is an equivalence relation.

Solution. Let $x \in S$. Then $x\rho x$ and $x\sigma x$ (since ρ, σ are reflexive). Therefore $x(\rho\cap\sigma)x$. Hence $\rho \cap \sigma$ is reflexive.

Let $x(\rho\cap\sigma)y$. Then $x\rho y$ and $x\sigma y$. Therefore $y\rho x$ and $y\sigma x$ (since ρ, σ are symmetric). Therefore $y(\rho \cap \sigma)x$ and hence $\rho \cap \sigma$ is symmetric.

Let $x(\rho \cap \sigma)y$ and $y(\rho \cap \sigma)z$. Then ($x\rho y$ and $x\sigma y$) and ($y\rho z$ and $y\sigma z$). Therefore ($x\rho y$ and $x\sigma y$) and ($y\rho z$ and $y\sigma z$). Therefore $x\rho z$ and $x\sigma z$ (since ρ, σ are transitive). Therefore $x(\rho \cap \sigma)z$. Hence $\rho \cap \sigma$ is transitive.

Problem 1.1.19. Show that the union of two equivalence relations need not be equivalence relation.

Solution. Let $S = \{1, 2, 3\}$. Let $\rho = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$ and $\sigma = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$. Clearly ρ and σ are equivalence relations on S. Now $\rho \cup \sigma = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$, $\rho \cup \sigma$ is not transitive since $(1, 2), (2, 3) \in \rho \cup \sigma$ but $(1, 3) \notin \rho \cup \sigma$. Therefore $\rho \cup \sigma$ is not an equivalence relation.

Problem 1.1.20. What are the smallest and largest equivalence relations on a set S.

Solution. Any relation on S is a subset $S \times S$. Consider the subset $\triangle$ of $S \times S$ given by $\triangle = \{(x, x) : x \in S\}$. Now let ρ be any other equivalence relation on S. Since ρ is reflxive, ρ contains $\triangle$. Hence $\triangle$ is the smallest equivalence relation on S.

Obviously the largest equivalence relation on S is given by the subset $S \times S$.

Problem 1.1.21. Let A be a set with n elements.

(i) Find the number of relations that can be defined on A.

(ii) Find the number of reflexive relations that can be defined on A.

Solution. (i) Any relation on a A is a subset of $A \times A$. Since A has n elements, $A \times A$ has n^2 elements. Therefore the number of relations that can be defined on A is equal to the number of subsets of $A \times A = 2^{n^2}$.

(ii) Let $\triangle = \{(a,a) : \ a \in A\}$. Any reflexive relation A is of the form $\triangle \cup B$ where B is any subset of $(A \times A) - \triangle$. Further $(A \times A) - \triangle$ has $n^2 - n$ elements. Therefore the number of reflexive relation on A is equal to the number of subsets of $(A \times A) - \triangle = 2^{n^2-n}$.

1.2 Functions

Definition 1.2.1. Let A and B be non-empty sets. A *function* or a *mapping* f from A to B, written as $f : A \to B$ is a rule which asigns to each element $a \in A$ a unique elements $b \in B$.

The element b which corresponds in this way to a given element $a \in A$ is called the *image* of a under f and is written as $f(a)$.

Also if $f(a) = b$ then a is called a *pre-image* of b under f. A is called the *domain* of f and $\{f(a) : \ a \in A\}$ is called the *range* of f.

Two functions $f, g : A \to B$ are said to be *equal* if $f(x) = g(x)$ for all $x \in A$.

Examples 1.2.2.

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$. Clearly the domain of f is $\mathbb{Z}$. The range of f is given by $\{f(x) : \ x \in \mathbb{Z}\} = \{2x : \ x \in \mathbb{Z}\} = 2\mathbb{Z}$.

2. Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. Any positive real number x has two pre-image under f given by $\sqrt{x}$ and $-\sqrt{x}$ and any negative real number x does not have a pre-image under f. Hence the range of f is $\mathbb{R}^+ \cup \{0\}$.

3. Let $\mathbb{E} \subset \mathbb{R}$. The function $\chi_{\mathbb{E}} : \mathbb{R} \to \mathbb{R}$ defined by

$$\chi_{\mathbb{E}}(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

is called the characteristic function on $\mathbb{E}$.

Definition 1.2.3. Let $f : A \to B$ be a function. The graph of f is defined to be $\{(a, f(a)) : \ a \in A\}$. A function may be specified by its graph, which is a subset of

$A \times B$. Thus a function from A to B is a relation such that each element of A is related to exactly one element of B.

Remark 1.2.4. A relation from A to B may be fail to be a function in any one of the following ways.

(i) An element $a \in A$ may be related to more than one element in B.

(ii) An element $a \in A$ may not be related to any element in B.

Examples 1.2.5. 1. Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{2, 4, 6, 8\}$. Consider the relation from A to B given by the following subsets of $A \times B$.

$$\{(1, 2), (1, 4), (3, 6), (5, 8), (7, 4)\}.$$

This is not a function from A to B. Since 1 is related to 2 and 4. Further 9 is not related to any element of B.

2. The following relation defined on $\mathbb{R}$ by $\{(x, cos^{-1}x) : \ x \in \mathbb{R}\}$ is not a function, since $x = 0$ is related to more than one element.

Definition 1.2.6. A function $f : A \to B$ is *one-one(injective)* if distinct elements in A have distinct images in B under f. In other words f is 1-1 if $x, y \in A$ and $x \neq y \Rightarrow f(x) \neq f(y)$ or equivalently $f(x) = f(y) \Rightarrow x = y$.

The mapping f is called *onto(surjective)* if the range of f is equal to B. Thus if f is onto, every element of B has a pre-image in A.

If $f : A \to B$ is both 1-1 and onto then f is called *bijective*. In this case every element in B has exactly one pre-image in A.

Examples 1.2.7. 1. Consider $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 2x$ is 1-1, but not onto. For, $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$. Hence f is 1-1. The element $3 \in \mathbb{Z}$ does not have any pre-image. Hence f is not onto.

2. Consider $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x + 3$. f is 1-1 for, $f(x) = f(y) \Rightarrow x + 3 = y+3 \Rightarrow x = y$. Also any element y has $x = y-3$ as its pre-image under f. Hence f is onto. Hence f is bijection.

3. $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x$ is 1-1 and onto. Each element $y \in \mathbb{R}$ has $y/2$ as its pre-image.

4. Consider $f : \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = e^x$. Clearly $f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow x = y$. Therefore f is 1-1. Also any element $y \in \mathbb{R}^+$ has $x = log\ y$ as its pre-image under f. Therefore f is onto. Hence f is bijection.

5. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1/(1 + x^2)$ is not 1-1, since the elements a and $-a$ have the same image under f. Further f is not onto, since every element ≤ 0 does not have a pre-image.

Definition 1.2.8. Let $f : A \to B$ be a function. Let $S \subseteq A$. The *restriction* of f to S, denote by $f|S$, is a function from S to B defined by $(f|S)(x) = f(x)$ for all $x \in S$.

Example 1.2.9. Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 1/(1 + |x|)$. $f|\mathbb{R}^+ : \mathbb{R}^+ \to \mathbb{R}$, is given by $(f|\mathbb{R}^+)(x) = 1/(1 + x)$.

Definition 1.2.10. Let $f : A \to B$ and $g : B \to C$ be two functions. We define the *composite* of these functions $g \circ f : A \to C$ by the rule $(g \circ f)(a) = g(f(a))$ for all $a \in A$.

Examples 1.2.11. 1. If $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ is given by $g(x) = sin\ x$, then $(f \circ g)(x) = f(g(x)) = f(sin\ x) = (sin\ x)^2$ and $(g \circ f)(x) = g(f(x)) = g(x^2) = sin\ x^2$. Thus in general $g \circ f \neq f \circ g$.

2. If $f : \mathbb{R} \to \mathbb{Z}$ is given by $f(x) = [x]$ and $g : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is given by $g(n) = |n|$, then $g \circ f : \mathbb{R} \to \mathbb{N} \cup \{0\}$ is given by $(g \circ f)(x) = g(f(x)) = g([x]) = |[x]|$.

Theorem 1.2.12. *let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$. That is, composition of functions is associative.*

Proof. First note that $h \circ (g \circ f) : A \to D$ and $(h \circ g) \circ f : A \to D$.

Let $x \in A$.

Then $[h \circ (g \circ f)](x) = h[(g \circ f)(x)] = h[g(f(x))] = (h \circ g)(f(x)) = [(h \circ g) \circ f](x)$.

Thus, by the equality of two functions, $h \circ (g \circ f) = (h \circ g) \circ f$. □

Theorem 1.2.13. *Let $f : A \to B$, $g : B \to C$ be bijections. Then $g \circ f : A \to C$ is also bijection.*

Proof. Let $x, y \in A$. Then

$$\begin{aligned} (g \circ f)(x) = (g \circ f)(y) &\Rightarrow g(f(x)) = g(f(y)). \\ &\Rightarrow f(x) = f(y) \text{ (since } g \text{ is } 1-1) \\ &\Rightarrow x = y \text{ (since } f \text{ is } 1-1) \end{aligned}$$

Therefore $g \circ f$ is 1-1.

Now, let $z \in C$. Since $g : B \to C$ is onto, there exists $y \in B$ such that $g(y) = z$. Again, since $f : A \to B$ is onto, there exists $x \in A$ such that $f(x) = y$. Therefore $(g \circ f)(x) = g(f(x)) = g(y) = z$ and so $g \circ f$ is onto. Hence $g \circ f$ is bijection. □

Theorem 1.2.14. *Let $f : A \to B$, $g : B \to C$ be two functions. Then*

(i) $g \circ f$ is 1-1$\Rightarrow$ f is 1-1.

(ii) $g \circ f$ is onto$\Rightarrow$ g is onto.

Proof. (i) Let $g \circ f$ be 1-1. Let $x, y \in A$. Then

$$\begin{aligned} f(x) = f(y) &\Rightarrow g(f(x)) = g(f(y)) \\ &\Rightarrow (g \circ f)(x) = (g \circ f)(y) \\ &\Rightarrow x = y (since\ g \circ f\ is\ 1-1). \end{aligned}$$

Therefore f is 1-1.

(ii) Let $g \circ f$ be onto. Let $z \in C$. Then there exists $x \in A$ such that $(g \circ f)(x) = z$. Therefore $g(f(x)) = z$ and so z has $f(x)$ as its pre-image under g. Hence g is onto. □

1.3 Inverse of a function

Definition 1.3.1. Let $f : A \longrightarrow B$ be a bijection. Then for each $b \in B$, there exists a unique element $a \in A$ such that $f(a) = b$. We now define $f^{-1} : B \to A$ by $f^{-1}(b) = a$. f^{-1} is called the *inverse* of the function f.

Problem 1.3.2. Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x - 3$ is a bijection and find its inverse. Compute $f^{-1} \circ f$ and $f \circ f^{-1}$.

Solution. Let $x, y \in \mathbb{R}$. Suppose $f(x) = f(y)$. Then $2x - 3 = 2y - 3$ and so $x = y$. Hence f is 1-1. Let $y \in \mathbb{R}$. If $f(x) = y$, then $2x - 3 = y$ and so $x = (y + 3)/2$. Hence $(y + 3)/2$ is the pre-image of y under f and so f is onto. Hence f is a bijection and $f^{-1} : \mathbb{R} \to \mathbb{R}$ is given by $f^{-1}(x) = (x + 3)/2$. Now $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(2x - 3) = [(2x - 3) + 3]/2 = x$ and $(f^{-1} \circ f)(x) = x$.

Problem 1.3.3. Show that $f : \mathbb{R} - \{3\} \to \mathbb{R} - \{1\}$ given by $f(x) = \frac{x-2}{x-3}$ is a bijection and find its inverse.

Solution. Let $x, y \in \mathbb{R}$. Suppose $f(x) = f(y)$. Then $\frac{x-2}{x-3} = \frac{y-2}{y-3}$ and so $x = y$. Hence f is 1-1. Now, let $y \in \mathbb{R} - \{1\}$. If $f(x) = y$, then $x = \frac{2-3y}{1-y}$ is the pre-image of y under f and so f is onto. Hence f is bijection and $f^{-1} : \mathbb{R} - \{1\} \to \mathbb{R} - \{3\}$ is given by $f^{-1}(x) = \frac{2-3x}{1-x}$.

Problem 1.3.4. Show that $f : \mathbb{R} \to (0, 1)$ defined by $f(x) = \frac{1}{2}\left[1 + \frac{x}{1+|x|}\right]$ is a bijection.

Solution. Clearly $f(0) = 1/2$. When $x > 0, f(x) = \frac{1}{2}\left[1 + \frac{x}{1+x}\right]$. Hence $(1/2) < f(x) < 1$. Similarly when $x < 0, f(x) = \frac{1}{2}\left[1 + \frac{x}{1-x}\right]$ and hence $0 < f(x) < 1/2$. Hence f maps $(0, \infty)$ to $(1/2, 1)$ and $(-\infty, 0)$ to $(0, 1/2)$. Let $x, y \in (0, \infty)$. Then
$f(x) = f(y) \Rightarrow \frac{1}{2}\left[1 + \frac{x}{1+x}\right] = \frac{1}{2}\left[1 + \frac{y}{1+y}\right] \Rightarrow \frac{x}{1+x} = \frac{y}{1+y} \Rightarrow x(1+y) = y(1+x) \Rightarrow x = y$. Hence f is 1-1. Now, let $y \in (1/2, 1)$. To prove f is onto we must find $x \in (0, \infty)$ such that $f(x) = y$. Now, $f(x) = y \Rightarrow \frac{1}{2}\left[1 + \frac{x}{1+x}\right] = y \Rightarrow \frac{x}{1+x} = 2y - 1 \Rightarrow x = \frac{2y-1}{2(1-y)}$
Hence f is onto.

Problem 1.3.5. Show that a set X is infinite if and only if there exists a bijection between X and a proper subset A of X.

Solution. Suppose X is finite and suppose there exists a bijection $f : A \to X$ where A is a proper subset of X. Since f is a bijection A and X have the same number of elements. But $A \subset X$. Hence $A = X$ which is a contradiction. Hence X is infinite.

Conversely suppose X is infinite. Choose a sequence of distinct elements $x_1, x_2, \ldots, x_n, \ldots$ in X. Let $A = X - \{x_1\}$. Clearly A is a proper subset of X. Define $f : X \to A$ by $f(x_i) = x_{i+1}$ and $f(x) = x$ if $x \neq x_i$. Hence f is a bijection from X to A.

Definition 1.3.6. Let A be any set. The function $i_A : A \to A$ defined by $i_A(x) = x$ for all $x \in A$ is called the *identity function* on A. Thus i_A leaves every element of A fixed.

Theorem 1.3.7. Let $f : A \to A$ be any function. Then $f \circ i_A = i_A \circ f = f$.

Proof. Let $x \in A$. Then $(f \circ i_A)(x) = f(i_A(x)) = f(x)$. Hence $f \circ i_A = f$. Similarly $i_A \circ f = f$. □

Theorem 1.3.8. Let $f : A \to B$ be a bijection. Then $f^{-1} : B \to A$ is also a bijection and $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

Proof. Let $y_1, y_2 \in B$. Since $f : A \to B$ is a bijection, there exist $x_1, x_2 \in A$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$. Therefore $f^{-1}(y_1) = x_1$ and $f^{-1}(y_2) = x_2$. Now $f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow x_1 = x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow y_1 = y_2$. Hence f^{-1} is 1-1.

Now, let $x \in A$. Let $f(x) = y$. Then $f^{-1}(y) = x$. Thus every element $x \in A$ has $f(x)$ as its pre-image under f^{-1}. Hence f^{-1} is onto. Also $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = i_A(x)$. Hence $f^{-1} \circ f = i_A$. Similarly $f \circ f^{-1} = i_B$. □

Theorem 1.3.9. A function $f : A \to B$ is a bijection if and only if there exists a unique $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$.

Proof. Let $f : A \to B$ be a bijection. Then $f^{-1} : B \to A$ is also a bijection and $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$. Now, let $g : B \to A$ be any other function such that $g \circ f = i_A$ and $f \circ g = i_B$. Let $y \in B$. Let $g(y) = x$. Then $f(x) = f(g(y)) = (f \circ g)(y) = i_B(y) = y$. Hence $f^{-1} = x = g(y)$. Thus $f^{-1} = g$.

Conversely, suppose there exists a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$. Let $x, y \in A$. Then $f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow (g \circ f)(x) = (g \circ f)(y) \Rightarrow i_A(x) = i_A(y) \Rightarrow x = y$. Hence f is 1-1. Now, let $y \in B$. Then $g(y) \in A$. Also, $f(g(y)) = (f \circ g)(y) = i_B(y) = y$. Therefore f is onto. Hence f is a bijection. □

Theorem 1.3.10. *If $f : A \to B$ and $g : B \to C$ are bijection then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Proof. Since f and g are bijections, $(g \circ f) : A \to C$ is a bijection. Therefore $(g \circ f)^{-1} : C \to A$ is a bijection. Also $f^{-1} : B \to A$ and $g^{-1} : C \to B$ are bijections. Therefore $f^{-1} \circ g^{-1} : C \to A$ is a bijection. Now, let $z \in C$. Since g is onto, there exists $y \in B$ such that $g(y) = z$. Since f is onto, there exists $x \in A$ such that $f(x) = y$. Now, by definition $g^{-1}(z) = y$ and $f^{-1}(y) = x$. Hence $(f^{-1} \circ g^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x$. Also $(g \circ f)(x) = g(f(x)) = g(y) = z$ and hence $(g \circ f)^{-1}(z) = x$. From this, we get $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Definition 1.3.11. Any function $f : A \to B$ induces two natural set mappings. If $S \subseteq A$, the *image* of S under f denoted by $f(S)$ is the subset of B given by $\{f(x) : x \in S\}$. Again if $T \subseteq B$, the *inverse image* of T under f denoted by $f^{-1}(T)$ is the subset of A given by $\{x : f(x) \in T\}$.

Examples 1.3.12.

1. Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = 2x$. Then

(a) $f(\{1, 2, 3\}) = \{2, 4, 6\}$.

(b) $f^{-1}(\{1, 3, 5\}) = \emptyset$, since there is no element $x \in \mathbb{Z}$ such that $f(x) = 1$ or 3 or 5.

(c) $f^{-1}(\{2, 3, 5\}) = \{1\}$.

2. Let $f : \mathbb{R} \to \mathbb{R}$ be the constant function given by $f(x) = 3$. Then $f(S) = \{3\}$ for any non-empty subset S or $\mathbb{R}$ and

$$f^{-1}(T) = \begin{cases} \Phi & \text{if } 3 \notin T \\ \mathbb{R} & \text{if } 3 \in T, \text{ where } T \subseteq \mathbb{R}. \end{cases}$$

Note that the image of a non-empty set is non-empty whereas the inverse image of a non-empty set may be empty.

Remark 1.3.13. The associated with any function $f : A \to B$, there are two functions; one from $\varrho(A) \to \varrho(B)$, which also denoted by f, which assigns to each subset S of A the image set $f(S) \subseteq B$ and another from $\varrho(B) \to \varrho(A)$, denoted by f^{-1}, which assigns to each subset T of B its inverse image $f^{-1} \subseteq A$. The reader should carefully note this double meaning for the symbols f and f^{-1}. The function $f^{-1} : \varrho(B) \to \varrho(A)$ is not in general the inverse of the function $f : \varrho(A) \to \varrho(B)$.

Theorem 1.3.14. Let $f : A \to B$ be a function. Let A_1 and A_2 be subsets of A and B_1 and B_2 be subsets of B. Then
(i) $f(\emptyset) = \emptyset$
(ii) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$
(iii) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
(iv) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
(v) $f^{-1}(\emptyset) = \emptyset$
(vi) $f^{-1}(B) = A$
(vii) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
(viii) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
(ix) $f^{-1}(B_1^c) = [f^{-1}(B_1)]^c$.

Proof. (i) Clearly $f(\emptyset) = \emptyset$.
(ii) Let $x \in f(A_1)$. Then $x = f(y)$ for some $y \in A_1 \subseteq A_2$ and so $x \in f(A_2)$.
(iii) Let $x \in f(A_1 \cup A_2)$. Then $x = f(y)$ for some $y \in A_1 \cup A_2$ and $x \in f(A_1) \cup f(A_2)$. Let $z \in f(A_1) \cup f(A_2)$. Then $z = f(x_1) = f(x_2)$ for some $x_i \in A_i$ for $i = 1, 2$. Hence $z \in f(A_1 \cup A_2)$.
(iv) Suppose $x \in f(A_1 \cap A_2)$. Then $x = f(y)$ for some $y \in A_1 \cap A_2$ Clearly $x \in f(A_1)$ and $x \in f(A_2)$. Hence $x \in f(A_1) \cap f(A_2)$.
(v) and (vi) follows from definition.
(vii) Suppose $x \in f^{-1}(B_1 \cup B_2)$. Then $f(x) \in B_1 \cup B_2 \Rightarrow f(x) \in B_1$ or $f(x) \in B_2$ $\Rightarrow x \in f^{-1}(B_1)$ or $x \in f^{-1}(B_2) \Rightarrow x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Hence $f^{-1}(B_1 \cup B_2) \subseteq f^{-1}(B_1) \cup f^{-1}(B_2)$. The reverse inclusion can be proved by retracing the steps. Hence $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

Similar way, we prove the remaining. □

Problem 1.3.15. Let $f : X \to Y$ be a function. If $A \subseteq X$ and $B \subseteq Y$ show that (i) $A \subseteq f^{-1}[f(A)]$

(ii) $f^{-1}[f(B)] \subseteq B$.

(iii) Give an example to show that equality need not hold in (i) and (ii).

(iv) In each case when will the equality hold?

Solution. (i) Let $x \in A$. Then $f(x) \in f(A)$ and so $x \in f^{-1}[f(A)]$. Hence $A \subseteq f^{-1}[f(A)]$.

(ii) Let $y \in f[f^{-1}(B)]$. Then there exists $x \in f^{-1}(B)$ such that $y = f(x)$. Now, $x \in f^{-1}(B) \Rightarrow f(x) \in B \Rightarrow y \in B$. Hence $f[f^{-1}(B)] \subseteq B$.

(iii) Consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. Let $A = (0, 1)$. Then $f(A) = (0, 1)$ and $f^{-1}[f(A)] = (-1, 1)$ which is not a subset of A. Consider $B = (-1, 0)$. Then $f^{-1}(B) = \emptyset$. Therefore $f[f^{-1}(B)] = f(\emptyset) = \emptyset$ and so B is not a subset of $f[f^{-1}(B)]$.

(iv) We claim that the reverse inclusion is true in (i) if f is 1-1. Let $x \in f^{-1}[f(A)]$. Then $f(x) \in f(A)$. Since f is 1-1, $x \in A$ and so $f^{-1}[f(A)] \subseteq A$. Hence equality is true in (i) if f is 1-1. We claim that the reverse inclusion is true in (ii) if f is onto. Let $y \in B$. Since f is onto there exists $x \in X$ such that $f(x) = y$. $\therefore y \in B \Rightarrow f(x) \in B \Rightarrow x \in f^{-1}(B) \Rightarrow f(x) \in f[f^{-1}(B)] \Rightarrow y \in f[f^{-1}(B)]$. Hence $B \subseteq f[f^{-1}(B)]$ and so equality is true in (ii) if f is onto.

1.4 Groups

Definition 1.4.1. A *group* is an ordered pair $(G, *)$, where G is a nonempty set and $*$ is a binary operation on G such that the following properties hold:

(G1) For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$ (associative law).

(G2) There exists $e \in G$ such that for all $a \in G$, $a * e = a = e * a$ (existence of an identity).

(G3) For all $a \in G$, there exists $a' \in G$ such that $a * a' = e = a' * a$ (existence of an inverse).

Examples 1.4.2.

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

2. The set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{R}$ is a group under matrix addition. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity element and $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

3. The set of all 2×2 non-singular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{R}$ is a group under matrix multiplication. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element. The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{|A|}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $|A| = ad - bc \neq 0$.

4. $\mathbb{N}$ is not a group under usual addition since there is no element $e \in \mathbb{N}$ such that $x + e = x$.

5. The set $\mathbb{E}$ of all even integers under usual addition is a group.

6. $\mathbb{Q}^*$ and $\mathbb{R}^*$ under usual multiplication are groups. 1 is the identity element and the inverse of a non-zero element a is $1/a$.

7. $\mathbb{Q}^+$ is a group under usual multiplication. For $a, b \in \mathbb{Q}^+ \Rightarrow ab \in \mathbb{Q}^+$. Therefore usual multiplication is a binary operation in $\mathbb{Q}^+$.
   $1 \in \mathbb{Q}^+$ is the identity element. If $a \in \mathbb{Q}^+$, $(1/a) \in \mathbb{Q}^+$ is the inverse of a.

8. $\mathbb{Z}$ under the usual multiplication is not a group.

9. Let A be any non-empty set. Let $B(A)$ be the set of all bijections from A to itself. $B(A)$ is a group under the composition of functions. We know that $f, g \in B(A) \Rightarrow f \circ g \in B(A)$(by Theorem 1.4.4). The composition of functions is associative (by Theorem 1.4.3). $i_A : A \to A$ is the identity element (by Theorem 1.5.7). If $f : A \to A$ is a bijection, then $f^{-1} : A \to A$ is also a bijection and $f \circ f^{-1} = f^{-1} \circ f = i_A$(by Theorem 1.5.8)

10. Let $G = \{e\}$ and $e * e = e$. Obviously G is a group.

11. Let $G = \{1, -1\}$. G is a group under multiplication. 1 is the identity element. The inverse of each element is itself. The Cayley table for this group is

*	1	-1
1	1	1
-1	-1	1

12. $(\varrho(S), \triangle)$ is a group. $\triangle$ is associative. Also $A \triangle \Phi = \Phi \triangle A = A$ for all $A \in \varrho(S)$. Hence Φ is the identity element. $A \triangle A = \Phi$ so that inverse of each element is itself.

13. $G = \{1, i, -1, -i\}$. G is a group under usual multiplication. The identity element is 1. The inverse of $1, i, -1$ and $-i$ are $1, -i, -1$ and i respectively.
The Cayley table for this group is given by

*	1	i	-1	-i
1	1	i	-1	i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

14. Let $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$
G is a group under matrix multiplication. [Construct the Cayley table for this group]

15. $\mathbb{C}^*$ is a group under usual multiplication given by $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$.

Proof. (15) Let $x, y \in \mathbb{C}^*$. Then $x = a + ib$ where a and b are not simultaneously zero and $y = c + id$ where c and d are simultaneously zero. Now, $xy = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$. We shall first prove that $ad - bc$ and $ad + bc$ are not simultaneously zero. Suppose,

$$ac - bd = 0 \tag{1.1}$$

$$\text{and } ad + bc = 0 \tag{1.2}$$

Multiplying (1.1) by d and (1.2) by c and subtracting, we get $b(d^2+c^2)=0$. Therefore either $b=0$ or $d^2+c^2=0$. Thus either $b=0$ or ($c=0$ and $d=0$). Similarly, either $a=0$ or ($c=0$ and $d=0$). Thus ($a=0$ and $b=0$) or ($c=0$ and $d=0$). Thus $x=0$ or $y=0$ which is a contradiction. Hence $xy \in \mathbb{C}^*$. Now, let $x=a+ib, y=c+id$ and $z=e+if$. Then $x(yz)=(a+ib)[(ce-df)+i(de+cf)]=(ace-adf-bde-bcf)+(bce+bdf+ade+acf)$. Similarly, $(xy)z=(ace-adf-bde-bcf)+(bce+bdf+ade+acf)$. Hence $x(yz)=(xy)z$. Clearly $1+i0$ is the identity element. Also $\frac{1}{x}=\frac{1}{a+ib}=\frac{a-ib}{(a+ib)(a-ib)}=\frac{a-ib}{a^2+b^2}=(\frac{a}{a^2+b^2})-i(\frac{b}{a^2+b^2})$ Since $a^2+b^2\neq 0$, $1/x\in\mathbb{C}^*$ and is the inverse of x. Hence $\mathbb{C}^*$ is a group under usual multiplication. □

16. Let $G=\{z:\ z\in\mathbb{C} \text{ and } |z|=1\}$. Then G is a under usual multiplication.

Proof. (16) Let $z_1,z_2\in G$. Then $|z_1|=|z_2|=1$, $|z_1z_2|=|z_1||z_2|=1$ and so $z_1,z_2\in G$. We know that usual multiplication of complex numbers is associative. Also $1=1+i0\in G$ and is the identity element. Now, let $z\in G$. Then $|z|=1$. Hence $|1/z|=1/|z|=1$ and so $1/z\in G$ and is the inverse of z. Hence G is a group. □

17. The set of all n^{th} roots of unity with usual multiplication is a group.

Proof. (17) Let $\omega=cos(2\pi/n)+i\ sin(2\pi/n)$. Then the n^{th} roots of unity are given by $1,\omega,\omega^2,\ldots,\omega^{n-1}$. Let $G=\{1,\omega,\omega^2,\ldots,\omega^{n-1}\}$. We know that $\omega^n=1,\omega^{n+1}=\omega$ etc. Let $\omega^r,\omega^s\in G$. Let $r+s=qn+t$ where $0\leq t<n$. Then $\omega^r\omega^s=\omega^{r+s}=\omega^{qn+t}=(\omega^n)^q\omega^t=\omega^t\in G$ We know that usual multiplication of complex number is associative. Clearly $1\in G$ is the identity element and the inverse of ω^r is ω^{n-r}. Hence G is a group. □

18. Let $G=\{a+b\sqrt{2}:\ a,b\in\mathbb{Z}\}$. Then G is a group under addition.

Proof. (18) Let $a+b\sqrt{2}$ and $c+d\sqrt{2}\in G$. Then $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in G$. We know that usual addition is associative. Clearly $0=0+0\sqrt{2}\in G$ is the identity element and $-a-b\sqrt{2}$ is the inverse of $a+b\sqrt{2}$. Hence G is a group. □

19. Let G be the set of all real numbers except -1. Define $*$ on G by $a*b=a+b+ab$. Then $(G,*)$ is a group.

Proof. Let $a, b \in G$. Then $a \neq -1$ and $b \neq -1$. We claim that $a * b \neq -1$. Suppose $a * b = -1$. Then $a + b + ab = -1$ so that $a + b + ab + 1 = 0$, i.e., $(a + 1)(b + 1) = 0$ so that either $a = -1$ or $b = -1$ which is a contradiction. Hence $a * b \neq -1$ and thus $*$ is a binary operation on G. Now $a*(b*c) = a*(b+c+bc) = a+(b+c+bc)+a(b+c+bc) = a+b+c+bc+ab+ac+abc.\text{Also}(a*b)*c = (a+b+ab)*c = a+b+ab+c+(a+b+bc)c = a + b + c + ab + ac + bc + abc$. Hence $a * (b * c) = (a * b) * c$. Also 0 is the identity, for $a * 0 = a + 0 + 0a = a$ and $0 * a = 0 + a + 0a = a$. Now, let a' be such that $a * a' = 0$. Then $a + a' + aa' = 0$ so that $a' = -a/(1 + a)$. Since $a \neq -1$, we have $a' \in \mathbb{R} - \{-1\}$. Also $a' * a = \frac{-a}{1+a} * a = \frac{-a}{1+a} + a + \frac{-a^2}{1+a} = 0$. Hence a' is the inverse of a and so G is a group. □

20. In $\mathbb{R}^*$ we define $a * b = (1/2)ab$. Then $(\mathbb{R}^*, *)$ is a group.

Proof. Obviously $*$ is a binary operation in $\mathbb{R}^*$. Let $a, b, c \in \mathbb{R}^*$. Then $(a * b) * c = [(1/2)ab] * c = (1/4)abc = a * (b * c)$. Hence $*$ is associative. Let $e \in \mathbb{R}^*$ be such that $a * e = a$. Therefore $(1/2)ae = a$ and hence $e = 2$. Let $a \in \mathbb{R}^*$. Let $b \in R^*$ be such that $a * b = 2$. Then $a \in \mathbb{R}^*$ be such that $a * b = 2$. Then $(1/2)ab = 2$, (i.e) $b = 4/a$. Thus $a * (4/a) = 1/2(4/a)a = 2$ i.e., $(4/a)$ is the inverse of a. Thus $(\mathbb{R}^*, *)$ is a group. □

21. Let $f_a : \mathbb{R} \to \mathbb{R}$ be the function defined by $f_a(x) = x + a$. Then $G = \{f_a : \ a \in \mathbb{R}\}$ is a group under composition of functions.

Proof. (21) Let $f_a, f_b \in G$. Then $(f_a \circ f_b)(x) = (f_a(f_b(x))) = f_a(x + b) = x + b + a = f_{b+a}(x)$. Hence $f_a \circ f_b = f_{b+a} \in G$. We know that composition of mappings is associative. Also $f_a \circ f_0 = f_a = f_0 \circ f_a$ and so f_0 is the identity. Also $f_a \circ f_{-a} = f_0 = f_{-a} \circ f_a$. Hence f_{-a} is the inverse of f_a. Hence G is a group. □

Definition 1.4.3. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$. Let $a, b \in \mathbb{Z}_n$. Then $a + b = qn + r$ where $0 \leq r < n$. We define $a \oplus b = r$. Let $ab = q'n + s$ where $0 \leq s < n$. We define $a \odot b = s$. The binary operations $\oplus$ and $\odot$ are called *addition modulo n* and *multiplication modulo n* respectively.

Examples 1.4.4. Show that $(\mathbb{Z}_n, \oplus)$ is a group.

Proof. Clearly $\oplus$ is a binary operation in $\mathbb{Z}_n$. Let $a, b \in \mathbb{Z}_n$. Then

$$\begin{aligned} a + b &= q_1 n + r_1 \text{ where } 0 \leq r_1 < n \quad (1.3) \\ b + c &= q_2 n + r_2 \text{ where } 0 \leq r_2 < n \quad (1.4) \\ r_1 + c &= q_3 n + r_3 \text{ where } 0 \leq r_3 < n \quad (1.5) \end{aligned}$$

and so $a + b + c = (q_1 + q_3)n + r_3$ and $a + q_2 n + r_2 = (q_1 + q_3)n + r_3$. Hence $a + r_2 = q_4 n + r_3 \quad where \quad q_4 = q_1 + q_3 - q_2$. Now $(a \oplus b) \oplus c = r_1 \oplus c = r_3$. Also $a \oplus (b \oplus c) = a \oplus r_2 = r_3$. Hence $\oplus$ is associative. Clearly the identity element is 0 and the inverse of $a \in \mathbb{Z}_n$ is $n - a$. Hence $(\mathbb{Z}_n, \oplus)$ is a group. □

2. Let n be a prime. Then $\mathbb{Z}_n - \{0\}$ is a group under multiplication modulo n.

Proof. Let $a, b \in \mathbb{Z}_n - \{0\}$. Then $a \neq 0$ and $b \neq 0$. Now, by definition $a \odot b \in \mathbb{Z}_n$. We claim that $a \odot b \neq 0$. Suppose $a \odot b = 0$. Then $n|ab$. Since n is prime, $n|a$ or $n|b$ and so $a = 0$ or $b = 0$ which is a contradiction. Hence $a \odot b \in \mathbb{Z}_n - \{0\}$. Now, let $a, b, c \in \mathbb{Z}_n - \{0\}$. Clearly

$$\begin{aligned} ab &= q_1 n + r_1 \text{ where } 0 \leq r_1 < n \quad (1.6) \\ bc &= q_2 n + r_2 \text{ where } 0 \leq r_2 < n \quad (1.7) \\ r_1 c &= q_3 n + r_3 \text{ where } 0 \leq r_3 < n \quad (1.8) \end{aligned}$$

Thus $abc = q_1 nc + r_1 c$ and so $a(q_2 n + r_2) = q_1 cn + q_3 n + r_3$. Hence $ar_2 = q_4 n + r_3$, where $q_4 = q_1 c + q_3 - aq_2$. Now, $(a \cdot b) \cdot c = r_1 \cdot c = r_3$. Also, $a \cdot (b \cdot c) = a \cdot r_2 = r_3$. Thus $a \cdot b) \cdot c = a \cdot (b \cdot c)$ and hence $\odot$ is associative. Clearly $1 \in \mathbb{Z}_n - \{0\}$ is the identity element. Let $a \in \mathbb{Z}_n - \{0\}$. Since n is prime $(a, n) = 1$. Hence the linear congruence $ax \equiv 1 (mod\ n)$ has a unique solution, say, $b \in \mathbb{Z}_n - \{0\}$. Clearly $a \cdot b = b \cdot a = 1$. Thus b is the inverse of a. Hence $\mathbb{Z}_n - \{0\}$ is a group. □

3. The set of all positive integers less than n and prime to it is a group under multiplication modulo n.

Proof. Let $G = \{m : \ m < n \text{ and } (m, n) = 1\}$. Let $p, q \in G$. Obviously $pq \neq n$

and $(pq, n) = 1$. Now let $pq = sn + r$, $0 < r < n$. Then $p \odot q = r$. We claim that $(r, n) = 1$. Suppose $(r, n) = a > 1$. Then $a|r$ and $a|n$. Hence $a|(r + sn)$ i.e., $a|pq$. Also $a|n$. Hence $(pq, n) \neq 1$ which is a contradiction. Thus $r \in G$ and so G is closed under $\oplus$. We know that multiplication modulo n is associative. Clearly $1 \in G$ is the identity element. Let $a \in G$. Then $(a, n) = 1$. Hence the linear congruence $ax \equiv 1(mod\ n)$ has a unique solution for x say b. Clearly $ab \equiv 1(mod\ n)$ and so $a \odot b = 1$. Now we have to prove that $b \in G$. Suppose $(b, n) = c$. Since $ab \equiv 1(mod\ n), ab = qn + 1$. Now $c|b$ and $c|n \Rightarrow c|(ab - qn) \Rightarrow c|1 \Rightarrow c = 1$. Thus $(b, n) = 1$ and $b \in G$ and is the inverse of a. Thus G is a group. □

4. Let G denotes the set of all matrices of the form $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ where $x \in \mathbb{R}^*$. Then G is a group under multiplication.

Proof. Let $A, B \in G$. Let $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ and $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix}$.

Then $AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G$. We know that matrix multiplication is associative.

Let $E = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$ be such that $AE = A$. Then $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$ and so $\begin{pmatrix} 2xe & 2xe \\ 2xe & 2xe \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$. Therefore $2xe = x$ and $e = 1/2$. Hence $E = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is the identity element of G. Let $\begin{pmatrix} y & y \\ y & y \end{pmatrix}$ be the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$. Then $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ and so $\begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$. Thus $2xy = 1/2$ and $y = x/4$. Inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ is $\begin{pmatrix} x/4 & x/4 \\ x/4 & x/4 \end{pmatrix}$. Hence G is a group. □

5. In $\mathbb{N}$ we define $a * b = a$. Then $(\mathbb{N}, *)$ is not a group.

Proof. Clearly $*$ is an associative binary operation on $\mathbb{N}$. However, there is no element

$e \in \mathbb{N}$ such that $e * a = a$ for all $a \in \mathbb{N}$. Hence there is no identity element in $(\mathbb{N}, *)$. Hence $(\mathbb{N}, *)$ is not a group. □

Definition 1.4.5. A group G is said to be *abelian* if $ab = ba$ for all $a, b \in G$. A group which is not abelian is called a *non-abelian* group.

Examples 1.4.6.

1. $\mathbb{Z} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ under usual multiplication are abelian groups.
2. $(\varrho(S), \triangle)$ is an abelian group, since $A \triangle B = B \triangle A$ for all $A, B \in \varrho(S)$.
3. $(\mathbb{Z}_n, \oplus)$ is an abelian group.

1.5 Elementary Properties of a Group

Theorem 1.5.1. Let G be a group. Then
(i)] There exists a unique identity element $e \in G$ such that $e * a = a = a * e$ for all $a \in G$.
(ii) For all $a \in G$, there exists a unique inverse $a' \in G$ such that $a * a' = e = a' * a$.

Proof. (i) Now G is group. Therefore, by (G2), there exists $e \in G$ such that $e * a = a = a * e$ for all $a \in G$. Suppose, let e and e' be two identity elements of G. Then $ee' = e'$ (since e is an identity element). Also $ee' = e$(since e' is an identity element). Hence $e = e'$.

(ii) Let $a \in G$. By (G3), there exists $a' \in G$ such that $a * a' = e = a' * a$. Suppose there exists $a'' \in G$ such that $a * a'' = e = a'' * a$. We show that $a' = a''$. Now

$$\begin{aligned} a' &= a' * e = a' * (a * a'')(\text{substituting } e = a * a'') \\ &= (a' * a) * a'' = e * a''(\text{because } a' * a = e) = a''. \end{aligned}$$

Thus, a' is unique. □

We denote the inverse of a by a^{-1}.

Theorem 1.5.2. *In a group, the left and right cancellation laws hold (i.e,) $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.*

Proof. Suppose $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c$. Similarly, we can prove that $ba = ca \Rightarrow b = c$. □

Theorem 1.5.3. *Let G be a group and $a, b \in G$. Then the equation $ax = b$ and $ya = b$ have unique solutions for x and y in G.*

Proof. Consider $a^{-1}b \in G$. Then $a(a^{-1}b) = (aa^{-1})b = eb = b$. Hence $a^{-1}b$ is a solution of $ax = b$. Now, to prove the uniqueness, let x_1 and x_2 be two solutions of $ax = b$. Then $ax_1 = b$ and $ax_2 = b$. Therefore $ax_1 = ax_2$ which implies $x_1 = x_2$. Hence $x = a^{-1}b$ is the unique solution for $ax = b$. Similarly we can prove that $y = ba^{-1}$ is the solution of the equation $ya = b$. □

Theorem 1.5.4. *Let G be a group. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.*

Proof. Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly $(b^{-1}a^{-1})(ab) = e$. Hence $(ab)^{-1} = b^{-1}a^{-1}$. Proof of the second part is obvious. □

Corollary 1.5.5. *If $a_1, a_2, \ldots, a_n \in G$ then $(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_1^{-1}$.*

Definition 1.5.6. Let G be a group and $a \in G$. For any positive integer n, we define $a^n = aa\cdots a$(a written n times). Clearly $(a^n)^{-1} = (aa\cdots a)^{-1} = (a^{-1}a^{-1}\cdots a^{-1}) = (a^n)^{-1}$. Now we define $a^{-n} = (a^{-1})^n = (a^n)^{-1}$. Finally we define $a^0 = e$. Thus a^n is defined for all integers n.

When the binary operation on G is "+", we denote $a + a + \cdots + a$ (a written n times) as na.

Theorem 1.5.7. *Let G be a group and $a \in G$. Then*
(i) $a^ma^n = a^{m+n}$, $m, n \in \mathbb{Z}$.
(ii) $(a^m)^n = a^{mn}$, $m, n \in \mathbb{Z}$.

Proof. (i) When $n = 0$ the result follows directly from the definition. Now let $n > 0$. We prove the result by induction n. When $m \geq 0$, $a^{m+1} = a^ma^1$(by definition). When $m = -1$, $a^{m+1} = a^0 = e$ and $a^ma^1 = a^{-1}a = e$. Hence $a^{m+1} = a^ma^1$.

When $m \leq -2$, let $m = -p$, where $p \geq 2$.

$\therefore (a^m)a = (a^{-p})a = (a^{-1})^p a = (a^{-1})^{p-1}a^{-1}a = (a^{-1})^{p-1} = a^{-p+1} = a^{m+1}$

Hence $a^{m+1} = a^m a^1$, for all $m \in \mathbb{Z}$ and so the result is true for $n = 1$. Suppose now that the theorem is valid for $n = k > 1$. Then $a^m a^k = a^{m+k}$.

$$\begin{aligned} a^m a^{k+1} &= a^m(a^k a) = (a^m a^k)a = a^{m+k}a \text{ (hypothesis)} \\ &= a^{m+k+1} \text{ (by definition)} \end{aligned}$$

Thus is follows that the theorem is valid for $n = k+1$. Hence by induction the theorem holds for all positive integers n. Finally if $n < 0$, we can prove the result by induction on $-n$.

(ii) Obvious. □

Problem 1.5.8. Show that, in a group G, $x^2 = x$ if and only if $x = e$.

Solution. Clearly $e^2 = ee = e$. Conversely, let $x^2 = x$. Then $xx = xe$. Hence by cancellation law $x = e$.

An element $a \in G$ is called *idempotent* if $a^2 = a$. Thus we have shown that in a group G. the identity element is the only idempotent element.

Problem 1.5.9. In an abelian group, $(ab)^2 = a^2b^2$.

Solution. Clearly $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$.

In general for any positive integer n, $(ab)^n = a^n b^n$ (prove by using induction)

Problem 1.5.10. *Let G be a group such that $a^2 = e$ for all $a \in G$. Then G is abelian.*

Solution. Since $a^2 = e$, $aa = e \Rightarrow a = a^{-1}$. Now, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Hence G is abelian.

Problem 1.5.11. *Let G be a group in which $(ab)^m = a^m b^m$ for three consecutive integers and for all $a, b \in G$. Then G is abelian.*

Solution. Let $a, b \in G$. Then by hypothesis, $(ab)^m = a^m b^m$; $(ab)^{m+1} = a^{m+1}b^{m+1}$ and $(ab)^{m+2} = a^{m+2}b^{m+2}$. Now, $(ab)^{m+1} = a^{m+1}b^{m+1} \Rightarrow (ab)^m(ab) = (a^m a)(b^m b)$ $\Rightarrow (a^m b^m)(ab) = (a^m a)(b^m b)$. Hence $b^m a = ab^m$ (by cancellation law).

Similarly $(ab)^{m+2} = a^{m+2}b^{m+2} \Rightarrow b^{m+1}a = ab^{m+1} \Rightarrow b^m ba = ab^m b \Rightarrow b^m ba = b^m ab$ and so $ba = ab$. Hence G is abelian.

Problem 1.5.12. Let $(H, \cdot)$ and $(K, *)$ be groups. We define a binary operation $\Box$ on $H \times K$ by $(h_1, k_1)\Box(h_2, k_2) = (h_1h_2, k_1 * k_2)$. Then $H \times K$ is a group. ($H \times K$ is called the *direct product* of H and K).

Solution. First we shall prove that $\Box$ is associative. Let $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$.

$$[(h_1, k_1)\Box(h_2, k_2)]\Box(h_3, k_3) = (h_1h_2, k_1 * k_2)\Box(h_3, k_3) = ((h_1h_2)h_3, (k_1 * k_2) * k_3)$$
$$= ((h_1(h_2h_3), k_1 * (k_2 * k_3)) = (h_1, k_1)\Box(h_2h_3, k_2 * k_3) = (h_1, k_1)\Box[(h_2, k_2)\Box(h_3, k_3)].$$

Let e, e_1 be the identities of the groups H and K respectively. Clearly (e, e_1) is the identity element in $H \times K$. Also (h^{-1}, k^{-1}) is the inverse of (h, k). Hence $H \times K$ is a group.

1.6 Permutation Groups

Definition 1.6.1. Let A be a finite set. A bijection from A to itself is called a permutation of A.

For example, if $A = \{1, 2, 3, 4\}$ $f : A \longrightarrow A$ given by $f(1) = 2, f(2) = 1, f(3) = 4$ and $f(4) = 3$ is a permutation of A. We shall write this permutation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. An element in the bottom row is the image of the element just above it in the upper row.

Definition 1.6.2. Let A be a finite set containing n elements. The set of all permutations of A is clearly a group under the composition of functions. This group is called the *symmetric group* of degree n and is denoted by S_n.

Example 1.6.3. Let $A = \{1, 2, 3\}$. Then S_3 consists of $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$;
$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$; $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$;
$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. In this group, e is the identity element. We now compute the product p_1p_2.

$$\begin{array}{rccc} & 1 & 2 & 3 \\ p_1: & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \\ p_2: & \downarrow & \downarrow & \downarrow \\ & 1 & 2 & 3 \end{array} \quad \text{Hence } p_1p_2: \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{array}$$

So that $p_1p_2 = e$. Now, $p_1p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = p_5$. Similarly we can compute all other products and Cayley table for this group is given by

	e	p_1	p_2	p_3	p_4	p_5
e	e	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	e	p_4	p_5	p_3
p_2	p_2	e	p_1	p_5	p_3	p_4
p_3	p_3	p_5	p_4	e	p_2	p_1
p_4	p_4	p_3	p_5	p_1	e	p_2
p_5	p_5	p_4	p_3	p_2	p_1	e

Thus S_3 is a group containing $3! = 6$ elements.

In S_3, $p_1p_2 = p_2p_1 = e$ so that the inverse of p_1 is p_2. In general the inverse of a permutation can be obtained by interchanging the rows of the permutation.

For example, if $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$ then the inverse of p is the permutation given by $p^{-1} = \begin{pmatrix} 3 & 4 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$.

In S_3, $p_1p_4 = p_5$ and $p_4p_1 = p_3$. Hence $p_1p_4 \neq p_4p_1$ so that S_3 is non-abelian.

The symmetric group S_n containing $n!$ elements, for, let $A = \{1, 2, \ldots, n\}$. Any permutation on A is given by specifying the image of each element. The image of 1 can be chosen in n different ways. Since the image of two is different from the image of 1, it can be chosen in $(n-1)$ different ways and so on. Hence the number of permutations of A is $n(n-1)\cdots 2\cdot 1 = n!$ so that the number of elements in S_n is $n!$.

Definition 1.6.4. Let G be a finite group. Then the number of elements in G is called the order of G and is denoted by $|G|$ or $o(G)$.

Definition 1.6.5. Let p be a permutation on $A = \{1, 2, \ldots, n\}$. p is called *a cycle* of length r if there exist distinct symbols $a_1, a_2, \ldots, a_r$ such that $p(a_1) = a_2, p(a_2) = a_3, \ldots, p(a_{r-1}) = a_r$, and $p(a_r) = a_1$, and $p(b) = b$ for all $b \in A - \{a_1, a_2, \ldots, a_r\}$. This cycle is represented by the symbol $(a_1, a_2, \cdots, a_r)$.

Thus under the cycle $(a_1, a_2, \cdots, a_r)$ each symbol is mapped onto the following symbol except the last one which is mapped onto the first symbol and all the other symbols not in the cycle are fixed.

Example 1.6.6. Let $A = \{1, 2, 3, 4, 5\}$. Consider the cycle of length 4 given by $p = (2451)$. Then $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ and so $(2451) = (4521) = (5124) = (1245)$.

Remark 1.6.7. Since cycles are special types of permutations, they can be multiplied in the usual way. The product of cycles need not be a cycle.

For example, let $p_1 = (234)$ and $p_2 = (1, 5)$. Then $p_1p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$ which is not a cycle.

Definition 1.6.8. Two cycles are said to be disjoint if they have any no symbols in common.

For example (2 1 5) and (3 4) are disjoint cycles.

Remark 1.6.9. If p_1 and p_2 are disjoint cycles the symbols which are moved by p_1 are fixed by p_2 and vice versa. Hence multiplication of disjoint cycles is commutative.

Examples 1.6.10. (1) Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 6 & 7 & 4 \end{pmatrix}$.
We shall write this permutation as a product of disjoint cycles. First of all 1 is moved to

2 and then 2 is moved to 1 thus giving the cycle (1 2). The element 3 is left fixed. Again starting with 4, 4 is moved to 5, 5 is moved to 6, 6 is moved to 7 and 7 is moved to 4, thus giving the cycle (4 5 6 7). Thus $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 6 & 7 & 4 \end{pmatrix} = (12)(4567) = (4567)(12)$

(2) Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 5 & 4 & 1 & 6 \end{pmatrix} \in S_7$. Starting with 1 we get the cycle (1 2 3 7 6). The elements 4,5 do not appear in it. Starting with 4 we get the cycle (4 5). Each element of the set $\{1, 2, \ldots, 7\}$ occurs in one of the two cycles. Thus $\alpha = (12376)(45)$.

(3) Consider the permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix}$. Clearly $\alpha = (143)(265)$.

Theorem 1.6.11. *Any permutation can be expressed as a product of disjoint cycles.*

Proof. Let p be a given permutation of the set $S = \{1, 2, \ldots, n\}$. Let us start with any symbol $a_1 \in S$. Let $p(a_1) = a_2, p(a_2) = a_3, \ldots$. Since S is finite, these symbols cannot all the distinct and hence there exists a least positive integer r such that $1 \leq r \leq n$ and $p(a_r) = a_1$.

Let $c = (a_1, a_2, \cdots, a_r)$. If $r = n$ then $p = c$ so that p is cycle. If $r < n$, let b_1 be a symbol in S such that $b_1 \notin (a_1, a_2, \cdots, a_r)$. Starting with b_1 we can construct the cycles $d = (b_1, b_2, \cdots, b_s)$ as before. Clearly the cycles c and d are disjoint. If $r + s = n$ then $p = cd$. If $r + s < n$ then we repeat this process to obtain more cycles until all symbols appear in one of the cycles. Thus we get a decomposition of p into disjoint cycles. □

The decomposition of a permutation into disjoint cycles is unique except for the order of the factors.

Definition 1.6.12. A cycle of length two is called a *transposition* . Thus a transposition $(a_1 a_2)$ interchanges the symbols a_1 and a_2 and leaves all the other elements fixed.

Theorem 1.6.13. *Any permutation can be expressed as a product of transpositions.*

Proof. Since any permutation is a product of disjoint cycles it is enough to prove that each cycle is a product of transpositions. Let $c = (a_1a_2\cdots a_1)$ be a cycle. Then $(a_1a_2\cdots a_1) = (a_1a_2)(a_2a_3)\cdots(a_1a_r)$. This proves the theorem. □

Examples 1.6.14. (i) Let $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1245) = (12)(14)(15)$. Then $(1245) = (2451) = (24)(25)(21)$ and so the representation of a permutation as a product of transpositions is unique.

(ii) Clearly $(1345)(26) = (13)(14)(15)(26) = (13)(12)(12)(14)(15)(26)$. Thus in the representation of a permutation as a product of transpositions one can always insert $(ab)(ab)$ in any place since $(ab)(ab)$ is the identity permutation.

Theorem 1.6.15. *If a permutation $p \in S_n$ is a product of r transpositions and also a product of s transpositions then either r and s are both even or both odd.*

Proof. Let $p = t_1t_2\cdots t_r = t_1^1t_2^1\cdots t_s^1$ where t_i, t_i^1 are transpositions. Now consider the polynomial in n variables $x_1, x_2, \cdots, x_n$ given by

$$\triangle = (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n) \times (x_2 - x_3)(x_2 - x_4)\cdots(x_2 - x_n) \\ \times \cdots\cdots \times (x_{n-1} - x_n) = \prod_{i<j}(x_i - x_j)$$

For any permutation $p \in S_n$ we define

$$p(\triangle) = \textstyle\prod_{i<j}(x_{p(i)} - x_{p(j)}).$$

Consider the transposition $t = (ij)$. Then the factor $x_i - x_j$ in $\triangle$ becomes $x_j - x_i$. Any factor of $\triangle$ in which neither i nor j is equal to k or l is unchanged. All other factors of $\triangle$ can be paired to form products of the form $\pm(x_i - x_k)(x_k - x_j)$, the sign being determined by the relative magnitudes of i, j and k. Since t interchanges x_i and x_j any such product is unchanged. Hence the effect of the transposition t on $\triangle$ is just to change the sign of $\triangle$ i. e, $t(\triangle) = -\triangle$. Therefore $p(\triangle) = (t_1t_2\cdots t_r)(\triangle) = (-1)^r\triangle$. Also $p(\triangle) = (t_1^1t_2^1\cdots t_r^1)(\triangle) = (-1)^s\triangle$. Therefore $(-1)^r = (-1)^s \Rightarrow r$ and s are both even or both odd. □

Definition 1.6.16. A permutation $p \in S_n$ is called *even* or *odd* according as p can be expressed as a product of an even number of transpositions or an odd number of transpositions respectively.

Examples 1.6.17. (i) Consider the permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 7 & 2 & 5 \end{pmatrix}$ and $p = (134)(26)(57) = (13)(14)(26)(57)$. Therefore p is a product of 4 transposition. Hence p is an even permutation.

(ii) Consider the permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$
$p = (1256)(34)(89) = (12)(15)(16)(34)(89)$. Therefore p is a product of 5 transposition and so p is an odd permutation.

Theorem 1.6.18. *(i) The product of two even permutations is an even permutation.*
(ii) The product of two odd permutations is an even permutation.
(iii) The product of an even permutation and an odd permutation is an odd permutation.
(iv) The inverse of an even permutation is an even permutation.
(v) The inverse of an odd permutation is an odd permutation.
(vi) The identity permutation e is an even permutation.

Proof. Let p_1, p_2 be two permutations. If p_1 is a product of r transpositions and p_2 is a product of s transposition, then p_1p_2 is a product of $r + s$ transpositions. Hence (i), (ii) and (iii) follows. Now suppose that a permutation p is a product of r transpositions, say, $p = t_1, t_2, \ldots, t_r$. Then $p^{-1} = (t_1, t_2, \cdots, t_r)^{-1} = t_r^{-1} \cdots t_2^{-1} t_1^{-1} = t_r \cdots t_2 t_1$ and so p^{-1} is also a product of r transpositions. This proves (iv) and (v). Now, $e = (12)(12)$ and hence e is an even permutation which proves (vi). □

Theorem 1.6.19. *Let A_n be the set of all even permutations in S_n. Then A_n is a group containing $\frac{n!}{2}$ permutations.*

Proof. From (i),(vi) and (iv) of Theorem 1.6.18, we see that A_n is a group.
Now let B_n be the set of all permutations in S_n. Define $f : A_n \to B_n$ by $f(p) = (12)p$. Suppose $f(p_1) = f(p_2) \Rightarrow (12)p_1 = (12)p_2 \Rightarrow p_1 = p_2$. Hence f is 1-1. If $\alpha \in B_n$, then

$(12)\alpha \in A_n$ and $f[(12)\alpha] = (12)(12)\alpha = \alpha$. Hence f is onto. Thus f is a bijection and hence the number of odd permutations in S_n =the number of even permutations in S_n. Since S_n contains $n!$ permutations, A_n has $\frac{n!}{2}$ elements. □

Definition 1.6.20. The group A_n of all even permutations in S_n is called the *alternating group* on n symbols.

1.7 Subgroups

Definition 1.7.1. Let G be a set with binary operation $*$ defined on it. Let $S \subseteq G$. If for each $a, b \in S$, $a * b$ is in S, we say that S is *closed* with respect to the binary operation $*$.

Examples 1.7.2. (i) $(\mathbb{Z}, +)$ is a group. The set $\mathbb{E}$ of all even integers is closed under $+$ and further $(\mathbb{E}, +)$ is itself a group.

(ii) The set of G of all non-singular 2×2 matrices form a group under matrix multiplication. Let H be the set of all matrices of the form $\begin{pmatrix} cos\ \theta & -sin\ \theta \\ sin\ \theta & cos\ \theta \end{pmatrix}$. Then H is subset of G and H itself a group under matrix multiplication.

Definition 1.7.3. A subset H of group G is called *subgroup* of G if H forms a group with respect to the binary operation in G.

Examples 1.7.4. (i) Let G be any group. Then $\{e\}$ and G are trivial subgroups of G. They are called improper subgroups of G.

(ii) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$ and $(\mathbb{R}, +)$ is a subgroup of $(\mathbb{C}, +)$.

(iii) In $(\mathbb{Z}_8, \oplus)$, let $H_1 = \{0, 4\}$ and $H_2 = \{0, 2, 4, 6\}$. The Cayley tables for H_1 and H_2 are given by

$\oplus$	0	4
0	0	4
4	4	0

$\oplus$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

It is easily seen that H_1 and H_2 are closed under $\oplus$ and $(H_1, \oplus)$ and $(H_2, \oplus)$ are groups. Hence H_1 and H_2 are subgroups of $\mathbb{Z}_8$.

(iv) $\{1, -1\}$ is a subgroup of $(\mathbb{R}^*, \cdot)$.

(v) $\{1, i, -1, -i\}$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

(vi) For any integer n we define $n\mathbb{Z} = \{nx : \ x \in \mathbb{Z}\}$. Then $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. For, let $a, b \in n\mathbb{Z}$. Then $a = nx$ and $b = ny$ where $x, y \in \mathbb{Z}$. Hence $a + b = n(x + y) \in n\mathbb{Z}$ and so $n\mathbb{Z}$ is closed under $+$. Clearly $0 \in n\mathbb{Z}$ is the identity element. Inverse of nx is $-nx = n(-x) \in n\mathbb{Z}$. Hence $(n\mathbb{Z}, +)$ is a group.

(vii) In the symmetric group S_3, $H_1 = \{e, p_1, p_2\}; H_2 = \{e, p_3\}; H_3 = \{e, p_4\}$; and $H_4 = \{e, p_5\}$ are subgroups.

(viii) A_n is a subgroup of S_n.

(ix) The set of permutations $H = \{e, p_1, p_2, p_3\}$, where $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}; p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, is a subgroup of S_4.

In all the above examples we see that the identity element in the subgroup is the same as the identity element of the group.

Theorem 1.7.5. *Let H be a subgroup of G. Then*

(a) the identity element of H is the same as that of G.

(b) for each $a \in H$ the inverse of a in H is the same as the inverse of a in G.

Proof. (a) Let e and e' be the identity of G and H respectively. Let $a \in H$. Now,

$$e'a = a (\text{since e' is the identity of } H)$$
$$= ea (\text{since e' is the identity of } G \text{ and } a \in G)$$
$$\therefore \quad e'a = ea \Rightarrow e' = a (\text{by cancellation law})$$

(b) Let a' and a'' be the inverse of a in G and H respectively. Since by (a), G and H have the same identity element e, we have $a'a = e = a''a$. Hence by cancellation law, $a' = a''$. □

Theorem 1.7.6. *A subset H of a group G is a subgroup of G if and only if*
(i) it is closed under the binary operation in G.
(ii) The identity e of G is in H. (iii) $a \in H \Rightarrow a^{-1} \in H$.

Proof. Let H be subgroup of G. The result follows immediately from Theorem 1.7.5.

Conversely, let H be a subset of G satisfying conditions (i), (ii) and (iii). Then, obviously H itself a group with respect to the binary operation in G. Therefore H is a subgroup of G. □

Theorem 1.7.7. *A non-empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.*

Proof. Let H be a subgroup of G. Then $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow ab^{-1} \in H$. Conversely, suppose H is a non-empty subset of G such that $a, b \in H \Rightarrow ab^{-1} \in H$. Since $H \neq \emptyset$, there exists $a \in H$. Hence $a, a^{-1} \in H$. Therefore, $e = aa^{-1} \in H$, i.e., H contains the identity element e. Also, since $a, b \in H$. $ea^{-1} \in H$. Hence $a^{-1} \in H$. Now, let $a, b \in H$. Then $a, b^{-1} \in H$. Hence $a(b^{-1})^{-1} = ab \in H$ and so H is closed under the binary operation in G. Hence by Theorem 1.7.8, H is a subgroup of G. □

If the operation is $+$ then H is a subgroup of G if and only if $a, b \in H \Rightarrow a - b \in H$.

Theorem 1.7.8. *Let H be a non-empty finite subset subset of G. If H is closed under the operation in G then H is a subgroup of G.*

Proof. Let $a \in H$. Then $a, a^2, \ldots, a^n, \ldots$ are all elements of H. But since H is finite the elements $a, a^2, a^3 \ldots,$ cannot all be distinct. Hence let $a^r = a^s, r < s$. Then $a^{s-r} = e \in H$. Now, let $a \in H$. We have proved that $a^n = e$ for some n. Hence $aa^{n-1} = e$. Hence $a^{-1} = a^{n-1} \in H$. Thus H is a subgroup of G. □

Theorem 1.7.8 is not true if H is infinite. For example, $\mathbb{N}$ is an infinite subset of $(\mathbb{Z}, +)$ and $\mathbb{N}$ is closed under addition. However $\mathbb{N}$ is not a subgroup of $(\mathbb{Z}, +)$.

Theorem 1.7.9. *If H and K are subgroups of a group G then $H \cap K$ is also a subgroup of G.*

Proof. Clearly $e \in H \cap K$ and so $H \cap K$ is non-empty. Now let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$. Therefore $ab^{-1} \in H \cap K$. Hence by Theorem 1.7.8, $H \cap K$ is a subgroup of G. □

It can be similarly proved that the intersection of any number of subgroups of G is again a subgroup of G.

The union of two subgroups of a group need not be a subgroup. For example, $2\mathbb{Z}$ and $3\mathbb{Z}$ are subgroups of $(\mathbb{Z}, +)$ but $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$ since $3, 2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ but $3 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Theorem 1.7.10. *The union of two subgroups of a group G is a subgroup if and only if one is contained in the other.*

Proof. Let H and K be two subgroups of G such that one is contained in the other. Then either $H \subseteq K$ or $K \subseteq H$. Therefore $H \cup K = K$ or $H \cup K = H$. Hence $H \cup K$ is a subgroup of G.

Conversely, suppose H is not contained in K and K is not contained in H. Then there exist elements a, b such that $a \in H$, $a \notin K$, $b \in K$, and $b \notin H$.

Clearly $a, b \in H \cup K$. Since $H \cup K$ is a subgroup of G $ab \in H \cup K$. Hence $ab \in H$ or $ab \in K$. If $ab \in H$, then $a^{-1} \in H$ since $a \in H$. Hence $a^{-1}(ab) = b \in H$, a contradiction. If $ab \in K$, $b^{-1} \in K$ since $b \in K$. Hence $(ab)b^{-1} = a \in K$, a contradiction. Hence our assumption that H is not contained in K and K is not contained in H is false. Therefore $H \subseteq K$ or $K \subseteq H$. □

Definition 1.7.11. *Let A and B be two subsets of a group G. We define $AB = \{ab : \ a \in A, b \in B\}$.*

If A and B are two subgroups of G, then AB need not be a subgroup of G.

For example, consider $G = S_3$. $A = \{e, p_3\}$ and $B = \{e, p_4\}$. Then A and B are subgroups of S_3. Also $AB = \{ee, ep_4, ep_3, p_3p_4\} = \{e, p_4, p_3, p_2\}$. Now, $p_4p_2 = p_5 \notin AB$. Hence AB is not a subgroup of S_3.

Theorem 1.7.12. *Let H and K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.*

Proof. Suppose HK is a subgroup of G. Let $kh \in KH$, where $h \in H$ and $k \in K$. Now $h = he \in HK$ and $k = ek \in HK$. Because HK is a subgroup, it follows that $kh \in HK$. Hence, $KH \subseteq HK$. On the other hand, let $hk \in HK$. Then $(hk)^{-1} \in HK$, so $(hk)^{-1} = h_1k_1$ for some $h_1 \in H$ and $k_1 \in K$. Thus, $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$. This implies that $HK \subseteq KH$. Hence, $HK = KH$.

Conversely, suppose $HK = KH$. Let $h_1k_1, h_2k_2 \in HK$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We show that $(h_1k_1)(h_2k_2)^{-1} \in HK$. Now $k_2 \in K$ and $h_2 \in H$. Therefore, $k_2^{-1}h_2^{-1} \in KH = HK$. This implies that $k_2^{-1}h_2^{-1} = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$. Similarly, $k_1h_3 \in KH = HK$, so $k_1h_3 = h_4k_4$ for some $h_4 \in H$ and $k_4 \in K$. Thus,

$$\begin{aligned}(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1}(\text{because } (h_2k_2)^{-1} = k_2^{-1}h_2^{-1})\\ &= h_1k_1h_3k_3(\text{substitute } k_2^{-1}h_2^{-1} = h_3k_3)\\ &= h_1h_4k_4k_3 \in HK(\text{substitute } k_1h_3 = h_4k_4)\end{aligned}$$

Hence, HK is a subgroup of G. □

Corollary 1.7.13. *If A and B are subgroups of an abelian group G, then AB is a subgroup of G.*

Proof. Let $x \in AB$. Then $x = ab$ where $a \in A$ and $b \in B$. Since G is abelian, $ab = ba$ and so $x \in BA$. Hence $AB \subseteq BA$. Similarly $BA \subseteq AB$ and $AB = BA$. Hence AB is a subgroup of G. □

Problem 1.7.14. Let $a \in \mathbb{R}^*$. Let $H = \{a^n : n \in \mathbb{Z}\}$. Then H is a subgroup of $\mathbb{R}^*$.

Solution. Clearly H is non-empty. Now, let $x, y \in H$. Then $x = a^s$ and $y = a^t$ where $s, t \in \mathbb{Z}$. Thus $xy^{-1} = a^s(a^t)^{-1} = a^{s-t} \in H$ and so H is a subgroup of $\mathbb{R}^*$.

Problem 1.7.15. Let H denote the set of all permutations in S_n fixing the symbol 1. Then H is a subgroup of S_n.

Solution. Clearly $e \in H$ and so$H$ is non-empty. Let $\alpha, \beta \in H$. Then α and β fix the symbol 1. Now β fixes the symbol $1 \Rightarrow \beta^{-1}$ fixes the symbol 1. Hence $\alpha\beta^{-1}$ fixes symbol 1. Hence $\alpha\beta^{-1} \in H$. Thus H is a subgroup of S_n.

Problem 1.7.16. Let G be the set of all 2×2 matrices with entries from $\mathbb{R}$. Then G is a group under matrix addition. Let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}$. Then H is a subgroup of G.

Solution. Let $A, B \in H$. Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$. Now $A - B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in H$. Hence H is a subgroup of G.

Problem 1.7.17. Let G be a group. Let $H = \{a : a \in G$ and $ax = xa$ for all $x \in G\}$. (ie) H is the set of all elements which commute with every other element. Show that H is a subgroup of G.

Solution. Clearly $ex = xe = x$ for all $x \in G$. Hence $e \in H$, so that H is non-empty. Now, let $a, b \in H$. Then $ax = xa$ and $bx = xb$ for all $x \in G$. Now, $bx = xb \Rightarrow b^{-1}(bx)b^{-1} = b^{-1}(xb)b^{-1} \Rightarrow (b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1}) \Rightarrow exb^{-1} = b^{-1}xe \Rightarrow xb^{-1} = b^{-1}x$.

Now $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$. Thus ab^{-1} commutes with every element of G and so $ab^{-1} \in H$. Hence H is a subgroup of G.

Note 1.7.18. The above subgroup of G is called the *center* of G and is denoted by $Z(G)$.

Problem 1.7.19. Let G be a group and let a be a fixed element of G. Let $H_a = \{x : x \in G$ and $ax = xa\}$. Show that H_a is a subgroup of G.

Solution. Clearly $ea = ae = a$. Hence $e \in H_a$ so that H_a is non-empty. Then $ax = xa$ and $ay = ya$. Now, $ay = ya \Rightarrow y^{-1}a = ay^{-1}$. Hence $a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(y^{-1}a) = (xy^{-1})a$. Hence xy^{-1} commutes with a, $xy^{-1} \in H_a$ and so H_a is a subgroup of G.

Note 1.7.20. H_a is called the *normalizer* of a in G.

1.8 Cyclic Groups

Definition 1.8.1. Let G be a group. Let $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

H is called the cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

Examples 1.8.2. 1. In $(\mathbb{Z}, +), \langle a \rangle = 2\mathbb{Z}$ which is the group of even integers.

2. In the group $G = (\mathbb{Z}_{12}, \oplus)$, $\langle 3 \rangle = \{0, 3, 6, 9\}$, $\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}$.

3. In the group $G = \{1, i, -1, -i\}$, $\langle i \rangle = \{i, i^2, i^3, \cdots\} = \{i, -1, -i, 1\} = G$.

Definition 1.8.3. Let G be a group and let $a \in G$, a is called a **generator** of G if $\langle a \rangle = G$.

A group G is *cyclic* if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Note 1.8.4. If G is cyclic group generated by an element a, then every element of G is of the form a^n for some $n \in \mathbb{Z}$.

Examples 1.8.5. 1. $(\mathbb{Z}, +)$ is a cyclic group and 1 is the generator of this group. Clearly -1 is also a generator of this group. Thus a cyclic group can have more than one generator.

2. $(n\mathbb{Z}, +)$ is a cyclic group and n and $-n$ are generators of this group.

3. $(\mathbb{Z}_8, \oplus)$ is a cyclic group and $1, 3, 5, 7$ are all generators of this group.

4. $(\mathbb{Z}_n, \oplus)$ is a cyclic group for all $n \in \mathbb{N}$; 1 is a generator of this group. In fact if $m \in \mathbb{Z}_n$ and $(m, n) = 1$ then m is a generator of this group.

5. $G = \{1, i, -1, -i\}$ is a cyclic group under usual multiplication; i is a generator, $-i$ is also a generator of G. However -1 is not a generator of G since $\langle -1 \rangle = \{1, -1\} \neq G$.

6. $G = \{1, \omega, \omega^2\}$ where $\omega \neq 1$ is a cube root of unity is a cyclic group, ω and ω^2 are both generators of this group.

7. In this group $G = (\mathbb{Z}_7 - \{0\}, \odot)$, 3 and 5 are both generators. Here 2 is not a generator of G since $\langle 2 \rangle = \{2, 4, 1\} \neq G$.

8. Let A be a set containing more than one element. Then $(\varrho(A), \triangle)$ is not cyclic; for let $B \in \varrho(A)$ be any element. Then $B \triangle B = \Phi$ so that $\langle B \rangle = \{B, \Phi\} \neq \varrho(A)$.

9. $(\mathbb{R}, +)$ is not a cyclic group since for any $x \in \mathbb{R}, \langle x \rangle = \{nx : \ n \in Z\} \neq \mathbb{R}$

Theorem 1.8.6. *Any cyclic group is abelian.*

Proof. Let $G = \langle a \rangle$ be a cyclic group. Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$. Hence $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$. Hence G is abelian. □

Theorem 1.8.7. *A subgroup of cyclic group is cyclic.*

Proof. Let G be a cyclic group generated by a and let H be a subgroup of G. We claim that H is cyclic. Clearly every element of H is of the form a^n for some integer n. Let m be the smallest positive integer such that $a^m \in H$. We claim that a^m is the generator of H. Let $b \in H$. Then $b = a^n$ for some $n \in \mathbb{Z}$. Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$. Therefore $a^r = (a^m)^{-q} b$. Now, $a^m \in H$. Since H is a subgroup, $(a^m)^{-q} \in H$. Also, $b \in H$. Clearly $a^r \in H$ and $0 \leq r < m$. But m is the least positive integer such that $a^n \in H$. Therefore $r = 0$. Hence $b = a^n = a^{qm} = (a^m)^q$. Every element of H is a power of a^m. Thus $H = \langle a^m \rangle$ and so H is cyclic. □

Chapter 2

UNIT II: Group

2.1 Order of an Element

Definition 2.1.1. Let G be a group and let $a \in G$. The least positive integer n(if it exists) such that $a^n = e$ is called the **order** of a. If there is no positive integer n such that $a^n = e$, then the order of a is said to be infinite.

Examples 2.1.2.

1. Consider the group S_3, $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $p_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_4$ and $p_1^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$.
   In this case, 3 is the least positive integer such that $p_1^3 = e$. Thus p_1 is of order 3.

2. Consider $(\mathbb{R}^*, \cdot)$, From this sequence of elements $2, 2^2, 2^3, \ldots, 2^n, \ldots$. In this case there is no positive integer n such that $2^n = 1$ and $\langle 2 \rangle$ contains infinite numbers of elements. Thus the order 2 is infinite.

Theorem 2.1.3. *Let G be a group and $a \in G$. Then the order of a is the same as the order of the cyclic group generated by a.*

Proof. Let a be an element of order n. Then $a^n = e$. We claim that $e, a, a^2, \ldots, a^{n-1}$ are all distinct. Suppose $a^r = a^s$ where $0 < r < s < n$. Then $a^{s-r} = e$ and $s - r < n$

which contradicts the definition of the order of a. Hence $e, a, a^2, \ldots, a^{n-1}$ are n distinct elements and $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ which is of order n.

If a is of infinite order, the sequence of elements $e, a, a^2, \ldots, a^{n-1}, \ldots$ are all distinct and are in $\langle a \rangle$. Hence $\langle a \rangle$ is an infinite group. □

Theorem 2.1.4. *In a finite group every element is of finite order.*

Proof. Let $a \in G$. If a is of infinite order, then $\langle a \rangle$ is an infinite subgroup of G, which is a contradiction since G is finite. Hence the order of a is finite. □

Remark 2.1.5. The converse of the above theorem is not true, i. e., if G is of group in which every element is of finite order then the group G need not be finite. For example, if S is of infinite set, then $(\varrho(S), \triangle)$ is an infinite group. In this group $A \triangle A = \Phi$ for every $A \in \varrho(S)$ so that the order of every element other than $\emptyset$ is 2.

Theorem 2.1.6. Let G be a group and a be an element of order n in G. Then $a^m = e$ if and only if n divides m.

Proof. Suppose $n|m$. Then $m = nq$ where $q \in \mathbb{Z}$ and $a^m = a^{nq} = (a^n)^q = e^q = e$.

Conversely, let $a^m = e$. Let $m = nq + r$ where $0 \leq r < n$. Now $a^m = a^{nq+r} = a^{nq}a^r = ea^r = a^r$. Thus $a^r = e$ and $0 \leq r < n$. Now, since n is the least positive integer such that $a^n = e$, we have $r = 0$. Hence $m = nq$ and so $n|m$. □

Theorem 2.1.7. Let G be a group and $a, b \in G$. Then
(i) order of a=order of a^{-1}.
(ii) order of a=order of $b^{-1}ab$.
(iii) order of ab=order of ba.

Proof. (i) Let a be an element of order n. Then $a^n = e$ and $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. Now, if possible let $0 < m < n$ and $(a^{-1})^m = e$. Therefore $(a^m)^{-1} = e$ and $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(a^{-1})^n = e$. Hence the order of a^{-1} is n.

(ii) We shall first prove that for any positive integer r. Now $(b^{-1}ab)^r = b^{-1}a^rb$ and is trivially true if $r = 1$. Now, suppose that it is true for $r = k$ so that $(b^{-1}ab)^k = b^{-1}a^kb$.

Then $(b^{-1}ab)^{k+1} = (b^{-1}ab)^k(b^{-1}ab) = (b^{-1}a^kb)(b^{-1}ab) = b^{-1}a^{k+1}b$. Henceit is true for all positive integers. Now, let a be an element of order n. Then $a^n = e$. and so $(b^{-1}ab)^n = b^{-1}a^nb = b^{-1}eb = e$.

Now, if possible, let $0 < m < n$ and $(b^{-1}ab)^m = e$. Then $b^{-1}a^mb = e$ and $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(b^{-1}ab)^n = e$. Therefore the order of $b^{-1}ab$ is n.

(iii) The order of ab =the order of $a^{-1}(ab)a$ =the order of ba by (i). □

Theorem 2.1.8. Let G be a group and let a be an element of order n in G. Then the order of a^s, where $0 < s < n$, is n/d where d is the g.c.d of n and s.

Proof. Let $(n/d) = k$ and $(s/d) = l$ so that k and l are relatively prime. Now, $(a^s)^k = a^{sk} = a^{ldk} = a^{ln} = (a^n)^l = e$. Further if m is any positive integer such that $(a^s)^m = e$ then $a^{sm} = e$. Since order of a is n, we have $n|sm$. Therefore $kd|ldm$ and so $k|lm$. But k and l are relatively prime. Hence $k|m$ so that $m \geq k$. Thus k is the least positive integer such that $(a^s)^k = e$. Hence the order of $a^s = k = n/d$. □

Corollary 2.1.9. The order of any power of a cannot exceed the order of a.

Corollary 2.1.10. Let G be a finite cyclic group of order n generated by an element a. Then a^s generates a cyclic group of order n/d where d is the g.c.d of n and s.

Corollary 2.1.11. Let G be a finite cyclic group of order n generated by an element a. a^s is a generator of G if and only if s and n are relatively prime. Hence the number of generators of a cyclic group of order n is $\phi(n)$ where $\phi(n)$ is the number of positive integers less than n and relatively prime to n.

For example, consider the group $(\mathbb{Z}_{12}, \oplus)$. $\phi(12) = 4$. Hence the group has exactly 4 generators and they are $1, 5, 7$ and 11.

Problem 2.1.12. If G is a finite group with even number of elements then G contains at least one element of order 2.

Solution. Clearly a is an element of order 2 $\Leftrightarrow a^2 = e \Leftrightarrow a^{-1} = a$. Hence it is enough if we prove that there exists an element different from e in G whose inverse is itself.

Let $S = \{a : \ a \in G, a \neq a^{-1}\}$. Then $a \in S \Rightarrow a^{-1} \in S$ and $a \neq a^{-1}$. Hence S contains an even number of elements. Also $e \notin S$. Hence $S \cup \{e\}$ contains an odd number of elements. Since the order of the group is even, there exists at least one element $a \notin S \cup \{e\}$ such that $a = a^{-1}$.

Problem 2.1.13. The order of a permutation p is the l.c.m of the lengths if its disjoint cycles.

Solution. Let $p = c_1 c_2 \cdots c_r$ where the c_i's are mutually disjoint cycles of lengths l_i. Now, let $p^m = e$. Since product of disjoint cycles is commutative, $e = p^m = (c_1 c_2 \ldots c_r)^m = c_1^m c_2^m \cdots c_r^m$. Now, since the elements moved by one cycle are left fixed by all the other cycles, $c_1^m = c_2^m = \cdots = c_r^m = e$. Now, $c_1^m = e \Rightarrow l_1 | m$ since the order of $c_1 = l_1$. Similarly $l_2, l_3, \ldots, l_r$ divide m. Thus m is a common multiple of $l_1, l_2, \ldots, l_r$. Thus the order of p is the least such m which is obviously the l.c.m of $l_1, l_2, \ldots, l_r$.

Problem 2.1.14. If a is a generator of the cyclic group G and if there exist two unequal integers m and n such that $a^m = a^n$, prove that G is a finite group.

Solution. Since m and n are unequal we may assume that $m > n$. Hence $m - n$ is a positive integer. Also $a^m = a^n \Rightarrow a^{m-n} = e$. Therefore the order of a is finite and so $G = \langle a \rangle$ is a finite group.

2.2 Cosets

In S_3, let $H = \{e, p_3\}$. Then H is a subgroup of S_3. This subgroup does not contain the elements p_1, p_2, p_4 and p_5. Let us now perform the binary operation between p_1 and each element of H. We denote the resultant set by the symbol $p_1 H$. Thus $p_1 H = \{p_1 e, p_1 p_3\} = \{p_1, p_4\}$.

Now the element p_2 belongs neither to H nor to $p_1 H$. Therefore, we now perform the binary operation between p_2 and the elements of H. Thus $p_2 H = \{p_2 e, p_2 p_3\} = \{p_2, p_5\}$. The union of the three sets $H, p_1 H, p_2 H$ gives all the elements of S_3 (i. e.,) $S_3 = H \cup p_1 H \cup p_2 H$. Further H, $p_1 H$ and $p_2 H$ are mutually disjoint. Hence $\{H, p_1 H, p_2 H\}$ is a partition of S_3.

Definition 2.2.1. Let H be a subgroup of a group G and $a \in G$. The sets $aH = \{ah : h \in H\}$ and $Ha = \{ha : h \in H\}$ are called the *left* and *right cosets* of H in G, respectively. The element a is called a representative of aH and Ha.

Examples 2.2.2.

1. Let us determine the left cosets of $(5\mathbb{Z}, +)$ in $(\mathbb{Z}, +)$. Here the operation is $+$.
$0 + 5\mathbb{Z} = 5\mathbb{Z}$ is itself a left coset. Another left coset is $1 + 5\mathbb{Z} = \{1 + 5n : n \in \mathbb{Z}\}$. We notice that this left coset contains all integers having remainder 1 when divided by 5. Similarly $2 + 5\mathbb{Z} = \{2 + 5n : n \in \mathbb{Z}\}$, $3 + 5\mathbb{Z} = \{3 + 5n : n \in \mathbb{Z}\}$ and $4 + 5\mathbb{Z} = \{4 + 5n : n \in \mathbb{Z}\}$.

   These are all the left cosets of $(5\mathbb{Z}, +)$ in $\mathbb{Z}$. Here also we note that all the left cosets are mutually disjoint, and their union is $\mathbb{Z}$. In other words the collection of all left cosets forms a partition of the group.

2. Consider $(\mathbb{Z}_{12}, \oplus)$. Then $H = \{0, 4, 8\}$ is a subgroup of G. The left cosets of H are given by $0 + H = \{0, 4, 8\} = H$, $1 + H = \{1, 5, 9\}$, $2 + H = \{2, 6, 10\}$, and $3 + H = \{3, 7, 11\}$. We notice that $4 + H = \{4, 8, 0\} = H$, and $5 + H = \{5, 9, 1\}$ etc.

Theorem 2.2.3. *Let G be a group and H be a subgroup of G. Then*
(i) $a \in H \Rightarrow aH = H$.
(ii) $aH = bH \Rightarrow a^{-1}b \in H$. (iii) $a \in bH \Rightarrow a^{-1} \in Hb^{-1}$.
(iv) $a \in bH \Rightarrow aH = bH$.

Proof. (i) Let $a \in H$. We claim that $aH = H$. Let $x \in aH$. Then $x = ah$ for some $h \in H$. Now, $a \in H$ and $h \in H \Rightarrow ah = x \in H$(since H is a subgroup). Hence $aH \subseteq H$. Let $x \in H$. Then $x = a(a^{-1}x) \in aH$. Hence $H \subseteq aH$. Thus $H = aH$. Conversely, let $aH = H$. Now $a = ae \in aH$ and $a \in H$.

(ii) Let $aH = bH$. Then $a^{-1}(aH) = a^{-1}(bH)$ and $H = (a^{-1}b)H$. Hence $a^{-1}b \in H$(by (i)).

Conversely let $a^{-1}b \in H$. Then $a^{-1}bH = H$(by (i)), $aa^{-1}bH = aH$ and so $bH = aH$.

(iii) Let $a \in bH$. Then $a = bH$ for some $h \in H$ and so $a^{-1} = (bH)^{-1} = h^{-1}b^{-1} \in Hb^{-1}$. Converse can be similar proved.

(iv) Let $a \in bH$. We claim that $aH = bH$. Let $x \in aH$. Then $x = ah_1$ for some $h_1 \in H$. Also $a \in bH \Rightarrow a = bh_2$ for some $h_2 \in H$. Therefore $x = ((bh_2)h_1) = b(h_2h_1) \in bH$ and so $aH \subseteq bH$. Now, let $x \in bH$. Then $x = bh_3$ for some $h_3 \in H$ and so $b = ah_2^{-1}$. Therefore $x = ah_2^{-1}h_3 \in aH$ and so $bH \subseteq aH$. Hence $aH = bH$.

Conversely, let $aH = bH$. Then $a = ae \in aH$ and so $a \in bH$. □

Theorem 2.2.4. *Let H be a subgroup of G. Then*
(i) any two left cosets of H are either identical or disjoint.
(ii) union of all the left cosets of H is G.
(iii) the number of elements in any left coset aH is the same as the number of elements in H.

Proof. (i) Let aH and bH be two left cosets. Suppose aH and bH are not disjoint. We claim that $aH = bH$. Since aH and bH are not disjoint, $aH \cup bH \neq \emptyset$ and so there exists an element $c \in aH \cup bH$. Clearly $c \in aH$, $c \in bH$ and so $aH = cH$, $bH = cH$. Hence $aH = bH$.

(ii) Let $a \in G$. Then $a = ae \in aH$ and every element of G belongs to a left cosets of H. Thus the union of all the left cosets of H is G.

(iv) The map $f : H \to aH$ defined by $f(h) = ah$ is clearly a bijection. Hence every left coset has the same number of elements as H. □

This theorem shows that the collection of all left cosets forms a partition of the group. The above result is true if we replace left cosets by right cosets. In what follows, the result we prove for left cosets are also true for right cosets.

Remark 2.2.5. Let H be a subgroup of G. We define a relation in G as follows. Define $a \sim b \Leftrightarrow a^{-1}b \in H$. Then $\sim$ is an equivalence relation.

For, $a^{-1}a = e \in H$, $a \sim a$ and hence $\sim$ is reflexive.

Now , $a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \sim a$.
Therefore $a \sim b \Rightarrow b \sim a$ and $\sim$ is symmetric.

Now, $a \sim b$ and $b \sim c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) \in H \Rightarrow a^{-1}c \in H \Rightarrow a \sim c$. Hence $\sim$ is transitive and so $\sim$ is an equivalence relation.

Now, we claim that equivalence class $[a] = aH$. Let $b \in [a]$. Then $b \sim a$.

$\therefore \ a^{-1}b \in H$.

$\therefore \ a^{-1}b = h$ for some $h \in H$.

$\therefore \ b = ah$ Hence $b \in aH$.

$\therefore \ [a] \subseteq aH$.

Also, $b \in aH \Rightarrow b = ah$ for some $h \in H$.

$$\Rightarrow a^{-1}b = h \in H \Rightarrow a \sim b \Rightarrow b \in [a].$$

Thus the left cosets of H in G are precisely the equivalence classes determined by $\sim$. Hence the left cosets form a partition of G.

Theorem 2.2.6. *Let H be a subgroup of G. The number of left cosets of H is the same as the number of right cosets of H.*

Proof. Let L and R respectively denote the set of left and right cosets of H. We define a map $f : L \to R$ by $f(aH) = Ha^{-1}$. f is well defined. For $aH = bH \Rightarrow a^{-1}b \in H \Rightarrow a^{-1} \in Hb^{-1} \Rightarrow Ha^{-1} = Hb^{-1}$ f is 1-1. For, $f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow a^{-1} \in Hb^{-1} \Rightarrow a^{-1} = hb^{-1}$ for some $h \in H \Rightarrow a = bh^{-1} \Rightarrow a \in bH \Rightarrow aH = bH$. f is onto. For, every right coset Ha has a pre-image under f namely $a^{-1}H$. Hence f is a bijection from L to R. Hence the number of left cosets is the same as the number of right cosets. □

Definition 2.2.7. Let H be a subgroup of G. The number of distinct left (right) cosets of H in G is called the *index* of H in G and is denoted by $[G : H]$.

Example 2.2.8. In $(\mathbb{Z}_8, \oplus)$, $H = \{0, 4\}$ is a subgroup. The left cosets of H are given by

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

These are the four distinct left cosets of H. Hence the index of the subgroup H is 4. Note that $[\mathbb{Z}_8 : H] \times [H] = 4 \times 2 = 8 = |\mathbb{Z}_8|$.

Theorem 2.2.9 (Lagrange's theorem)**.** *Let G be a finite group of order n and H be a subgroup of G. Then the order of H divides the order of G.*

Proof. Let $|H| = m$ and $[G : H] = r$. Then the number of distinct left cosets of H in G is r. By Theorem 2.2.4, these r left cosets are mutually disjoint, they have the same number of elements namely m and their union is G. Hence $n = rm$ and so m divides n. □

Corollary 2.2.10. $[G : H] = \frac{|G|}{|H|}$

Note 2.2.11. Lagrange's theorem has many important application in group theory. For example, a group G of order 8 cannot have subgroups of order 3,5,6 and 7. In fact any proper subgroup of G must be of order 2 or 4.

Note 2.2.12. Any group of prime order has no proper subgroups.

Note 2.2.13. The converse of Lagrange's theorem is false. (ie) If G is a group of order n and m divides n, then G need not have a subgroup of order m. For example A_4 is a group of order 12 and it does not have a subgroup of order 6.
However there are groups in which the converse of Lagrange's theorem is true.

For example, consider S_3. This is a group of order 6. $\{e, p_4\}$ is a subgroup of order 2 and $\{e, p_1, p_2\}$ is a subgroup of order 3. Hence for every divisor m of 6, there is a subgroup of S_3 of order m.

Theorem 2.2.14. *The order of any element of a finite group G divides the order of G.*

Proof. Let G be a group of order n. Let $a \in G$ be an element of order m. Then the order of a is the same as the order of cyclic group $\langle a \rangle$. Now, by Lagrange's theorem the order of the subgroup $\langle a \rangle$ divides the order of G. Hence $m|n$. □

Theorem 2.2.15. *Every group of prime order is cyclic.*

Proof. Let G be a group of order p where p is prime. Let $a \in G$ and $a \neq e$. By above theorem order of a divides p. The order of a is 1 or p. Since $a \neq e$ order of a is p. Hence $G = \langle a \rangle$ so that G is cyclic. □

Theorem 2.2.16. *Let G be a group of order n. Let $a \in G$ then $a^n = e$.*

Proof. Let the order of a is m. Then m divides n and so $n = mq$. Hence $a^n = a^{mq} = (a^m)^q = e^q = e$. □

Theorem 2.2.17 (Euler's theorem)**.** *If n is any integer and $\langle a, n\rangle = 1$ then $a^{\phi(n)} \equiv 1(mod\ n)$. ($\phi(n)$ is the number of positive integers less than n relatively prime to n)*

Proof. Let $G = \{m : \ m < n \text{ and } (m, n) = 1\}$. G is a group under multiplication modulo n. This group is of order $\phi(n)$. Now, let $(a, n) = 1$. Let $a = qn + r$; $0 \leq r < n$ so that $a \equiv r(mod\ n)$. Since $(a, n) = 1$ we have $(n, r) = 1$ so that $r \in G$.

$\therefore \quad r^{\phi(n)} = 1$

$\therefore \quad r^{\phi(n)} \equiv 1(mod\ n)$

Also $a^{\phi(n)} \equiv r^{\phi(n)}(mod\ n)$ so that $a^{\phi(n)} \equiv 1(mod\ n)$ (since '$\equiv$'is transitive). □

Theorem 2.2.18 (Fermat's theorem)**.** *Let p be a prime number and a be any integer relatively prime to p. Then $a^{p-1} \equiv 1(mod\ p)$.*

Proof. Since p is prime, $\phi(p) = p - 1$ and hence the result follows from Euler's theorem. □

Theorem 2.2.19. *A group G has no proper subgroups if and only if is a cyclic group of prime order.*

Proof. Suppose G is a group of prime order. Then by Lagrange's theorem, G has no proper subgroups. Conversely, let G be a group having no proper subgroup. First we shall prove that G is cyclic. Suppose G is not cyclic. Let $a \in G$ and $a \neq e$. Then the cyclic group $\langle a\rangle$ is a proper subgroup of G which is a contradiction. Hence G is cyclic. Also G cannot be infinite, for an infinite cyclic group contains a proper subgroup $\langle a^2\rangle$. Hence G must be of finite order, say, n. We claim that n is prime. If possible let n be a composite number. Let $n = pq$ where $p, q > 1$. let $a \in G$ be a generator of the group. Then $\langle a^2\rangle$ is a subgroup of order q and hence is a proper subgroup of G which is a contradiction. Hence n is prime and G is a cyclic group of prime order. □

Theorem 2.2.20. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H||K|}{H \cap K}.$$

Proof. Let us write $A = H \cap K$. Since H and K are subgroups of G, A is a subgroup of G and since $A \subseteq H$, A is also a subgroup of H. By Lagranges theorem,$|A|$ divides $|H|$. Let $n = \frac{|H|}{|A|}$. Then $[H : A] = n$ and so A has n distinct left cosets in H. Let $\{x_1A, x_2A, \ldots, x_nA\}$ be the set of all distinct left cosets of A in H. Then $H = \cup_{i=1}^{n} x_iA$. Since $A \subseteq K$, it follows that

$$HK = (\cup_{i=1}^{n} x_iA)K = \cup_{i=1}^{n} x_iK.$$

We now show that $x_iK \cap x_jK = \Phi$ if $i \neq j$. Suppose $x_iK \cap x_jK \neq \Phi$ for some $i \neq j$. Then $x_jK = x_iK$. Thus, $x_i^{-1}x_j \in K$. Since $x_i^{-1}x_j \in H$, $x_i^{-1}x_j \in A$ and so $x_jA = x_iA$. This contradicts the assumption that $x_1A, \ldots, x_nA$ are all distinct left cosets. Hence, $x_1K, \ldots, x_nK$ are distinct left cosets of K. Also, $|K| = |x_iK|$ by theorem 2.2.4 for all $i = 1, 2, \ldots, n$. Thus,

$$|HK| = |x_1K| + \cdots + |x_nK| = n|K| = \frac{|H||K|}{|A|} = \frac{|H||K|}{|H \cap K|}. \qquad \square$$

2.2.1 Solved problems

Problem 2.2.21. *Let A and B be subgroups of a finite group G such that A is a subgroup of B. Show that*

$$[G : A] = [G : B][B : A].$$

Solution. By Lagrange's theorem, $[G : A] = \frac{|G|}{|A|}$, $[G : B] = \frac{|G|}{|B|}$ and $[B : A] = \frac{|B|}{|A|}$. Hence $[G : A][B : A] = \frac{|G|}{|B|}\frac{|B|}{|A|} = \frac{|G|}{|A|} = [G : A]$

Problem 2.2.22. *Let A and B be two finite subgroups of a group G such that $|A|$ and $|B|$ have no common divisors. Then show that $A \cap B = \{e\}$.*

Solution. $A \cap B$ is a subgroup of A and B. Then by Lagrange's theorem, $|A \cap B|$ divides $|A|$ and $|B|$. But by hypothesis $|A|$ and $|B|$ have no common divisors and so $|A \cap B| = 1$. Hence $A \cap B = \{e\}$.

Problem 2.2.23. *Let H and K be two subgroups of a finite group G such that $|H| > \sqrt{|G|}$ and $|K| > \sqrt{|G|}$. Then $H \cap K \neq \{e\}$.*

Proof. Suppose $H \cap K = \{e\}$. Then n $|H \cap K| = 1$ and $|HK| = \frac{|H||K|}{|H \cap K|}$. Thus $|H||K| > \sqrt{|G|}\sqrt{|G|} = |G|$, which is a contradiction. Hence $H \cap K \neq \{e\}$. □

2.3 Normal Subgroups

Definition 2.3.1. A subgroup H of G is called a *normal subgroup* of G if $aH = Ha$ for all $a \in G$.

Examples 2.3.2.

1. For any group G, $\{e\}$ and G are normal subgroups.
2. In S_3, the subgroup $\{e, p_1, p_2\}$ is normal.
3. In S_3, the subgroup $\{e, p_3\}$ is not a normal subgroup.

Theorem 2.3.3. *Every subgroup of an abelian group is a normal subgroup.*

Proof. Let G be an abelian group and let H be a subgroup of G. Let $a \in G$. We claim that $aH = Ha$. Let $x \in aH$. Then $x = ah$ for some $h \in H$ and $x = ha$ (since G is abelian). Hence $x \in Ha$ and so $aH \subseteq Ha$. Similarly $Ha \subseteq aH$, $aH = Ha$ and hence H is a normal subgroup of G. □

Examples 2.3.4.

1. $n\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$.
2. Every subgroup of $(\mathbb{Z}_n, \oplus)$ is normal.
3. Since any cyclic group is abelian any subgroup of a cyclic is normal.

Theorem 2.3.5. *Let H be a subgroup of index 2 in a group G. Then H is a normal subgroup of G.*

Proof. If $a \in H$ then $H = aH = Ha$. If $a \notin H$, then aH is a left coset different from H. Hence $H \cap aH = \emptyset$. Further, since index of H in G is 2, $H \cup aH = G$. Hence $aH = G - H$. Similarly $Ha = G - H$ so that $aH = Ha$. Hence H is a normal subgroup of G. □

Example 2.3.6. The alternating group A_n is a subgroup of index 2 in S_n and hence is a normal subgroup of S_n.

Theorem 2.3.7. *Let N be a subgroup of G. Then the following are equivalent.*
(ii) $aNa^{-1} = N$ for all $a \in G$.
(iii) $aNa^{-1} \subseteq N$ for all $a \in G$.
(iv) $ana^{-1} \in N$ for all $n \in N$ and $a \in G$.

Proof. $(i) \Rightarrow (ii)$ Suppose N is a normal subgroup of G.

$\therefore \quad aN = Na$ for all $a \in G$.

$\therefore \quad aNa^{-1} = Naa^{-1} = Ne = N$.

$(ii) \Rightarrow (iii)$ and $(iii) \Rightarrow (iv)$ are obvious.

$(iv) \Rightarrow (i)$ Suppose that $ana^{-1} \in N$ for all $n \in N$ and $a \in G$. We claim that $aN = Na$. Let $x \in aN$.

$\therefore \quad x = an$ for some $n \in N$.

$\therefore \quad x = (ana^{-1})a \in Na$ (since $ana^{-1} \in N$).

$$\therefore \qquad aN \subseteq Na \qquad \cdots (1)$$

Now, let $x \in Na$.

$\therefore \quad x = na$ for some $n \in N$.

$\therefore \quad x = a(a^{-1}n(a^{-1})^{-1}) \in aN$.

$$\therefore \qquad Na \subseteq aN \qquad \cdots (2)$$

From (1) and (2) we get $aN = Na$. Hence N is a normal subgroup of G. □

2.3.1 Solved problems

Problem 2.3.8. Prove that the intersection two normal subgroups of a group G is a normal subgroup.

Solution. Let H and K be two normal subgroups of G. Then $H \cap K$ is a subgroup of G. Now, let $a \in G$ and $x \in H \cap K$. Then $x \in H$ and $x \in K$. Since H and K are normal $axa^{-1} \in H$ and $axa^{-1} \in K$. Hence $axa^{-1} \in H \cap K$. Thus $H \cap K$ is a normal subgroup of G.

Problem 2.3.9. The center H of a group G is a normal subgroup of G.

Solution. The center H of G is given by

$$H = \{a : \; a \in G, ax = xa \text{ for all } x \in G\}$$

Now let $x \in H$ and $a \in G$. Hence $ax = xa$ and so $x = axa^{-1} \in H$ Hence H is a normal subgroup of G.

Problem 2.3.10. Let H be a subgroup of G. Let $a \in G$. Then aHa^{-1} is a subgroup of G.

Solution. $e = aea^{-1} \in aHa^{-1}$ and hence $aHa^{-1} \neq \Phi$. Now, let $x, y \in aHa^{-1}$. Then $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$ where $h_1, h_2 \in H$. Now, $xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$. Hence aHa^{-1} is a subgroup of G.

Problem 2.3.11. Show that if a group G has exactly one subgroup H of given order, then H is a normal subgroup of G.

Solution. Let the order of H be m. Let $a \in G$. Then by above problem, aHa^{-1} is also a subgroup of G. We claim that $|H| = |aHa^{-1}| = m$. Now, consider $f : H \to aHa^{-1}$ defined by $f(h) = aha^{-1}$. f is 1-1, for, $f(h_1) = f(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$. f is onto, for, let $x = aha^{-1} \in aHa^{-1}$. Then $f(h) = x$. Thus f is a bijection and so $|H| = |aHa^{-1}| = m$. But H is the only subgroup of G of order m and so $aHa^{-1} = H$. Hence $aH = Ha$ and so H is a normal subgroup of G.

Problem 2.3.12. Show that if H and N are subgroups of a group G and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

Solution. Let $x \in H \cap N$ and $a \in H$. We claim that $axa^{-1} \in H \cap N$. Now, $x \in N$ and $a \in H \Rightarrow axa^{-1} \in N$ (since N is a normal subgroup). Also $x \in H$ and $a \in H \Rightarrow axa^{-1} \in H$ (since H is a group). Hence $axa^{-1} \in H \cap N$. Hence $H \cap N$ is a normal subgroup of H.

The following example shows that $H \cap N$ need not be normal in G. Let $G = S_3$. Take $N = G$ and $H = \{e, p_3\}$. Now $H \cap N = H$ which is not normal in G.

Problem 2.3.13. If H is a subgroup of G and N is a normal subgroup of G then HN is a subgroup of G.

Solution. To prove that HN is a subgroup of G, it is enough if we prove that $HN = NH$.

Let $x \in HN$. Then $x = hn$ where $h \in H$ and $n \in N$. Therefore $x \in hN$. But $hN = Nh$(since N is normal). Therefore $x \in Nh$ and so $x = n_1h$ where $n_1 \in N$. Hence $x \in Nh$ and so $HN \subseteq NH$. Similarly $NH \subseteq HN$ and hence HN is a subgroup of G.

Problem 2.3.14. M and N are normal subgroups of a group G such that $M \cap N = \{e\}$. Show that every element of M commutes with element of N.

Solution. Let $a \in M$ and $b \in N$. We claim that $ab = ba$.

Consider the element $aba^{-1}b^{-1}$. Since $a^{-1} \in M$ and M is normal, $ba^{-1}b^{-1} \in M$. Also, since $b \in M$, so that $aba^{-1}b^{-1} \in N$. Thus $aba^{-1}b^{-1} \in M \cap N = \{e\}$. Hence $aba^{-1}b^{-1} = e$, so that $ab = ba$.

Theorem 2.3.15. A subgroup N of G is normal if and only if the product of two right cosets of N is again a right coset of N.

Proof. Suppose N is a normal subgroup of G. Then $NaNb = N(aN)b = N(Nab) = NNab = Nab$.

Conversely suppose that the product of any two right cosets of N is again a right coset of N. Then $NaNb$ is a right coset of N. Further $ab = (ea)(eb) \in NaNb$. Hence $NaNb$ is the right coset containing ab. Hence $NaNb = Nab$.

Now, we prove that N is a normal subgroup of G. Let $a \in G$ and $n \in N$. Then $ana^{-1} = eana^{-1} \in NaNa^{-1} = Naa^{-1} = N$ and so $ana^{-1} \in N$. Hence N is a normal subgroup of G. □

Theorem 2.3.16. *Let N be a normal subgroup of a group G. Then G/N is a group under the operation defined by $NaNb = Nab$.*

Proof. By above theorem the operation given by $NaNb = Nab$ is well defined binary operation in G/N. Now, let $Na, Nb, Nb \in G/N$. Then $Na(NbNc) = Na(Nbc) = Na(bc) = N(ab)c = (NaNb)Nc$. Thus the binary operation is associative. Now, $Ne = N \in G/N$ and $NaNe = Nae = Na = NeNa$. Thus Ne is the identity element. Also $NaNa^{-1} = Naa^{-1} = Ne = Na^{-1}Na$ and Na^{-1} is the inverse of Na. Hence G/N is a group. □

2.4 Quotient Groups

Definition 2.4.1. Let N be a normal subgroup of G. Then the group G/N is called the *quotient group(factor group) of G modulo N.*

Example 2.4.2. $3\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$. The quotient group $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}+0, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$. Hence $\mathbb{Z}/3\mathbb{Z}$ is a group of order 3.

2.5 Isomorphism

Let $\omega \neq 1$ be a cubic root of unity. Let $G = \{1, \omega, \omega^2\}$. G is a group under usual multiplication. The Cayley table for G is given by

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$(\mathbb{Z}_3, \oplus)$ is a group and its Cayley table is given by

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We note that these two tables for the groups of order 3 keep the same *pattern*. In fact any group of order 3 is cyclic and hence it is easily seen that all groups with 3 elements are ”like” each other. Thus if two groups G and G' are ”like” each other, it should be possible for us to obtain G' from G by remaining each element x in G with the name of an element x' in G'. The renaming of the elements of G can be achieved by means of a bijection $f : G \to G'$. If $x \in G$ we view $f(x)$ as a new name for x. Finally if the groups are to be ”like” each other, then if x and y are in G the new name for xy should be $f(x)f(y)$ so that $f(xy) = f(x)f(y)$. Note that the product xy is computed in G and the product $f(x)f(y)$ is computed in G'. Two groups which are like each other are usually called *isomorphic*. The following definition makes these ideas mathematically precise.

Definition 2.5.1. Let G and G' be two groups. A map $f : G \to G'$ is called an **isomorphic** if

(i) f is bijection.

(ii) $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Two groups G and G' are said to be *isomorphic* if there exists an isomorphism $f : G \to G'$. If two groups G and G' are isomorphic we write $G \cong G'$.

Theorem 2.5.2. Isomorphism is an equivalence relation among groups.

Proof. For any group G, $i_G : G \to G$ is clearly an isomorphism. Hence $G \cong G'$. Therefore the relation is reflexive. Now, let $G \cong G'$ and let $f : G \to G'$ be an isomorphism. Then f is a bijection. $\therefore$ $f^{-1} : G' \to G$ is also a bijection.

Now, let $x', y' \in G'$. Let $f^{-1}(x') = x$ and $f^{-1}(y') = y$. Then $f(x') = x$ and $f(y') = y$. $\therefore$ $f(xy) = f(x)f(y) = x'y'$. $\Rightarrow$ $f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$. Hence f is an isomorphism. Thus $G \cong G'$ and hence the relation is symmetric.

Now, let $G \cong G'$ and $G' \cong G''$. Then there exists isomorphisms $f : G \to G'$ and $g : G' \to G''$. Since f and g are bijections, $g \circ f : G \to G''$ is also a bijection. Now, let $x, y \in G$. Then

$$\begin{aligned}(g \circ f)(xy) = g[f(xy)] &= g[f(x)f(y)](\text{since } f \text{ is an isomorphism})\\ &= g[f(x)]g[f(y)](\text{since } g \text{ is an isomorphism})\\ &= (g \circ f)(x)(g \circ f)(y)\end{aligned}$$

Hence $g \circ f$ is an isomorphism. Thus $G \cong G''$ and hence the relation is transitive. Hence isomorphism is an equivalence relation among groups. □

Examples 2.5.3.

1. $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$. Consider $f : \mathbb{Z} \to 2\mathbb{Z}$ given by $f(x) = 2x$. Clearly f is a bijection. Also $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$ Hence f is an isomorphism.

2. Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R}^* \right\}$. G is a group under matrix multiplication. We claim that $G \cong (\mathbb{R}^*, \cdot)$. Consider $f : G \to \mathbb{R}^*$ given by $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$. Clearly f is a bijection. Now, let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$. Then $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$ and so $f(AB) = ab = f(A)f(B)$. Hence f is an isomorphism.

3. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. Consider $f : \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = e^x$. Clearly f is a bijection. Also $f(x + y) = 2e^{x+y} = e^x + e^y = f(x) + f(y)$. Hence f is an isomorphism.

4. $G = \mathbb{R} - \{-1\}$ is a group under $*$ defined by $a * b = a + b + ab$. We claim that $G \cong (\mathbb{R}^*, \cdot)$. Consider $f : G \to \mathbb{R}^*$ given by $f(x) = x + 1$. Clearly f is a bijection. Also $f(x * y) = f(x + y + xy) = x + y + xy + 1 = (x + 1)(y + 1) = f(x)f(y)$ Hence f is an isomorphism.

5. $(\mathbb{Z}_n, \oplus)$ is a group. Let G denote the set of all n^{th} root of unity. G is a group under usual multiplication. We claim that $(\mathbb{Z}_n, \oplus) \cong G$. Consider $f : \mathbb{Z}_n \to G$ given by $f(m) = \omega^m$ where $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$. Clearly f is a bijection. Let $a, b \in \mathbb{Z}_n$.

Let $a+b=qn+r$ where $0 \leq r \leq n$. Then $a \oplus b = r$. Hence

$$f(a \oplus b) = \omega^r \qquad \cdots (1)$$

Also $f(a)f(b) = \omega^a\omega^b = \omega^{a+b} = \omega^{qn+r} = \omega^{qn}\omega^r = 1\omega^r = \omega^r \qquad \cdots (2)$

From (1) and (2), we get $f(a \oplus b) = f(a)f(b)$. Hence f is an bijection.

Theorem 2.5.4. Let $f : G \to G'$ be an isomorphism. Then

(i) $f(e) = e'$ where e and e' are the identity elements of G and G' respectively. (ie). In an isomorphism identity is mapped onto identity.

(ii) $f(a^{-1}) = [f(a)]^{-1}$.

Proof.

(i) To prove that $f(e) = e'$ it is enough if we prove that $a'f(e) = f(e)a' = a'$ for all $a' \in G'$. Let $a' \in G'$. Since $f : G \to G'$ is a bijection, there exists such that $a \in G$ such that $f(a) = a'$. Hence $a'f(e) = f(a)f(e) = f(ae) = f(a) = a'$. Similarly, $f(e)a' = a'$. Hence $f(e) = e'$

(ii) It is enough to prove that $f(a)f(a^{-1}) = f(a^{-1})f(a) = e'$. Now, $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'$. Also, $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$. Thus $f(a)f(a^{-1}) = f(a^{-1})f(a) = e'$ and so $[f(a)]^{-1} = f(a^{-1})$. □

Remark 2.5.5. The concept of isomorphism for groups is extremely important. Since two isomorphic groups G and G' have essentially the same structure, if one group G has an additional property (for example abelian or cyclic) then the group G' also has its additional property. This seen in the following three theorems.

Theorem 2.5.6. Let $f : G \to G'$ be an isomorphism. If G is abelian, then G' is also abelian.

Proof. Let $a', b' \in G'$. Then there exist $a, b \in G$ such that $f(a) = a'$ and $f(b) = b'$. Now, $a'b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b'a'$. Hence G' is abelian. □

Theorem 2.5.7. Let $f : G \to G'$ be an isomorphism. Let $a \in G$. Then the order of a is equal to the order of $f(a)$. (ie) Isomorphism preserves the order of each element in a group.

Proof. Suppose the order of a is n. Then n is the least positive integer such that $a^n = e$. Now,

$$\begin{aligned} [f(a)]^n &= f(a) \cdots f(a) \text{ } (f(a) \text{ written } n \text{ times}) \\ &= f(a)^n \text{ (since } f \text{ is an isomorphism)} \\ &= f(e) = e'. \end{aligned}$$

Now, if possible let m be a positive integer such that $0 < m < n$ and $[f(a)]^m = e'$. Then $f(a^m) = [f(a)]^m = e'$. But $f(e) = e'$. Since f is 1-1 we have $a^m = e$ which contradicts the definition of the order of a. Hence n is the least positive integer such that $[f(a)]^n = e'$ and so the order of $f(a)$ is n. □

Theorem 2.5.8. *Let $f : G \to G'$ be an isomorphism. Let G is cyclic then G' is also cyclic.*

Proof. Let a be a generator of the group G. We shall prove that $f(a)$ is a generator of the group G'. Let $x' \in G'$. Since f is a bijection, there exists $x \in G$ such that $f(x) = x'$. Now, since $G = \langle a \rangle, x = a^n$ for some integer n. Hence $x' = f(x) = f(a^n) = [f(a)]^n$. Since $x' \in G'$ is arbitrary every element of G' is of the form $[f(a)]^n$ so that $G' = \langle f(a) \rangle$. Hence G' is cyclic. □

2.5.1 Solved problems

Problem 2.5.9. Show that $(\mathbb{R}^*, \cdot)$ is not isomorphic to $(\mathbb{R}, +)$.

Solution. In $(\mathbb{R}, +)$ every element other than 0 is of infinite order. But in $(\mathbb{R}^*, \cdot)$ there exists an element (other than 1) of finite order. For example, -1 is of order 2 in $(\mathbb{R}^*, \cdot)$. Hence we cannot find an isomorphism from $\mathbb{R}^*, \cdot$ to $(\mathbb{R}, +)$.

Problem 2.5.10. Show that $(\mathbb{Z}_4, \oplus)$ is not isomorphic to V_4.

Solution. In $\mathbb{Z}_4$, 1 is an element of order 4. But in V_4 every element other than e is of order 2. Hence the two groups are not isomorphic. This can also be proved by nothing that $\mathbb{Z}_4$ is cyclic and V_4 is not cyclic.

Problem 2.5.11. If G is a group and G' is a set with a binary operation and there exists a 1-1 mapping f from G onto G' such that $f(ab) = f(a)f(b)$ for all $a, b \in G$ then show that G' is also a group.

Solution. Let $a', b', c' \in G'$ Since $f : G \to G'$ is a bijection, there exists $a, b, c \in G$ such that $f(a) = a'; f(b) = b'; f(c) = c'$. Since G is a group, $(ab)c = a(bc) \Rightarrow f[(ab)c] = f[a(bc)] \Rightarrow f(ab)f(c) = f(a)f(bc)$ (by hypothesis) $\Rightarrow [f(a)f(b)]f(c) = f(a)[f(b)f(c)]$ $\Rightarrow (a'b')c' = a'(b'c')$. Thus the binary operation in G' is associative.

Now, let $e \in G$ be the identity element. Let $a' \in G'$. Since $f : G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$. Now, $ae = ea = a$. $\Rightarrow f(ae) = f(ea) = f(a)$ $\Rightarrow f(a)f(e) = f(e)f(a) = f(a) \Rightarrow a'f(e) = f(e)a' = a' \Rightarrow f(e)$ is the identity in G'. Let $a' \in G'$. Since $f : G \to G'$ is a bijection, there exists $a \in G$ such that $f(a) = a'$. Now, $aa^{-1} = a^{-1}a = e$. $\Rightarrow f(aa^{-1}) = f(a^{-1}a) = f(e)$. $\Rightarrow f(a)f(a^{-1}) = f(a^{-1})f(a) = f(e)$. $\Rightarrow a'f(a^{-1}) = f(a^{-1})a' = f(e)$. $\Rightarrow f(a^{-1})$ is the inverse of a' in G'. Hence G' is a group.

Problem 2.5.12. Let G be any group. Show that $f : G \to G$ given by $f(x) = x^{-1}$ is an isomorphism $\Leftrightarrow$ G is abelian.

Solution. Let $f : G \to G$ given by $f(x) = x^{-1}$ be an isomorphism. We claim that G is abelian. Let $x, y \in G$. Then

$$\begin{aligned} & f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1}) \text{ (since } f \text{ is an isomorphism).} \\ \therefore\ & (x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} \\ \therefore\ & (y^{-1})^{-1}(x^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} \Rightarrow yx = xy. \end{aligned}$$

Hence G is abelian.

Conversely, suppose G is abelian. Clearly $f : G \to G$ given by $f(x) = x^{-1}$ is a bijection. Now, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ (since G is abelian) $= f(x)f(y)$. Hence f is an isomorphism.

Theorem 2.5.13. Any infinite cyclic group G is isomorphic to $(\mathbb{Z}, +)$.

Proof. Let G be an infinite cyclic group with generator a. Then $G = \{a^n : n \in \mathbb{Z}\}$. Define $f : \mathbb{Z} \to G$ by $f(n) = a^n$. Since G is infinite, $n \neq m \Rightarrow a^n \neq a^m$. Hence f is

1-1. Obviously f is onto. Now, $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$. Hence f is an isomorphism. □

Corollary 2.5.14. Any two infinite cyclic groups are isomorphic to each other. Let G and G' be two infinite cyclic groups. By above theorem, $G \cong (\mathbb{Z}, +)$ and $(\mathbb{Z}, +) \cong G'$. Thus $G \cong G'$ (since $\cong$ is an equivalence relation).

Theorem 2.5.15. *Any finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, \oplus)$.*

Proof. Let G be a cyclic group of order n with generator a. Then $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Define $f : \mathbb{Z}_n \to G$ by $f(r) = a^r$. Clearly f is a bijection. Now, let $r, s \in \mathbb{Z}_n$. Let $r \oplus s = t$. Then $r + s = qn + t$, where $0 \leq t < n$ and so

$f(r \oplus s) = a^{r \oplus s} = a^t \qquad \cdots (1)$

Also, $f(r)f(s) = a^r a^s = a^{r+s} = a^{qn+t} = a^{qn}a^t = (a^n)^q a^t = ea^t = a^t \qquad \cdots (2)$

From (1) and (2), we get $f(r \oplus s) = f(r)f(s)$. Hence f is an isomorphism. □

Corollary 2.5.16. Any two finite cyclic groups of the same order are isomorphic.

Theorem 2.5.17 (Cayley's theorem)**.** Any finite group is isomorphic to a group of permutations.

Proof. We shall prove this theorem in 3 steps. We shall first find a set G' of permutations. Then we prove that G' is a group of permutations and finally we exhibit an isomorphism $\phi : G \to G'$.

Step 1.L et G be a finite group of order n. Let $a \in G$. Define $f : G \to G$ by $f_a(x) = ax$. Now, f_a is 1-1, since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$. f_a is onto(since if $y \in G$, then $f_a(a^{-1}y) = a(a^{-1}y) = y$). Thus f_a is a bijection. Since G has n elements, f_a is just a permutation on n symbols.

Let $G' = \{f_a : \ a \in G\}$.

Step 2. We prove G' is a group. Let $f_a, f_b \in G'$. $(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$. Hence $f_a \circ f_b = f_{ab}$. Hence G' is closed under composition of mappings $f_e \in G'$ is the identity element. The inverse of f_a in G is f_a^{-1}.

Step 3. We prove $G \cong G'$. Define $\phi : G \to G'$ by $\phi(a) = f_a$. $\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow ax = bx \Rightarrow a = b$. Hence ϕ is 1-1. Obviously ϕ is onto. Also $\phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$. Hence ϕ is an isomorphism. □

Example 2.5.18. Consider the group $G = \{e, a, b\}$ whose multiplication table given by

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

By Cayley's theorem G is isomorphic to the permutation group $G' = \{f_e, f_a, f_b\}$ where

$$f_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}; f_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}; \text{ and } f_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$$

Definition 2.5.19. An isomorphism of a group G to itself is called an *automorphism* of G.

Examples 2.5.20.

1. Any group G has at least one automorphism namely i_G.

2. The map $f : \mathbb{R}^* \to \mathbb{R}^*$ defined by $f(a) = a^{-1}$ is an automorphism. Then f is a bijection. Also $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$. More generally if G is abelian, $f : G \to G$ defined by $f(a) = a^{-1}$ is an automorphism.

3. The mapping ϕ given by $\phi(z) = \bar{z}$ is an automorphism of the additive group of complex numbers. Clearly ϕ is a bijection and $\phi(z + w) = (\overline{z + w}) = \bar{z} + \bar{w} = \phi(z) + \phi(w)$.

4. Let G be any group. Let $a \in G$. Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism of G. For, let $x, y \in G$. Then $\phi_a(x) = \phi_a(y) \Rightarrow axa^{-1} =$

$aya^{-1} \Rightarrow x = y$(by cancellation law). Thus ϕ_a is 1-1. Also $\phi_a(axa^{-1}) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = exe = x$. Hence $a^{-1}xa$ is the pre-image of x under ϕ. Also $\phi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$. Thus ϕ_a is an automorphism of G.

Definition 2.5.21. The automorphism $\phi_a : G \to G$ defined in example 4(2.5.20) is called an *inner automorphism* of the group G.

Let G be a group. The set of all automorphisms of G is denoted by $Aut\ G$. The set of all inner automorphisms of G is denoted by $I(G)$.

Theorem 2.5.22. For any group G,
(i) $Aut\ G$ is a group under composition of functions.
(ii) $I(G)$ is a normal subgroup of $Aut\ G$.

Proof.

(i) Let $f, g \in Aut\ G \Rightarrow f$ and g are isomorphisms of G to itself $\Rightarrow f \circ g$ is an isomorphism of G to itself (Theorem 2.4.2).

$f \in Aut\ G \Rightarrow f^{-1} \in Aut\ G$. Clearly composition of functions is associative. Hence $Aut\ G$ is a group.

(ii) Let $\phi_a, \phi_b \in I(G)$. Then $(\phi_a\phi_b)(x) = \phi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$. Hence $\phi_a\phi_b = \phi_{ab} \in I(G)$. ϕ_e is the identity element of $I(G)$ and the inverse of ϕ_a is $\phi_{a^{-1}}$. Hence $I(G)$ is a subgroup of $Aut\ G$.

We now prove that $I(G)$ is a normal subgroup of $Aut\ G$. Let $\alpha \in Aut\ G$ and $\phi_a \in I(G)$. Then $(\alpha\phi_a\alpha^{-1})(x) = \alpha\phi_a(\alpha^{-1}(x)) = \alpha(a\alpha^{-1}(x)a^{-1}) = \alpha(a)\alpha\alpha^{-1}(x)\alpha(a^{-1}) = \alpha(a)x[\alpha(a)]^{-1} = \phi_{\alpha(a)}(x) \therefore\ \alpha\phi_a\alpha^{-1} = \phi_{\alpha(a)} \in I(G)$. Hence $I(G)$ is a normal subgroup of $Aut\ G$. □

Theorem 2.5.23. Let G be a cyclic group generated by a. Let $f : G \to G$ be a mapping such that $f(xy) = f(x)f(y)$. Then f is an automorphism of G if and only if $f(a)$ is a generator of G.

Proof. Let f be an automorphism of G. We shall prove that $f(a)$ is a generator of G.

Case 1. *Let G be a finite cyclic group of order n. Then order of a is n. By theorem, $f(a)$ is also an element of order n and hence $f(a)$ is a generator of G.*

Case 2. *Let G be infinite. Suppose $f(a)$ is not a generator of G. Let $H = \langle f(a)\rangle$. Then H is a proper subgroup of G.*

We claim that $f(G) = H$. Let $x' \in f(G)$. Then $x' = f(x)$ for some $x \in G$. Now, $x = a^n$ for some n since $G = \langle a\rangle$. Therefore $x = f(a^n) = [f(a)]^n \in H$ and so $f(G) \subseteq H$.

Now, let $x \in H$. Then $x = [f(a)]^n$ for some n. Therefore $x = f(a^n)$. Hence $x \in f(G)$, $H \subseteq f(G)$ and hence $f(G) = H$. Since H is a proper subgroup of G, f is not onto which is a contradiction. Hence $f(a)$ is a generator of G.

Conversely let $f : G \to G$ be a mapping such that $f(xy) = f(x)f(y)$ and let $f(a)$ be a generator of G. We shall prove that f is an automorphism. It is enough if we prove that f is 1-1 and onto. Let $x \in G$. Since $f(a)$ is a generator of G, $x = [f(a)]^n$ for some n. Clearly $f(a^n) = [f(a)]^n = x$. Thus x has a pre-image a^n under f. Hence f is onto. Now, to prove f is 1-1.

Case 3. *G is finite.*

Since any function from a finite set onto itself is necessarily 1-1(verify), f is 1-1.

Case 4. *G is infinite.*

Let $x, y \in G$ and let $x = a^n, y = a^m$ and $n \geq m$. Now, $f(x) = f(y) \Rightarrow f(a^n) = f(a^m) \Rightarrow [f(a)]^n = [f(a)]^m \Rightarrow [f(a)]^{n-m} = 0 \Rightarrow n - m = 0$ (since $f(a)$ is an element of finite order) $\Rightarrow n = m \Rightarrow a^n = a^m \Rightarrow x = y$ Hence f is 1-1. Thus f is an automorphism. □

Note 2.5.24. Let G be a cyclic group generated by a. Then any automorphism $f : G \to G$ is completely determined by the image $f(a)$ of the generator. For, if $x \in G$ is any element then $x = a^n$ for some integer n and hence $f(x) = f(a^n) = [f(a)]^n$.

As an example, consider $(\mathbb{Z}_4, \oplus)$. Here 1 is a generator of this cyclic group.
If $f(1) = 3$, then

$$f(2) = f(1 \oplus 1) = f(1) \oplus f(1) = 3 \oplus 3 = 2;$$

$$f(3) = f(2 \oplus 1) = f(2) \oplus f(1) = 2 \oplus 3 = 1;$$
$$f(0) = f(3 \oplus 1) = f(3) \oplus f(1) = 1 \oplus 3 = 0.$$

Theorem 2.5.25. The number of automorphism of a cyclic group of order n is $\phi(n)$.

Proof. Let G be a cyclic group of order n. Let $a \in G$ be a generator. If $f : G \to G$ is an automorphism then f is completely determined by specifying the image of a. The only possible images of a are any one of the generators of G. Hence the number of automorphisms is equal to the number of generators of G. But the number of generators of a cyclic group of order n is $\phi(n)$. (by corollary). Hence the number of automorphisms of a cyclic group of order n is $\phi(n)$. □

2.5.2 Solved problems

Problem 2.5.26. Construct the group of automorphisms of $(\mathbb{Z}_4, \oplus)$.

Solution. 1 and 3 are the only 2 generators of $\mathbb{Z}_4$. Hence there are only 2 automorphisms of $\mathbb{Z}_4$, say f and g. They are given by $f(1) = 1$ and $g(1) = 3$. Hence $Aut\ G = \{f, g\} \cong \mathbb{Z}_2$.

Problem 2.5.27. Construct the group of automorphisms of $(\mathbb{Z}, +)$.

Solution. 1 and -1 are the only 2 generators of $\mathbb{Z}$. Hence there are only 2 automorphisms of $\mathbb{Z}$ say f and g. They are given by $f(1) = 1$ and $g(1) = -1$. $f(1) = 1$ gives the identity automorphism. $g(1) = -1$ determines the automorphism given by $g(x) = -x$. Hence $Aut\ \mathbb{Z} = \{f, g\} \cong \mathbb{Z}_2$.

Problem 2.5.28. Let G be a finite abelian group of order n and let m be a positive integer relatively prime to n. Then $f : G \to G$ defined by $f(x) = x^m$ is an automorphism of G.

Solution. since m and n are relatively prime, there exist integers u and v such that $mu + nv = 1$. Now, let $x \in G$. Then $x = x^{mu+nv} = x^{mu}x^{nv} = x^{mu}e = x^{mu}$. Hence $x = x^{mu}$. Now, $f(x) = f(y) \Rightarrow x^m = y^m \Rightarrow x^{mu} = y^{mu} \Rightarrow x = y$ Hence f is 1-1.

Also $f(x^u) = x^{mu} = x$. $\therefore$ Every element x has pre-image x^u under f. Hence f is onto. Also, $f(xy) = (xy)^m = x^m y^m$ (since G is abelian) $= f(x)f(y)$ Hence f is an isomorphism.

Problem 2.5.29. Show that $Aut\ \mathbb{Z}_8 \cong \mathbb{V}_4$.

Solution. The generators of $\mathbb{Z}_8$ are 1, 3, 5, 7. The different automorphisms of $\mathbb{Z}_8$ are f_1, f_2, f_3, f_4 given by $f_1(1) = 1; f_2(1) = 3; f_3(1) = 5$; and $f_4(1) = 7$. We shall now compute $f_2 \circ f_3$. $(f_2 \circ f_3)(1) = f_2(f_3(1)) = f_2(5) = f_2(1 \oplus 1 \oplus 1 \oplus 1) = f_2(1) \oplus f_2(1) \oplus f_2(1) \oplus f_2(1) \oplus f_2(1) = 3 \oplus 3 \oplus 3 \oplus 3 \oplus 3 = 7 = f_4(1)$ Thus $f_2 \circ f_3 = f_4$. Similarly we can find $f_i \circ f_j$, $i, j = 1, 2, 3, 4$. The Cayley table of $Aut\ \mathbb{Z}_8$ is

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Clearly $Aut\ \mathbb{Z}_8 \cong \mathbb{V}_4$

Example 2.5.30. Let n be any given positive integer. Let $x \in \mathbb{Z}$ and $x = qn + r$, where $0 \le r < n$. We define $f(x) = r$. f is mapping from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, \oplus)$. We claim that $f(a + b) = f(a) \oplus f(b)$ for all $a, b \in \mathbb{Z}$. Let $a = q_1 n + r_1$, $0 \le r_1 < n$ so that $f(a) = r_1$ and $b = q_2 n + r_2$, $0 \le r_2 < n$ so that $f(a) = r_2$. Let $r_1 + r_2 = q_3 n + r_3$ $0 \le r_3 < n$ so that $r_1 \oplus r_2 = r_3$. Therefore $a + b = (q_1 + q_2 + q_3) + r_3 \Rightarrow f(a + b) = r_3$. Also $f(a) \oplus f(b) = r_1 \oplus r_2 = r_3$ and so $f(a + b) = f(a) \oplus f(b)$. Note that f is not an isomorphism since f is not 1-1.

Definition 2.5.31. A map f form a group G into a group G' is called a *homomorphism* if $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Obviously every isomorphism is a homomorphism and a bijective homomorphism is an *isomorphism.*

Examples 2.5.32.

1. $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f(x) = 2x$ is a homomorphism. For, $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$. Note that f is 1-1.
2. $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ defined by $f(x) = |x|$ is a homomorphism. For, $f(xy) = |xy| = |x||y| = f(x)f(y)$. This homomorphism is onto.
3. $f : G \to G'$ defined by $f(a) = e'$, where e' is the identity in G' is a trivial homomorphism. For, $f(ab) = e' = e'e' = f(a)f(b)$.
4. $f : (\mathbb{Z}, +) \to (\mathbb{C}^*, \cdot)$ defined by $f(n) = i^n$ is a homomorphism. For, $f(n + m) = i^{n+m} = i^n i^m = f(n)f(m)$. Note that f is neither 1-1 nor onto.
5. $f : (\mathbb{R} \times \mathbb{R}, +) \to (\mathbb{R}, +)$ given by $f(x, y) = x$ is a homomorphism.
6. Let G be a group and N a normal subgroup of G, $f : G \to G/N$ given by $f(a) = Na$ is a homorphism. f is called the *canonical homomorphism* from G to G/N. Note that f is onto.

Definition 2.5.33. Let $f : G \to G'$ be a homomorphism.
(i) If f is onto, then it is called an *epimorphism.*
(ii) If f is 1-1, then it is called a *monomorphism.*

Note 2.5.34. If $f : G \to G'$ is an epimorphism then G' is called a *homomorphic image* of G.
A homomorphism of a group to itself is called an *endomorphism.*

Theorem 2.5.35. Let $f : G \to G'$ be a homomorphism. Then
(i) $f(e) = e'$.
(ii) $f(a^{-1}) = [f(a)]^{-1}$.
(iii) If H is a subgroup of G, then $f(H)$ is a subgroup of G'.
(iv) If H is normal in G, then $f(H)$ is normal in $f(G)$.
(v) If H' is a subgroup of G', then $f^{-1}(H')$ is a subgroup of G.
(vi) If H' is normal in $f(G)$, then $f^{-1}(H')$ is normal in G.

Proof. (i) Let $a \in G$. Then $f(a) = f(ae) = f(a)f(e)$. Hence $f(e) = e'$. (ii) $f(a)f(a^{-1}) = f(e) = e'$. Hence $f(a^{-1}) = [f(a)]^{-1}$. (iii) Let H be a subgroup of G.

Since H is non-empty, $f(H)$ is also non-empty. Now, let $x, y \in f(H)$. Then $x = f(a)$ and $y = f(b)$ where $a, b \in H$ and so $xy^{-1} = f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Now, since H is a subgroup of G, $ab^{-1} \in H$. Therefore $xy^{-1} = f(ab^{-1}) \in f(H) \Rightarrow f(H)$ is a subgroup of G'.

(iv) Let H be normal in G. Let $x \in f(H)$ and $y \in f(G)$. We claim that $yxy^{-1} \in f(H)$. Now, $x = f(a)$ and $y = f(b)$ where $a \in H$ and $b \in G$. Since H is normal in G, $bab^{-1} \in H$ and so $f(bab^{-1}) \in f(H) \Rightarrow f(b)f(a)f(b^{-1}) \in f(H) \Rightarrow yxy^{-1} \in f(H)$. Hence $f(H)$ is normal in $f(G)$.

(v) Since $f(e) = e' \in H'; e \in f^{-1}(H')$ and hence $f^{-1}(H') \neq \Phi$. Now, let $a, b \in f^{-1}(H')$. Then $f(a), f(b) \in H' \Rightarrow f(a)[f(b)]^{-1} \in H'$. $\Rightarrow f(ab^{-1}) \in H'$ (ie), $ab^{-1} \in f^{-1}(H')$. Hence $f^{-1}(H')$ is a subgroup of G.

(vi) Let $x \in f^{-1}(H')$ and $a \in G$. Then $f(x) \in H'$ and $f(a) \in f(G)$. Since H' is normal in $f(G)$, $f(a)f(x)[f(a)]^{-1} \in H'$ and so $f(axa^{-1}) \in H'$. Thus $f^{-1}(H')$ is normal in G. □

Examples 2.5.36.

1. Consider the homomorphism $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, \oplus)$ which is given in the beginning of this section.

   Let $K = \{x : x \in \mathbb{Z}, f(x) = 0\}$. Clearly $K = n\mathbb{Z}$ which is a normal subgroup of $\mathbb{Z}$.

2. Consider the homomorphism $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^+, \cdot)$ which is given by $f(x) = |x|$. Let $K = \{x : x \in \mathbb{R}^*, f(x) = 1\}$. Clearly $K = \{1, -1\}$ which is a normal subgroup of $(\mathbb{R}^*, \cdot)$.

Definition 2.5.37. Let $f : G \to G'$ be a homomorphism. Let $K = \{x : x \in G, f(x) = e'\}$. Then K is called the *Kernel* of f and is denoted by $ker(f)$.

Theorem 2.5.38. *Let $f : G \to G'$ be a homomorphism. Then the kernel K of f is a normal subgroup of G.*

Proof. Since $f(e) = e', e \in K$ and hence $K \neq \Phi$. Now, let $x, y \in K$. Then $f(x) = e' = f(y)$ and so $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = e'(e')^{-1} = e'e' = e'$. Thus $xy^{-1} \in K$. Hence K is a subgroup of G. Now, let $x \in K$ and $a \in G$. Then,

$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e'[f(a)]^{-1}$

$= f(a)[f(a)]^{-1} = e'$. and $axa^{-1} \in K$. Hence K is a normal subgroup of G.

Aliter. $\{e'\}$ is a normal subgroup of $f(G)$. Hence $ker\ f = f^{-1}(\{e'\})$ is a normal subgroup of G. □

Theorem 2.5.39 (Fundamental theorem of homomorphism)**.** *Then Let* $f : G \to G'$ *be a homomorphism. Let* K *be the kernel of* f*. Then* $G/K \cong G'$

Proof. Define $\phi : G/K \to G'$ by $\phi(Ka) = f(a)$.

Step(i) ϕ is well defined.

Let $Kb = Ka$. Then $b \in Ka$. Hence $b = ka$ where $k \in K$. Now, $f(b) = f(ka) = f(k)f(a) = e'f(a) = f(a)$ and so $\phi(Kb) = f(b) = f(a) = \phi(Ka)$. Hence $\phi(Ka) = \phi(Kb)$.

Step(ii) ϕ is 1-1.

For $\phi(Ka) = \phi(Kb) \Rightarrow f(a) = f(b) \Rightarrow f(a)[f(b)]^{-1} = e' \Rightarrow f(ab)^{-1} = e' \Rightarrow ab^{-1} \in K \Rightarrow a \in Kb \Rightarrow Ka = Kb$.

Step(iii) ϕ is onto.

Let $a' \in G'$. Since f is onto, there exists $a \in G$ such that $f(a) = a'$.

Step(iv) ϕ is a homomorphism. $\phi(KaKb) = \phi(Kab) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$. Thus ϕ is an isomorphism from G/K onto G'. Hence $G/K \cong G'$. □

2.5.3 Solved problems

Problem 2.5.40. Let $f : G \to G'$ be a homomorphism. Then f is 1-1 if and only if $ker\ f = \{e\}$.

Solution. Obviously f is 1-1 $\Rightarrow f = \{e\}$.

Conversely let $ker\ f = \{e\}$. We prove f is 1-1. $f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = e' \Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in ker\ f \Rightarrow xy^{-1} = e' \Rightarrow x = y$. Hence f is 1-1.

Problem 2.5.41. Let G be any group and H be the *center* of G. Then $G/H \cong I(G)$, the group of inner automorphisms of G.

Solution. Consider $f : G \to I(G)$ defined by $f(a) = \phi_a$. Then $f(ab) = \phi_{ab} = \phi_a \circ \phi_b = f(a)f(b)$. Hence f is a homomorphism. Clearly f is onto. Now, we claim that $ker\ f = H$. $a \in ker\ f \Leftrightarrow f(a) = \phi_e \Leftrightarrow \phi_a = \phi_e$.
$\Leftrightarrow \phi_a(x) = x$ for all $x \in G \Leftrightarrow axa^{-1} = x$ for all $x \in G \Leftrightarrow ax = xa$ for all $x \in G \Leftrightarrow a \in H$. Hence $ker\ f = H$. By the fundamental theorem of homomorphism $G/K \cong I(G)$.

Problem 2.5.42. Show that $\mathbb{R}^*/\{1, -1\} \cong \mathbb{R}^+$.

Solution. Consider $f : \mathbb{R}^* \to \mathbb{R}^+$ defined by $f(x) = |x|$. Clearly f is an epimorphism and $ker\ f = \{1, -1\}$. Hence by the fundamental theorem of homomorphism $\mathbb{R}^*/\{1, -1\} \cong \mathbb{R}^+$.

Problem 2.5.43. Any homomorphic image of a cyclic group is cyclic.

Solution. Let G be a cyclic group and $f : G \to G'$ be an epimorphism. Let a is a generator of G. Then $f(a)$ is a generator of G'. Hence G' is cyclic.

Problem 2.5.44. Show that the map $f : (\mathbb{C}, +) \to (\mathbb{R}, +)$ defined by $f(x + iy) = y$ is an epimorphism and $ker\ f = \mathbb{R}$. Deduce that $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

Solution. Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$.
$\therefore\ f(z_1 + z_2) = y_1 + y_2 = f(z_1) + f(z_2)$. Hence f is a homomorphism. Clearly f is onto. Now, $ker\ f = \{x + iy :\ f(x + iy) = 0\} = \{x + iy :\ y = 0\} = \mathbb{R}$. By the fundamental theorem of homomorphism, $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

Chapter 3

UNIT III: Ring

3.1 Definitions and examples

A group is an algebraic system with one binary operation. The familiar examples of real numbers and 2×2 matrices are systems which involve two binary operations. In this chapter we study algebraic systems with two binary operations. We start considering the system $\mathbb{Z}$ of integers. $\mathbb{Z}$ has two binary operations "$+$" and "$\cdot$" $(\mathbb{Z}, +)$ is an abelian group. Multiplication is an associative binary operation in $\mathbb{Z}$. These two binary operations are connected by the two distributive laws given by $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$. A generalization of these basic properties in $\mathbb{Z}$ leads us to the concept of a system called *ring*.

Definition 3.1.1. A non-empty set R together with two binary operations denoted by $+$ and $\cdot$ and called addition and multiplication which satisfy the following axioms is called a *ring* .
(i) $(R, +)$ is an abelian group.
(ii) $\cdot$ is an associative binary operation on R.
(iii) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

Notation 3.1.2. The unique identity of the additive group $(R, +)$ is denoted by 0 and is called the **zero element** of the ring and the unique additive *inverse* of a is denoted by $-a$.

Examples 3.1.3.

1. $(\mathbb{Z},+,\cdot)$; $(\mathbb{Q},+,\cdot)$; $(\mathbb{R},+,\cdot)$; $(\mathbb{C},+,\cdot)$ are all rings.

2. $(2\mathbb{Z},+,\cdot)$ is a ring.

3. Let $R=\{a+b\sqrt{2}:\ a,b\in \$Z\}$. Clearly R is an abelian group under usual addition. let $a+b\sqrt{2}$ and $c+d\sqrt{2}\in R$. Then $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+bd)+(bc+ad)\sqrt{2}\in R$. Since the two binary operations are the usual addition and multiplication, the distributive laws and the associative law hold. Thus R is a ring with usual addition and multiplication.

4. Let $R=\{a+ib:\ a,b\in\mathbb{Z}\}$. Then R is a ring under usual addition and multiplication. This ring is called the **ring of Gaussian integers**. In general, any subset of complex numbers which is a group under addition and is closed for multiplication is a ring(Verify).

5. $\{0\}$ with binary operation ”+” and ”$\cdot$” defined as $0+0=0$ and $0\cdot 0=0$ is a ring. This is called the *null ring*.

6. In $R\times R$ we define $(a,b)+(c,d)=(a+c,b+d)$ and $(a,b)\cdot(c,d)=(ac,bd)$. Here $(R\times R,+)$ is an abelian group. The identity is $(0,0)$ and the inverse of (a,b) is $(-a,-b)$. Further $(a,b)[(c,d)+(e,f)]=(a,b)(c+e,d+f)=(ac+ae,bd+bf)=(ac,bd)+(ae,bf)=(a,b)(c,d)+(a,b)(e,f)$. Similarly $[(a,b)+(c,d)](e,f)=(a,b)(e,f)+(c,d)(e,f)$. Hence $(R\times R,+,\cdot)$ is a ring.

7. Let $(R,+)$ be any abelian group with identity 0. We define multiplication in R by $ab=0$ for all $a,b\in R$. Clearly $a(bc)=0=(ab)c$ so that multiplication is associative. Also $a(b+c)=0=ab+ac$ and $(a+b)c=0=ac+bc$. Hence R is a ring under these operations. This ring is called the *zero ring*. This example shows that any abelian group with identity 0 can be made into a ring by defining $ab=0$.

8. $(\mathbb{Z}_n,\oplus,\odot)$ is a ring, for, we know that $(\mathbb{Z}_n,\oplus)$ is an abelian group and $\odot$ is an associative binary operation. We now prove the distributive laws. Let $a,b,c\in\mathbb{Z}_n$. Then $b\oplus c\equiv(b+c)(mod\, n)$. Hence $a\odot(b\oplus c)\equiv a(b+c)(mod\, n)$. Also $a\odot b\equiv ab(mod\, n)$ and $a\odot c\equiv ac(mod\ n)$ so that $(a\odot b)\oplus(a\odot c)\equiv(ab+ac)(mod\ n)$. Since $a\odot(b\oplus c)$

and $(a \odot b) \oplus (a \odot c) \in \mathbb{Z}_n$, we have $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$. Similarly $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$. Hence $(\mathbb{Z}_n, \oplus, \odot)$ is a ring.

9. $(\varrho(S), \Delta, \cap)$ is a ring. We know that $(\varrho(S), \Delta)$ is an abelian group(refer example 12 of section 1.1). Also $\cap$ is an associative binary operation on $\varrho(S)$. It can easily be verified that $A \cap (B \Delta C) = (A \cap B)\Delta(A \cap C)$ and $(A \Delta B) \cap C = (A \cap C)\Delta(B \cap C)$. Hence $(\varrho(S), \Delta, \cap)$ is a ring.

10. $M_2(R)$ under matrix addition and multiplication is a ring.

11. Let R be the set of all real functions. We define addition and multiplication by $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$. Then R is a ring. Clearly addition of functions is associative and commutative. The constant function $\mathbf{0}$ defined by $\mathbf{0}(x) = 0$, is the zero element of R and $-f$ is the additive inverse of f. Hence R is an abelian group. The associativity of multiplication and the distributive laws are consequences of the corresponding properties in R. Hence R is a ring.

12. Let A be any group. Let $Hom(A)$ be the set of all endomorphisms of A. Let $f, g \in Hom(A)$. We define $f+g$ by $(f+g)(x) = f(x)+g(x)$ and $fg = f \circ g$. Then $Hom(A)$ is a ring.

Proof. Let $f, g \in Hom(A)$. Then $(f+g)(x+y) = f(x+y)+g(x+y) = f(x)+f(y)+g(x)+g(y) = f(x)+g(x)+f(y)+g(y) = (f+g)(x)+(f+g)(y)$. Hence $f+g \in Hom(A)$. Obviously $+$ is associative. Since A is an abelian group $f+g = g+f$.

If 0 is the identity element of the group A then the homomorphism $\mathbf{0}$ defined by $\mathbf{0}(a) = 0$, for all $a \in A$ is the zero element of $Hom(A)$.

Now, let $f \in Hom(A)$. The function $-f$ defined by $(-f)(x) = -[f(x)]$ is also a homomorphism, since $(-f)(x+y) = -[f(x+y)] = -[f(x)+f(y)] = (-f)(x)+(-f)(y)$. Clearly $f+(-f) = 0$ and hence $-f$ is the additive inverse of f. Thus $Hom(A)$ is an abelian group.

Now, $(f \circ g)(x+y) = f[g(x+y)] = f[g(x)+g(y)] = f[g(x)]+f[g(y)] = (f \circ g)(x)+(f \circ g)(y)$. Hence $f \circ g \in Hom(A)$. Similarly $(f+g) \circ h = f \circ h + g \circ h$. Thus $Hom(A)$ is a ring. □

13. Let Q be the set of all symbols of the form $a_0+a_1i+a_2j+a_3k$ where $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Two such symbols $a_0+a_1i+a_2j+a_3k$ and $b_0+b_1i+b_2j+b_3k$ are defined to be equal if and only if $a_i = b_i, i = 1, 2, 3$. We now make Q into a ring by defining $+$ and $\cdot$ as follows. For any $x = a_0+a_1i+a_2j+a_3k$ and $y = b_0+b_1i+b_2j+b_3k$,

$$\begin{aligned} x+y &= (a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k) \\ &= (a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k \text{ and} \\ xy &= (a_0+a_1i+a_2j+a_3k)b_0+b_1i+b_2j+b_3k) \\ &= (a_0b_0-a_1b_1-a_2b_2-a_3b_3)+(a_0b_1+a_1b_0+a_2b_3-a_3b_2)i+ \\ &\quad (a_0b_2+a_2b_0+a_3b_1-a_1b_3)j+(a_0b_3+a_3b_0+a_1b_2-a_2b_1)k. \end{aligned}$$

The formula for the product comes form multiplying the two symbols formally and collecting the terms using the relations $i^2 = j^2 = k^2 = ijk = -1, ij = -ji = k, jk = -kj = i$ and $ki = -ik = j$. Clearly $+$ is associative and commutative. $0 = 0+i0+0j+0k$ is the zero element. $-a_0-a_1i-a_2j-a_3k$ is the additive inverse of $a_0+a_1i+a_2j+a_3k$. The associative law of multiplication and the two distributive laws can be easily verified. Hence $(Q, +, \cdot)$ is a ring. This ring is called the **ring of quaternions**.

14. The set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbb{R}$ is a ring under matrix addition and multiplication.

Proof. Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in R$.

$A+B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R$

$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+ac) & ac-bd \end{pmatrix} \in R$. Clearly matrix addition is commutative and associative. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ is the zero element. $\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ is the inverse of the matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Further matrix multiplication is associative and the distributive laws are valid for 2×2 matrices. Hence R is a ring. □

3.2 Elementary properties of rings

Theorem 3.2.1. Let R be a ring and $a, b \in R$. Then

(i) $0a = a0 = 0$

(ii) $a(-b) = (-a)b = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) $a(b-c) = ab - ac$.

Proof.

(i) $a0 = a(0+0) = a0 + a0$. $\therefore \quad a0 = 0$.(by cancellation law in $(\mathbb{R}, +)$). Similarly $0a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a0 = 0 \Rightarrow a(-b) = -(ab)$. Similarly, $(-a)b = -(ab)$.

(iii) By(ii), $(-a)(-b) = -[a(-b)] = -(-ab) = ab$.

(iv) $a(b-c) = a[b + (-c)] = ab + a(-c) = ab - ac$. □

3.2.1 Solved problems

Problem 3.2.2. If R is a ring such that $a^2 = a$ for all $a \in R$, prove that

(i) $a + a = 0$

(ii) $a + b = 0 \Rightarrow a = b$

(iii) $ab = ba$

Proof. (i) $a+a = (a+a)(a+a) = a(a+a)+a(a+a) = aa+aa+aa+aa = (a+a)+(a+a)$ Hence $a + a = 0$.

(ii) let $a + b = 0$. By (i) $a + a = 0$. Therefore $a + b = a + a$ so that $a = b$.

(iii) $a + b = (a+b)(a+b) = a(a+b) + b(a+b) = aa + ab + ba + bb = a + ab + ba + b$. Hence $ab + ba = 0$, so that by(ii), $ab = ba$. □

Problem 3.2.3. Complete the Cayley table for the ring $R = \{a, b, c, d\}$

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

Solution. First we shall compute cb.

$cb = (b + d)b$ from addition table

$= bb + db = b + b$ from multiplication table

$= a$ from addition table Now, $cc = c(b + d) = cb + cd = a + a = abc = (c + d)c = cc + dc = a + c = cbd = b(b + c) = bb + bc = b + c = ddd = (b + c)d = bd + cd = d + a = d$ Hence the completed table for multiplication is

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

3.3 Isomorphism

In the study of any algebraic system, the idea of two systems being structurally the same is of basic importance. In algebra, this concept is always called **isomorphism**. As in the case of groups, isomorphism between two rings can be defined as follows.

Definition 3.3.1. Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings. A bijection $f : R \to R'$ is called an **isomorphism** if

(i) $f(a + b) = f(a) + f(b)$ and

(ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

If $f : R \to R'$ is an isomorphism, we say that R is isomorphic to R' and write $R \approx R'$.

Note 3.3.2. Let R and R' be two rings and $f : R \to R'$ be an isomorphism. Then clearly f is an isomorphism of the group $(R, +)$ to the group $(R', +)$. Hence $f(0) = 0'$ and $f(-a) = -f(a)$.

Examples 3.3.3. 1. $f : \mathbb{C} \to \mathbb{C}$ defined by $f(z) = \bar{z}$ is an isomorphism. For, clearly f is a bijection. Also $f(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z_1} + \bar{z_2} = f(z_1) + f(z_2)$, and$f(z_1z_2) = \overline{z_1z_2} = \bar{z_1}\bar{z_2} = f(z_1)f(z_2)$.

2. Let $\mathbb{C}$ be the ring of complex numbers. Let S be the set of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbb{R}$. Then S is a ring under matrix addition and matrix multiplication. Refer example 14 of section 3.1. Now the mapping $f : \mathbb{C} \to S$ defined by $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism. Clearly f is a bijection. Now let $x = a + ib$ and $y = c + id$. $f(x + y) = f[(a + ib) + (c + id)] = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = f(x) + f(y)$. Similarly $f(xy) = f(x)f(y)$.(verify).

3. The groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic under the map $f : \mathbb{Z} \to 2\mathbb{Z}$ given by $f(x) = 2x$. However f is not an isomorphism of the ring $(\mathbb{Z}, +)$ to $(2\mathbb{Z}, +)$. Since $f(xy) = 2xy$ and $f(x)f(y) = 2x2y = 4xy$ so that $f(xy) \neq f(x)f(y)$. In fact there is no isomorphism between the rings $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$(verify).

3.4 Types of Rings

Compared with addition in R, the multiplication in R is relatively unknown to us. For example the definition of a ring does not guarantee the existence of an identity with respect to multiplication. The ring $(2\mathbb{Z}, +, \cdot)$ has no multiplicative identity. Even if a ring has a multiplicative identity some elements of the ring may not have multiplicative inverses. For example, the ring $(\mathbb{Z}, +, \cdot)$ has 1 as a multiplicative identity and all the elements of $\mathbb{Z}$ except 1 and -1 do not have multiplicative inverses.

Again in a ring R, the multiplication need not be commutative. For example, in the ring of 2×2 matrices matrix multiplication is not commutative. Hence we get several special classes of rings by imposing conditions on the multiplication structure.

Definition 3.4.1. A ring R is said to be *commutative* if $ab = ba$ for all $a, b \in R$.

Examples 3.4.2.

1. The familiar rings, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all commutative. The following are examples of non-commutative rings.
2. Let F denote the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. We define $(f+g)(x) = f(x)+g(x)$ and $f \cdot g = f \circ g$. Then $(F, +, \cdot)$ is non-commutative ring.
3. The ring of quaternions given in section 13 of section 3.1 is a non-commutative ring since $ij = k$ and $ji = -k$.
4. $M_2(\mathbb{R})$ is non-commutative ring.

Definition 3.4.3. Let R be a ring. We say that R is a *ring with identity* if there exists an element $1 \in R$ such that $a1 = a = 1a$ for all $a \in R$.

Examples 3.4.4.

1. The familiar rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all rings with identity.
2. $(n\mathbb{Z}, +, \cdot)$ when $n > 1$ is a ring which has no identity.
3. $M_2(\mathbb{R})$ is a ring with identity.

Note 3.4.5. Consider the null ring $\{0\}$. In this case 0 is both additive identity and multiplicative identity. This is the only case where 0 can act as the multiplicative identity, for if 0 is the multiplicative identity in a ring R, then $0a = a$ for all $a \in R$. But in any ring $0a = 0$. Hence $a = 0$, so that $R = \{0\}$. In what follows we will exclude this trivial case when speaking of the multiplicative identity. Hence whenever we speak of a multiplicative identity in a ring, we assume that the multiplcative identity is not 0.

Theorem 3.4.6. In a ring with identity the identity element is unique.

Proof. Let $1, 1'$ be multiplicative identities. Then $1 \cdot 1' = 1$(considering $1'$ as identity) and $1 \cdot 1' = 1'$(considering 1 as identity). Therefore $1 = 1'$. Hence the identity element is unique. □

Definition 3.4.7. Let R be a ring with identity. An element $u \in R$ is called a *unit* in R if it has a multiplicative inverse in R. The multiplicative inverse of u is denoted by u^{-1}.

For example, $(\mathbb{Z}, +, \cdot)$, 1 and -1 are units.

In $M_2(\mathbb{R})$, all the non-singular matrices are unit.

In $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ every non-zero elements are unit.

Theorem 3.4.8. Let R be a ring with identity. The set of all units in R is a group under multiplication.

Proof. Let U denote the set of all units in R. Clearly $1 \in U$. Let $a, b \in U$. Hence a^{-1}, b^{-1} exists in R. Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$. Similarly $(b^{-1}a^{-1})(ab) = 1$. Hence $ab \in U$. Also $(a^{-1})^{-1} = a$ and so $a \in U \Rightarrow a^{-1} \in U$. Hence U is a group under multiplication. □

Definition 3.4.9. Let R be a ring with identity element. R is called a *skew field* or a *division ring* if every non-zero element in R is a unit.

(i. e.,) For every non-zero $a \in R$, there exists a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Then in a skew field the non-zero elements form a group under multiplication.

Definition 3.4.10. A commutative skew field is called a **field**. In other words a field is a system $(F, +, \cdot)$ satisfying the following conditions.
(i) $(F, +)$ is an abelian group.
(ii) $(F - \{0\}, \cdot)$ is an abelian group.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Examples 3.4.11. 1. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields under usual addition and multiplication.
2. Let p be a prime. Then $(\mathbb{Z}_p, \oplus, \odot)$ is field.

Proof. $(\mathbb{Z}_p, \oplus, \odot)$ is a ring (by example 8 in section 3.1). Also since p is prime $(\mathbb{Z}_p - \{0\}, \odot)$ is an abelian group.

Hence $(\mathbb{Z}_p, \oplus, \odot)$ is a field. □

3. Let M be the set of all matrices of the form $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ where $a, b \in \mathbb{C}$. Then M is a skew field under matrix addition and multiplication.

Proof. Let $A, B \in M$. Let $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}$. Then $A + B = \begin{pmatrix} a+c & b+d \\ -\overline{b} - \overline{d} & \overline{a} + \overline{c} \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -\overline{(b+d)} & \overline{a+c} \end{pmatrix} \in M$. Hence M is closed under matrix addition. Obviously matrix addition is associative and commutative. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element of M. $\begin{pmatrix} -a & -b \\ \overline{b} & -\overline{a} \end{pmatrix}$ is an additive inverse of $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$. Hence M is an abelian group under matrix addition. Now, $AB = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}$ $= \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{b}c - \overline{ad} & -\overline{b}d + \overline{ac} \end{pmatrix}$ which is of the form $\begin{pmatrix} z & \omega \\ -\overline{\omega} & \overline{z} \end{pmatrix}$. Hence M is closed under matrix multiplication.

Further matrix multiplication is associative and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is the multiplicative identity. Now, let $A = \begin{pmatrix} a & b \\ \overline{b} & \overline{a} \end{pmatrix}$ be a non-zero matrix in M. Then either $a \neq 0$ or $b \neq 0$ so that either $|a| > 0$ or $|b| > 0$. Hence $|A| = a\overline{a} + b\overline{b} = |a|^2 + |b|^2 > 0$. Thus A is a non-singular matrix and has an inverse and $A^{-1} \in M$. Thus M is a skew field. Also since matrix multiplication is not commutative, M is not a field. □

4. Let Q be the ring of quarternions given in example 13 of section 3.1. Q is a skew field but not a field.

Proof. We have proved that $(Q, +, \cdot)$ is a ring. $1 = 1 + 0i + 0j + 0k$ is the identity element. Let $x = a_0 + a_1 i + a_2 j + a_3 k$ be a non-zero element in Q. Then not all

a_0, a_1, a_2, a_3 are zero. Let $\alpha = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Clearly $\alpha \neq 0$. Let $y = (a_0/\alpha) - (a_1/\alpha)i - (a_2/\alpha)j - (a_3/\alpha)k$. Now, $y \in Q$ and $xy = yx = 1$(verify). Thus Q is a skew field. In Q, multiplication is not commutative since $ij = k$ and $ji = -k$. Hence Q is not a field. □

5. $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity but not a field since 1 and -1 are the only non-zero elements which have inverses.

Theorem 3.4.12. In a skew field R, (i) $ax = ay, a \neq 0 \Rightarrow x = y$
(ii) $xa = ya, a \neq 0 \Rightarrow x = y$((i) and (ii) are cancellation laws in rings)
(iii) $ax = 0 \Leftrightarrow a = 0$ or $x = 0$.

Proof.

(i) Let $ax = ay$ and $a \neq 0$. Since R is a skew field there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Hence $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow x = y$.

(ii) can be proved similarly.

(iii) If $a = 0$ or $x = 0$ clearly $ax = 0$. Conversely let $ax = 0$ and $a \neq 0$. Then $ax = a0$ $\Rightarrow x = 0$ by(i). □

Note 3.4.13. Thus in a skew field the product of two non-zero elements is again a non-zero element. However this is not true in an arbitrary ring. For example,

1. Consider the ring $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ where '+'and '$\cdot$'are defined by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac, bd)$. $\mathbb{R} \times \mathbb{R}$ is a commutative ring with identity. Here $(1, 0)(0, 1) = (0, 0)$.

2. The product of two non-zero matrices can be equal to the zero matrix. For example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Definition 3.4.14. Let R be a ring. A non-zero element $a \in R$ is said to be a *zero-divisor* if there exists a non-zero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Examples 3.4.15.

1. In the ring $\mathbb{R} \times \mathbb{R}$, $(1, 0)$ and $(0, 1)$ are zero divisors, since $(1, 0)(0, 1) = (0, 0)$. In fact all the elements of the form $(a, 0)$ and $(0, a)$ where $a \neq 0$ are zero divisors.

2. In the ring of matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ are zero divisors, since $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

3. In the ring $\mathbb{Z}_{12}$, 3 is a zero-divisor, since $3 \odot 4 = 0$. Also 2,4,6 are zero-divisors.

4. In the ring of integers, no element is a zero-divisor.

5. No skew field has any zero-divisor.

Theorem 3.4.16. A ring R has no zero-divisors if and only if cancellation law is valid in R.

Proof. Let R be a ring without zero-divisors. Let $ax = ay$ and $a \neq 0$. Then $ax - ay = 0$ and so $a(x - y) = 0$ and $a \neq 0$. This implies $x - y = 0$ (since R has no zero-divisors) $\Rightarrow x = y$. Thus cancellation law is valid in R.

Conversely let the cancellation law be valid in R. Let $ab = 0$ and $a \neq 0$. Then $ab = 0 = a0$. Hence by cancellation law $b = 0$. Hence R has no zero-divisors. □

Theorem 3.4.17. *Any unit in R cannot be a zero-divisor.*

Proof. Let $a \in R$ be a unit. Then $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$. Similarly $ba = 0 \Rightarrow b = 0$. Hence a cannot be a zero-divisor. □

Note 3.4.18. The converse of the above theorem is not true. (ie.,) a is not a zero-divisor does not imply a is a unit. For example, in $\mathbb{Z}$, 2 is not a zero-divisor and 2 is not a unit.

Definition 3.4.19. A commutative ring with identity having no zero-divisor is called in *integral domain*. Thus in an integral domain $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$. Or equivalently $ab = 0$ and $a \neq 0 \Rightarrow b = 0$; or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Examples 3.4.20. 1. $\mathbb{Z}$ is an integral domain.

2. $n\mathbb{Z}$ where $n > 1$ is not an integral domain since the ring $n\mathbb{Z}$ does not have an identity.

3. $\mathbb{Z}_{12}$ is not an integral domain since 4 is a zero-divisor in $\mathbb{Z}_{12}$.

4. $\mathbb{Z}_7$ is an integral domain.

Theorem 3.4.21. $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

Proof. Let $\mathbb{Z}_n$ be an integral domain. We claim that n is prime. Suppose n is not prime. Then $n = pq$ where $1 < p < n$ and $1 < q < n$. Clearly $p \odot q = 0$. Hence p and q are zero-divisors and so $\mathbb{Z}_n$ is not an integral domain which is a contradiction. Hence n is prime.

Conversely, suppose n is prime. Let $a, b \in \mathbb{Z}_n$. Then $a \odot b = 0 \Rightarrow ab = qn$ where $q \in \mathbb{Z}_n$. $\Rightarrow n|ab \Rightarrow n|a$ or $n|b$ (since n is prime) $\Rightarrow a = 0$ or $b = 0$. $\therefore$ $\mathbb{Z}_n$ has no zero-divisors. Also $\mathbb{Z}_n$ is a commutative ring with identity. Hence $\mathbb{Z}_n$ is an integral domain. □

Theorem 3.4.22. Any field F is an integral domain.

Proof. It is enough to prove that F has no zero-divisors. Let $a, b \in F, ab = 0$ and $a \neq 0$. Since F is a field a^{-1} exists. Now, $ab = 0 \Rightarrow a^{-1}(ab) = 0 \Rightarrow b = 0$. $\therefore$ F has no zero-divisors. Hence F is an integral domain. □

Note 3.4.23. The converse of the above theorem is not true. (i. e.,)An integral domain need not be a field. For example $\mathbb{Z}$ is an integral domain but not a field.

Theorem 3.4.24. Let R be a commutative ring with identity 1. Then R is an integral domain if and only if the set of non-zero elements in R is closed under multiplication.

Proof. Let R be an integral domain. Let $a, b \in R - \{0\}$. Since R has no zero-divisors $ab \neq 0$ so that $R - \{0\}$ is closed under multiplication.

Conversely, suppose $R - \{0\}$ is closed under multiplication. Then the product of any two non-zero elements is a non-zero element. Hence R has no zero-divisors so that R is an integral domain. □

Theorem 3.4.25. Let R be a commutative ring with identity. Then R is an integral domain if and only if cancellation law is valid in R.

Theorem 3.4.26. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain. We need only to prove that every non-zero element in R has a multiplicative inverse. Let $a \in R$ and $a \neq 0$. Let $R = \{0, 1, a_1, a_2, \ldots, a_n\}$. Consider $\{a1, aa_1, aa_2, \ldots, aa_n\}$. By theorem 3.4.24 all these elements are non-zero and all these elements are distinct by Theorem 3.4.25. Hence $aa_i = 1$ for some $a_i \in R$. Since R is commutative , $aa_i = a_i a = 1$ and so that $a = a^{-1}$. Hence R is a field. □

Remark 3.4.27. The above result is not true for an infinite integral domain. For example consider the ring of integers. It is an integral domain but not a field.

Theorem 3.4.28. $\mathbb{Z}_n$ is a field if and only if n is prime.

Proof. By theorem 3.4.26, $\mathbb{Z}_n$ is an integral domain if and only if n is prime. Further $\mathbb{Z}_n$ is finite. Hence the result follows from Theorem 3.4.26. □

Theorem 3.4.29. A finite commutative ring R without zero-divisors is a field.

Proof. If we prove that R has an identity element then R becomes an integral domain and hence by Theorem 3.4.26 it is a field. So we prove the existence of identity. Let $R = \{0, 1, a_1, a_2, \ldots, a_n\}$. Let $a \in R$ and $a \neq 0$. Then the elements $a1, aa_1, aa_2, \ldots, aa_n$, are distinct and non-zero and so $aa_i = a$ for some i. Since R is commutative, we have $aa_i = a_i a = a$. We now prove that a_i is the identity element of R. Let $b \in R$. Then $b = aa_j$ for some j and so $a_i b = a_i(aa_j) = (a_i a)a_j = aa_j = b$. Thus $a_i b = ba_i = b$. Since $b \in R$ is arbitrary, a_i is the identity of R. Hence the theorem. □

3.4.1 Solved problems

Problem 3.4.30. Prove that the set F of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$ is a field under the usual addition and multiplication of real numbers.

Solution. Obviously, $(F, +, \cdot)$ is an abelian group with 0 as the zero element. Now, let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in F$. Then $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)(ad+bc)\sqrt{2} \in F$. Since the two binary operations are the usual addition and multiplication of real numbers, multiplication of real numbers, multiplication is associative and commutative and the two distributive laws are true. $1 = 1+0\sqrt{2} \in F$ and is the multiplicative identity. Now, let $a + b\sqrt{2} \in F - \{0\}$. Then a and b are not simultaneously 0. Also $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$. We claim that $a^2 - 2b^2 \neq 0$.

Case(i) $a \neq 0$ and $b = 0$, then $a^2 - 2b^2 = a^2 \neq 0$.

Case(i) $a = 0$ and $b \neq 0$, then $a^2 - 2b^2 = -2b^2 \neq 0$.

Case(i) $a \neq 0$ and $b \neq 0$. Suppose $a^2 - 2b^2 = 0$.

Then $a^2 = 2b^2$ so that $a^2/b^2 = 2$. Hence $a/b = \pm\sqrt{2}$. Now, $a/b \in \mathbb{Q}$ and $\sqrt{2} \notin \mathbb{Q}$. This is a contradiction. Hence $a^2 - 2b^2 \neq 0$ and so $\frac{1}{a+b\sqrt{2}} = \left(\frac{a}{a^2-2b^2}\right) - \left(\frac{b}{a^2-2b^2}\right)\sqrt{2} \in F$ and is the inverse of $a + b\sqrt{2}$. Hence F is a field.

Problem 3.4.31. $\mathbb{Z}$ is a ring of integers and R is any ring.
Then $\mathbb{Z} \times R = \{(m, x) : \ m \in \mathbb{Z} \text{ and } x \in R\}$. We define $\oplus$ and $\odot$ on $\mathbb{Z} \times R$ as follows. $(m, x) \oplus (n, y) = (m + n, x + y); (m, x) \odot (n, y) = (mn, my + nx + xy)$ where nx and my denote respectively the concerned multiples of the elements x and y in R. Prove that $\mathbb{Z} \times R$ is a ring under $\oplus$ and $\odot$. Also prove that $\mathbb{Z} \times R$ is commutative if and only if R is commutative.

Solution. Clearly $\mathbb{Z} \times R$ is an abelian group under $\oplus$ with $(0, 0)$ as the identity element and the additive inverse of (m, x) is $(-m, -x)$. Clearly $\mathbb{Z} \times R$ is closed under $\odot$. Let $(m, x), (n, y), (p, z) \in \mathbb{Z} \times R$.

$$\begin{aligned}[(m, x) \odot (n, y)] \odot (p, z) &= (mn, my + nx + xy) \odot (p, z)\\ &= (mnp, mnz + p(my + nx + xy) + (my + nx + xy)z)\\ &= (mnp, mnz + pmy + pnx + pxy + myz + znx + xyz)\end{aligned}$$

Now, $$\begin{aligned}(m, x) \odot [(n, y) \odot (p, z)] &= (m, x) \odot (np, nz + py + yz)\\ &= (mnp, m(nz + py + yz) + npx + x(nz + py + yz))\\ &= (mnp, mnz + mpy + myz + npx + nzx + pxy + xyz)\end{aligned}$$

Hence $\odot$ is associative. Now, $(m, x) \odot (1, 0) = (m, x)$ and $(1, 0) \odot (m, x) = (m, x)$.

$\therefore$ $(1,0)$ is the identity element of $\mathbb{Z}\times R$. Now,

$$\begin{aligned}(m,x)\odot[(n,y)\oplus(p,z)] &= (m,x)\odot(n+p,y+z)\\ &= (m(n+p),m(y+z)+(n+p)x+x(y+z))\\ &= (mn+mp,my+mz+nx+px+xy+xz)\\ &= (mn+mp,my+nx+xy+mz+px+xz)\\ &= (mn,my+nx+xy)\oplus(mp,mz+px+xz)\\ &= (m,x)\odot(n,y)\oplus(m,x)(p,z)\end{aligned}$$

$\therefore$ Left distributive law is true. Similarly we can verify the right distributive law,

$$[(m,x)\oplus(n,y)]\odot(p,z)=(m,x)\odot(p,z)\oplus(n,y)(p,z)$$

Hence $\mathbb{Z}\times R$ is a ring with identity. Suppose R is commutative. Then

$$\begin{aligned}(m,x)\odot(n,y) &= (mn,my+nx+xy)\\ &= (nm,nx+my+yx) \text{ (since } R \text{ is commutative } xy=yx)\\ &= (n,y)\odot(m,x) \therefore\ \mathbb{Z}\times R \text{ is commutative.}\end{aligned}$$

Conversely, suppose $\mathbb{Z}\times R$ is commutative. Hence

$(m,x)\odot(n,y)=(n,y)\odot(m,x)(mn,my+nx+xy)=(nm,nx+my+yx)$

Hence $my+nx+xy=nx+my+yx=my+nx+yx$.

$\therefore$ $xy=yx\Rightarrow R$ is commutative.

Problem 3.4.32. Give an examples of

(i) a finite commutative ring with identity which is not an integral domain.

(ii) a finite non-commutative ring.

(iii) an infinite non-commutative ring with identity.

(iv) an infinite ring having no identity.

Solution.

(i) $A=(\mathbb{Z}_4,\oplus,\odot)$ is a finite commutative ring with identity 1. We have $2\odot 2=0$. Thus 2 is a zero-divisor in A and hence A is not an integral domain.

(ii) Consider the set $M_2(\mathbb{Z}_3)$ of all matrices with entries from $\mathbb{Z}_3$. Clearly $M_2(\mathbb{Z}_3)$ is finite and is also a ring under matrix addition and multiplication.

Further $\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}=\begin{pmatrix}1&2\\1&2\end{pmatrix}$ and $\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}1&0\\0&2\end{pmatrix}=\begin{pmatrix}1&1\\2&2\end{pmatrix}$
and hence $M_2(\mathbb{Z}_3)$ is non-commutative.

(iii) $M_2(\mathbb{R})$ is an infinite non-commutative ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(iv) $(\mathbb{Z}_2, +, \cdot)$ is an infinite ring with no identity.

Problem 3.4.33. Prove that the only idempotentt elements of an integral domain are 0 and 1.

Solution. Let R be an integral domain. Let $a \in R$ be an idempotent element. Then $a^2 = a$ so that $a^2 - a = a(a-1) = 0$. Since R has no zer-divisors, $a(a-1) = 0 \Rightarrow a = 0$ or $a - 1 = 0$. Hence $a = 0$ or $a = 1$. Hence 0 and 1 are the only idempotent elements of R.

Problem 3.4.34. Let F be a finite field with n elements. Prove that $a^n = a$ for all $a \in F$.

Solution. If $a = 0$, then obviously $a^n = a = 0$. Hence, let $a \neq 0$. Since F is a field, $F - \{0\}$ is a group under multiplication and $|F - \{0\}| = n - 1$. Hence $a^{n-1} = 1$ and so $a^n = a$.

Problem 3.4.35. Prove that in the case of a ring with identity the axiom $a+b = b+a$ is redundant. (i. e.,) The axiom $a + b = b + a$ can be derived from the other axioms of the ring.

Solution. Using the two distributive laws of a ring. $(1+1)(a+b) = 1(a+b)+1(a+b) = a+b+a+b$ and$(1+1)(a+b) = (1+1)a+(1+1)b = a+a+b+b$. $\therefore a+b+a+b = a+a+b+b$. Hence $b + a = a + b$(by cancellation laws).

Problem 3.4.36. If the additive group of a ring R is cyclic prove that R is commutative. Deduce that a ring with 7 elements is commutative.

Solution. $(R, +)$ is a cyclic group. Let $R = \langle a \rangle$. Let $x, y \in R$. Then $x = ma$ and $y = na$ where $m, n \in \mathbb{Z}$ Now, $xy = mana = (\underbrace{a + a + \cdots + a}_{m\ times})(\underbrace{a + a + \cdots + a}_{n\ times}) = mna^2 = nma^2 = nama = yx$. Hence R is a commutative ring.

Now, let R be a ring with 7 elements. Then $(R, +)$ is a group of order 7. Hence $(R, +)$ is cyclic. Hence R is commutative.

Problem 3.4.37. Let R and R' be rings and $f : R \to R'$ be an isomorphism. Then

(i) R is commutative$\Rightarrow$ R' is commutative.

(ii) R is ring with identity$\Rightarrow$ R' is a ring with identity.

(iii) R is an integral domain$\Rightarrow$ R' is an integral domain.

(iv) R is a field$\Rightarrow$ R' is a field.

Solution.

(i) Let $a', b' \in R'$. Since f is onto, there exists $a, b \in R$ such that $f(a) = a'$ and $f(b) = b'$. Now, $a'b' = f(a)f(b) = f(ab)$ (since f is an isomorphism)

$= f(ba)$ (since R is a commutative ring)

$= f(b)f(a) = b'a'$. Hence R' is a commutative ring.

(ii) Let $1 \in R$ be the identity element of R. Let $a' \in R'$. Then there exists $a \in R$ such that $f(a) = a'$. Now, $f(1)a' = f(1)f(a) = f(1a) = f(a) = a'$. Similarly $a'f(1) = a'$ and so $f(1)$ is the identity element in R'. Hence R' is a ring with identity.

(iii) Let R be an integral domain. Then by (i) and (ii), R' is a commutative ring with identity . Now, we prove that R' has no zero-divisors. Let $a', b' \in R'$ and $a'b' = 0$. Since f is onto there exist $a, b \in R$ such that $f(a) = a'$ and $f(b) = b'$.

$\therefore\ a'b' = 0 \Rightarrow f(a)f(b) = 0 \Rightarrow f(ab) = 0 \Rightarrow ab = 0$ (since f is 1-1)

$\Rightarrow a = 0$ or $b = 0$ (since R is an integral domain)

$\Rightarrow f(a) = 0$ or $f(b) = 0 \Rightarrow a' = 0$ or $b' = 0$ and so R' is an integral domain.

(iv) We need to prove that every non-zero element in R' has an inverse. Let $a' \in R'$ and $a' \neq 0$. Then there exists $a \in R - \{0\}$ such that $f(a) = a'$. Now, $f(a^{-1})a' = f(a^{-1})f(a) = f(a^{-1}a) = f(1)$. Hence $f(a^{-1})$ is the inverse of a'.

Problem 3.4.38. Prove that the only isomorphism $f : \mathbb{Q} \to \mathbb{Q}$ is the identity map.

Solution. Since f is an isomorphism $f(0) = 0$ and $f(1) = 1$. Now, let n be a positive integer.

$$\begin{aligned} f(n) &= f(1 + 1 + \cdots + 1)(\text{written } n \text{ times}) \\ &= f(1) + f(1) + \cdots + f(1)(\text{written } n \text{ times}) \\ &= 1 + 1 + \cdots + 1(\text{written } n \text{ times}) = n. \end{aligned}$$

Now, if n is a negative integer, let $n = -m$ where $m \in \mathbb{N}$. Then $f(n) = f(-m) = -f(m) = -m = n$. Thus for any integer n, $f(n) = n$. Now,let $a \in \mathbb{Q}$. Then $a = p/q$ where $p, q \in \mathbb{Z}$. Hence $f(a) = f(p/q) = f(pq^{-1}) = f(p)f(q^{-1}) = f(p)[f(q)]^{-1} = pq^{-1} = p/q = a$. Hence f is the identity map.

3.5 Characteristic of a ring

Let R be a ring. Then $(R, +)$ is a group. For any $a \in R$ we have $na = a + a + ... + a$ (written n times).

Note 3.5.1. For the ring $\mathbb{Z}_6$ we have $6a = 0$ for all $a \in \mathbb{Z}_6$.

Definition 3.5.2. Let R be a ring. If there exists a positive integer n such that $na = 0$, for all $a \in R$ then the least such positive integer is called the *characteristic of the ring R*. If no such positive integer exists then the ring is said to be of *characteristic zero.*

Examples 3.5.3.

1. $\mathbb{Z}_6$ is a ring of characteristic 6.
2. $\mathbb{Z}$ is a ring of characteristic zero, since there is no positive integer n such that $na = 0$ for all $a \in \mathbb{Z}$.
3. $M_2(\mathbb{R})$ is a ring of characteristic zero.
4. $(\varrho(S), \Delta, \cap)$ is a ring of characteristic 2, since $2A = A\Delta A = \Phi$ for all $A \in \varrho(S)$.
5. Any boolean ring is of characteristic 2(refer solved problem 1 of section 3.2)

Theorem 3.5.4. Let R be a ring with identity 1. If 1 is an element of finite order in the group $(R, +)$ then the order of 1 is the characteristic of R. If 1 is of infinite order, the characteristic of the ring is 0.

Proof. Suppose the order of 1 is n. Then n is the least positive integer such that $n \cdot 1 = 0$. (ie.,) $1 + 1 + \cdots + 1$(n times)= 0. Now, let $a \in R$. Then, $na = a + a + \cdots + a$ (n times) $= 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a = (1 + 1 + \cdots + 1)a. = 0 \cdot a = 0$. Thus $na = 0$ for all $a \in R$. Hence the characteristic of the ring is n. If 1 is of infinite order then there, is no positive integer n such that $n \cdot 1 = 0$. Hence the characteristic of the ring is 0. □

Theorem 3.5.5. The characteristic of an integral domain D is either 0 or a prime number.

Proof. If the characteristic of D is 0 then there is nothing to prove. If not be the characteristic of D be n.

If n is not prime, let $n = pq$ where $1 < p < n$ and $1 < q < n$. Since characteristic of D is n we have $n \cdot 1 = 0$. Hence $n \cdot 1 = pq \cdot 1 = (p \cdot 1)(q \cdot 1) = 0$. Since D is an integral domain either $p \cdot 1 = 0$ or $q \cdot 1 = 0$. Since $p \cdot q$ are both less than n, this contradicts the definition of the characteristic of D. Hence n is a prime number. □

Corollary 3.5.6. The characteristic of any field is either 0 or a prime number.

Proof. Since every field is an integral domain the result follows. □

Note 3.5.7.

1. The characteristic of an arbitrary ring need not be prime. For example $\mathbb{Z}_6$ is of characteristic 6.
2. The converse of the above theorem is not true. (ie.,) If the characteristic of a ring R is prime then R need not be an integral domain. For example the ring $(\varrho(S), \Delta, \cap)$ is of characteristic 2 but not an integral domain. If A and B are two disjoint nonempty subsets of S we have $A \cap B = \Phi$ and hence A and B are zero divisors in $\varrho(S)$.

Theorem 3.5.8. In an integral domain D of characteristic p, the order of every element in the additive group is p.

Proof. Let $a \in D$ be any non-zero element. Let the order of a be n. Then n is the least positive integer such that $na = 0$. Now, by the definition of characteristic of D we have $pa = 0$. Hence $n|p$. Now, since p is prime, $n = 1$ or $n = p$. If $n = 1, na = a = 0$ which is a contradiction. Hence $n = p$. Thus the order of a is p. □

Note 3.5.9. The above result is not true for an arbitrary ring. For example the characteristic of the ring $\mathbb{Z}_6$ is 6 whereas the order of $2 \in \mathbb{Z}_6$ is 3.

3.6 Subrings

Definition 3.6.1. A non-empty subset S of a ring $(R, +, \cdot)$ is called a **subring** if S itself is a ring under the same operations as in R.

Examples 3.6.2.

1. $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

2. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

3. $\mathbb{Q}$ is a subring of $\mathbb{R}$.

4. $\mathbb{R}$ is a subring of $\mathbb{C}$.

5. The set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a subring of $M_2(\mathbb{R})$.

6. $\{0\}$ and R are subrings of any ring. They are called the *trivial subrings* of R.

7. $S = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$.

8. $\{0, 2\}$ is a subring of $\mathbb{Z}_4$.

Theorem 3.6.3. A non-empty subset S of a ring R is a subring if and only if $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$.

Proof. Let S be a subring of R. Then $(S, +)$ is a subgroup of $(R, +)$ Hence $a, b \in S \Rightarrow a - b \in S$. Also since S itself is a ring $ab \in S$.

Conversely, let S be a non-empty subset of R such that $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$. Then $(S, +)$ is a subring of $(R, +)$. Also S is closed under multiplication. The associative and distributive laws are consequences of the corresponding laws in R. Hence S is a subring. □

3.6.1 Solved problems

Problem 3.6.4. Let X be any set and let F be the set of $(\varrho(S), \Delta, \cap)$.

Solution. Let $A, B \in F$. Then A and B are finite sets. Hence $(A - B) \cup (B - A) = A\Delta B$ is a finite set so that $A\Delta B \in F$.

Similarly $A \cap B \in F$. Thus F is a subring.

Problem 3.6.5. Let R be a ring with identity. Then $S = \{n \cdot 1 : \ n \in \mathbb{Z}\}$ is a subring of R.

Solution. Let $a, b \in S$. Then $a = n \cdot 1$ and $b = m \cdot 1$ for some $n, m \in \mathbb{Z}$. Hence $a - b = n \cdot 1 - m \cdot 1 = (n - m) \cdot 1 \in S$. Also $ab = (n \cdot 1)(m \cdot 1) = (nm) \cdot 1 \in S$. Hence S is a subring of R.

Problem 3.6.6. Give an example of

(a) a ring without identity in which a subring has an identity.

(b) a subring without identity, of a ring with identity.

(c) a ring with identity 1 in which a subring has identity $1' \neq 1$.

(d) a subring of a non-commutative ring which is commutative.

(e) a subring of a field, which is not a field.

Solution.

(a) Consider the set R of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ where $a, b \in \mathbb{R}$. Then R is a ring under matrix addition and multiplication(verify). We now prove that this ring does not have an identity. Let $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$ be a matrix such that

$$\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

Now, $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} ac & 0 \\ ad & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$

$\Rightarrow ac = a$ and $ad = b \Rightarrow c = 1$ and $d = ba^{-1}$.

Hence the matrix $\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$ depends on the matrix $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ so that the ring R does not have an identity element.

However the subring S of R consisting of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ has $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as identity.

(b) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$, $\mathbb{Z}$ has 1 as the identity but $2\mathbb{Z}$ does not have an identity.

(c) $M_2(\mathbb{R})$ is a ring with identity $\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}$. The subring $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$ has the identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

(d) Example give in (c).

(e) $\mathbb{Q}$ is a field, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but $\mathbb{Z}$ is not a field.

Theorem 3.6.7. The intersection of two subrings of a ring R is a subring of R.

Proof. Let A, B be two subrings of R. Let $a, b \in A \cap B$. Then $a, b \in A$ and B. Since A and B are subrings $a - b$,$ab \in A$ and B and so $a - b$ and $ab \in A \cap B \Rightarrow A \cap B$ is subring of R. □

Note 3.6.8.

1. The union of the two subring need not be a subring.

2. The union of two subrings of a ring is again a subring if and only if one is contained in the other.

Definition 3.6.9. A non-empty subset S of a field $(F, +, \cdot)$ is called a *subfield* if S is a field under the same operations as in F.

For example, $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Theorem 3.6.10. *A non-empty subset S of a field F is a subfield if and only if*
(i) $a, b \in S \Rightarrow a - b \in S$ and
(ii) $a, b \in S$ and $b \neq 0 \Rightarrow ab^{-1} \in S$.

Proof. The proof follows by applying theorem 1.9.8 to the groups $(F, +)$ and $(F - \{0\}, \cdot)$ □

3.7 Ideals

We now introduce the concept of an ideal in a ring. Ideals play an important role in the development of ring theorey similar to the role played by normal subgroups in group theory.

Definition 3.7.1. Let R be a ring. A non-empty subset of R is called a *left ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$.

(ii) $a \in I$ and $r \in R \Rightarrow ra \in I$.

I is called a *right ideal* of R if

(i) $a, b \in I \Rightarrow a - b \in I$.

(ii) $a \in I$ and $r \in R \Rightarrow ar \in I$.

I is called an *ideal* of R if I is both a left ideal and right ideal.

Thus in an ideal the product of an element in the ideal and an element in the ring is an element of the ideal. In a commutative ring the concepts of the left ideal, right ideal and ideal ccoincide.

Examples 3.7.2.

1. In any ring, R, $\{0\}$ and R are ideals. They are called improper ideals of R.
2. $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proof. Let $a, b \in 2\mathbb{Z}$. Then $a - b \in 2\mathbb{Z}$. Let $a \in 2\mathbb{Z}$ and $b \in 2\mathbb{Z}$. Then ab is even and hence $ab \in 2\mathbb{Z}$. Thus $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. In general $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$(prove). □

3. In $M_2(\mathbb{R})$ the set of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal and it is not a right ideal. Clearly $A, B \in S \Rightarrow A - B \in S$. Now, let $A \in S$ and $B \in M_2(\mathbb{R})$. Let $A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ and $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Then

$$BA = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} pa + qb & 0 \\ ra + sb & 0 \end{pmatrix} \in S.$$

Hence S is a left ideal. However

$$AB = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap & aq \\ bp & bq \end{pmatrix} \notin S.$$ Hence S is not a right ideal.

4. Let R be any ring. Let $a \in R$. Let $aR = \{ax : \ x \in R\}$. Then aR is a right ideal of R. Similarly $Ra = \{xa : \ x \in R\}$. Then Ra is a left ideal of R. Let $ax, ay \in aR$. Then $ax - ay = a(x - y) \in aR$. Let $ax \in aR$ and $y \in R$. Then $(ax)y = a(xy) \in aR$. Thus aR is a right ideal. Similarly Ra is a left ideal of R.

Definition 3.7.3. If R is a commutative ring then $aR = Ra$ is an ideal. This is called the *principal ideal* generated by a and is denoted by $\langle a \rangle$.

Note 3.7.4. If R is a commutative ring with identity 1 then $a = a1 \in \langle a \rangle$. This may not be true if the ring R does not have an identity.

For example,consider the ring $2\mathbb{Z}$. Here $\langle 4 \rangle = \{0, \pm 8, \pm 16, \pm 24, \ldots, \}$ and $4 \in \langle 4 \rangle$.

Remark 3.7.5. (i) Every left ideal of a ring R is a subring of R. Let I be a left ideal of R. Let $a, b \in I$. Then by definition, $a - b$ and $ab \in I$. Hence I is a subring of R.
(ii) Similarly every right ideal of R is also a subring of R.
(iii) Any ideal of R is a subring of R. (by(i) and (ii))
(iv) However, a subring of R need not be an ideal of R.
For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$ since $1 \in \mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q}$ but $1 \cdot \frac{1}{2} \notin \mathbb{Z}$.

Theorem 3.7.6. Let R be a ring with identity 1. If I is an ideal of R and $1 \in I$, then $I = R$.

Proof. Obviously $I \subseteq R$. Now, let $r \in R$. Since $1 \in I$, $r \cdot 1 = r \in I$. Thus $R \subseteq I$. Hence $R = I$. □

Theorem 3.7.7. Let F be any field. Then the only ideals of F are $\{0\}$ and F. (i.e.,)A field has no proper ideal.

Proof. Let I be an ideal of F. Suppose $I \neq \{0\}$. We shall prove that $I = F$. Since $I \neq \{0\}$, there exists an element $a \in I$ such that $a \neq 0$. Since F is a field a has a multiplicative inverse $a^{-1} \in F$. Now, $a \in I$ and $a^{-1} \in F \Rightarrow aa^{-1} = 1 \in I$. Hence by above theorem, $I = F$. □

Theorem 3.7.8. Let R be a commutative ring with identity. Then R is a field if and only if R has no proper ideals.

Proof. If R is a field, by above theorem, R has no proper ideals.

Conversely, suppose R has no proper ideals. To prove that R is a field we need to show that every non-zero elementt in R has an inverse. Let $a \in R$ and $a \neq 0$. Consider the principal ideal aR. Since R is a ring with identity, $a = a \cdot 1 \in aR$ and so $aR \neq \{0\}$. Since R has no proper ideals, $aR = R$. Hence there exists $x \in R$ such that $ax = 1$ and x is the inverse of a. Hence R is a field. □

Definition 3.7.9. An integral domain R is said to be a *prinipal ideal domain(PID)* if every ideal is a principal ideal.

Examples 3.7.10.

1. $\mathbb{Z}$ is a principal ideal domain since every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.
2. Any field F is a principal ideal domain since the only ideals of F are $\{0\}$ and $\langle 1 \rangle = F$.

3.8 Quotient rings

Let R be a ring. Let $(I, +)$ be a subgroup of $(R, +)$. Since addition is commutative in R, I is a normal subgroup of $(R, +)$ and hence the collection $R/I = \{I + a : \ a \in R\}$ is a group under the operation defined by $(I+a)+(I+b) = I+(a+b)$. To make R/I a ring, we have to define a multiplication in R/I. It is natural to define $(I+a)(I+b) = I+ab$. But we have to prove the multiplication is well defined (ie.,) it is independent of the choice of the representatives from the casets. We shall prove that this happens if and only if I is an ideal.

Theorem 3.8.1. Let R be a ring and I be a subgroup of $(R, +)$. The multiplication in R/I given by
$(I + a)(I + b) = I + ab$ is well defined if and only if I is an ideal of R.

Proof. Let I be an ideal of R. To prove multiplication is well defined, let $I+a_1 = I+a$ and $I + b_1 = I + b$. Then $a_1 \in I + a$ and $b_1 \in I + b$. $\therefore \ \ a_1 = i_1 + a$ and $b_1 = i_2 + b$ where $i_1, i_2 \in I$. Hence $a_1b_1 = (i_1 + a)(i_2 + b) = i_1i_2 + i_1b + ai_2 + ab$. Now since I is an ideal we have $i_1i_2, i_1b, ai_2 \in I$. Hence $a_1b_1 = i_3 + ab$ where $i_3 = i_1i_2 + i_1b + ai_2 \in I$. $\therefore \ \ a_1b_1 \in I + ab$. Hence $I + ab = I + a_1b_1$.

Conversely suppose that the multiplication in R/I given by $(I+a)(I+b) = I+ab$ is well defined. To prove that I is an ideal of R. Let $i \in I$ and $r \in R$. We have to prove that $ir, ri \in I$ Now, $I + ir = (I+i)(I+r) = (I+0)(I+r) = I + 0r = I$. $\therefore ir \in I$. Similarly $ri \in I$. Hence I is an ideal. □

Definition 3.8.2. Let R be any ring and I be an ideal of R. We have two well defined binary operations in R/I given by $(I+a)+(I+b) = I+(a+b)$ and $(I+a)(I+b) = I+ab$. It is easy to verify that R/I is a ring under these operations.

The ring R/I is called the *quotient ring of R modulo I*

Examples 3.8.3.

1. The subset $I = \{0, 3\}$ of $\mathbb{Z}_6$ is an ideal (verify) $\mathbb{Z}_6/I = \{I, I+1, I+2\}$ is a ring isomorphism to $\mathbb{Z}_3$. Here $\mathbb{Z}_6$ is not an integral domain but the quotient ring $\mathbb{Z}_6/I$ is an integral domain.
2. The subset $p\mathbb{Z}$ where p is prime is an ideal of the ring R. $\mathbb{Z}/p\mathbb{Z} = \{p\mathbb{Z}, p\mathbb{Z}+1, \cdots, p\mathbb{Z}+(p-1)\}$. It is easy to see that the ring $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p$. Here $\mathbb{Z}$ is an integral domain but not a field whereas $\mathbb{Z}/p\mathbb{Z}$ is a field.

3.9 Maximal ideals

We have seen that if R is a ring and I is an ideal of R then R/I is a ring. Further is R is commutative then R/I is also commutative. We now proceed to answer the following questions for commutative rings with identity. Which ideals I give rise to quotient rings that are (i) and (ii) integral domains?

Definition 3.9.1. Let R be a ring. An ideal $M \neq R$ is said to be a *maximal ideal* of R if whenever U is an ideal of R such that $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. That is, there is no proper ideal of R property containing M.

Examples 3.9.2.

1. $\langle 2 \rangle$ is a maximal ideal in $\mathbb{Z}$. For, let U be an ideal properly containing $\langle 2 \rangle$. Then U contains an odd integer say, $2n+1$ and so $1 = (2n+1) - 2n \in U \Rightarrow U = \mathbb{Z}$. Thus

there is no proper ideal of $\mathbb{Z}$ properly containing $\langle 2\rangle$. Hence $\langle 2\rangle$ is a maximal ideal of $\mathbb{Z}$.

2. Let p be any prime. Then $\langle p\rangle$ is maximal ideal in $\mathbb{Z}$. Let U be any ideal of $\mathbb{Z}$ such that $\langle p\rangle \subseteq U$. Since every ideal of $\mathbb{Z}$ is a principal ideal $U = \langle n\rangle$ for some $n \in \mathbb{Z}$. Now, $p \in \langle p\rangle \subseteq U \Rightarrow p \in U = \langle n\rangle$ and $p = mn$ for some integer m. Since p is prime either $n = 1$ or $n = p$. Suppose $n = 1$. Then $U = \mathbb{Z}$.

   Suppose $n = p$. Then $U = \langle p\rangle$ and so there is no proper ideal of $\mathbb{Z}$ properly containing $\langle p\rangle$. Hence $\langle p\rangle$ is a maximal ideal in $\mathbb{Z}$.

3. In any field F, $\langle 0\rangle$ is a maximal ideal of F since the only ideals of F are $\{0\}$ and F.

4. Let R be the ring of all real valued continuous functions on $[0, 1]$. Let $M = \{f \in R : f(1/2) = 0\}$. Clearly M is an ideal of R. Let U be any ideal of R properly containing M. Then there exists a function $g(x) \in U$ such that $g(1/2) \neq 0$. Let $g(1/2) = c$. Take $h(x) = g(x) - c$. Then $h(1/2) = g(1/2) - c = c - c = 0$ and so $h(x) \in M \subseteq U$. Also $g(x) \in U$. Hence $g(x) - h(x) \in U$ and so $c \in U \Rightarrow 1 = cc^{-1} \in U$ $\Rightarrow U = R$. Thus there is no proper ideal of R properly containing M. Hence M is maximal in R.

5. $\langle 4\rangle$ is not a maximal ideal in $\mathbb{Z}$. For, $\langle 2\rangle$ is proper ideal of $\mathbb{Z}$ properly containing $\langle 4\rangle$.

Theorem 3.9.3. Let R be a commutative ring with identity. An ideal M of R is maximal if and only if R/M is field.

Proof. Let M be a maximal ideal in R. Since R is a commutative ring with identity and $M \neq R$, R/M is also a commutative ring with identity. Now, let $M + a$ be a non-zero element in R/M is that $a \notin M$. We shall now prove that $M + a$ has multiplicative inverse in R/M.

Let $U = \{ra + m : \ r \in R \ \text{ and } m \in M\}$. We claim that U in an ideal of R. $(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2) \in U$. Also, $r(r_1a + m_1) = (rr_1)a + rm_1 \in U$ (since $rm_1 \in M$). Therefore U is an ideal of R.

Now, let $m \in M$. Then $m = 0a + m \in U$ and so $M \subseteq U$. Also $a = 1a + 0 \in U$ and $a \notin M$. Therefore $M \neq U$. $\Rightarrow U$ is an ideal of R properly containing M. But M

is a maximal ideal of R. Therefore $U = R$. Hence $1 \in U$ and so $1 = ba + m$ for some $b \in R$.

Now, $M + 1 = M + ba + m = M + ba$(since $m \in M$) $= (M + b)(M + a)$. Hence $M + b$ is the inverse of $M + a$. Thus every non-zero element of R/M has inverse. Hence R/M is a field.

Conversely, suppose R/M is a field. Let U be any ideal of R properly containing M. Then there exists an element $a \in U$ such that $a \notin M$. $M + a$ is a non-zero element of R/M. Since R/M is a field $M + a$ has an inverse, say $M + b$. Therefore $(M + a)(M + b) = M + 1 \Rightarrow M + ab = M + 1 \Rightarrow 1 - ab \in M$. But $M \subseteq U$. Hence $1 - ab \in U$. Also $a \in U \Rightarrow ab \in U$. Clearly $1 = (1 - ab) + ab \in U$, $1 \in U$ and so $U = R$. Thus there is no proper ideal of R properly containing M. Hence M is a maximal ideal in R. □

3.10 Prime ideal

Definition 3.10.1. Let R be a commutative ring. An idesl $P \neq R$ is called a *prime ideal* if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Examples 3.10.2.

1. Let R be an integral domain. Then $\langle 0 \rangle$ is a prime ideal of R. For, $ab \in \langle 0 \rangle \Rightarrow ab = 0$ $\Rightarrow a = 0$ or $b = 0$(since R is an I.D) $\Rightarrow a \in \langle 0 \rangle$ or $b \in \langle 0 \rangle$.

2. $\langle 3 \rangle$ is a prime ideal of $\mathbb{Z}$. For, $ab \in \langle 3 \rangle \Rightarrow ab = 3n$ for some integer n.

$$\Rightarrow 3|ab \Rightarrow 3|a \text{ or } 3|b \Rightarrow a \in \langle 3 \rangle \text{ or } b \in \langle 3 \rangle.$$

$\therefore$ $\langle 3 \rangle$ is a prime ideal.

Note 3.10.3. In fact for any prime number p, the ideal $\langle p \rangle$ is a prime ideal in $\mathbb{Z}$. $\langle 4 \rangle$ is not a prime ideal in $\mathbb{Z}$.

For, $2 \times 2 \in \langle 4 \rangle$, But $2 \notin \langle 4 \rangle$.

Theorem 3.10.4. Let R be any commutative ring with identity. Let P be an ideal of R. Then P is a prime ideal $\Leftrightarrow$ R/P is an integral domain.

Proof. Let P be a prime ideal. Since R is a commutative ring with identity R/P is also commutative ring with identity. Now, $(P + a)(P + b) = P + 0 \Rightarrow P + ab = P$ $\Rightarrow ab \in P \Rightarrow a \in P$ or $b \in P$ (since P is a prime ideal) $\Rightarrow P + a = P$ or $P + b = P$ Thus R/P has no zero divisors and so R/P is an integral domain.

Conversely, suppose R/P is an integral domain. We claim that P is a prime ideal of R. Let $ab \in P$. Then $P + ab = P \Rightarrow (P + a)(P + b) = P \Rightarrow P + a = P$ or $P + b = P$(since R/P is an integral domain) $\Rightarrow a \in P$ or $b \in P \Rightarrow P$ is a prime ideal of R. □

Corollary 3.10.5. Let R be a commutative ring with identity. Then every maximal ideal of R is a prime ideal of R.

Proof. Let M be a maximal ideal of R. Then R/M is a field $\Rightarrow R/M$ is an integral domain $\Rightarrow M$ is a prime ideal. □

For example, $\langle 0\rangle$ is a prime ideal of $\mathbb{Z}$ but not a maximal ideal of $\mathbb{Z}$.

3.11 Homomorphism of rings

Definition 3.11.1. Let R and R' be rings. A function $f : R \to R'$ is called a *homomorphism* if
(i) $f(a + b) = f(a) + f(b)$ and
(ii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

If f is 1-1, then f is called a *monomorphism*. If f is onto, then f is called an *epimorphism*. A homomorphism of a ring onto itself is called an *endomorphism*.

Note 3.11.2.

1. Obviously an isomorphism of a ring is a homomorphism and a 1-1, onto homomorphism is an isomorphism.

2. The name homomorphism is used for mapping between groups and between rings. In groups, a homomorphism preserves the binary operation of the group. Since rings have two binary operations, a ring homomorphism is defined as a mapping preserving the two binary operations in a ring.

3. Condition (i) of ring homomorphism says that f is a group homomorphism from the additive group $(R,+)$ to the additive group $(R',+)$.

Examples 3.11.3.

1. $f : R \to R'$ defined by $f(a) = 0$ for all $a \in R$ is obviously a homomorphism. f is called the *trivial homomorphism.*

2. Let R be any ring. The identity map $i : R \to R$ is obviously a homomorphism.

3. Let R be any ring. $f : R \times R \to R$ given by $f(x,y) = x$ is a ring homomorphism. For, $f[(a,b)+(c,d)] = f(a+c, b+d) = a+c = f(a,b)+f(c,d)$
Also, $f[(a,b)(c,d)] = f(ac,bd) = ac = f(a,b)f(c,d)$.

4. $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = r$ where $x = qn + r$, $0 \leq r < n$ is a homomorphism. For, let $a, b \in \mathbb{Z}$. Let $a = q_1 n + r_1$ where $0 \leq r_1 < n$, $b = q_2 n + r_2$ where $0 \leq r_2 < n$, $r_1 + r_2 = q_3 n + r_3$ where $0 \leq r_3 < n$ and $r_1 r_2 = q_4 n + r_4$ where $0 \leq r_4 < n$.
Now, $(a+b) = (q_1+q_2)n + r_1 + r_2 = (q_1+q_2+q_3)n + r_3$
$$\therefore\ f(a+b) = r_3 = r_1 \oplus r_2 = f(a) \oplus f(b)$$
Also,
$ab = (q_1 n + r_1)(q_2 n + r_2) = n(q_1 q_2 n + r_1 q_2 + r_2 q_1) + r_1 r_2 = n(q_1 q_2 n + r_1 q_2 + r_2 q_1 + q_4) + r_4$
$$\therefore\ f(ab) = r_4 = r_1 \odot r_2 = f(a) \odot f(b)$$
Hence f is a homomorphism.

5. Let R be a ring and I be an ideal of R. Then $\Phi : R \to R/I$ defined by $\Phi(x) = I + x$ is a ring homomorphism. Φ is called the *natural homomorphism.*
$$\Phi = I + (x+y) = (I+x) + (I+y) = \Phi(x) + \Phi(y)$$
$$\Phi(xy) = I + xy = (I+x)(I+y) = \Phi(x)\Phi(y)$$
Hence Φ is a ring homomorphism.

Theorem 3.11.4. Let R and R' be rings and $f : R \to R'$ be a homomorphism. Then,
(i) $f(0) = 0'$
(ii) $f(-a) = -f(a)$ for all $a \in R$.
(iii) If S is a subring of R, then $f(S)$ is a subring of R'. In particular $f(R)$ is an subring of R'.

(iv) If S is an ideal of R, then $f(S)$ is an ideal of $f(R)$.

(v) If S' is a subring of R', then $f^{-1}(S)$ is a subring of R.

(vi) If S' is an ideal of $f(R)$, then $f^{-1}(S')$ is an ideal of R.

(vii) If R is a ring with identity 1 and $f(1) \neq 0'$, then $f(1) = 1'$ is the identity of $f(R)$.

(viii) If R is a commutative ring then $f(R)$ is also commutative.

Proof. Since f is a homomorphism of the group $(R, +)$ to $(R', +)$, the results (i) and (ii) are obvious.

(iii) Since S is a subring of R, $(S, +)$ is a subgroup of $(R, +)$ and hence $f(S)$ is a subgroup of $(R', +)$. Now, let $a', b' \in f(S)$. Then $a' = f(a)$ and $b' = f(b)$ for some $a, b \in S$ and $a'b' = f(a)f(b) = f(ab) \in f(S)$. Hence $f(S)$ is a subring of R'.

(iv) Let S be an ideal of R. To prove that $f(S)$ is an ideal of $f(R)$ it is enough if we prove that $r' \in f(R)$ and $a' \in f(S) \Rightarrow r'a'$ and $a' = f(a)$ where $r \in R$ and $a \in S$. Now, since S is an ideal of R, ra and $ar \in S$. Hence $f(ra) = f(r)f(a) = r'a' \in f(S)$. Similarly $a'r' \in f(S)$. Hence $f(S)$ is an ideal of $f(R)$.

(v) Let S' be a subring of R'. Since $(S', +)$ is a subgroup of $(R', +)$, $f^{-1}(S')$ is a subgroup of $(R, +)$. Now, let $a, b \in f^{-1}(S')$. Then $f(a), f(b) \in S' \Rightarrow f(ab) = f(a)f(b) \in S'$ (since S' is a subring of R) $\Rightarrow ab \in f^{-1}(S')$. Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is similar to that of (v).

(viii) Let R be a ring with identity 1. Let $a' \in f(R)$. Then $a' = f(a)$ for some $a \in R$. Now, $a'f(1) = f(a)f(1) = f(a1) = f(a) = a'$. Similarly $f(1)a' = a'$. Also $f(1) \neq 0$. Hence $f(1)$ is the identity of $f(R)$. □

Definition 3.11.5. The *kernel* K of a homorphism f of a ring R to a ring R' is defined by $\{a : a \in R \text{ and } f(a) = 0\}$.

Theorem 3.11.6. Let $f : R \to R'$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of R.

Proof. By definition, $K = f^{-1}(\{0\})$. Since $\{0\}$ as an ideal of $f(R)$, by (vi) of theorem, K is an ideal of R. □

Theorem 3.11.7 (The fundamental theorem of homomorphism)**.** Let R and R' be rings and $f : R \to R'$ be an epimorphism. Let K be the kernel of f. Then $R/K \cong R'$.

Proof. Define $\Phi : R/K \to R'$ by $\Phi(K + a) = f(a)$.

(i) Φ is well defined, for, let $K+b = K+a$. Then $b \in K+a \Rightarrow b = k+a$ where $k \in K \Rightarrow f(b) = f(k+a) = f(k)+f(a) = 0+f(a) = f(a) \Rightarrow \Phi(K+b) = f(b) = f(a) = \Phi(K+a)$.

(ii) Φ is 1-1.

For, $\Phi(K + a) = \Phi(K + b) \Rightarrow f(a) = f(b) \Rightarrow f(a) - f(b) = 0$
$\Rightarrow f(a) + f(-b) = 0 \Rightarrow f(a - b) = 0 \Rightarrow a - b \in K \Rightarrow a \in K + b \Rightarrow K + a = K + b$

(iii) Φ is onto. For, let $a' \in R'$. Since f is onto, there exists $a \in R$ such that $f(a) = a'$. Hence $\Phi(K + a) = f(a) = a'$.

(iv) Φ is homomorphism.

For, $\Phi[(K + a) + (K + b)] = \Phi[K + (a + b)] = f(a + b)$
$= f(a) + f(b)$ (since f is a homomorphism) $= \Phi(K + a) + \Phi(K + b)$.

and $\Phi[(K + a)(K + b)] = \Phi(K + ab) = f(ab)$
$= f(a)f(b)$ (since f is a homomorphism) $= \Phi(K + a)\Phi(K + b)$

Hence Φ is an homomorphism. Hence $R/K \cong R'$ □

3.11.1 Solved problems

Problem 3.11.8. The homomorphic image of an integral domain need not be an integral domain.

Solution. $f : \mathbb{Z} \to \mathbb{Z}_4$ defined by $f(a) = r$ where $a = 4q + r$, $0 \leq r < 4$ is a homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_4$. Here $\mathbb{Z}$ is an integral domain and $\mathbb{Z}_4$ is not an integral domain since $2 \odot 2 = 0$.

Problem 3.11.9. Any hoomomorphism of a field to itself is either 1-1 or maps every element to 0.

Solution. Let F be a field and $f : F \to F$ be a homomorphism. Let K be the kernel of f. Then K is an ideal of F and$K = \{0\}$ or $K = F$. If $K = \{0\}$ then f is 1-1. If $K = F$ then $f(a) = 0$ for all $a \in F$.

Chapter 4

UNIT IV: Vector Space

4.1 Introduction

Upto this point we have been introduced to two basic algebraic systems namely *groups* and *rings*. In this chapter we introduce another algebraic system known as *vector spaces*. The idea of a vector arises in the study of various physical applications. Many physical entites like mass, temperature etc., are characterised in terms of a real number and are called scalars. Other physical entities such as the velocity of a particle or force acting at a point are determined only when both magnitude and direction are specified. Such entities are called *vectors*. Since the concept of direction is geometrical a vector can be represented geometrically by a line segment whose direction is that of the given vector and whose length represents the magnitude of the vector. Two vectors $\mathbf{u}$ and $\mathbf{v}$ passing through a point O can be added by the usual parallelogram law of forces and we obtain the vector $\mathbf{u}+\mathbf{v}$. The vector of zero magnitude is the zero vector denoted by $\mathbf{0}$ and clearly $\mathbf{u}+\mathbf{0}=\mathbf{0}+\mathbf{u}=\mathbf{u}$. If a vector $\mathbf{u}$ is represented by a line segment $\overrightarrow{AB}$, then the vector represented by the line segment $\overrightarrow{BA}$, is called the *negative* of $\mathbf{u}$ and is denoted by $-\mathbf{u}$ and it is clear that $\mathbf{u}+(-\mathbf{u})=(-\mathbf{u})+\mathbf{u}=\mathbf{0}$. Further this addition of vectors is commutative and associative. Hence the set V of vectors at a point O in a plane is an abelian group with respect to addition.

If $\mathbf{u}$ is a vector then $\mathbf{u}+\mathbf{u}=2\mathbf{u}$ is evidently a vector in the same direction as $\mathbf{u}$, but of twice its magnitude. This introduces a new concept of multiplication of a vector by a scalar, the resulting product being a vector. Thus given any real number α and a vector $\mathbf{u}$ passing through O then $\alpha\mathbf{u}$ is the vector whose direction is either the same as that of $\mathbf{u}$ or opposite to that of $\mathbf{u}$ according as $\alpha > 0$ or $\alpha < 0$ and whose magnitude is $|\alpha|$ times the magnitude of $\mathbf{u}$. This association gives rise to a map from $\mathbb{R} \times V$ to V given by $(\alpha, \mathbf{u}) \to \alpha\mathbf{u}$. It can be easily be verified that $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$ and $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$ where $\mathbf{u}, \mathbf{v} \in V$ and $\alpha, \beta \in \mathbb{R}$. These ideas motivate the following abstract definition of a vector space V over a field F.

4.2 Definition and Examples

Definition 4.2.1. A non-empty set V is said to be a vector space over a field F if

(i) V is an abelian group under an poeration called **addition** which we denote by $+$.

(ii) For every $\alpha \in F$ and $v \in V$, there is defined an element αv in V subject to the following conditions.

(a) $\alpha(u + v) = \alpha u + \alpha v$ for all $u, v \in V$ and $\alpha \in F$.

(b) $(\alpha + \beta)u = \alpha u + \beta u$ for all $u \in V$ and $\alpha, \beta \in F$.

(c) $\alpha(\beta u) = (\alpha\beta)u$ for all $u \in V$ and $\alpha, \beta \in F$.

(d) $1u = u$ for all $u \in V$.

Remark 4.2.2.

1. The elements of F are called **scalars** and the elements of V are called **vectors**.

2. The rule which associates with each scalar $\alpha \in F$ and a vector $v \in V$, a vector αv is called the **scalar multiplication**. Thus a scalar multiplication gives rise to a function from $F \times V \to V$ defined by $(\alpha, v) \to \alpha v$.

Examples 4.2.3.

1. $\mathbb{R} \times \mathbb{R}$ is a vector space over a field $\mathbb{R}$ under the addition and scalar multiplication defined by $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ and $\alpha(x_1, x_2) = (\alpha x_1, \alpha x_2)$.

Proof. Clearly the binary operation $+$ is commutative and associative and $(0,0)$ is the zero element. The inverse of (x_1, x_2) is $(-x_1, -x_2)$. Hence $(\mathbb{R}\times\mathbb{R}, +)$ is an abelian group. Now, let $u = (x_1, x_2)$ and $v = (y_1, y_2)$ and let $\alpha, \beta \in \mathbb{R}$. Then

$$\alpha(u+v) = \alpha[(x_1,x_2)+(y_1,y_2)] = \alpha(x_1+y_1, x_2+y_2) = (\alpha x_1+\alpha y_1, \alpha x_2+\alpha y_2)$$
$$= (\alpha x_1, \alpha x_2) + (\alpha y_1, \alpha y_2) = \alpha(x_1,x_2)+\alpha(y_1,y_2) = \alpha u+\alpha v. \text{ Now,}$$
$$(\alpha+\beta) = (\alpha+\beta)(x_1,x_2) = ((\alpha+\beta)x_1, (\alpha+\beta)x_2) = (\alpha x_1+\beta x_1, \alpha x_2+\beta x_2)$$
$$= (\alpha x_1, \alpha x_2)+(\beta x_1, \beta x_2) = \alpha(x_1,x_2)+\beta(x_1,x_2) = \alpha u+\beta u.$$

Also $\alpha(\beta u) = \alpha(\beta(x_1,x_2)) = \alpha(\beta x_1, \beta x_2) = (\alpha\beta x_1, \alpha\beta x_2) = (\alpha\beta)(x_1,x_2) = (\alpha\beta)u$

Obviously $1u = u$ $\therefore$ $\mathbb{R}\times\mathbb{R}$ is a vector space over $\mathbb{R}$. □

2. $\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : \ x_i \in \mathbb{R}, 1 \le i \le n\}$. Then $\mathbb{R}^n$ is a vector space over $\mathbb{R}$ under addition and scalar multiplication defined by $(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$ and $\alpha(x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$.

Proof. Clearly the binary operation $+$ is commutative and associative. $(0,0,\ldots,0)$ is the zero element. The inverse of $(x_1, x_2, \ldots, x_n)$ is $(-x_1, -x_2, \ldots, -x_n)$. Hence $(\mathbb{R}^n, +)$ is an abelian group. Now, let $u = (x_1, x_2, \ldots, x_n)$ and $v = (y_1, y_2, \ldots, y_n)$ and let $\alpha, \beta \in \mathbb{R}$. Then

$$\alpha(u+v) = \alpha[(x_1,x_2,\cdots,x_n)+(y_1,y_2,\cdots,y_n)] = \alpha(x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$$
$$= (\alpha x_1+\alpha y_1, \alpha x_2+\alpha y_2, \ldots, \alpha x_n+\alpha y_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)+(\alpha y_1, \alpha y_2, \ldots, \alpha y_n)$$
$$= \alpha(x_1, x_2, \ldots, x_n)+\alpha(y_1, y_2, \ldots, y_n) = \alpha u+\alpha v.$$ Similarly $(\alpha+\beta)u = \alpha u+\beta u$ and $\alpha(\beta u) = (\alpha\beta)u$. $\therefore 1u = u$. $\therefore \mathbb{R}^n$ is vector space over $\mathbb{R}$. □

Note 4.2.4. We denote this vector space over by $V_n(\mathbb{R})$.

3. Let F be any field. Let $F^n = \{(x_1, x_2, \ldots, x_n) : \ x_i \in F\}$. In F^n we define addition and scalar multiplication as in above example. Then F^n is a vector space over F and we denote this vector space by $V_n(F)$.

Note 4.2.5. In this example if we take $n = 1$ then we see that any field F is a vector space over itself. The addition and scalar multiplication in this vector space are simply the addition and multiplication of the field F.

4. $\mathbb{C}$ is a vector space over the field $\mathbb{R}$. Here addition is the usual addition in $\mathbb{C}$ and the scalar multiplication is the usual multiplication of a real number and a complex number. (ie).,$(x_1+ix_2)+(y_1+iy_2) = (x_1+y_1)+i(x_2+y_2)$ and $\alpha(x_1+ix_2) = \alpha x_1+i\alpha x_2$.

Proof. Clearly $(\mathbb{C}, +)$ is an abelian group. Also the remaining axioms of a vector space are true since the scalars and vectors involved are complex numbers and further the operations are usual addition and multiplication. Hence $\mathbb{C}$ is a vector space over $\mathbb{R}$. □

5. Let $V = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$. Then V is a vector space over $\mathbb{Q}$ under addition and multiplication.

Proof. Obviously V is an abelian group under usual addition. The remaining axioms of a vector space are true since the scalars and vectors are real numbers and the operations are usual addition and multiplication. Hence V is a vector space over $\mathbb{Q}$. □

6. Let F be a field. Then $F[x]$, the set of all polynomials over F, is a vector space over F under the addition of polynomials and scalar multiplication defined by
$\alpha(a_0 + a_1x + \cdots + a_nx^n) = \alpha a_0 + \alpha a_1x + \cdots + \alpha a_nx^n$.

7. The set V of all polynomials of degree $\leq n$ including the zero polynomial in $F[x]$ is a vector space over the field F under the addition and scalar multiplication defined as in example 6.

Proof. Let $f, g \in V$. Then f and g are polynomials of degree $\leq n$. $\therefore f + g$ and αf are of degree $\leq n$. $\therefore f + g, \alpha f \in V$. The other axioms of a vector space can easily be verified. Hence V is a vector space over F. □

8. The set $M_2(\mathbb{R})$ of all 2×2 matrices is a vector space over $\mathbb{R}$ under matrix addition and scalar multiplication defined by

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

9. Let V be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. Let $f, g \in V$. We define $(f + g)(x) = f(x) + g(x)$ and $(\alpha f)(x) = \alpha[f(x)]$. V is a vector space over $\mathbb{R}$.(verify)

10. Let V denote the set of all solutions of the dif and only iferential equation $2\frac{d^2y}{dx^2} - 7\frac{dy}{dx} + 3y = 0$. Then V is a vector space over $\mathbb{R}$.

Proof. Let $f, g \in V$ and $\alpha \in \mathbb{R}$. Then

$$2\frac{d^2f}{dx^2} - 7\frac{df}{dx} + 3f = 0 \text{ and } 2\frac{d^2g}{dx^2} - 7\frac{dg}{dx} + 3g = 0$$

$$\therefore\ 2\left(\frac{d^2f}{dx^2} + \frac{d^2g}{dx^2}\right) - 7\left(\frac{df}{dx} + \frac{dg}{dg}\right) + 3(f+g) = 0$$

$$2\frac{d^2}{dx^2}(f+g) - 7\frac{d}{dx}(f+g) + 3(f+g) = 0$$

Hence $f + g \in V$. Also $2\frac{d^2}{dx^2}(\alpha f) - 7\frac{d}{dx}(\alpha f) + 3(\alpha f) = 0$. Hence $\alpha f \in V$. Since the operations are usual addition and scalar multiplication, the axioms of vector space are true. Hence V is a vector space over $\mathbb{R}$. □

11. Any sequence of real numbers $a_1, a_2, \ldots, a_n, \ldots$ is usually denoted by the symbol (a_n). Let V denote the set of all sequence of real numbers. V is a vector space over the field of real numbers. The addition and scalar multiplication are defined by $(a_n) + (b_n) = (a_n + b_n)$ and $\alpha(a_n) = (\alpha a_n)$.

12. Let $V = \{0\}$. V is a vector space over any field F under the obvious operations of addition and scalar multiplication.

13. $\mathbb{R}$ is not a vector space over $\mathbb{C}$. Clearly $(\mathbb{R}, +)$ is an abelian group. But the scalar multiplication is not defined, for if $\alpha = a + ib \in \mathbb{C}$ and $u \in \mathbb{R}$, then $\alpha u = au + ibu \notin \mathbb{R}$. Therefore $\mathbb{R}$ is not vector space over $\mathbb{C}$.

14. Consider $\mathbb{R} \times \mathbb{R}$ with usual addition. We define scalar multiplication by $\alpha(x, y) = (\alpha x, \alpha^2 y)$. Then $\mathbb{R} \times \mathbb{R}$ is not a vector space over $\mathbb{R}$. Clearly $\mathbb{R} \times \mathbb{R}$ with usual addition is an abelian group. $(\alpha+\beta)(x, y) = ((\alpha+\beta)x, (\alpha+\beta)^2 y) = (\alpha x + \beta x, \alpha^2 y + \beta^2 y + 2\alpha\beta y)$ Also, $\alpha(x, y) + \beta(x, y) = (\alpha x, \alpha^2 y) + (\beta x, \beta^2 y) = (\alpha x + \beta x, \alpha^2 y + \beta^2 y)$.Hence $(\alpha + \beta)(x, y) \neq \alpha(x, y) + \beta(x, y)$. $\therefore \mathbb{R} \times \mathbb{R}$ is not a vector space over $\mathbb{R}$.

15. Consider $\mathbb{R} \times \mathbb{R}$ with usual addition. Define the scalar multiplication as $\alpha(a, b) = (0, 0)$. Clearly $\mathbb{R} \times \mathbb{R}$ is an abelian group. Also,

(i) $\alpha(u + v) = 0$ and $\alpha u + \alpha v = 0 + 0 = 0$; so that $\alpha(u + v) = \alpha u + \alpha v$.

(ii) Similarly $(\alpha + \beta)u = \alpha u + \beta u = 0$.

(iii) $\alpha(\beta u) = (\alpha\beta)u = 0$.

However $1(a, b) = (0, 0)$. Hence it is not a vector space.

Note 4.2.6. In this example all the axioms except the axiom $1u = u$ cannot be derived from the other axioms of the vector space. Thus the axiom $1u = u$ is independent of the other axioms of the vector space. We say that the axiom $1u = u$ is irredundant.

16. Let V be the set of all ordered pairs of real numbers. Addition and multiplication are defined by $(x, y) + (x_1, y_1) = (x + x_1, y + y_1)$ and $\alpha(x, y) = (x, \alpha y)$ where x, y, x_1, y_1 and α are real numbers. Then V is not a vector space over $\mathbb{R}$. Clearly V is an abelian group under the operation $+$ defined above.

Let $\alpha, \beta \in \mathbb{R}$ and $(x, y) \in V$. Now,

$$(\alpha + \beta)(x, y) = (x, (\alpha + \beta)y) = (x, \alpha y + \beta y)$$

Also
$$\alpha(x, y) + \beta(x, y) = (x, \alpha y) + (x, \beta y) = (2x, \alpha x + \beta y)$$

$$\therefore \quad (\alpha + \beta)(x, y) \neq \alpha(x, y) + \beta(x, y)$$

Hence V is not a vector space over $\mathbb{R}$.

17. Let $\mathbb{R}^+$ be the set of all positive real numbers. Define addition and scalar multiplication as follows $u + v = uv$ for all $u, v \in \mathbb{R}^+$; $\alpha u = u^\alpha$ for all $u \in \mathbb{R}^+$ and $\alpha \in \mathbb{R}$. Then $\mathbb{R}^+$ is a real vector space.

Proof. Clearly $(\mathbb{R}^+, +)$ is an abelian group with identity 1.(verify) Now,
$\alpha(u + v) = \alpha(uv) = (uv)^\alpha = u^\alpha v^\alpha = \alpha u + \alpha v$.
$(\alpha + \beta)u = u^{\alpha+\beta} = u^\alpha u^\beta = \alpha u + \beta u$.
$\alpha(\beta u) = \alpha u^\beta = (u^\beta)^\alpha = u^{\beta\alpha} = u^{\alpha\beta} = (\alpha\beta)u$.
Also $1u = u1 = u$. $\therefore \mathbb{R}^+$ is a vector space over $\mathbb{R}$. □

Remark 4.2.7. Commutativity of addition in a vector space can be derived from the other axioms of the vector space (ie.,) the axiom of commutativity of addition in a vector space is redundant, for,
$(1 + 1)(u + v) = 1(u + v) + 1(u + v) = 1u + 1v + 1u + 1v = u + v + u + v$
Also $(1 + 1)(u + v) = (1 + 1)u + (1 + 1)v = u + u + v + v$.
$\therefore \quad u + v + u + v = u + u + v + v$.
$\therefore \quad v + u = u + v$.

Theorem 4.2.8. Let V be a vector space over a field F, Then
(i) $\alpha\mathbf{0} = \mathbf{0}$ for all $\alpha \in F$.

(ii) $0v = \mathbf{0}$ for all $v \in V$.

(iii) $(-\alpha)v = \alpha(-v) = -(\alpha v)$ for all $\alpha \in F$ and $v \in V$.

(iv) $\alpha v = \mathbf{0} \Rightarrow \alpha = 0$ or $v = \mathbf{0}$.

Proof.

(i) $\alpha\mathbf{0} = \alpha(\mathbf{0} + \mathbf{0}) = \alpha\mathbf{0} + \alpha\mathbf{0}$. Hence $\alpha\mathbf{0} = \mathbf{0}$.

(ii) $0v = (0 + 0)v = 0v + 0v$. Hence $0v = \mathbf{0}$.

(iii) $\mathbf{0} = [\alpha + (-\alpha)]v = \alpha v + (-\alpha)v$. Hence $(-\alpha)v = -(\alpha v)$. Similarly $\alpha(-v) = -(\alpha v)$. Hence $(-\alpha)v = \alpha(-v) = -(\alpha v)$.

(iv) Let $\alpha v = \mathbf{0}$. If $\alpha = 0$, there is nothing to prove. $\therefore$Let $\alpha \neq 0$. Then $\alpha^{-1} \in F$. Now, $v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1}\mathbf{0} = \mathbf{0}$. □

4.3 Subspaces

Definition 4.3.1. Let V be a vector space over a field F. A non-empty subset W of V is called a **subspace** of V if W itself is a vector space over F under the operations of V.

Theorem 4.3.2. Let V be a vector space over a field F. A non-empty subset W of V is a subspace of V if and only if W is closed with respect to vector addition and sccalar multiplication V.

Proof. Let W be a subspace of V. Then W itself is a vector space and hence W is closed with respect to vector addition and scalar multiplication.

Conversely, let W be a non-empty subset of V such that $u, v \in W \Rightarrow u + v \in W$ and $u \in W$ and $\alpha \in F \Rightarrow \alpha u \in W$. We prove that W is a subspace of V. Since W is non-empty, there exists an element $u \in W$. $\therefore$ $0u = \mathbf{0} \in W$. Also $v \in W \Rightarrow (-1)v = -v \in W$. Thus W contains $\mathbf{0}$ and the additive inverse of each of its element. Hence W is an additive subgroup of V. Also $u \in W$ and $\alpha \in F \Rightarrow \alpha u \in W$. Since the elements of W are the elements of V the other axioms of a vector space are true in W. Hence W is a subspace of V. □

Theorem 4.3.3. Let V be a vector space over a field F. A non-empty subset W of V is a subspace of V if and only if $u, v \in W$ and $\alpha, \beta \in F \Rightarrow \alpha u + \beta v \in W$.

Proof. Let W be a subspace of V. Let $u, v \in W$ and $\alpha, \beta \in F$. Then αu and $\beta v \in W$ and hence $\alpha u + \beta v \in W$.

Conversely, let $u, v \in W$ and $\alpha, \beta \in F \Rightarrow \alpha u + \beta v \in W$. Taking $\alpha = \beta = 1$, we get $u, v \in W \Rightarrow u + v \in W$. Taking $\beta = 0$, we get $\alpha \in F$ and $u \in W \Rightarrow \alpha \in F$ and $u \in W \Rightarrow \alpha u \in W$. Hence W is a subspace of V. □

Examples 4.3.4.

1. $\{0\}$ and V are subspaces of any vector space V. They are called the trivial subspaces of V.

2. $W = \{(a, 0, 0) : \ a \in \mathbb{R}\}$ is a subspace of R^3, for, let $u = (a, 0, 0), v = (b, 0, 0) \in W$ and $\alpha, \beta \in \mathbb{R}$. Then $\alpha u + \beta v = \alpha(a, 0, 0) + \beta(b, 0, 0) = (\alpha a + \beta b, 0, 0) \in W$. Hence W is a subspace of $\mathbb{R}^3$.

Note 4.3.5. Geometrically W consists of all points on the x-axis in the Euclidean 3 space.

3. In $\mathbb{R}^3$, $W = \{(ka, kb, kc) : \ k \in \mathbb{R}\}$ is a subspace of $\mathbb{R}^3$. For, if $u = (k_1 a, k_1 b, k_1 c)$ and $v = (k_2 a, k_2 b, k_2 c) \in W$ and $\alpha, \beta \in \mathbb{R}$ then $\alpha u + \beta v = \alpha(k_1 a, k_1 b, k_1 c) + \beta(k_2 a, k_2 b, k_2 c)$ $= ((\alpha k_1 + \beta k_2)a, (\alpha k_1 + \beta k_2)b, (\alpha k_1 + \beta k_2)c) \in W$ Hence W is a subspace of $\mathbb{R}^3$.

Note 4.3.6. Goemetrically W consists of all points of the line $\frac{x}{a} = \frac{y}{b} = \frac{z}{c}$ provided a, b, c are not all zero. Thus the set of all points on a line through the origin is a subspace of $\mathbb{R}^3$. However a line not passing through the origin is not a subspace of $\mathbb{R}^3$, since the additive identity $(0, 0, 0)$ does not lie on the line.

4. $W = \{(a, b, 0) : \ a, b \in \mathbb{R}\}$ is a subspace of $\mathbb{R}^3$. W consists of all points of the xy-plane.

5. Let W be the set of all points in $\mathbb{R}^3$ satisfying the equation $lx + my + nz = 0$. W is a subspace of $\mathbb{R}^3$. For, let $u = (a_1, b_1, c_1)$ and $v = (a_2, b_2, c_2) \in W$ and $\alpha, \beta \in \mathbb{R}$. Then we have $la_1 + mb_1 + nc_1 = 0 = la_2 + mb_2 + nc_2$. Hence $\alpha(la_1 + mb_1 + nc_1) + \beta(la_2 + mb_2 + nc_2) =$

0. (ie.,) $l(\alpha a_1 + \beta a_2) + m(\alpha b_1 + \beta b_2) + n(\alpha c_1 + \beta c_2) = 0$. (ie.,) $\alpha u + \beta v \in W$ so that W is a subspace of $\mathbb{R}^3$.

Note 4.3.7. Geometrically W consists of all points on the plane $lx + my + nz = 0$, which passes through the origin.

6. Let $W = \{f : \ f \in F[x] \text{ and } f(a) = 0\}$. (ie.,) W is the set of all polynomials in $F[x]$ having a as a root where $a \in F$. Then W is a vector space over F. We observe that $x - a \in W$ and hence W is non-empty. Let $f, g \in F[x]$ and $\alpha, \beta \in F$. To prove that $\alpha f + \beta g \in W$ we have to shoe that a is a root of $\alpha f + \beta g$. Now, $(\alpha f + \beta g)(a) = \alpha f(a) + \beta g(a) = \alpha 0 + \beta 0 = 0$. Hence a is a root of $\alpha f + \beta g$. $\therefore \ \alpha f + \beta g \in W$ and W is a subspace of $F[x]$.

7. $W = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : \ a, b \in \mathbb{R} \right\}$ is a subspace of $M_2(\mathbb{R})$.

4.3.1 Solved problems

Problem 4.3.8. Prove that the intersection of two subspaces of a vector space V is a subspace.

Solution. Let A and B be two subspaces of a vector space V over a field F. We claim that $A \cap B$ is a subspace of V. Clearly $\mathbf{0} \in A \cap B$ and hence $A \cap B$ is non-empty. Now, let $u, v \in A \cap B$ and $\alpha, \beta \in F$. Then $u, v \in A$ and $u, v \in B$. $\therefore \alpha u + \beta v \in A$ and $\alpha u + \beta v \in B$ (since A and B are subspaces) $\therefore \alpha u + \beta v \in A \cap B$. Hence $A \cap B$ is a subspace of V.

Problem 4.3.9. *Prove that the union of two subspaces of a vector space need not be a subspace.*

Solution. Let $A = \{(a, 0, 0) : \ a \in \mathbb{R}\}$, $B = \{(0, b, 0) : \ b \in \mathbb{R}\}$. Clearly A and B are subspaces of $\mathbb{R}^3$ (example 2 of section 4.2). However $A \cup B$ is not a subspace of $\mathbb{R}^3$. For, $(1, 0, 0)$ and $(0, 1, 0) \in A \cup B$. But $(1, 0, 0) + (0, 1, 0) = (1, 1, 0) \notin A \cup B$.

Problem 4.3.10. If A and B are subspaces of V prove that $A+B=\{v\in V:\ v=a+b,a\in A,b\in B\}$ is a subspace of V. Further show that $A+B$ is the smallest subspace containing A and B. (ie.,)If W is any subspace of V containing A and B then W contains $A+B$.

Solution. Let $v_1,v_2\in A+B$ and $\alpha\in F$. Then $v_1=a_1+b_1,v_2=a_2+b_2$ where $a_1,a_2\in A$ and $b_1,b_2\in B$. Now, $v_1+v_2=(a_1+b_1)+(a_2+b_2)=(a_1+a_2)+(b_1+b_2)\in A+B$ Also $\alpha(a_1+b_1)=\alpha a_1+\alpha b_1\in A+B$. Hence $A+B$ is a subspace of V. Clearly $A\subseteq A+B$ and $B\subseteq A+B$. Now, let W be any subspace of V containing A and B. We shall prove that $A+B\subseteq W$. Let $v\in A+B$. Then $v=a+b$ where $a\in A$ and $b\in B$. Since $A\subseteq W$, $a\in W$. Similarly $b\in W$ and $a+b=v\in W$. Therefore $A+B\subseteq W$ so that $A+B$ is the smallest subspace of V containing A and B.

Problem 4.3.11. Let A and B be subspace of a vector space V. Then $A\cap B=\{0\}$ if and only if every vector $v\in A+B$ can be uniquely expressed in the form $v=a+b$ where $a\in A$ and $b\in B$.

Solution. Let $A\cap B=\{0\}$. let $v\in A+B$. Let $v=a_1+b_1=a_2+b_2$ where $a_1,a_2\in A$ and $b_1,b_2\in B$. Then $a_1-a_2=b_2-b_1$. But $a_1-a_2\in A$ and $b_2-B_1\in B$. Hence $a_1-a_2,b_2-b_1\in A\cap B$. Since $A\cap B=\{0\}$, $a_1-a_2=0$ and $b_2-b_1=0$ so that $a_1=a_2$ and $b_1=b_2$. Hence the expression of v in the form $a+b$ where $a\in A$ and $b\in B$ is unique. Conversely suppose that any element in $A+B$ can be uniquely expressed in the form $a+b$ where $a\in A$ and $b\in B$. We claim that $A\cap B=\{0\}$. If $A\cap B\neq\{0\}$, let $v\in A\cap B$ and $v\neq 0$. Then $\mathbf{0}=v-v=\mathbf{0}+\mathbf{0}$. Thus $\mathbf{0}$ has been expressed in the form $a+b$ in two dif and only iferent ways which is a contradiction. Hence $A\cap B=\{0\}$

Definition 4.3.12. Let A and B be subspaces of a vector space V. Then V is called the **direct sum** of A and B if
(i) $A+B=V$
(ii) $A\cap B=\{0\}$
If V is the direct sum of A and B we write $V=A\oplus B$.

Note 4.3.13. $V = A \oplus B$ if and only if every element of V can be uniquely expressed in the form $a + b$ where $a \in A$ and $b \in B$.

Examples 4.3.14.

1. In $V_3(\mathbb{R})$ let $A = \{(a, b, 0) : \ a, b \in \mathbb{R}\}$ and $B = \{(0, 0, c) : \ c \in \mathbb{R}\}$. Clearly A and B are subspaces of V and $A \cap B = \{0\}$. Also let $v = (a, b, c) \in V_3(\mathbb{R})$. Then $v = (a, b, 0) + (0, 0, c)$ so that $A + B = V_3(\mathbb{R})$. Hence $V_3(\mathbb{R}) = A \oplus B$.

2. In $M_2(\mathbb{R})$, let A be the set of all matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ and B be the set of all matrices of the form $\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$. Clearly A and B are subspaces of $M_2(\mathbb{R})$ and $A \cap B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $A + B = M_2(\mathbb{R})$. Hence $M_2(\mathbb{R}) = A \oplus B$.

Theorem 4.3.15. Let V be a vector space over F and W a subspace of V. Let $V/W = \{W + v : \ v \in V\}$. Then V/W is a vector space over F under the following operations.
(i) $(W + v_1) + (W + v_2) = W + v_1 + v_2$
(ii) $\alpha(W + v_1) = W + \alpha v_1$.

Proof. Since W is a subspace of V it is a subgroup of $(V, +)$. Since $(V, +)$ is abelian, W is normal subgroup of $(V, +)$ so that (i) is a well defined operation. Now we shall prove that (ii) is a well defined operation. $W + v_1 = W + v_2 \Rightarrow v_1 - v_2 \in W \Rightarrow \alpha(v_1 - v_2) \in W$ since W is a subspace $\Rightarrow \alpha v_1 - \alpha v_2 \in W \Rightarrow \alpha v_1 \in W + \alpha v_2 \Rightarrow W + \alpha v_1 = W + \alpha v_2$ Hence (ii) is a well defined operation.

Now, let $W + v_1, W + v_2, W + v_3 \in V/W$.
Then $(W+v_1)+[(W+v_2)+(W+v_3)] = (W+v_1)+(W+v_2+v_3) = W+v_1+v_2+v_3 = (W + v_1 + v_2) + (W + v_3) = [(W + v_1) + (W + v_2)] + (W + v_3)$ Hence $+$ is associative. $W + 0 = W \in V/W$ is the additive identity element. For $(W + v_1) + (W + 0) = W + v_1 = (W + 0) + (W + v_1)$ for all $v_1 \in V$. Also $W - v_1$ is the additive inverse of $W + v_1$. Hence V/W is a group under $+$.

Further,$(W+v_1)+(W+v_2)=W+v_1+v_2=W+v_2+v_1=(W+v_2)+(W+v_1)$ Hence V/W is an abelian group.

Now, let $\alpha,\beta\in F$. $\alpha[(W+v_1)+(W+v_2)]=\alpha(W+v_1+v_2)=W+\alpha(v_1+v_2)=W+\alpha v_1+\alpha v_2=(W+\alpha v_1)+(W+\alpha v_2)=\alpha(W+v_1)+\alpha(W+v_2)(\alpha+\beta)(W+v_1)=W+(\alpha+\beta)v_1=W+\alpha v_1+\beta v_1=(W+\alpha v_1)+(W+\beta v_1)=\alpha(W+v_1)+\beta(W+v_1)\alpha[\beta(W+v_1)]=\alpha(W+\beta v_1)=W+\alpha\beta v_1 1(W+v_1)=W+1v_1=W+v_1$ Hence V/W is a vector space. The vector space V/W is called the **quotient space** of V by W. □

4.4 Linear Transformation

Definition 4.4.1. Let V and W be vector space over a field F. A mapping $T:V\to W$ is called a **homomorphism** if
(a) $T(u+v)=T(u)+T(v)$ and
(b) $T(\alpha u)=\alpha T(u)$ where $\alpha\in F$ and $u,v\in V$.
A homomorphism T of vector space is also called a **linear transformation**.
(i) If T is 1-1 then T is called **monomorphism**.
(ii) If T is onto then T is called an **epimorphism**.
(iii) If T is 1-1 and onto then T is called an **isomorphism**.
(iv) Two vector spaces V and W are said to be isomorphic if there exists an isomorphism T from V to W and we write $V\cong W$.
(v) A linear transformation $T:V\to F$ is called a **linear functional**.

Examples 4.4.2.

1. $T:V\to W$ defined by $T(v)=\mathbf{0}$ for all $v\in V$ is a **trivial linear transformation**.
2. $T:V\to V$ defined by $T(v)=v$ for all $v\in V$ is a **identity linear transformation**.
3. Let V be a vector space over a field F and W a subspace of V. Then $T:V\to V/W$ defined by $T(v)=W+v$ is a linear transformation,
for, $T(v_1+v_2)=T+v_1+v_2=(W+v_1)+(W+v_2)=T(v_1)+T(v_2)$
Also $T(\alpha v_1)=W+\alpha v_1=\alpha(W+v_1)=\alpha T(v_1)$.

This is called the **natural homomorphism** from V to V/W. Clearly T is onto and hence T is an epimorphism.

4. $T : V_3(\mathbb{R}) \to V_3(\mathbb{R})$ defined by $T(a, b, c) = (a, 0, 0)$ is a linear transformation.

5. Let V be the set of all polynomials of degree $\leq \quad n$ in $\mathbb{R}[x]$ including the zero polynomial. $T : V \to V$ defined by $T(f) = \frac{\mathrm{d}f}{\mathrm{d}x}$ is a linear transformation.
For, $\quad T(f+g) = \frac{\mathrm{d}(f+g)}{\mathrm{d}x} = \frac{\mathrm{d}f}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x} = T(f) + T(g)$.
Also $T(\alpha f) = \frac{\mathrm{d}(\alpha f)}{\mathrm{d}x} = \alpha\frac{\mathrm{d}f}{\mathrm{d}x} = \alpha T(f)$.

6. Let V be as in example 5. Then $T : V \to V_{n+1}(\mathbb{R})$ defined by $T(a_0+a_1x+\cdots+a_0x^n) = (a_0, a_1, \ldots, a_n)$ is a linear transformation.
For, let $f = a_0 + a_1x + \cdots + a_0x^n$ and $g = b_0 + b_1x + \cdots + b_0x^n$.
Then $f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$.
$$\begin{aligned}\therefore \quad T(f+g) &= ((a_0+b_0), (a_1+b_1), \ldots, (a_n+b_n)) = (a_0, a_1, \ldots, a_n) + (b_0, b_1, \ldots, b_n)\\ &= T(f) + T(g)\end{aligned}$$
Also $\quad T(\alpha f) = (\alpha a_0, \alpha a_1, \ldots, \alpha a_n) = \alpha(a_0, a_1, \ldots, a_n) = \alpha T(f)$.
Clearly T is 1-1 and onto and hence T is an isomorphism.

7. Let V denote the set of all sequence in $\mathbb{R}$. $T : V \to V$ defined by $T(a_1, a_2, \ldots, a_n, \ldots) = (0, a_0, a_1, \ldots, a_n, \ldots)$ is a linear transformation.

8. $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(a, b) = (2a - 3b, a + 4b)$ is a linear transformation.
Let $u = (a, b)$ and $v = (c, d)$ and $\alpha \in \mathbb{R}$.
$$\begin{aligned}\therefore \quad T(u+v) &= T((a,b)+(c,d)) = T(a+c, b+d) = (2(a+c)-3(b+d), (a+c)+4(b+d))\\ &= (2a+2c-3b-3d, a+c+4b+4d) = (2a-3b+2c-3d, a+4b+c+4d)\\ &= (2a-3b, a+4b) + (2c-3d, c+4d) = T(a,b) + T(c,d) = T(u) + T(v).\end{aligned}$$
$$\begin{aligned}\text{Also} \quad T(\alpha u) &= T(\alpha(a,b)) = T(\alpha a, \alpha b) = (2\alpha a - 3\alpha b, \alpha a + 4\alpha b)\\ &= \alpha(2a-3b, a+4b) = \alpha T(a,b) = \alpha T(u) \therefore T \text{ is a linear transformation.}\end{aligned}$$

Theorem 4.4.3. *Let $T : V \to W$ be a linear transformation. Then $T(V) = \{T(v) : v \in V\}$ is a subspace of W.*

Proof. Let w_1 and $w_2 \in T(V)$ and $\alpha \in F$. Then there exist $v_1, v_2 \in V$ such that $T(v_1) = w_1$ and $T(v_2) = w_2$. Hence $w_1 + w_2 = T(v_1) + T(v_2) = T(v_1 + v_2) \in T(V)$. Similarly $\alpha w_1 = \alpha T(v_1) = T(\alpha v_1) \in T(V)$. Hence $T(V)$ is subspace of W. □

Definition 4.4.4. Let V and W be vector spaces over a field F and $T : V \to W$ be a linear transformation. Then the **kernel** of T is defined to be $\{v :\ v \in V \text{ and } T(v) = 0\}$ and is denoted by $ker\ T$. Thus $ker\ T = \{v :\ v \in V \text{ and } T(v) = 0\}$.

For example, in example 1, $ker\ T = V$. In example 2, $ker\ T = \{\mathbf{0}\}$. In example 5, $ker\ T$ is the set of all constant polynomials.

Note 4.4.5. Let $T : V \to W$ be a linear transformation. Then T is a monomorphism if and only if $ker\ T = \{\mathbf{0}\}$.

Theorem 4.4.6. [Fundamental theorem of homomorphism] Let V and W be vector spaces over a field F and $T : V \to W$ be an epimorphism. Then
(i) $ker\ T = V_1$ is a subspace of V and
(ii) $\frac{V}{V_1} \cong W$.

Proof.

(i) Given $V_1 = ker\ T = \{v :\ v \in V \text{ and } T(v) = \mathbf{0}\}$ Clearly $T(\mathbf{0}) = \mathbf{0}$. Hence $\mathbf{0} \in ker\ T = V_1 \therefore V_1$ is non-empty subset of V. Let $u, v \in ket\ T$ and $\alpha, \beta \in F$. $\therefore T(u) = 0$ and $T(v) = 0$. Now $T(\alpha u + \beta v) = T(\alpha u) + T(\beta v) = \alpha T(u) + \beta T(v) = \alpha\mathbf{0} + \beta\mathbf{0} = \mathbf{0}$ and so $\alpha u + \beta v \in ker\ T$. Hence $ker\ T$ is a subspace of V.

(ii) We define a map $\varphi : \frac{V}{V_1} \to W$ by $\varphi(V_1 + v) = T(v)$. φ is well defined. Let $V_1 + v = V_1 + w$. $\therefore v \in V_1 + w$. $\therefore v = v_1 + w$ where $v_1 \in V$. $\therefore T(v) = T(v_1 + w) = T(v_1) + T(w) = \mathbf{0} + T(w) = T(w) \therefore \varphi(V_1 + v) = \varphi(V_1 + w) \therefore \varphi$ is 1-1. $\varphi(V_1 + v) = \varphi(V_1 + w) \Rightarrow T(v) = T(w) \Rightarrow T(v) - T(w) = \mathbf{0} \Rightarrow T(v) + T(-w) = \mathbf{0}$
$\Rightarrow T(v - w) = \mathbf{0} \Rightarrow v - w \in ker\ T = V_1 \Rightarrow v \in V_1 + w \Rightarrow V_1 + v = V_1 + w$. φ is onto. Let $w \in W$. Since T is onto, there exists $v \in V$ such that $T(v) = w$ and so $\varphi(V_1 + v) = w$. φ is a homomorphism. $\varphi[(V_1+v)+(V_1+w)] = \varphi[(V_1+(v+w)] = T(v+w) = T(v)+T(w) = \varphi(V_1+v)+\varphi(V_1+w)$ Also $\varphi[\alpha(V_1+v)] = \varphi[(V_1+\alpha v)] = T(\alpha v) = \alpha T(v) = \alpha T(V_1+v)$. Hence φ is an isomorphism from $\frac{V_1}{V}$ onto W and so $\frac{V_1}{V} \cong W$. □

Theorem 4.4.7. Let V be a vector space over a field F. Let A and B be subspaces of V. Then $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

Proof. We know that $A+B$ is a subspace of V containing A. Hence $\frac{A+B}{A}$ is also a vector space over F. An element of $\frac{A+B}{A}$ is of the form $A+(a+b)$ where $a \in A$ and $b \in B$. But $A+a=A$. Hence an element of $\frac{A+B}{A}$ is of form $A+b$. Now, consider $f : B \to \frac{A+B}{A}$ defined by $f(b) = A+b$. Clearly f is onto. Also $f(b_1+b_2) = A+(b_1+b_2) = (A+b_1)+(A+b_2) = f(b_1)+f(b_2)$ and $f(\alpha b_1) = A+\alpha b_1 = \alpha(A+b_1) = \alpha f(b_1)$. Hence f is a linear transformation. Let K be the kernel of f. Then $K = \{b : b \in B, A+b = A\}$. Now, $A+b=A$ if and only if $b \in A$. Hence $K = A \cap B$ and so $\frac{B}{A\cap B} \cong \frac{A+B}{A}$. □

Theorem 4.4.8. Let V and W be vector spaces over a field F. Let $L(V,W)$ represent the set of all linear transformations from V to W. Then $L(V,W)$ itself is a vector space over F under addition and scalar multiplication defined by $(f+g)(v) = f(v)+g(v)$ and $(\alpha f)(v) = \alpha f(v)$.

Proof. Let $f, g \in L(V,W)$ and $v_1, v_2 \in V$. Then

$$\begin{aligned}(f+g)(v_1+v_2) &= f(v_1+v_2)+g(v_1+v_2) = f(v_1)+f(v_2)+g(v_1)+g(v_2)\\ &= f(v_1)+g(v_1)+f(v_2)+g(v_2) = (f+g)(v_1)+(f+g)(v_2)\end{aligned}$$

Also $(f+g)(\alpha v) = f(\alpha v)+g(\alpha v) = \alpha f(v)+\alpha g(v) = \alpha[f(v)+g(v)] = \alpha(f+g)(v)$.
Hence $(f+g) \in L(V,W)$.

Now, $$\begin{aligned}(\alpha f)(v_1+v_2) &= (\alpha f)(v_1)+(\alpha f)(v_2) = \alpha f(v_1)+\alpha f(v_2)\\ &= \alpha[f(v_1)+f(v_2)] = \alpha f(v_1+v_2).\end{aligned}$$

Also $(\alpha f)(\beta v) = \alpha[f(\beta v)] = \alpha[\beta f(v)] = \beta[\alpha f(v)] = \beta[(\alpha f)(v)]$. Hence $\alpha f \in L(V,W)$.
Addition defined on $L(V,W)$ is obviously commutative and associative.
The function $f : V \to W$ defined by $f(v) = \mathbf{0}$ for all $v \in V$ is clearly a linear transformation and is the additive identity of $L(V,W)$. Further $(-f) : V \to W$ defined by $(-f)(v) = -f(v)$ is the additive inverse of f. Thus $L(V,W)$ is an abelian group under addition. The remaining axioms for a vector space can be easily verified. Hence $L(V,W)$ is a vector space over F. □

4.5 Span of a set

Definition 4.5.1. Let V be a vector space over a field F. Let $v_1, v_2, \ldots, v_n \in V$. Then an element of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ where $\alpha_i \in F$ is called a

linear combnation of the vectors $v_1, v_2, \ldots, v_n$.

Definition 4.5.2. Let S be a non-empty subset of a vector space V. Then the set of all linear combinations of finite sets of elements of S is called the **linear span** of S and is denoted by $L(S)$.

Note 4.5.3. Any element of $L(S)$ is of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ where $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$.

Theorem 4.5.4. Let V be a vector space over a field F and S be a non-empty subset of V. Then
(i) $L(S)$ is a subspace of V.
(ii)$S \subseteq L(S)$.
(iii) If W is any subspace of V such that $S \subseteq W$, then $L(S) \subseteq W$ (ie.,) S is the smallest subspace of V containing S.

Proof.

(i) Let $v, w \in L(S)$ and $\alpha, \beta \in F$. Then $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ where $v_i \in S$ and $\alpha_i \in F$. Also, $w = \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m$ where $w_j \in S$ $\beta_j \in F$.
Now, $\alpha v + \beta w = \alpha(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) + \beta(\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m)$.
$= (\alpha\alpha_1)v_1 + \cdots + (\alpha\alpha_n)v_n + (\beta\beta_1)w_1 + \cdots + (\beta\beta_m)w_m$. and so $\alpha v + \beta w$ is also a linear combination of a finite number of elements of S. Hence $\alpha v + \beta w \in L(S)$ and so $L(S)$ is a subspace of S.

(ii) Let $u \in S$. Then $u = 1u \in L(S)$. Hence $S \subseteq L(S)$.

(iii) Let W be any subspace of V such that $S \subseteq W$. Let $u \in L(S)$. Then $u = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$ where $u_i \in S$ and $\alpha_i \in F$. Since $S \subseteq W$, we have $u_1, u_2, \ldots, u_n \in W$ and so $u \in W$. Hence $L(S) \subseteq W$. □

Note 4.5.5. $L(S)$ is called the subspace **spanned(generated)** by the set S.

Examples 4.5.6.

1. In $V_3(\mathbb{R})$ let $e_1 = (1, 0, 0); e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$

(a) Let $S = \{e_1, e_2\}$. Then $L(S) = \{\alpha e_1 + \beta e_2 : \alpha, \beta \in \mathbb{R}\} = \{(\alpha, \beta, 0) : \alpha, \beta \in \mathbb{R}\}$

(b) Let $S = \{e_1, e_2, e_3\}$. Then $L(S) = \{\alpha e_1 + \beta e_2 + \gamma e_3 : \alpha, \beta, \gamma \in \mathbb{R}\} = \{(\alpha, \beta, \gamma) : \alpha, \beta, \gamma \in \mathbb{R}\} = V_3(\mathbb{R})$ Thus $V_3(\mathbb{R})$ is spanned by $\{e_1, e_2, e_3\}$.

2. In $V_n(\mathbb{R})$ let $e_1 = (1, 0, \cdots, 0); e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$.
Let $S = \{e_1, e_2, \ldots, e_n\}$. Then $L(S) = \{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_n e_n : \alpha_i \in \mathbb{R}\} = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) : \alpha_i \in \mathbb{R}\} = V_n(\mathbb{R})$ Thus $V_n(\mathbb{R})$ is spanned by $\{e_1, e_2, \ldots, e_n\}$.

Theorem 4.5.7. Let V be a vector space over a field F. Let $S, T \subseteq V$. Then
(a) $S \subseteq T \Rightarrow L(S) \subseteq L(T)$.
(b) $L(S \cup T) = L(S) + L(T)$.
(c) $L(S) = S$ if and only if S is a subspace of V.

Proof.

(a) Let $S \subseteq T$. Let $s \in L(S)$ Then $s = \alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n$ where $s_i \in S$ and $\alpha_i \in F$. Now, since $S \subseteq T, s_i \in T$. Hence $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n \in L(T)$.

(b) Let $s \in L(S \cup T)$. Then $s = \alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_n s_n$ where $s_i \in S \cup T$ and $\alpha_i \in F$. Without loss of generality we can assume that $s_1, s_2, \ldots, s_m \in S$ and $s_{m+1}, \ldots, s_n \in T$. Hence $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_m s_m \in L(S)$ and $\alpha_{m+1} s_{m+1} + \cdots + \alpha_n s_n \in L(T)$. $\therefore s = (\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_m s_m) + (\alpha_{m+1} s_{m+1} + \cdots + \alpha_n s_n) \in L(S) + L(T)$. Also by (a) $L(S) \subseteq L(S \cup T)$ and $L(T) \subseteq L(S \cup T)$. Hence $L(S) + L(T) \subseteq L(S \cup T)$. Hence $L(S) + L(T) = L(S \cup T)$.

(c) Let $L(S) = S$. Then $L(S) = S$ is a subspace of V. Conversely, let S be a subspace V. Then the smallest subspace containing S is S itself. Hence $L(S) = S$. □

Corollary 4.5.8. $L[L(S)] = S$.

4.6 Linear Independence

In $V_3(\mathbb{R})$, let $S = \{e_1, e_2, e_3\}$. We have seen that $L(S) = V_3(\mathbb{R})$. Thus S is a subset of $V_3(\mathbb{R})$ which spans the whole space $V_3(\mathbb{R})$.

Definition 4.6.1. Let V be a vector space over a field F. V is said to be **finite dimensional** if there exists a *finite* subset S of V such that $L(S) = V$.

Examples 4.6.2.

1. $V_3(\mathbb{R})$ is a finite dimensional vector space.
2. $V_n(\mathbb{R})$ is a finite dimensional vector space, since $S = \{e_1, e_2, \ldots, e_n\}$ is a finite subset of $V_n(\mathbb{R})$ such that $L(S) = V_n(\mathbb{R})$. In general if F is any field $V_n(F)$ is a finite dimensional vector space over F.
3. Let V be the set of all polynomials in $F[x]$ of degree $\leq\ n$. Let $S = \{1, x, x^2, \ldots, x^n\}$. Then $L(S) = V$ and hence V is finite dimensional.
4. $\mathbb{C}$ is a finite dimensional vector space over $\mathbb{R}$, since $L(\{1, i\}) = \mathbb{C}$.
5. In $M_2(\mathbb{R})$ consider the set S consisting of the matrices
$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; D = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aA + bB + cC + dD$. Hence $L(S) = M_2(\mathbb{R})$ so that $M_2(\mathbb{R})$ is finite dimensional.

Note 4.6.3. All the vector spaces we have considered above are finite dimensional. However there are vector spaces which cannot be spanned by a finite number of vectors. For example, consider $\mathbb{R}[x]$. Let S be any finite subset of $\mathbb{R}[x]$. Let f be a polynomial of maximum degree in S. Let *deg* $f = n$. Then any element of $L(S)$ is a polynomial of degree $\leq\ n$ and hence $L(S) \neq \mathbb{R}[x]$. Thus $\mathbb{R}[x]$ is not finite dimensional.

Throughout the rest of this chapter all the vector spaces we consider are finite dimensional. Although we have defined what is meant by a finite dimensional space we have not yet defined what is meant by the *dimension* of a vector space. We now proceed to introduce the concepts necessary to define the dimension of a finite dimensional vector space.

Consider the vectors $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$ in $V_3(\mathbb{R})$.
Suppose that $\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = \mathbf{0}$. Then $(\alpha_1, 0, 0) + (0, \alpha_2, 0) + (0, 0, \alpha_3) = (0, 0, 0)$.

$\therefore (\alpha_1, \alpha_2, \alpha_3) = (0, 0, 0)$. $\therefore \alpha_1 = \alpha_2 = \alpha_3 = 0$. (ie.,)$\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = \mathbf{0}$ if and only if $\alpha_1 = \alpha_2 = \alpha_3 = 0$. Thus a linear combination of the vectors e_1, e_2 and e_3 will yield the zero vector if and only if all the coefficients are zero.

Definition 4.6.4. Let V be a vector space over a field F. A finite set of vectors $v_1, v_2, \ldots, v_n$ in V is said to be **linearly independent** if $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. If $v_1, v_2, \ldots, v_n$ are not linearly independent, then they are said to be **linearly dependent**.

Note 4.6.5. If $v_1, v_2, \ldots, v_n$ are linearly dependent then there exist scalars $\alpha_1, \alpha_2, \ldots, \alpha_n$ not all zero such that $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$.

Examples 4.6.6.

1. In $V_n(F)$, $\{e_1, e_2, \ldots, e_n\}$ is a linearly independent set of vectors, for, $\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n = 0$. $\Rightarrow \alpha_1(1, 0, \ldots, 0) + \alpha_2(0, 1, \ldots, 0) + \cdots + \alpha_n(0, 0, \ldots, 1) = (0, 0, \ldots, 0) \Rightarrow (\alpha_1, \alpha_2, \ldots, \alpha_n) = (0, 0, \ldots, 0) \Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$.

2. In $V_3(\mathbb{R})$ the vectors $(1, 2, 1), (2, 1, 0)$ and $(1, -1, 2)$ are linearly independent. For, let $\alpha_1(1, 2, 1) + \alpha_2(2, 1, 0) + \alpha_3(1, -1, 2) = (0, 0, 0)$ $\therefore (\alpha_1 + 2\alpha_2 + \alpha_3, 2\alpha_1 + \alpha_2 - \alpha_3, \alpha_1 + 2\alpha_3) = (0, 0, 0)$

$$\begin{aligned} \therefore \quad \alpha_1 + 2\alpha_2 + \alpha_3 &= 0 & \cdots (1) \\ 2\alpha_1 + \alpha_2 - \alpha_3 &= 0 & \cdots (2) \\ \alpha_1 + 2\alpha_3 &= 0 & \cdots (3) \end{aligned}$$

   Solving equations (1),(2) and (3) we get $\alpha_1 = \alpha_2 = \alpha_3 = 0$. $\therefore$ The given vectors are linearly independent.

3. In $V_3(\mathbb{R})$ the vectors $(1, 4, -2), (-2, 1, 3)$ and $(-4, 11, 5)$ are linearly dependent. For, let $\alpha_1(1, 4, -2) + \alpha_2(-2, 1, 3) + \alpha_3(-4, 11, 5) = (0, 0, 0)$

$$\begin{aligned} \therefore \quad \alpha_1 - 2\alpha_2 - 4\alpha_3 &= 0 & \cdots (1) \\ 4\alpha_1 + \alpha_2 + 11\alpha_3 &= 0 & \cdots (2) \\ -2\alpha_1 + 3\alpha_2 + 5\alpha_3 &= 0 & \cdots (3) \end{aligned}$$

   From (1) and (2), $\frac{\alpha_1}{-18} = \frac{\alpha_2}{-27} = \frac{\alpha_3}{9} = k(\text{say})$ $\therefore$ $\alpha_1 = -18k, \alpha_2 = -27k, \alpha_3 = 9k$. These values of α_1, α_2 and α_3, for any k satisfy (3) also. Taking $k = 1$ we get $\alpha_1 =$

$-18, \alpha_2 = -27, \alpha_3 = 9$ as a non-trivial solution. Hence the three vectors are linearly dependent.

4. Let V be a vector space over a field F. Then any subset S of V containing the zero vector is linearly dependent.

Proof. Let $S = \{\mathbf{0}, v_1, \ldots, v_n\}$ Clearly $\alpha\mathbf{0} + 0v_1 + 0v_2 + \cdots + 0v_n = \mathbf{0}$ where α is any element of F. Hence for any $\alpha \neq \mathbf{0}$, we get a non-trivial linear combination of vectors in S giving the zero vector. Hence S is linearly dependent. □

Theorem 4.6.7. Any subset of a linearly independent set is linearly independent.

Proof. Let V be a vector space over a field F. Let $S = \{v_1, v_2, \ldots, v_n\}$ be a linearly independent set. Let S' be a subset of S. Without loss of generality we take $S' = \{v_1, v_2, \ldots, v_k\}$ where $k \leq n$. Suppose S' is a linearly dependent set. Then there exist $\alpha_1, \alpha_2, \ldots, \alpha_k$ in F not all zero, such that $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = \mathbf{0}$. Hence $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k + 0v_{k+1} + \cdots + 0v_n = \mathbf{0}$ is a non-trivial linear combination giving the zero vector. Here S is a linearly dependent set which is a contradiction. Hence S' is linearly independent. □

Theorem 4.6.8. Any set containing a linearly dependent set is also linearly dependent.

Proof. Let V be a vector space. Let S be a linearly dependent set. Let $S' \supset S$. If S' is linearly independent S is also linearly independent (by theorem 4.5.7) which is a contradiction. Hence S' is linearly dependent. □

Theorem 4.6.9. Let $S = \{v_1, v_2, \ldots, v_n\}$ be a linearly independent set of vectors in a vector space V over a field F. Then every element of $L(S)$ can be uniquely written in the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where $\alpha_i \in F$.

Proof. By definition every elements of $L(S)$ is of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ Now, $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$. Hence $(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \cdots + (\alpha_n - \beta_n)v_n = \mathbf{0}$. Since S is a linearly independent set, $\alpha_i - \beta_i = 0$ for all i. $\therefore \alpha_i = \beta_i$ for all i. Hence the theorem. □

Theorem 4.6.10. $S = \{v_1, v_2, \ldots, v_n\}$ be a linearly independent set of vectors in a vector space V if and only if there exists a vector $v_k \in S$ such that v_k is a linear combination of the preceding vectors $v_1, v_2, \ldots, v_{k-1}$.

Proof. Suppose $v_1, v_2, \ldots, v_n$ are linearly dependent. Then there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, not all zero, such that $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$. Let k be the largest integer for which $\alpha_k \neq 0$. Then $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = \mathbf{0}$. $\therefore \alpha_k v_k = -\alpha_1 v_1 - \alpha_2 v_2 - \cdots - \alpha_{k-1} v_{k-1}$. $\therefore v_k = (-\alpha_k^{-1}\alpha_1)v_1 + \cdots + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$. $\therefore v_k$ is a linear combination of the preceding vectors. Conversely, suppose there exists a vector v_k such that$v + k = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1}$. Hence $-\alpha_1 v_1 - \alpha_2 v_2 - \cdots - \alpha_{k-1} v_{k-1} + v_k + 0v_{k+1} + \cdots + 0v_n = \mathbf{0}$. Since the coefficient of $v_k = 1$, we have $S = \{v_1, v_2, \ldots, v_n\}$ is linearly dependent. □

Example 4.6.11. In $V_3(\mathbb{R})$, let $S = [(1,0,0), (0,1,0), (0,0,1), (1,1,1)]$ Here $(1,1,1) = (1,0,0) + (0,1,0) + (0,0,1)$. Thus $(1,1,1)$ is a linear combination of the preceding vectors. Hence S is a linearly dependent set.

Theorem 4.6.12. Let V be a vector space over F. Let $S = \{v_1, v_2, \ldots, v_n\}$ and $L(S) = W$. Then there exists a linearly independent subset S' of S such that $L(S') = W$.

Proof. Let $S = \{v_1, v_2, \ldots, v_n\}$. If S is linearly independent there is nothing to prove. If not, let v_k be the first vector in S which is a linear combination of the preceding vectors. Let $S_1 = \{v_1, v_2, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$. (ie.,) S_1 is obtained by deleting the vector v_k from S. We claim that $L(S_1) = L(S) = W$. Since $S_1 \subseteq S$, $L(S_1) \subseteq L(S)$. Now, let $v \in L(S)$. Then $v = \alpha_1 v_1 + \cdots + \alpha_k v_k + \cdots + \alpha_n v_n$. Now, v_k is a linear combination of the preceding vectors. Let $v_k = \beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1}$. Hence $v = \alpha_1 v_1 + \cdots + \alpha_{k-1} v_{k-1} + \alpha_k(\beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1}) + \alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n$. $\therefore v$ can be expressed as a linear combination of the vectors of S_1 so that $v \in L(S_1)$. Hence $L(S) \subseteq L(S_1)$. Thus $L(S) = L(S_1) = W$. Now, if S_1 is linearly independent, the proof is complete. If not, we continue the above process of removing a vector from S_1, which is a linear combination of the preceeding vectors until we arrive at a linearly independent subset S' of S such that $L(S') = W$. □

4.7 Basis and Dimension

Definition 4.7.1. A linearly independent subset S of a vector space V which spans the whole space V is called a *basis* of the vector space.

Theorem 4.7.2. Any finite dimensional vector space V contains a finite number of linearly independent vectors which span V. (ie.,) A finite dimensional vector space has a basis consisting of a finite number of vectors.

Proof. Since V is finite dimensional there exists a finite subset S of V such that $L(S) = V$. Clearly this set S contains a linearly independent subset $S' = \{v_1, v_2, \ldots, v_n\}$ such that $L(S') = L(S) = V$. Hence S' is a basis for V. □

Theorem 4.7.3. Let V be a vector space over a field F. Then $S = \{v_1, v_2, \ldots, v_n\}$ is a basis for V if and only if every element of V can be uniquely expressed as a linear combination of element of S.

Proof. Let S be a basis for V. Then by definition S is linearly independent and $L(S) = V$. Hence by theorem 4.5.9 every element of V can be uniquely expressed as a linear combination of elements of S.

Conversely, suppose every element of V can be uniquely expressed as a linear combination of elements of S. Clearly $L(S) = V$. Now, let $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$. Also, $0v_1 + 0v_2 + \cdots + 0v_n = \mathbf{0}$. Thus we have expresssed $\mathbf{0}$ as a linear combination of vectors of S in two ways. By hypothesis $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. Hence S is linearly independent. Hence S is a basis. □

Examples 4.7.4.

1. $S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ is a basis for $V_3(\mathbb{R})$ for, $(a, b, c) = a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1)$.

   Any vector (a, b, c) of $V_3(\mathbb{R})$ has been expressed uniquely as a linear combination of the elements of S and hence S is a basis for $V_3(\mathbb{R})$.

2. $S = \{e_1, e_2, \ldots, e_n\}$ is a basis for $V_n(F)$. This is known as the standard basis for $V_n(F)$.

3. $S = \{(1,0,0),(0,1,0),(1,1,1)\}$ is a basis for $V_3(\mathbb{R})$.

Proof. We shall show that any element (a,b,c) of $V_3(\mathbb{R})$ can be uniquely expressed as a linear combination of the vectors of S. Let $(a,b,c) = \alpha(1,0,0)+\beta(0,1,0)+\gamma(1,1,1)$ Then $\alpha+\gamma = a$, $\beta+\gamma = b$, $\gamma = c$. Hence $\alpha = a-c$ and $\beta = b-c$. Thus $(a,b,c) = (a-c)(1,0,0)+(b-c)(0,1,0)+c(1,1,1)$. $\therefore$ S is a basis for $V_3(\mathbb{R})$. □

4. $S = \{1\}$ is a basis for the vector space $\mathbb{R}$ over $\mathbb{R}$.

5. $S = \left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}$ is a basis for $M_2(\mathbb{R})$, since any matrix $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ can be uniquely written as $\begin{pmatrix}a & b\\ c & d\end{pmatrix} = a\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+b\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}+$ $c\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}+d\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$

6. $\{1,i\}$ is a basis for the vector space $\mathbb{C}$ over $\mathbb{R}$.

7. Let V be the set of all polynomials of degree $\leq\ n$ in $\mathbb{R}[x]$. Then $\{1,x,x^2,\ldots,x^n\}$ is a basis for V.

8. $\{(1,0),(i,0),(0,1),(0,i)\}$ is a basis for the vector space $\mathbb{C}\times\mathbb{C}$ over $\mathbb{R}$, for $(a+ib, c+id) = a(1,0)+b(i,0)+c(0,1)+d(0,i)$.

9. $S = \{(1,0,0),(0,1,0),(1,1,1),(1,1,0)\}$ spans the vector space $V_3(\mathbb{R})$ but is not a basis.

Proof. Let $S = \{(1,0,0),(0,1,0),(1,1,1),(1,1,0)\}$. Then $L(S) = V_3(\mathbb{R})$(refer example 3). Now, since $S \subseteq S'$, we get $L(S) = V_3(\mathbb{R})$. Thus S spans $V_3(\mathbb{R})$. But S is linearly dependent since $(1,1,0) = (1,0,0)(0,1,0)$. Hence S is not a basis. □

10. Let $S = \{(1,0,0),(1,1,0)\}$ is linearly independent but not a basis of $V_3(\mathbb{R})$.

Proof. Let $\alpha(1,0,0)+\beta(1,1,0) = (0,0,0)$. Then $\alpha+\beta = 0$ and $\beta = 0$. $\therefore \alpha = \beta = 0$. Hence S is linearly independent. Also $L(S) = \{(a,b,0) :\ a,b\in\mathbb{R}\} \neq V_3(\mathbb{R})$. $\therefore S$ is not a basis. □

Theorem 4.7.5. *Let V be a vector space over a field F. Let $S = \{v_1, v_2, \ldots, v_n\}$ span V. Let $S = \{w_1, w_2, \ldots, w_n\}$ be a linearly independent set of vectors in V. Then $m \leq n$.*

Proof. Since $L(S) = V$, every vector in V and in particular w_1, is a linear combination of $v_1, v_2, \ldots, v_n$. Hence $S_1 = \{w_1, v_1, v_2, \ldots, v_n\}$ is a linearly dependent set of vectors. Hence there exists a vector $v_k \neq w_1$ in S_1 which is a linear combination of the preceding vectors. Let $S_2 = \{w_1, v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$. Clearly, $L(S_2) = V$. Hence w_2 is a lnear combination of the vectors in S_2. Hence $S_3 = \{w_2, w_1, v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n\}$ is linearly dependent. Hence there exists a vector in S_3 which is a linear combination of the preceding vectors. Since the w_i's are linearly independent, this vector cannot be w_2 or w_1 and hence must be some v_j where $j \neq k$(say, with $j > k$). Deletion of v_j from the set S_3 gives the set $S_4 = \{w_2, w_1, v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\}$ of n vectors spanning V. In this process, at each step we insert one vector from $\{w_1, w_2, \ldots, w_m\}$ and delete one vector from $\{v_1, v_2, \ldots, v_n\}$. If $m > n$ after repeating this process n times, we arrive at the set $\{w_n, w_{n-1}, \ldots, w_1\}$ which spans V. Hence w_{n+1} is a linear combination of $w_1, w_2, \ldots, w_n$. Hence $\{w_1, w_2, \ldots, w_n, w_{n+1}, \ldots, w_n\}$ is linearly dependent which is a contradiction. Hence $m \leq n$. □

Theorem 4.7.6. *Any two bases of a finite dimensional vector space V have the same number of elements.*

Proof. Since V is finite dimensional, it has a basis say $S = \{v_1, v_2, \ldots, v_n\}$. Let $S' = \{w_1, w_2, \ldots, w_m\}$ be any other basis for V. Now, $L(S) = V$ and S' is a set of m linearly independent vectors. Hence $m \leq n$. Also, since $L(S') = V$ and S is a set of n linearly independent vectors, $n \leq m$. Hence $m = n$. □

Definition 4.7.7. Let V be a finite dimensional vector space over a field F. The number of elements in any basis of V is called the **dimension** of V and is denoted by *dim* V.

Theorem 4.7.8. *Let V be a vector space of dimension n. Then*

(i) *any set of m vectors where $m > n$ is linearly dependent.*

(ii) any set of m vectors where $m < n$ cannot span V.

Proof.

(i) Let $S = \{v_1, v_2, \cdots, v_n\}$ be a basis for V. Hence $L(S) = V$. Let S' be any set consisting of m vectors where $m > n$. Suppose S' is linearly independent. Since S spans V, $m \leq n$ which is a contradiction. Hence S' is linearly dependent.

(ii) Let S' be a set consisting of m vectors where $m < n$. Suppose $L(S') = V$. Now, $S = \{v_1, v_2, \cdots, v_n\}$ is a basis for V and hence linearly independent. Hence by theorem 4.6.5 $n \leq m$ which is a contradiction. Hence S' cannot span V. □

Theorem 4.7.9. Let V be a finite dimensional vector space over a field a field F. Any linear independent set of vectors in V is part of a basis.

Proof. Let $S = \{v_1, v_2, \ldots, v_r\}$ be a linearly independent set of vectors. If $L(S) = V$ then S itself is a basis. If $L(S) \neq V$, choose an element $v_{r+1} \in V - L(S)$. Now, consider $S_1 = \{v_{1,2}, \ldots, v_r, v_{r+1}\}$. We shall prove that S_1 is linearly independent by showing that no vector in S_1 is a linear combination of the preceding vectors. Since $\{v_1, v_2, \ldots, v_r\}$ is linearly independent v_i where $1 \leq i \leq r$ is not a linear combination of the preceding vectors. Also $v_{r+1} \in L(S)$ and hence v_{r+1} is not a linear combination of $v_1, v_2, \ldots, v_r$. Hence S_1 is linearly independent. If $L(S_1) = V$, then S_1 is a basis for V. If not we take an element $v_{r+2} \in V - L(S_1)$ and proceed as before. Since the dimension of V is finite, this process must stop at a certain stage giving the required basis containing S. □

Theorem 4.7.10. Let V be a finite dimensional vector space over a field F. Let A be a subspace of V. Then there exists a subspace B of V such that $V = A \oplus B$.

Proof. Let $S = \{v_1, v_2, \ldots, v_r\}$ be a basis of A. By theorem 4.6.9, we can find $w_1, w_2, \ldots, w_s \in V$ such that $S' = \{v_1, v_2, \cdots, v_r, w_1, w_2, \ldots, w_s\}$ is a basis of V. Now, let $B = L(\{w_1, w_2, \ldots, w_s\})$. We claim that $A \cap B = \{0\}$ and $V = A + B$. Now, let $v \in A \cap B$. Then $v \in A$ and $v \in B$. Hence $v = \alpha_1 v_1 + \cdots + \alpha_r v_r = \beta_1 w_1 + \cdots + \beta_s w_s$ $\therefore \alpha_1 v_1 + \cdots + \alpha_r v_r - \beta_1 w_1 - \cdots - \beta_s w_s = \mathbf{0}$. Now, since S' is linearly independent,

$\alpha_i = 0 = \beta_j$ for all i and j.

Hence $v = \mathbf{0}$. Thus $A \cap B = \{\mathbf{0}\}$.

Now, let $v \in V$. Then $v = (\alpha_1 v_1 + \cdots + \alpha_r v_r) + (\beta_1 w_1 + \cdots + \beta_s w_s) \in A + B$. Hence $A + B = V$ so that $V = A \oplus B$. □

Definition 4.7.11. Let V be a vector space and $S = \{v_1, v_2, \ldots, v_n\}$ be a set of independent vectors in V. Then S is called a **maximal linear independent set** if for every $v \in V - S$, the set $\{v, v_1, v_2, \ldots, v_n\}$ is linearly dependent.

Definition 4.7.12. Let $S = \{v_1, v_2, \ldots, v_n\}$ be a set of vectors in V and let $L(S) = V$. Then S is called a **minimal generating set** if for any $v_i \in S$, $L(S - \{v_i\}) \neq V$.

Theorem 4.7.13. Let V be a vector space over a field F. Let $S = \{v_1, v_2, \ldots, v_n\} \subseteq V$. Then the following are equivalent.

(i) S is a basis for V.

(ii) S is a maximal linearly independent set.

(iii) S is a minimal generating set.

Proof. **(i)⇒(ii)** Let $S = \{v_1, v_2, \ldots, v_n\}$ be a basis for V. Then by theorem 4.6.8 any $n+1$ vectors in V are linearly dependent and hence S is a maximal linearly independent set.

(ii)⇒(iii) Let $S = \{v_1, v_2, \ldots, v_n\}$ be a maximal linearly independent set. Now to prove that S is a basis for V we shall prove that $L(S) = V$. Obviously $L(S) \subseteq V$. Now, let $v \in V$. If $v \in S$, then $v \in L(S)$. (since $S \subseteq L(S)$) If $v \notin S$, $S' = \{v_1, v_2, \ldots, v_n, v\}$ is a linearly dependent set (since S is a maximal independent set) $\therefore$There exists a vector in S' which is a linear combination of the preceeding vectors. Since $v_1, v_2, \ldots, v_n$ are linearly independent, this vector must be v. Thus v is a linear combination of $v_1, v_2, \ldots, v_n$. Therefore $v \in L(S)$. Hence $V \subseteq L(S)$. Thus $V = L(S)$.

(i)⇒(iii) Let $S = \{v_1, v_2, \ldots, v_n\}$ be a basis. Then $L(S) = V$. If S is not minimal, there exists $v_i \in S$ such that $L(S - \{v_i\}) = V$. Hence S is a linearly independent, $S - \{v_i\}$ is also linearly independent. Thus $S - \{v_i\}$ is a basis consisting of $n - 1$ elements which is a contradiction. Hence S is a minimal generating set. **(iii)⇒((i)** Let

$S = \{v_1, v_2, \ldots, v_n\}$ be a minimal generating set. To prove that S is a basis, we have to show that S is linearly independent. If S is linearly dependent, there exists a vector v_k which is a linear combination of the preceeding vectors. Clearly $L(S - \{v_k\}) = V$ contradicting the minimality of S. Thus S is linearly independent and since $L(S) = V$, S is a basis for V. □

Theorem 4.7.14. *Any vector space of dimension n over a field F is isomorphic to $V_n(F)$.*

Proof. Let V be a vector space of dimension n. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis for V. Then we know that if $v \in V$, v can be written uniquely as $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where $\alpha_i \in F$. Now, consider the map $f : V \to V_n(F)$ given by $f(\alpha_1 v_1 + \cdots + \alpha_n v_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Clearly f is 1-1 and onto. Let $v, w \in V$. Then $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ and $w = \beta_1 v_1 + \cdots + \beta_n v_n$.

$f(v + w) = f[(\alpha_1 + \beta_1)v_1 + (\alpha_2 + \beta_2)v_2 + \cdots + (\alpha_n + \beta_n)v_n]$

$= ((\alpha_1 + \beta_1), (\alpha_2 + \beta_2), \cdots, (\alpha_n + \beta_n)) = (\alpha_1, \alpha_2, \cdots, \alpha_n) + (\beta_1, \beta_2, \cdots, \beta_n)$

Also $f(\alpha u) = f(\alpha\alpha_1 v_1 + \cdots + \alpha\alpha_n v_n) = (\alpha\alpha_1, \alpha\alpha_2, \cdots, \alpha\alpha_n)$

$= \alpha(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha f(v)$. Hence f is an isomorphism of V to $V_n(F)$. □

Corollary 4.7.15. Any two vector spaces of the same dimension over a field F are isomorphic, for, if the vector spaces are of dimension n, each is isomorphic to $V_n(F)$ and hence they are isomorphic.

Theorem 4.7.16. Let V and W be vector spaces over a field F. Let $T : V \to W$ be an isomorphism. Then T maps a basis of V onto a basis of W.

Proof. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis for V. We shall prove that $T(v_1), T(v_2), \ldots, T(v_n)$ are linearly independent and that they span W. Now, $\alpha_1 T(v_1) + \alpha_2 T(v_2) + \cdots + \alpha_n T(v_n) = 0$

$\Rightarrow T(\alpha_1 v_1) + T(\alpha_2 v_2) + \cdots + T(\alpha_n v_n) = 0 \Rightarrow T(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = 0 \Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ (since T is 1-1) $\Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ (since $v_1, v_2, \ldots, v_n$ are linearly independent). $\therefore$ $T(v_1), T(v_2), \ldots, T(v_n)$ are linearly independent. Now, let $w \in W$. Then since T is onto, there exists a vector $v \in V$

such that $T(v) = w$. Let $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$. Then $w = T(v) = T(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = \alpha_1 T(v_1) + \alpha_2 T(v_2) + \cdots + \alpha_n T(v_n)$. Thus w is a linear combination of the vectors $T(v_1), T(v_2) \ldots, T(v_n)$. $\therefore$ $T(v_1), T(v_2) \ldots, T(v_n)$ span W and hence is a basis for W. □

Corollary 4.7.17. Two finite dimensional vector space V and W over a field F are isomorphc if and only if they have the same dimension.

Theorem 4.7.18. Let V and W be finite dimensional vector spaces over a field F. Let $\{v_1, v_2, \cdots, v_n\}$ be a basis for V and let $w_1, w_2, \ldots, w_n$ be any n vectors in W (not necessarily distinct) Then there exists a unique linear transformation $T : V \to W$ such that $T(v_i) = w_i$, $i = 1, 2, \ldots, n$.

Proof. Let $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \in V$. We define $T(v) = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n$. Now, let $x, y \in V$. Let $x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ and $y = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$ $\therefore$ $(x+y) = (\alpha_1+\beta_1)v_1 + (\alpha_2+\beta_2)v_2 + \cdots + (\alpha_n+\beta_n)v_n$ $\therefore$ $T(x+y) = (\alpha_1+\beta_1)w_1 + (\alpha_2+\beta_2)w_2 + \cdots + (\alpha_n+\beta_n)w_n. = (\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n) + (\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_n w_n) = T(x) + T(y)$ Similarly $T(\alpha x) = \alpha T(x)$. Hence T is a linear transformation. Also $v_1 = 1v_1 + 0v_2 + \cdots + 0v_n$. Hence $T(v_1) = 1w_1 + 0w_2 + \cdots + 0w_n = w_1$. Similarly $T(v_i) = w_i$ for all $i = 1, 2, \ldots, n$. Now, to prove the uniqueness, let $T' : V \to W$ be any other linear transformation such that $T'(v_i) = w_i$. Let $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \in V$. $T'(v) = \alpha_1 T'(v_1) + \alpha_2 T'(v_2) + \cdots + \alpha_n T'(v_n) = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n = T(v)$. Hence $T = T'$. □

Remark 4.7.19. The above theorem shows that a linear transformation is completely determined by its values on the elements of a basis.

Theorem 4.7.20. Let V be a finite dimensional vector space over a field F. Let W be a subspace of V. Then
(i) $dim\ W \leq dim\ V$.
(ii) $dim\ \frac{V}{W} = dim\ V - dim\ W$.

Proof.

(i) Let $S = \{w_1, w_2, \ldots, w_m\}$ be a basis for W. Since W is a subspace of V, S is a part of a basis for V. Hence $dim\ W \leq dim\ V$.

(ii) Let $dim\ V = n$ and $dim\ W = m$ Let $S = \{w_1, w_2, \ldots, w_m\}$ be a basis for W. Clearly S is a linearly independent set of vectors in V. Hence S is a part of a basis in V. Let $S = \{w_1, w_2, \ldots, w_m, v_1, v_2, \cdots, v_r\}$ be a basis for V. Then $m + r = n$. Now, we claim $S' = \{W + v_1, W + v_2, \ldots, W + v_r\}$ is a basis for $\frac{V}{W}$. Suppose $\alpha_1(W + v_1) + \alpha_2(W + v_2) + \cdots + \alpha_r(W + v_r) = W + \mathbf{0} \Rightarrow (W + \alpha_1 v_1) + (W + \alpha_2 v_2) + \cdots + (W + \alpha_r v_r) = W \Rightarrow W + \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r = W \Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r \in W$. Now, since $\{w_1, w_2, \cdots, w_m\}$ is a basis for W, $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r = \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m$. Therefore $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r - \beta_1 w_1 - \beta_2 w_2 - \cdots - \beta_m w_m = 0$. Hence $\alpha_1 = \alpha_2 = \cdots = \alpha_r = \beta_1 = \beta_2 = \cdots = \beta_m = 0$ and so S' is a linearly independent set.

Now, let $W + v \in \frac{V}{W}$. Let $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r + \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m$. Then $W + v = W + (\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r + \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m) = W + (\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r)$(since $\beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_m w_m \in W) = (W + \alpha_1 v_1) + (W + \alpha_2 v_2) + \cdots + (W + \alpha_r v_r) = \alpha_1(W + v_1) + \alpha_2(W + v_2) + \cdots + \alpha_r(W + v_r)$ Hence S' spans $\frac{V}{W}$ so that S' is a basis for $\frac{V}{W}$ and $dim\ \frac{V}{W} = r = n - m = dim\ V - dim\ W$. □

Theorem 4.7.21. Let V be a finite dimensional vector space over a field F. Let A and B be subspaces of V. Then $dim\ (A + B) = dim\ A + dim\ B - dim\ (A \cap B)$

Proof. A and B are subspaces of V. Hence $A \cap B$ is subspace of V. Let $S = \{v_1, v_2, \ldots, v_r\}$ be a basis for $A \cap B$ Since $A \cap B$ is a subspace of A and B, S is a part of a basis for A and B. Let $\{v_1, v_2, \ldots, v_r, u_1, u_2, \cdots, u_s\}$ be a basis for A and $\{v_1, v_2, \ldots, v_r, w_1, w_2, \ldots, w_t\}$ be a basis for B.

We shall prove that $\{v_1, v_2, \ldots, v_r, u_1, u_2, \ldots, u_s, w_1, w_2, \ldots, w_t\}$ be a basis for $A+B$. Let $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r + \beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s + \gamma_1 w_1 + \gamma_2 w_2, \cdots + \gamma_t w_t = \mathbf{0}$. Then $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s = -(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r) - (\gamma_1 w_1 + \gamma_2 w_2, \cdots + \gamma_t w_t) \in B$. Hence $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s \in B$. Also $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s \in A$. Hence $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s \in A \cap B$ and so $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s = \delta_1 v_1 + \delta_2 v_2 + \cdots + \delta_r v_r$. $\beta_1 u_1 + \beta_2 u_2 + \cdots + \beta_s u_s - \delta_1 v_1 - \delta_2 v_2 - \cdots - \delta_r v_r = \mathbf{0}$. Thus $\beta_1 = \beta_2 = \cdots = \beta_s = \delta_1 = \delta_2 = \cdots = \delta_r = 0$ (Since $\{u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_r\}$ is linearly independent)

Similarly we can prove $\gamma_1 = \gamma_2 = \cdots = \gamma_t = 0$. Thus $\alpha_i = \beta_j = \gamma_k = 0$ for all $1 \leq i \leq r; 1 \leq j \leq s; 1 \leq k \leq t$. Thus S' is a linearly independent set. Clearly S' spans $A + B$ and so S' is a basis for $A + B$. Hence $dim\ (A + B) = r + s + t$. Also $dim\ A = r+s; dim\ B = r+t$ and $dim\ (A \cap B) = r$. Hence $dim\ A + dim\ B - dim\ A \cap B = (r + s) + (r + t) - r = r + s + t = dim\ (A + B)$. □

Corollary 4.7.22. If $V = A \oplus B, dim\ V = dim\ A + dim\ B$.

Proof. $V = A \oplus B \Rightarrow A + B = V$ and $A \cap B = \{0\}$. Then $dim\ (A \cap B) = 0$. Hence $dim\ V = dim\ A + dim\ B$. □

Chapter 5

UNIT V: Linear Transformation

5.1 Matrix of a Linear Transformation

Let V and W be finite dimensional vector spaces over a field F. Let $dim\ V = m$ and $dim\ W = n$. Fix an ordered basis $\{v_1, v_2, \ldots, v_m\}$ for V and an ordered basis $\{w_1, w_2, \ldots, w_n\}$ for W. Let $T : V \to W$ be a linear transformation. We have seen that T is completely specified by the elements $T(v_1), T(v_2), \ldots, T(v_m)$. Now, let

$$\left.\begin{array}{rc} T(v_1) = & a_{11}w_1 + a_{12}w_2 + \cdots + a_{1n}w_n \\ T(v_2) = & a_{21}w_1 + a_{22}w_2 + \cdots + a_{2n}w_n \\ \vdots & \\ T(v_m) = & a_{m1}w_1 + a_{m2}w_2 + \cdots + a_{mn}w_n \end{array}\right\} \qquad \cdots (1)$$

Hence $T(v_1), T(v_2), \ldots, T(v_m)$ are completely specified by the mn elements a_{ij} of the field F. These a_{ij} can be conveniently arranged in the form of m rows and n columns as follows.

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

Such an array of mn elements of F arranged in m rows and n columns is known as $m \times n$ **matrix** over the field F and is denoted by (a_{ij}). Thus to every linear transformation T there is associated with it an $m \times n$ matrix over F. Conversely any $m \times n$ matrix over F defines a linear transformation $T : V \to W$ given by the formula (1).

Note 5.1.1. The $m \times n$ matrix which we have associated with a linear transformation $T : V \to W$ depends on the choice of the basis for V and W.

For exaample, consider the linear transformation $T : V_2(\mathbb{R}) \to V_2(\mathbb{R})$ given by $T(a, b) = (a, a + b)$. Choose $\{e_1, e_2\}$ as a basis both for the domain and the range. Then $T(e_1) = (1, 1) = e_1 + e_2$

$T(e_2) = (0, 1) = e_2.$

Hence the matrix representing T is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Now, we choose $\{e_1, e_2\}$ as a basis for the domain and $\{(1, 1), (1, -1)\}$ as a basis for the range.

Let $w_1 = (1, 1)$ and $w_2 = (1, -1)$. Then $T(e_1) = (1, 1) = w_1$, and $T(e_2) = (0, 1) = (1/2)w_1 - (1/2)w_2$. Hence the matrix representing T is $\begin{pmatrix} 1 & 0 \\ 1/2 & -1/2 \end{pmatrix}$.

5.1.1 Solved problems

Problem 5.1.2. Obtain the matrix representing the linear transformation $T : V_3(\mathbb{R}) \to V_3(\mathbb{R})$ given by $T(a, b, c) = (3a, a - b, 2a + b + c)$ w.r.t the standard basis $\{e_1, e_2, e_3\}$.

Solution. $T(e_1) = T(1, 0, 0) = (3, 1, 2) = 3e_1 + e_2 + e_3$

$$T(e_2) = T(0,1,0) = (0,-1,1) = -e_2 + e_3$$
$$T(e_3) = T(0,0,1) = (0,0,1) = e_3$$

Thus the matrix representing T is $\begin{pmatrix} 3 & 1 & 2 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Problem 5.1.3. Find the linear transformation $T : V_3(\mathbb{R}) \to V_3(\mathbb{R})$ determined by the matrix $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ -1 & 3 & 4 \end{pmatrix}$ w.r.t the standard basis $\{e_1, e_2, e_3\}$.

Solution. $T(e_1) = e_1 + 2e_2 + e_3 = (1,2,1)$

$T(e_2) = 0e_1 + e_2 + e_3 = (0,1,1)$

$T(e_3) = -e_1 + 3e_2 + 4e_3 = (-1,3,4)$.

Now, $(a,b,c) = a(1,0,0) + b(0,1,0) + c(0,0,1) = ae_1 + be_2 + ce_3$.

$\therefore \quad T(a,b,c) = T(ae_1 + be_2 + ce_3) = aT(e_1) + bT(e_2) + cT(e_3)$

$= a(1,2,1) + b(0,1,1) + c(-1,3,4)$.

$\therefore \quad T(a,b,c) = (a-c, 2a+b+3c, a+b+4c)$

This is the required linear transformation.

Definition 5.1.4. Let $A = (a_{ij})$ and $B = (b_{ij})$ be two $m \times n$ matrices. We define the **sum** of these two matrices by $A + b = (a_{ij} + b_{ij})$.

Note that we have defined addition only for two matrices having the same number of rows and the same number of columns.

Definition 5.1.5. Let $A = (a_{ij})$ be an arbitrary matrix over a field F. Let $\alpha \in F$. We define $\alpha A = (\alpha a_{ij})$.

Theorem 5.1.6. *The set $M_{m\times n}(F)$ of all $m \times n$ matrices over the field F is a vector space of dimension mn over F under matrix addition and scalar multiplication defined above.*

Proof. Let $A = (a_{ij})$ and $B = (b_{ij})$ be two $m \times n$ matrices over the field F. The addition of $m \times n$ matrices is a binary operation which is both commutative and associative. The $m \times n$ matrix whose entries are 0 is the *identity* matrix and $(-a_{ij})$ is the *inverse* matrix of (a_{ij}). Thus the set of all $m \times n$ matrices over the field F is an *abelian group* with respect to addition. The verification of the following axioms are straight forward.

(a) $\alpha(A+B) = \alpha A + \alpha B$

(b) $(\alpha+\beta)A = \alpha A + \beta A$

(c) $(\alpha\beta)A = \alpha(\beta A)$

(d) $1A = A$.

Hence the set of all $m \times n$ over F is a vector space over F.

Now, we shall prove that the dimension of this vector space is mn. Let E_{ij} be the matrix with entry 1 in the $(i,j)^{th}$ place and 0 in the other places. We have mn matrices of this form. Also any matrix $A = (a_{ij})$ can be written as $A = \sum a_{ij}E_{ij}$. Hence A is a linear combination of the matrices E_{ij}. Further these mn matrices E_{ij} are linearly independent. Hence these mn matrices form a basis for the space of all $m \times n$ matrices. Therefore the dimension of the vector space is mn. □

Theorem 5.1.7. Let V and W be two finite dimensional vector spaces over a field F. Let $dim\ V = m$ and $dim\ W = n$. Then $L(V,W)$ is a vector space of dimension mn over F.

Proof. By theorem 4.3.8, $L(V,W)$ is a vector space over F. Now, we shall prove that the vector space $L(V,W)$ is isomorphic to the vector space $M_{m\times n}(F)$. Since $M_{m\times n}(F)$ is of dimension mn, it follows that $L(V,W)$ is also of dimension mn. Fix a basis $\{v_1, v_2, \ldots, v_m\}$ for V and a basis $\{w_1, w_2, \ldots, w_n\}$ for W. We know that any linear transformation $T \in L(V,W)$ can be represented by an $m \times n$ matrix over F. Let T be represented by $M(T)$. This function $M : L(V,W) \to M_{m\times n}(F)$ is clearly 1-1 and onto. Let $T_1, T_2 \in L(V,W)$ and $M(T_1) = (a_{ij})$ and $M(T_2) = (b_{ij})$.

$$M(T_1) = (a_{ij}) \Rightarrow T_1(v_i) = \textstyle\sum_{j=1}^{n} a_{ij}w_j$$

$$M(T_2) = (b_{ij}) \Rightarrow T_2(v_i) = \textstyle\sum_{j=1}^{n} b_{ij}w_j$$

$$\therefore \quad (T_1 + T_2) = \textstyle\sum_{j=1}^{n}(a_{ij} + b_{ij})w_j$$

$$\therefore \quad M(T_1 + T_2) = (a_{ij} + b_{ij}) = (a_{ij}) + (b_{ij}) = M(T_1) + M(T_2).$$

Similarly $M(\alpha T_1) = \alpha M(T_1)$. Hence M is the required isomorphism from $L(V, W)$ to $M_{m\times n}(F)$. □

5.2 Inner Product Space

Upto this point we have dealt with the algebraic properties of a vector space and these properties are consequences of the basic operations, namely, vector addition and scalar multiplcation defined in the vector space. We know that in the usual three dimensional vector space $V_3(\mathbb{R})$ it is possible to talk about the length of a vector and angle between two vectors. These concepts of length and angle can be defined in terms of the usual ”*dot product*” or ”*scalar product*” of two vectors. The dot product of $u = (a_1, b_1, c_1)$ and $v = (a_2, b_2, c_2)$ is defined by

$$u \cdot v = a_1a_2 + b_1b_2 + c_1c_2$$

We note that the length of u is given by $\sqrt{u \cdot u}$ and the angle θ between u and v is determined by $\cos\theta = \frac{u \cdot v}{\sqrt{u \cdot u}\sqrt{v \cdot v}}$. Hence u and v are perpendicular or orthogonal if and only if $u \cdot v = 0$.

An inner product on a vector space is a generalisation of the dot product and in terms of such an inner product we can define the length of a vector and angle between two vectors. Our study about angle will be restricted to the concept of perpendicularity of two vectors.

Throughtout this section we shall deal only with vector spaces over the field F of real or complex numbers.

5.2.1 Definition and Examples

Definition 5.2.1. Let V be a vector space over F. An **inner product** on V is a function which assigns to each ordered pair of vectors u, v in V a scalar in F denoted by $\langle u, v\rangle$ satifying the following conditions.

(i) $\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$

(ii) $\langle \alpha u, v\rangle = \alpha\langle u, v\rangle$

(iii) $\langle u, v\rangle = \overline{\langle v, u\rangle}$, where $\overline{\langle v, u\rangle}$ is the complex conjugate of $\langle u, v\rangle$.

(iv) $\langle u, u\rangle \geq 0$ and $\langle u, u\rangle = 0$ if and only if $u = 0$.

A vector space with an inner product defined on it is called an **inner product space**.

An inner product space is called an **Euclidean space** or **unitary space** according as F is the field of real numbers or complex numbers.

Note 5.2.2. If F is the field of real numbers then condition (iii) takes the form $\langle u, v\rangle = \langle v, u\rangle$. Further (iii) asserts that $\langle u, u\rangle$ is always real and hence (iv) is meaningful whether F is the field of real or complex numbers.

Note 5.2.3. $\langle u, \alpha v\rangle = \bar{\alpha}\langle u, v\rangle$. For, $\quad \langle u, \alpha v\rangle = \bar{\langle \alpha v, u\rangle} = \alpha\bar{\langle v, u\rangle} = \bar{\alpha}\bar{\langle v, u\rangle} = \bar{\alpha}\langle u, v\rangle$.

Note 5.2.4. $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle$

For, $\langle u, v + w\rangle = \bar{\langle v + w, u\rangle} = \bar{\langle v, u\rangle + \langle w, u\rangle} = \bar{\langle v, u\rangle} + \bar{\langle w, u\rangle} = \langle u, v\rangle + \langle u, w\rangle$.

Note 5.2.5. $\langle u, \mathbf{0}\rangle = \langle \mathbf{0}, v\rangle = 0$.

For, $\langle u, \mathbf{0}\rangle = \langle u, 0\mathbf{0}\rangle = 0\langle u, \mathbf{0}\rangle = 0$.

Similarly $\langle \mathbf{0}, v\rangle = 0$.

Examples 5.2.6.

1. $V_n(\mathbb{R})$ is a real inner product space with inner product defined by
$\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n$ where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.
This is called the standard inner product on $V_n(\mathbb{R})$.

Proof. Let $x, y, z \in V_n(\mathbb{R})$ and $\alpha \in \mathbb{R}$.

(i) $\quad \langle x + y, z\rangle = (x_1 + y_1)z_1 + (x_2 + y_2)z_2 + \cdots + (x_n + y_n)z_n$
$\qquad = (x_1z_1 + x_2z_2 + \cdots + x_nz_n) + (y_1z_1 + y_2z_2 + \cdots + y_nz_n) = \langle x, z\rangle + \langle y, z\rangle$.

(ii) $\quad \langle \alpha x, y\rangle = \alpha x_1y_1 + \alpha x_2y_2 + \cdots + \alpha x_ny_n = \alpha(x_1y_1 + x_2y_2 + \cdots + x_ny_n) = \alpha\langle x, y\rangle$.

(iii) $\quad \langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n = y_1x_1 + y_2x_2 + \cdots + y_nx_n = \langle y, x\rangle$.

(iv) $\quad \langle x, x\rangle = x_1^2 + x_2^2 + \cdots + x_n^2 \geq 0 and \langle x, x\rangle = 0$ if and only if $x_1 = x_2 = \cdots = x_n = 0$

$\therefore \quad \langle x, x\rangle = 0$ if and only if $x = \mathbf{0}$ □

2. $V_n(\mathbb{C})$ is a complex inner product space with inner product defined by
$\langle x, y\rangle = x_1\bar{y_1} + x_2\bar{y_2} + \cdots + x_n\bar{y_n}$ where $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$.
This is called the standard inner product on $V_n(\mathbb{R})$.

Proof. Let $x, y, z \in V_n(\mathbb{C})$ and $\alpha \in \mathbb{C}$

(i) $\quad \langle x + y, z\rangle = (x_1 + y_1)\bar{z_1} + (x_2 + y_2)\bar{z_2} + \cdots + (x_n + y_n)\bar{z_n}$

$$= (x_1\bar{z_1} + x_2\bar{z_2} + \cdots + x_n\bar{z_n}) + (y_1\bar{z_1} + y_2\bar{z_2} + \cdots + y_n\bar{z_n}) = \langle x, z\rangle + \langle y, z\rangle.$$

$(ii)\langle \alpha x, y\rangle = \alpha x_1\bar{y_1} + \alpha x_2\bar{y_2} + \cdots + \alpha x_n\bar{y_n} = \alpha(x_1\bar{y_1} + x_2\bar{y_2} + \cdots + x_n\bar{y_n}) = \alpha\langle x, y\rangle.$

$(iii)\ \langle y, \bar{x}\rangle = \overline{y_1\bar{x_1} + y_2\bar{x_2} + \cdots + y_n\bar{x_n}} = \bar{y_1}x_1 + \bar{y_2}x_2 + \cdots + \bar{y_n}x_n = \langle x, y\rangle.$

$(iv)\quad \langle x, x\rangle = x_1\bar{x_1} + x_2\bar{x_2} + \cdots + x_n\bar{x_n} = |x_1|^2 + |x_2|^2 + \cdots + |x_n|^2 \geq 0$

$\therefore\ \ \langle x, x\rangle = 0$ if and only if $x = \mathbf{0}$ □

3. Let V be the set of all continuous real valued functions defined on the closed interval $[0, 1]$. V is a real inner product space with inner product defined by $\langle f, g\rangle = \int_0^1 f(t)g(t)dt.$

Proof. Let $f, g, h \in V$ and $\alpha \in \mathbb{R}$.

$(i)\langle f + g, h\rangle = \int_0^1 [f(t) + g(t)]h(t)dt = \int_0^1 f(t)h(t)dt + \int_0^1 g(t)h(t)dt = \langle f, h\rangle + \langle g, h\rangle.$

$(ii)\langle \alpha f, g\rangle = \int_0^1 \alpha f(t)g(t)dt = \alpha \int_0^1 f(t)g(t)dt = \alpha\langle \alpha f, g\rangle.$

$(iii)\langle f, g\rangle = \int_0^1 f(t)g(t)dt \int_0^1 g(t)f(t)dt = \langle g, f\rangle.$

$(iv)\langle f, f\rangle = \int_0^1 |f(t)|^2 dt \geq 0$ and $\langle f, f\rangle = 0$ if and only if $f = 0$ □

Definition 5.2.7. Let V be an inner product space and let $x \in V$. The **norm** or **length** of x, denoted by $\|x\|$, is defined by $\|x\| = \sqrt{\langle x, x\rangle}$. x is called a **unit vector** if $\|x\| = 1$.

5.2.2 Solved Problems

Problem 5.2.8. Let V be the vector space of polynomials with inner product given by $\langle f, g\rangle = \int_0^1 f(t)g(t)dt$. Let $f(t) = t + 2$ and $g(t) = t^2 - 2t - 3$. Find
(i) $\langle f, g\rangle$ (ii) $\|f\|$.

Solution. $(i)\ \langle f, g\rangle = \int_0^1 f(t)g(t)dt = \int_0^1 (t + 2)(t^2 - 2t - 3)dt$

$= \int_0^1 (t^3 - 7t - 6)dt = \left[\frac{t^4}{4} - \frac{7t^2}{2} - 6t\right]_0^1 = \frac{1}{4} - \frac{7}{2} - 6 = -\frac{37}{4}.$

$(ii)\quad \|f\|^2 = \langle f, f\rangle = \int_0^1 [f(t)]^2 dt = \int_0^1 (t + 2)^2 dt = \int_0^1 (t^2 + 4 + 4)dt$

$= \left[\frac{t^3}{3} + 2t^2 + 4t\right]_0^1 = \frac{1}{3} + 2 + 4 = \frac{19}{3}$

$\therefore\ \ \|f\| = \frac{\sqrt{19}}{\sqrt{3}}$

Theorem 5.2.9. The norm defined in an inner product space V has the following properties.

(i) $\|x\| \geq 0$ and $\|x\| = 0$ if and only if $x = 0$.

(ii) $\|\alpha x\| = |\alpha|\|x\|$.

(iii) $|\langle x, y\rangle| \leq \|x\|\|y\|$ (Schwartz's inequality)

(iv) $\|x + y\| \leq \|x\| + \|y\|$ (Triangle inequality)

Proof. (i) $\|x\| = \sqrt{\langle x, x\rangle} \geq 0$ and $\|x\| = 0$ if and only if $x = 0$.
(ii) $\|\alpha x\|^2 = \langle \alpha x, \alpha x\rangle = \alpha\langle x, \alpha x\rangle = \alpha\bar{\alpha}\langle x, x\rangle = |\alpha|^2\|x\|^2$.
Hence $\|\alpha x\| = |\alpha|\|x\|$.

(iii) The inequality is trivially true when $x = \mathbf{0}$ or $y = \mathbf{0}$. Hence let $x \neq \mathbf{0}$ and $y \neq \mathbf{0}$. Consider $z = y - \frac{\langle y,x\rangle}{\|x\|^2}x$. Then

$$0 \leq \langle z, z\rangle = \langle y - \frac{\langle y,x\rangle}{\|x\|^2}x, y - \frac{\langle y,x\rangle}{\|x\|^2}x\rangle = \langle y, y\rangle - \frac{\overline{\langle y,x\rangle}}{\|x\|^2}\langle y, x\rangle - \frac{\langle y,x\rangle}{\|x\|^2}\langle x, y\rangle + \frac{\langle y,x\rangle\overline{\langle y,x\rangle}}{\|x\|^2\|x\|^2}\langle x, x\rangle$$
$$= \|y^2\| - \frac{\overline{\langle y,x\rangle}\langle y,x\rangle}{\|x\|^2} - \frac{\langle y,x\rangle\langle x,y\rangle}{\|x\|^2} + \frac{\langle y,x\rangle\overline{\langle y,x\rangle}}{\|x\|^2} = \|y^2\| - \frac{\overline{\langle x,y\rangle}\langle x,y\rangle}{\|x\|^2}$$

$\therefore\quad 0 \leq \|x\|^2\|y\|^2 - |\langle x, y\rangle|^2$

$\therefore\quad |\langle x, y\rangle|^2 \leq \|x\|^2\|y\|^2$.

(iv) $\|x + y\|^2 = \langle x + y, x + y\rangle = \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle$

$$= \|x\|^2 + \langle x, y\rangle + \overline{\langle x, y\rangle} + \|y\|^2 = \|x\|^2 + 2Re\langle x, y\rangle + \|y\|^2$$
$$\leq \|x\|^2 + 2|\langle x, y\rangle| + \|y\|^2 \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 \quad \text{(by (iii))}$$
$$\leq (\|x\| + \|y\|)^2$$

$\therefore\quad \|x + y\| \leq \|x\| + \|y\|$. □

5.3 Orthogonality

Definition 5.3.1. Let V be an inner product space and let $x, y \in V$. x is said to be **orthogonal** to y if $\langle x, y\rangle = 0$.

Note 5.3.2. x is orthogonal to $y \Rightarrow \langle x, y\rangle = 0 \Rightarrow \overline{\langle x, y\rangle} = \overline{0} \Rightarrow \langle y, x\rangle = 0$
$\Rightarrow y$ is orthogonal to x. Thus x and y are orthogonal if and only if $\langle x, y\rangle = 0$.

Note 5.3.3. x is orthogonal to $y \Rightarrow \alpha x$ is orthogonal to y.

Note 5.3.4. x_1 and x_2 are orthogonal to $y \Rightarrow x_1 + x_2$ is orthogonal to y.

Note 5.3.5. $\mathbf{0}$ is orthogonal to every vector in V and is the only vector with this property.

Definition 5.3.6. Let V be an inner product space. A set S of vectors in V is said to be an **orthogonal set** if any two distinct vectors in S are orthogonal.

Definition 5.3.7. S is said to be an **orthonormal set** if S is orthogonal and $\|x\| = 1$ for all $x \in S$.

Example 5.3.8. The standard basis $\{e_1, e_2, \ldots, e_n\}$ in $\mathbb{R}^n$ or $\mathbb{C}^n$ is an orthogonal set with respect to the standard inner product.

Theorem 5.3.9. Let $S = \{v_1, v_2, \ldots, v_n\}$ be an orthogonal set of non-zero vectors in an inner product space V. Then S is linearly independent.

Proof. Let $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$

Then $\langle \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n, v_1 \rangle = \langle \mathbf{0}, v_1 \rangle = 0$

$\therefore \quad \alpha_1 \langle v_1, v_1 \rangle + \alpha_2 \langle v_2, v_1 \rangle + \cdots + \alpha_n \langle v_n, v_1 \rangle = 0$

$\therefore \quad \alpha_1 \langle v_1, v_1 \rangle = 0$ (since S is orthogonal)

$\therefore \quad \alpha_1 = 0$ (since $v_1 \neq \mathbf{0}$)

Similarly $\alpha_2 = \alpha_3 = \cdots = \alpha_n = 0$. Hence S is linearly independent. □

Theorem 5.3.10. Let $S = \{v_1, v_2, \ldots, v_n\}$ be an orthogonal set of non-zero vectors in V. Let $v \in V$ and $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$. Then $\alpha_k = \frac{\langle v, v_k \rangle}{\|v_k\|^2}$.

Proof.
$$\begin{aligned} \langle v, v_k \rangle &= \langle \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n, v_k \rangle \\ &= \alpha_1 \langle v_1, v_k \rangle + \alpha_2 \langle v_2, v_k \rangle + \cdots + \alpha_k \langle v_k, v_k \rangle + \cdots + \alpha_n \langle v_n, v_k \rangle \\ &= \alpha_k \langle v_k, v_k \rangle \quad \text{(since } S \text{ is orthogonal)} \\ &= \alpha_k \|v_k\|^2 \\ \therefore \quad \alpha_k &= \frac{\langle v, v_k \rangle}{\|v_k\|^2} \end{aligned}$$
□

Theorem 5.3.11. Every finite dimensional inner product space has an orthonormal basis.

Proof. Let V be a finite dimensional inner product space. Let $\{v_1, v_2, \dots, v_n\}$ be a basis for V. From this basis we shall construct an orthonormal basis $\{w_1, w_2, \dots, w_n\}$ by means of a construction known as $Gram - Schmidt$ *orthogonalisation* process.

First we take $w_1 = v_1$. Let $w_2 = v_2 - \frac{\langle v_2, w_1\rangle}{\|w_1\|^2}w_1$. We claim that $w_2 \neq 0$. For, if $w_2 = 0$ then v_2 is a scalar multiple of w_1 and hence of v_1 which is a contradiction since v_1, v_2 are linearly independent.

Also, $\langle w_2, w_1\rangle = \langle v_2 - \frac{\langle v_2,w_1\rangle}{\|w_1\|^2}w_1, w_1\rangle = \langle v_2 - \frac{\langle v_2,v_1\rangle}{\|v_1\|^2}v_1, v_1\rangle \ \ (\because w_1 = v_1)$

$= \langle v_2, v_1\rangle - \frac{\langle v_2,v_1\rangle}{\|v_1\|^2}\langle v_1, v_1\rangle = \langle v_2, v_1\rangle - \langle v_1, v_1\rangle = 0.$

Now, suppose that we have constructed non-zero orthogonal vectors $w_1, w_2, \dots, w_k$. Then put

$$w_{k+1} = v_{k+1} - \sum_{j=1}^{k} \frac{\langle v_{k+1}, w_j\rangle}{\|w_j\|^2} w_j$$

We claim that $w_{k+1} \neq 0$. For, if $w_{k+1} = 0$, then v_{k+1} is a linear combination of $w_1, w_2, \dots, w_k$ and hence is a linear combination of $v_1, v_2, \dots, v_k$ which is a contradiction since $v_1, v_2, \dots, v_{k+1}$ are linearly independent. Also,

$\langle w_{k+1}, w_i\rangle = \langle v_{k+1}, w_i\rangle - \sum_{j=1}^{k} \frac{\langle v_{k+1},w_j\rangle}{\|w_j\|^2}\langle w_j, w_i\rangle$

$= \langle v_{k+1}, w_i\rangle - \frac{\langle v_{k+1},w_i\rangle}{\|w_i\|^2}\langle w_i, w_i\rangle = \langle v_{k+1}, w_i\rangle - \langle w_i, w_i\rangle = 0.$

Thus, continuing in this way we ultimately obtain a non-zero orthogonal set $\{w_1, w_2, \dots, w_n\}$. By theorem this set is linearly independent and hence a basis. To obtain an orthonormal basis we replace each w_i by $\frac{w_i}{\|w_i\|}$. □

5.3.1 Solved Problems

Problem 5.3.12. Apply Gram-Schmidt process to construct an orthonormal basis for $V_3(\mathbb{R})$ with the standard inner product for the basis $\{v_1, v_2, v_3\}$ where $v_1 = (1, 0, 1)$; $v_2 = (1, 3, 1)$ and $v_3 = (3, 2, 1)$.

Solution. Take $w_1 = v_1 = (1, 0, 1)$.

Then $\|w_1\|^2 = \langle w_1, w_1\rangle = 1^2 + 0^2 + 1^2 = 2$ and $\langle w_1, v_2\rangle = 1 + 0 + 1 = 2$

Put $w_2 = v_2 - \frac{\langle v_2,w_1\rangle}{\|w_1\|^2}w_1 = (1, 3, 1) - (1, 0, 1) = (0, 3, 0)$

$\therefore \ \ \|w_2\|^2 = 9.$

Also $\langle w_2, v_3\rangle = 0 + 6 + 0 = 6$ and $\langle w_1, v_3\rangle = 3 + 0 + 1 = 4$

Now, $w_3 = v_3 - \frac{\langle v_3,w_1\rangle}{\|w_1\|^2}w_1 - \frac{\langle v_3,w_2\rangle}{\|w_2\|^2}w_2 = (3,2,1) - \frac{4}{2}(1,0,1) - \frac{6}{9}(0,3,0)$

$= (3,2,1) - 2(1,0,1) - \frac{2}{3}(0,3,0) = (1,0,-1)$

$\therefore\ \|w_3\|^2 = 2.$

$\therefore$ The orthogonal basis is $\{(1,0,1),(0,3,0),(1,0,-1)\}$.

Hence the orthonormal basis is $\left\{\left(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}}\right),(0,1,0),\left(\frac{1}{\sqrt{2}},0,-\frac{1}{\sqrt{2}}\right)\right\}$.

Problem 5.3.13. Let V be the set of all polynomials of degree $\leq\ 2$ together with the zero polynomial. V is a real inner product space with inner product defined by $\langle f,g\rangle = \int_{-1}^{1} f(x)g(x)dx$. Starting with the basis $\{1,x,x^2\}$, obtain an orthogonal basis for V.

Solution. Let $v_1 = 1; v_2 = x$ and $v_3 = x^2$. Let $w_1 = v_1$.

Then $\|w_1\|^2 = \langle w_1,w_1\rangle = \int_{-1}^{1} 1dx = 2$

Hence $\|w_1\| = \sqrt{2}$

$w_2 = v_2 - \frac{\langle v_2,w_1\rangle}{\|w_1\|^2}w_1 = x - \frac{1}{2}\int_{-1}^{1} xdx = x$

$\therefore\ \|w_2\|^2 = \langle w_2,w_2\rangle = \int_{-1}^{1} x^2dx = \frac{2}{3}.$

Now, $w_3 = v_3 - \frac{\langle v_3,w_1\rangle}{\|w_1\|^2}w_1 - \frac{\langle v_3,w_2\rangle}{\|w_2\|^2}w_2 = x^2 - \frac{1}{2}\int_{-1}^{1} x^2dx - \left(\frac{3x}{2}\right)\int_{-1}^{1} x^3dx = x^2 - \frac{1}{3}$

$\therefore\ \|w_3\|^2 = \langle w_3,w_3\rangle = \int_{-1}^{1}\left(x^2 - \frac{1}{3}\right)dx = \frac{8}{45}.$

Hence the orthogonal basis is $\left\{1,x,x^2 - \frac{1}{3}\right\}$.

$\therefore$ The required orthonormal basis is $\left\{\frac{1}{\sqrt{2}}, \frac{\sqrt{3}}{2}x, \frac{\sqrt{10}}{4}(3x^2-1)\right\}$.

Problem 5.3.14. Find a vector of unit length which is orthogonal to $(1,3,4)$ in $V_3(\mathbb{R})$ with standard inner product.

Solution. Let $x = (x_1,x_2,x_3)$ be any vector orthogonal to $(1,3,4)$. Then $x_1 + 3x_2 + 4x_3 = 0$. Any solution of this equation gives a vector orthogonal to $(1,3,4)$. For example $x = (1,1,-1)$ is orthogonal to $(1,3,4)$. Also $\|x\| = \sqrt{3}$. Hence a unit vector orthogonal to $(1,2,3)$ is given by $\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}}\right)$

Note 5.3.15. The set of all vectors orthogonal to $(1,3,4)$ are points lying on the plane $x + 3y + 4z = 0$, which is a two dimensional subspace of $V_3(\mathbb{R})$.

Problem 5.3.16. Find an orthogonal basis containing the vector $(1,3,4)$ for $V_3(\mathbb{R})$ with the standard inner product.

Solution. $(1, 1, -1)$ is a vector orthogonal to $(1, 3, 4)$ (refer above problem).

Now, let $y = (y_1, y_2, y_3)$ be a vector orthogonal to both $(1, 3, 4)$ and $(1, 1, -1)$.

Then $y_1 + 3y_2 + 4y_3 = 0$

$$y_1 + y_2 - y_3 = 0$$

Any solution of this system of equations gives a vector orthogonal to $(1, 3, 4)$ and $(1, 1, -1)$. For example $(7, -5, 2)$ is one such vector. (by cross multiplication method). Hence $\{(1, 3, 4), (1, 1, -1), (7, -5, 2)\}$ is an orthogonal basis containing $(1, 3, 4)$.