ABSTRACT ALGEBRA

Dr.A. MALLIKA

B. Sc. MATHEMATICS- V YEAR

ABSTRACT ALGEBRA – JMMA51

SYLLABUS

UNIT -I: Groups: Definition and Examples – Properties – Permutation Groups – Subgroups – Cyclic Groups.

Chapter 3: Sections 3.1, 3.2, 3.4 to 3.6

UNIT- II: Order of an element – Cosets and Lagrange's Theorem – Normal subgroups and Quotient groups.

Chapter 3: Sections 3.7 to 3.9

UNIT- III: Isomorphism – Cayley's Theorem – Homomorphisms – Fundamental Theorem.

Chapter 3: Sections 3.10 and 3.11

UNIT- IV: Rings: Definition and examples – Properties – Types of rings – Characteristic of a ring – Subrings – Ideals. Some special classes of rings – Homomorphism of rings – Ideals and quotient rings – More ideals and quotient rings.

Chapter 4: Sections 4.1, 4.2, 4.4 to 4.7

UNIT- V: Quotient Rings – Maximal and Prime Ideals – Homomorphism and Isomorphism of Ring – The field of quotients of an Integral Domain.

Chapter 4: Sections 4.3, 4.8 to 4.11

Text Book: S.Arumugam and A. Thangapandiselvi Isaac, Modern Algebra, Scitech Publications, 2014.

ABSTRACT ALGEBRA

CONTENTS

UNIT V

UNIT I

3. Groups

3.0. Introduction

Modern Algebra is largely concerned with the study of abstract sets endowed with one or more binary operations. In this chapter we introduce one of the basic algebraic structures known as **groups**. A group is a set with one binary operation defined on it satisfying some natural conditions. The definition of a group is an abstraction of the familiar properties of $(\mathbb{Z}, +)$ given below.

(i) Addition is an associative binary operation in $\mathbb{Z}$.
(ii) The element $0 \in \mathbb{Z}$ is such that $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}m$. Hence (0) is the identity element w.r.t. addition.
(iii) Let $a \in \mathbb{Z}$. The element $-a \in \mathbb{Z}$ is such that $a + (-a) = (-a) + a = 0$. Hence $-a$ is the inverse of a.

We isolate these properties in the following definition.

3.1. Definition and Examples

Definition. A non-empty set G together with a binary operation $*: G \times G \to G$ is called a **group** if the following conditions are satisfied.

(i) $*$ is **associative** (i.e.) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
(ii) There exists an element $e \in G$ such that$a * e = e * a = a$ for all $a \in G$.e is called the **identity element** of G.
(iii) For any element a in G there exists an element a' in G such that $a * a' = a' * a = e$. a' is called the **inverse** of a.

Examples

1. Z,Q,R and C are groups under usual addition.

2. The set of all 2×2matrices$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a,b,c,d \in$ 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.

We know that matrix multiplication is associative.$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element.The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{|A|}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ 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 $a + e = a$.

5. The set E of all even integers under usual addition is a group.

For $a, b \in E \Rightarrow a + b \in E$. Therefore usual addition is a binary operation in E.

$0 \in E$ is the identity element. If $a \in E, -a \in E$is the inverse of a.

6. $\mathbb{Q}^*$ *and* $\mathbb{R}^*$under usual multiplication are groups.

1 is the identity element and the inverse of a is $1/a$.

7. $\mathbb{Q}^+$ is not 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 theidentity 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. $1 \in \mathbb{Z}$ is the identity element. However, any element other than 1 and -1 does not have an inverse.

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 $f, g \in B(A) \Rightarrow f \circ g \in B(A)$

The composition of functions is associative. $i_A: A \to A$ is the identity element. If $f: A \to A$ is a bijection, then $f^{-1}: A \to A$ is also a bijection and $(f \circ f^{-1} = f^{-1} \circ f = i_A)$.

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

11. Let $G = \{1, -1\}$. G is a group under usual 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. (P(S),Δ) is a group. Δ is associative. Also AΔΦ =ΦΔ A=A for all Aϵ P(S). Hence Φ is the identity element. AΔ A=Φ so that inverse of each element is itself.

Example 15

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

Proof. 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 not simultaneously zero.

Now, $xy = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$

To prove that ac - bd = 0 and ad+bc = 0 are not simultaneously zero.

Suppose,

$$ac - bd = 0 \ldots\ldots\ldots \quad (1)$$
$$ad + bc = 0 \ldots\ldots\ldots \quad (2)$$

Multiplying (1) by (bd) and (2) by (c) and subtracting, we get$b(d^2 + c^2) = 0$.

Either $b = 0\ or d^2 + c^2 = 0$.

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)

⇒ x=0 or y=0 which is a contradiction.

Hence $xy \in \mathbb{C}^*$.

Now, let $x = a + ib, y = c + id, z = e + if$.

Then $x(yz) = (a + ib)[(ce - df) + i(de + cf)] = (ace - adf - bde + bcf) + i(bce - bdf + ade + acf)$

Similarly $(xy)z = (ace - adf - dbe - bcf) + i(bce - bdf + ade + acf)$

Hence $x(yz) = (xy)z$.

1+i0 is the identity element.

Also

$$\frac{1}{x} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}$$

Since $a^2 + b^2 \neq 0, 1/x \in C*$ and is the inverse of x. Hence C^* is a group under usual multiplication.

Example. 16

Let G={z: zϵ C and |z|=1}. Then G is a group under multiplication.

Proof. Let $z_1, z_2 \in G$. Then $|z_1| = |z_2| = 1$.

$\therefore |z_1 z_2| = |z_1|\,|z_2| = 1$ and hence $z_1 z_2 \in G$.

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 $|1/z| = 1/|z| = 1$.

$\therefore 1/z \in G$ and is the inverse of z. Hence G is a group.

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

Proof. Let $w = \cos(2\pi/n) + i \sin(2\pi/n)$. Then the n^{th} roots of unity are given by

$1, w, w^2, \ldots, w^{n-1}$.

Let $G = \{1, w, w^2, \ldots, w^{n-1}\}$.

We know that $w^n = 1, w^{n+1} = w$ etc.

Let $w^r, w^s \in G$. Let $r + s = qn + t$ where $0 \leq t < n$.

$\therefore w^r w^s = w^{r+s} = w^{qn+t} = (w^n)^q w^t = w^t \in G$.

We know that usual multiplication of complex numbers is associative.

$1 \in G$ is the identity element.

Inverse of w^r is w^{n-r}. Hence G is a group.

Example 18. Let G={a+b√2 :a,bϵ Z}. Then G is a group under usual addition.

Proof. 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.

$0 = 0 + 0\sqrt{2} \in G$ is the identity element. $-a - b\sqrt{2}$ is the inverse of a $+b\sqrt{2}$.

Hence G is a group.

Example 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 ∈ G. Then a ≠ −1 and b ≠ −1. We claim that a $*$ b ≠ −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 ≠ −1 and thus $*$ is a binary operation on G.

To prove $*$ is associative

a $*$ (b $*$ c)= a $*$ (b + c + bc)
= a + (b + c + bc) + a(b + c + bc)
= a + b + c + bc + ab + ac + abc.

Also (a $*$ b) $*$ c = (a + b + ab) $*$ c
= a + b + ab + c + (a + b + ab)c
= a + b + c + ab + ac + bc + abc.

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

0 is the identity, for a $*$ 0 = a + 0 + a0 = a and 0 $*$ a = 0 + a + 0a = a.

Now, let a' be such that a $*$ a' = 0. Hence a + a' + aa' = 0 so that a' = −a/(1+a).

Since a ≠ −1, we have a' ∈ R − {−1}.

Also a' $*$ a = (−a/(1 + a)) $*$ a= −a/(1+a) + a + (−a²/(1+a))= 0.

Hence a' is the inverse of a. Thus G is a group.

Example 20. In R* we define a $*$ b = (1/2)ab. Then (R*, $*$) is a group.

Proof. Obviously $*$ is a binary operation in R*.

Let $a, b, c \in R*$.

Then $(a * b) * c = [(1/2)ab] * c = (1/4)abc = a * (b * c)$. Hence $*$ is associative.

Let $e \in R*$ be such that $a * e = a$.

$\therefore (1/2)ae = a$ and hence $e = 2$.

$\therefore 2 * a = a * 2 = a$. Hence 2 is the identity.

Let $a \in R*$. Let $b \in R*$ be such that $a * b = 2$. Then $(1/2)ab = 2$, i.e. $b = 4/a$.

$\therefore a * (4/a) = 1/2(a)(4/a) = 2$ i.e., $(4/a)$ is the inverse of a. Thus (R*, $*$) is a group.

Example 21.

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

Proof. 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 $f_a \circ f_0 = f_{a+0} = f_a = f_0 \circ f_a$. Hence 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. Let $Z_n = \{0, 1, 2, \ldots, n - 1\}$.

Let $a, b \in Z_n$. Let $a + b = qn + r$ 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.

Example 22. (Z_n, $\oplus$) is a group.

Proof. Clearly $\oplus$ is a binary operation in Z_n.

Let a, b, c $\in Z_n$. Let$a + b = q_1 n + r_1$ where $0 \leq r_1 < n$ … (1)

$b + c = q_2 n + r_2$ where $0 \leq r_2 < n$ … (2)

$r_1 + c = q_3 n + r_3$ where $0 \leq r_3 < n$ … (3)

$\therefore a + b + c = (q_1 + q_2)n + r_3$ (using 1 and 3)

$\therefore a + q_2 n + r_2 = (q_1 + q_3)n + r_3$ (by 2)

$a + r_2 = q_4 n + r_3$ where $q_4 = q_1 + q_2 - q3$ … (4)

Now $(a \oplus b) \oplus c = r_1 \oplus c = r_3$ (by 3)

Also $a \oplus (b \oplus c) = a \oplus r_2 = r_3$ (by 4). Hence $\oplus$ is associative.

Clearly the identity element is 0 and the inverse of $a \in Z_n$ is $n - a$.

Hence $(Z_n, \oplus)$ is a group.

Note 1. (Z_n, $\oplus$) is called the group of integers modulo n.

Note 2. This example shows that for any positive integer n there exists a group with n elements.

Example 23. Let n be a prime. Then $Zn - \{0\}$ is a group under multiplication modulo n.

Proof. Let $a, b \in Z_n - \{0\}$. Then a ≠ 0 and b ≠ 0.

Now by definition $a \odot b \in Z_n^*$

We claim that $a \odot b \neq 0$.

Suppose $a \odot b = 0$. Then $n|ab$. Since n is prime $n|a$ or $n|b$.

$\therefore a = 0$ or $b = 0$ which is a contradiction. Hence $a \odot b \in Z_n - \{0\}$.

Now, let $a, b, c \in Z_n - \{0\}$.

Let $ab = q_1n + r_1$ where $0 \leq r_1 < n$ … (1)
$bc = q_2n + r_2$ where $0 \leq r_2 < n$ … (2)

$r_1c = q_3n + r_3$ where $0 \leq r_3 < n$ … (3)

$\therefore abc = q_1nc + r_1c$ (by 1)
$= a(q_2n + r_2) = q_1n + q_3n + r_3$ (using 2 and 3)

$ar_2 = q_4n + r_3$ where $q_4 = q_1c + q_3 - aq_2$ … (4)

Now $(a \odot b) \odot c = r_1 \odot c = r_3$ (by 3)

Also $a \odot (b \odot c) = a \odot r_2 = r_3$ (by 4)

$(a \odot b) \odot c = a \odot (b \odot c)$

Hence $\odot$ is associative.

$1 \in Z_n - \{0\}$ is the identity element.

Let $a \in Z_n - \{0\}$.

Since n is prime $(a, n) = 1$. Hence the linear congruence $ax \equiv 1(\mathrm{mod} n)$ has a unique

Solution, say $b \in Z_n - \{0\}$. Clearly $a \odot b \equiv b \odot a \equiv 1$. Thus b is the inverse of a.

Hence $Z_n - \{0\}$ is a group.

Note. The above result is not true if n is a composite number.

For, if n is a composite number, let $n = pq$ where $1 < p < n$ and $1 < q < n$.

Clearly $p, q \in Z_n - \{0\}$. But $p \odot q \equiv 0$.

Hence $Z_n - \{0\}$ is not closed under $\odot$. Hence it is not a group.

Example 24. The set of all positive integers less than n and prime to it is a group under

Multiplication modulo n.

Proof. Let $G = \{m/m < n \; and \; (m, n) = 1\}$.

Let $p, q \in G$. Obviously $pq < n$ and $(pq, n) = 1$. Now let $pq = sn + r, 0 < r < n$.

Since $p \odot q = r$ (by definition).

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. Hence $r \in G$. Hence G is closed under $\odot$.

We know that multiplication modulo n is associative. $1 \in G$ is the identity element.

Let $a \in G$. Then $(a, n) = 1$. Hence the linear congruence $ax \equiv 1(\mathrm{mod} n)$ has a unique solution for x, say b.

$ab \equiv 1(\mathrm{mod} n), ab = qn + 1$.

Now $c|b$ and $c|n \Rightarrow c|(ab - qn) \Rightarrow c|1 \Rightarrow c = 1$.

Thus $(b, n) = 1$. Hence $b \in G$ and is the inverse of a. Thus G is a group.

Example 27. In N we define a * b = a. Then (N, *) is not a group.

Proof. Clearly * is an associative binary operation on N.

However, there is no element $e \in N$ such that $e * a = a$ for all $a \in N$. Hence there is no dentity element in $(N,*)$. Hence $(N,*)$ is not a group.

Definition. 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. Z, Q, R and C under usual addition are abelian groups.
2. $(P(S), \Delta)$ is an abelian group since A Δ B = B Δ A for all A, B ϵ P(S).
3. Let B(R) denote the set of all bijections from R to R. Then B(R) is a group under the composition of functions. This group is non-abelian. For, consider

   f : R → R given by f(x) = x + 3 and

   g : R → R given by g(x) = 2x. Clearly f and g are bijections.

   $(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 3$ and

   $(g \circ f)(x) = g(f(x)) = g(x + 3) = 2x + 6$.

Hence $f \circ g \neq g \circ f$.

Hence B(R) is non-abelian.

4. $(Z_n, \oplus)$ is an abelian group.

Exercises

1. Determine which of the groups given in 3.1 are abelian.
2. Let $5Z = 5x/x \in Z$. Show 5Z is an abelian group under usual addition.
3. Let n be a fixed integer. Let $nZ = \{nx \ /x \in Z\}$. Show that nZ is an abelian group under usual addition.
4. Let $G = \{2^n/n \in Z\}$. Show that G is an abelian group under usual multiplication.

3.2. Elementary Properties of Group

Theorem 3.1. Let G be a group. Then

(i) identity element of G is unique.

(ii) for any $a \in G$, the inverse of a is unique.

Proof.(i) Let e and e' be two identity elements of G. Then

$ee' = e'$ (since e' is an identity).

Also $ee' = e$ (since e' is an identity).

Hence $e = e'$.

(ii) Let a' and a'' be two inverses of a.

Hence $aa' = a'a = e$ and $aa'' = a''a = e$.

$\therefore a'' = a''e = a''(aa') = (a''a)a' = ea' = a'$.

Hence inverse is unique.

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

Theorem 3.2. In a group the left and right cancellation laws hold

(i.e.) $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

Proof. $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow eb = ec \Rightarrow b = c.$

Similarly we can prove that $ba = ca \Rightarrow b = c.$

Theorem 3.3. Let G be a group and $a, b \in G$. Then the equations 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 $x = a^{-1}b$ 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 $x_1 = x_2$.$\Rightarrow x = a^{-1}b$ is the unique solution for $ax = b$.Similarly we can prove that $y = ba^{-1}$ is the unique solution of the equation $ya = b$.

Theorem 3.4. Let G be a group. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$

Similarly $(b^{-1}a^{-1})(ab) = e$.
Hence $(ab)^{-1} = b^{-1}a^{-1}$.

Proof of the second part is obvious.

Corollary. 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. Let G be a group and a ϵ G. For any positive integer n we define $a^n = a.a \ldots . a$ (a written n times)

Clearly $(a^n)^{-1} = (a.a \ldots a)^{-1} = (a^{-1}a^{-1} \ldots . a^{-1}) = (a^{-1})^n$

We now define $a^{-n} = (a^{-1})^n = (a^n)^{-1}$

Finally we define $a^0 = e$. Thus $a^n$is defined for all integer n.

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

Theorem 3.5.

(i) $a^m a^n = a^{m+n}, m, n \in \mathbb{Z}$.

(ii) $(a^m)^n = a^{mn}, m, n \in \mathbb{Z}$.

Note. In additive notation the above results take the form

$ma + na = (m + n)a$ and

$n(ma) = (mn)a$.

Proof. (i) When n=0 the result follows directly from the definition. Now let n>0. We prove by induction on n.

When $m \geq 0, a^{m+1} = a^m a^1$ (by definition).

When $m = -1, a^{m+1} = a^0 = e$ and $a^m a^1 = a^{-1}a = e$.

Hence $a^{m+1} = a^m a^1$.

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

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

Hence $a^{m+1} = a^m a$ for all $m \in \mathbb{Z}$.

Hence the result is true for n=1. Suppose now that the theorem is valid for n=k>1.

Then $a^m a^k = a^{m+k}$.

$\therefore a^m a^{k+1} = a^m(a^k a) = (a^m a^k)a = a^{m+k}a(hypothesis)$

$= a^{m+k+1}(by\ definition)$.

Thus it 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.

Proof of (ii) is left to the reader.

Solved Problems

Problem 1. 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 x x = x e. Hence by cancellation law x = e.

Note. 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 2. In an abelian group $(ab)^2 = a^2b^2$.

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

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

Problem 3. Let G be a group such that $a^2 = e$ for all $a \in G$. Then G is abelian.

Solution. $a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$.

Now, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Hence G is abelian.

Problem 4. Let G be a group in which $(ab)^m = a^mb^m$ for three consecutive integers and for all $a, b \in G$. Then G is abelian.

Solution. Let $a, b \in G$.

Let $(ab)^m = a^mb^m$; $(ab)^{m+1} = a^{m+1}b^{m+1}$ and $(ab)^{m+2} = a^{m+2}b^{m+2}$.

Now, $(ab)^{m+1} = a^{m+1}b^{m+1} \Rightarrow (ab)^m(ab) = (a^ma)(bb^m)$

$$\Rightarrow (a^mb^m)(ab) = (a^ma)(bb^m)$$

$$\Rightarrow b^ma = ab^m (by\ cancellation\ law) \quad \ldots(1)$$

Similarly $(ab)^{m+2} = a^{m+2}b^{m+2} \Rightarrow b^{m+1}a = ab^{m+1}$

$$\Rightarrow b^mba = ab^mb$$

$$\Rightarrow b^mba = b^mab (by (1))$$

$$\Rightarrow ba = ab (by\ cancellation\ law)$$

Thus G is abelian.

Problem 5. Let $(H,\cdot)$ and $(K,*)$ be groups. We define a binary operation □ on $(H \times K)$ by $(h_1, k_1)\square(h_2, k_2) = (h_1h_2, k_1 * k_2)$. Then $H \times K$ is a group.

Note. $H \times K$ is called the *direct product* of H and K.

Solution. First we shall prove that □ is associative.

Let $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$.

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

Hence □ is associative.

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.

Exercises

1. Prove that if (H) and (K) are abelian groups, then $(H \times K)$ is also an abelian group.
2. Show that in a group $a^{-1} = b^{-1} \Rightarrow a = b$.

3.4. Permutation Groups

In example 9 of 3.1 we have seen that the set of all bijections B(A) from A to itself is a group under the composition of functions. In this section we make a detailed study of this group when A is finite.

Definition. 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 →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 upper row.

Note. $\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} = \begin{pmatrix}4 & 3 & 1 & 2\\ 3 & 4 & 2 & 1\end{pmatrix}$

Hence any rearrangement of columns in a permutation is immaterial.

Definition. Let A be a finite set containing 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. 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.

	1	2	3			
p_1:	↓	↓	↓	1	2	3
	2	3	1	Hence p_1p_2:	↓	↓
p_2:	↓	↓	↓		1	2
	1	2	3			

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 the other products and the 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:

Remarks.

1. In section 2.4 we have defined the composition fg of two functions f and g by $(g \circ f)(x) = g[f(x)]$.

Hence to find the image of any element x under $g \circ f$, we first apply f and then g.

However in forming the product of two permutations p_1 and p_2 we adopt a different convention. To find the image of x under the product p_1p_2, we first apply p_1 and then p_2.

2. 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

$$p^{-1} = \begin{pmatrix} 3 & 4 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

3. 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.

4. The symmetric group S_n contains ! elements, for, let $A = (1,2, \dots, n)$. 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 Λ is $n(n-1) \dots \dots 2.1 = n!$ so that the number of elements in S_n is $n!$.

Definition. 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 $\circ(G)$.

Exercises

1. Compute $\alpha\beta, \beta\alpha$ and α^{-1} if

(a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$; $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(b) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$; $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$

(c) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 7 & 2 & 5 & 6 & 1 \end{pmatrix}$; $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$.

In this permutation $1 \to 2 \to 3 \to 4 \to 5 \to 1$. Thus the permutation maps the symbols in a cyclic order. Now consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$. This permutation fixes the symbol 1 and maps the remaining symbols in a cyclic order.

Definition. Let p be a permutation on $A = \{1,2, \dots, n\}$. p is called a **cycle of length r** if there exist distinct symbols $a_1, a_2 \dots \dots, a_r$ such that
$p(a_1) = a_2, p(a_2) = a_3, \dots, p(a_{r-1}) = a_r$, and $p(a_r) = a_1$, and $p(b) = b$, for all $b \in A - \{a_1, a_2 \dots, a_r\}$.
This cycle is represented by the symbol $(a_1, a_2 \dots \dots a_r)$. Thus under the cycle ($a_1, a_2 \dots a_r$) 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. Let $A = \{1,2,3,4,5\}$. Consider the cycle of length 4 given by $p = (2451)$.

Then $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$
Obviously $(2451) = (4512) = (5124) = (1245)$.

Note. 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

$$p_1p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} \text{ which is not a cycle.}$$

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

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

Note. 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. Consider the permutation $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 2 & 1 & 3 & 5 & 6 & 7 & 4\end{pmatrix}$.

Now 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 (12). 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 (4567). 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 (45). Each element of the set $\{1,2, \dots, \dots, 7\}$ occurs in one of these 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 3.10. Any permutation can be expressed as a product of disjoint cycles.

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

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

Exercise. Express the following permutations as a product of disjoint cycles.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

(c) $(1234)(345)$

(d) $(13)(34)(45)$

(e) $(123)(16543)$

(f) $(4215)(3426)(5671)$

(g) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}$

(h) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 7 & 2 & 1 & 6 \end{pmatrix}$

Answers.

(a) (14) (35) (b) (135) (24)

(c) $(124)(35)$ (d)(1543)

(e) $(12)(3654)$ (f) $(16347)(25)$

(g) (134256) (h) (152476).

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

Definition. A cycle of length two is called a transposition. Thus a transposition (a_1a_2) interchanges the symbols a_1 and a_2 and leaves all the other elements fixed.

Theorem 3.11. Any permutation can be expressed as a product of transpositions.

Proof. Since any permutation is a product of disjoint cycles it is enough if we prove that each cycle is a product of transpositions. Hence let $c = (a_1a_2 \dots a_1)$ be a cycle.

Clearly $(a_1a_2 \dots a_1) = (a_1a_2)(a_1a_3) \dots \dots (a_1a_r)$. This proves the theorem.

Examples

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1245) = (12)(14)(15).$

Also $(1245) = (2451) = (24)(25)(21).$

Thus the representation of a permutation as a product of transpositions is not

unique.

2. $(1345)(26) = (13)(14)(15)(26) = (13)(12)(12)(14)(15)(26).$

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 3.12. 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 $p = t_1 t_2 \dots \dots t_r = t_1' t_2' \dots \dots t_s'$ where t_i, t_i' are transpositions. Now consider the polynomial in n variables $x_1, x_2, \dots \dots x_n$ given by

$$\begin{aligned} \Delta = & (x_1 - x_2)(x_1 - x_3) \dots \dots \dots (x_1 - x_n) \\ & \times (x_2 - x_3)(x_2 - x_4) \dots \dots \dots (x_2 - x_n) \\ & \dots \dots \dots \dots \dots \dots \dots \\ & \dots \dots \dots \dots \dots \dots \\ & \times (x_{n-1} - x_n) = \prod_{i<j} (x_i - x_j) \end{aligned}$$

For any permutation $p \in S_n$ we define

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

Consider the transposition $t = (ij)$. Then the factor $x_i - x_j$ in Δ becomes $x_j - x_i$. Any factor ($x_k - x_l$) of Δ in which neither i nor j is equal to k or l is unchanged. All other factors of Δ 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 Δ is just to change the sign of Δ ie, $t(\Delta) = -\Delta$.

$\therefore\ p(\Delta) = (t_1 t_2 \dots \dots t_r)(\Delta) = (-1)^r \Delta$.

Also $p(\Delta) = \left(t_1' t_2' \dots \dots t_s'\right)(\Delta) = (-1)^s \Delta$.

$\therefore\ (-1)^r = (-1)^s \Rightarrow r$ and s are both even or both odd.

Definition. 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. Consider the permutation

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

$$p = (134)(26)(57) = (13)(14)(26)(57)$$

$\therefore\ p$ is a product of 4 transpositions.

Hence p is an even permutation.

2. 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 transpositions.

Hence p is an odd permutation.

Exercises

1. Determine which of the following permutations are odd and which of them are even.

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

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

(c) $(1234)(356)(67)$

(d) (123) (45) (5672).

2. Find all the even permutations in S_3 and show that they form a group.

3. For what values of m is a cycle of length m an even permutation?

Answers.

(i) (a) even (b) odd (c) even (d) even

(ii) e, p_1, p_2

(iii) m is odd.

Theorem 3.13.

(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 transpositions, then $p_1 p_2$ is a product of $r + s$ transpositions. Hence (i), (ii) and (iii) follow.

Now suppose that a permutation p is a product of r transpositions, say, $p = t_1, t_2 \dots t_r$. Then

$$\begin{aligned} p^{-1} &= (t_1, t_2 \dots t_r)^{-1} \\ &= t_r^{-1} \dots \dots \dots t_2^{-1} t_1^{-1} = t_r \dots t_2 t_1 \end{aligned}$$

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 3.14. 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 3.13 we see that A_n is a group.

Now let B_n be the set of all odd permutations in S_n.

Define $f: A_n \to B_n$ by $f(p) = (12)p$

f is $1-1$, for $f(p_1) = f(p_2) \Rightarrow (12)\,p_1 = (12)p_2 \Rightarrow p_1 = p_2$.

f is onto, for, if $\alpha \in B_n$ then $(12)\,\alpha \in A_n$ and $f[(12)\alpha] = (12)(12)\alpha = \alpha$.

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

Exercises

1. Let G be a group of permutations. Show that either all the permutations in G are even or exactly half of them are even.
2. Let p be a permutation of a set A. Let $a \in A$ we say that p moves a if $p(a) \neq a$. How many elements are moved by a cycle of length ?
3. Show that the set of all permutations in S_n fixing the symbol 1 is a group.
4. Write down all the permutations of the set $\{1,2,3,4\}$ and determine which of them are even.
5. Determine which of the following statements are true and which of them are false.

(a) Every cycle is a permutation.

(b) Every permutation is a cycle.

(c) Product of two cycles is a cycle.

(d) Any transposition is an odd permutation.

(e) When $n \geq 3, S_n$ is nonabelian.

(f) Any permutation can be expressed as a product of cycles.

(g) The set of all odd permutations in S_n is a group.

(h) Any finite group is abelian.

Answers.

1. r elements

2. (a) True (b) False (c) False (d) True
(e) True (f) True. (g) False s (h) False.

3.5. Subgroups

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

Examples

1. (Z, +) is a group. The set E of all even integers is closed under + and further ($\boldsymbol{E}$, +) is itself a group.
2. 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 $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. H is subset of G. Also H itself is a group under matrix multiplication.

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

Examples.

1. Let G be any group. Then $\{e\}$ and G are subgroups of G. They are called improper subgroups of G.
2. (**Q**, +) is a subgroup of (**R**, +) ad (**R**, +) is a subgroup of (C, +).
3. In $(\mathbf{Z}_8, \oplus)$, let $H_1 = \{0,4\}$ and $H_2 = \{0,2,4,6\}$. The Cayley tabels 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 $\boldsymbol{Z}_8$.

4. $\{1, -1\}$ is a subgroup of $(R^*,\cdot)$.

5. $\{1,i, -1, -i\}$ is a subgroup of $(C^*,\cdot)$.

6. 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.

7. A_n is a subgroup of S_n (by theorem 3.14).

9. The set of permutations $\{e, p_1, p_2, p_3\}$ 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.

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

Theorem 3.15. 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 ϵ 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 identities of G and H respectively.

Let aϵ H. Now,

$e'a = a$(since e' is the identity of H)
$= ea$(since e is the identity of
G and $a \in G$)

$\therefore\ e'a = ea.$
$\therefore\ e' = e$(*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 3.16. A subset H of a group G is a subgroup of G iff
(i) it is closed under the binaty 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 a subgroup of G. The result follows immediately from theorem 3.15.

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

Therefore H is a subgroup of G.
Theorem 3.17.

A non-empty subset H of a group G is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

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 let H be a non-empty subset of G such that $a, b \in H \Rightarrow ab^{-1} \in H$.

Since $H \neq \Phi$, there exists an element $a \in H$.
Hence $aa^{-1} \in H$. Thus $e \in H$
Also since $e, a \in H, ea^{-1} \in H$. Hence $a^{-1} \in H$.
Now, let $a, b \in H$. Then $a, b^{-1} \in H$
Hence $a(b^{-1})^{-1} = ab \in H$. Thus H is closed under the binary operation in G.

Hence by theorem 3.16 H is a subgroup of G.

Note. If the operation is + then H is a subgroup of G iff $a, b \in H \Rightarrow a - b \in H$.

Theorem 3.18. Let H be a non-empty finite subset of G. If H is closed under the operation in G then H is a subgroup of G.

Proof. Let $a \in H$.

Since H is closed $a, a^2, a^3, \ldots \ldots, a^n$ ... are all elements of H. But since H is finite the elements $a, a^2, a^3, \ldots \ldots$ 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.

Note. The above theorem is not true if H is infinite. For example, **N** is an infinite subset of $(\mathbf{Z}, +)$ and **N** is closed under addition. However N is not a subgroup of ($Z, +$).

Theorem 3.19. If H and K are subgroups of a group G then is $H \cap K$ is also a subgroup of G.

Proof. Clearly e ϵ H∩K and hence H∩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 3.17, $H \cap K$ is a subgroup of G.

Note.

1. It can be similarly proved that the intersection of any number of subgroups of G is again a subgroup of G.
2. The union of two subgroups of a group need not be a subgroup.

For example, 2**Z** and 3**Z** are subgroups of (Z, +) but 2Z ∪ 3Z is not a subgroup of **Z** since $3,2 \in 2\mathbf{Z} \cup 3\mathbf{Z}$ but $3 + 2 = 5 \notin 2Z \cup 3Z$.

Theorem 3.20. The union of two subgroups of a group G is a subgroup iff one is contained in the other.

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

Suppose that H is not contained in K and K is not contained in H. Then there exist elements a, b such that

$$a \in H \quad \text{and} \quad a \notin K \ldots\ldots\ldots\ldots\ldots (1)$$
$$b \in K \quad \text{and} \quad b \notin H \ldots\ldots\ldots\ldots\ldots (2)$$

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 $ab \in K$.

Case (i) Let $ab \in H$. since $a \in H, a^{-1} \in H$.

Hence $a^{-1}(ab) = b \in H$ which is a contradiction to (2).

Case (ii) Let $ab \in K$. Since $b \in K, b^{-1} \in K$.

Hence $(ab)b^{-1} = a \in K$ which is a contradiction to (1).

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

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

Example.

In S_3, consider $A = \{e, p_3\}$ and $B = \{e, p_4\}$. Clearly A and B are subgroups of S_3.

$$\text{Also } AB = \{ee, ep_4, ep_3, p_3p_4\} = \{e, p_4, p_3, p_2\}$$

Now, $p_4p_2 = p_5 \notin AB$.

Hence AB is not a subgroup of S_3.

Theorem 3.21. Let A and B be two subgroups of a group G. Then AB is a subgroup of G iff $AB = BA$.

Proof. Let AB be a subgroup of G.

We claim that $AB = BA$.

Let $x \in AB$. Since AB is a subgroup of G, $x^{-1} \in AB$.

Let $x^{-1} = ab$ where $a \in A$ and $b \in B$.

$$\therefore\ x = (ab)^{-1} = b^{-1}a^{-1}$$

Since A and B are subgroups of $G, a^{-1} \in A$ and $b^{-1} \in B$.

$$\therefore\ x \in BA. \text{ Hence } AB \subseteq BA \ldots\ldots\ldots\ldots (1)$$

Now, let $x \in BA$. Then $x = ba$ where $b \in B$ and $a \in A$.

$$\therefore\ x^{-1} = (ba)^{-1} = a^{-1}b^{-1} \in AB$$

Now, since AB is a subgroup and $x^{-1} \in AB$, we have $x \in AB$,

$$\therefore\ BA \subseteq AB \ldots\ldots\ldots\ldots\ldots (2)$$

From (1) and (2) we get $AB = BA$.

Conversely, let $AB = BA$. We claim that AB is a subgroup of G. Clearly $e \in AB$ and hence AB is non-empty. Now let $x, y \in AB$. Then $x = a_1b_1$ and $y = a_2b_2$ where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

$$\therefore\ xy^{-1} = (a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}.$$

Now, $b_2^{-1}a_2^{-1} \in BA$. Since $BA = AB$, $b_2^{-1}a_2^{-1} \in AB$

$\therefore\ b_2^{-1}a_2^{-1} = a_3b_3$ where $a_3 \in A$ and $b_3 \in B$. $\therefore\ xy^{-1} = a_1b_1a_3b_3$.

Now $b_1a_3 \in BA$. Since $BA = AB, b_1a_3 \in AB$.

$\therefore\ b_1a_3 = a_4b_4$ where $a_4 \in A$ and $b_4 \in B$.

$\therefore\ xy^{-1} = a_1(a_4b_4)b_3 = (a_1a_4)(b_4b_3) \in AB$.

$\therefore\ AB$ is a subgroup of G.

Corollary. 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, $ab = ba$.

$\therefore\ x \in BA$. Hence $AB \subseteq BA$.

Similarly $BA \subseteq AB$.

$\therefore\ AB = BA$.

Hence AB is a subgroup of G.

Solved problems

Problem 1. Let $a \in \mathbf{R}^*$. Let $H = \{a^n / n \in \mathbf{Z}\}$. Then H is a subgroup of $\mathbf{R}^*$.

Solution. Clearly H is non-empty.

Now, let $x, y \in H$.

Then $x = a^s$ and $y = a^t$ where $s, t \in \mathbf{Z}$.

$\therefore\ xy^{-1} = a^s(a^t)^{-1} = a^{s-t} \in H.$

Hence H is a subgroup of $\mathbf{R}^*$.

Problem 2. 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 hence 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 the symbol 1 . Hence $\alpha\beta^{-1} \in H$.

Thus H is a subgroup of S_n.

Problem 3. Let G be the set of all 2×2 matrices with entries from $\mathbf{R}$. Then G is a group under matrix addition.

Let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \, a, b \in \mathbf{R} \right\}$. 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 4. Let G be a group.

Let $H = \{a / a \in G$ and $ax = xa$ for all $x \in G\}$.

(i.e) 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

$\Longrightarrow b^{-1}(bx)b^{-1} = (xb)b^{-1}$

$(b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1})$

$exb^{-1} = b^{-1}xe$

$\Longrightarrow xb^{-1} = b^{-1}x$.....(1)

$$\begin{aligned}\therefore\ (ab^{-1})x &= a(b^{-1}x)\\ &= a(xb^{-1}) \text{ (by (1))}\\ &= (ax)b^{-1}\\ &= (xa)b^{-1} \text{ (since } ax = xa)\\ &= x(ab^{-1}).\end{aligned}$$

Thus ab^{-1} commutes with every element of G.

$\therefore\ ab^{-1} \in H$ and hence H is a subgroup of G.

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

Problem 5. Let G be a group and let a be a fixed element of G.

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

(ie) H_a is the set of all elements in G which commute with a.

Show thatH_a is a subgroup of G.

Solution. Clearly $ea = ae = a$.

Hence $e \in H_a$ so that H_a is non-empty.

Now, let $x, y \in H_a$.

Then $ax = xa$ and $ay = ya$.

Now, $ay = ya \Rightarrow y^{-1}a = ay^{-1}$. (as in the pervious problem)

$$\begin{aligned}a(xy^{-1}) &= (ax)\\ &= (xa)y^{-1} \text{ (since } ax = xa)\\ &= x(ay^{-1})\\ &= x(y^{-1}a) \qquad \text{(by (1))}\\ &= (xy^{-1})a.\end{aligned}$$

Hence xy^{-1} commutes with a.

$\therefore\ xy^{-1} \in H_a$ and hence H_a is a subgroup of G.

Note. H_a is called the normaliser of a in G.

Exercises

1. Show that $\{a + bi/a, b \in \mathbf{Z}\}$ is a subgroup of (C, +).
2. Determine which of the following are subgroups of ($\mathbf{C}, +$)

(a) R

(b) $\{a + b\sqrt{-5}/a, b \in \text{N}\}$

(c) $\{z/|z| = a\}$

(d) $\{z/$ real part of z is 0$\}$

(e) $\{1, i, -1, -i\}$.

3. Let G_1 and G_2 be two groups. Let e_1 and e_2 be the identity elements of G_1 and G_2 respectively. Let $G_1 \times G_2$ be the direct product of these groups. Let $H = \{(e_1, y)/y \in G_2\}$ and $K = \{(x, e_2)/x \in G_1\}$. Show that H and K are subgroups of $G_1 \times G_2$.

3.6. Cyclic Groups

Definition. Let G be a group. Let $a \in G$.

Then $H = \{a^n/n \in \mathbf{Z}\}$ 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. In $(Z, +), \langle 2 \rangle = 2Z$ which is the group of even integers.
2. In the group $G = (\mathbf{Z}_{12}, \oplus), \langle 3 \rangle = \{0,3,6,9\}$. $\langle 5 \rangle = \{0,5,10,3,8,1,6,11,4,9,2,7\} = \mathbf{Z}_{12}$.
3. In the group $G = \{1, i - 1, -i\}\langle i \rangle = \{i, i^2, i^3 \ldots\} = \{i, -1, -i, 1\} = G$.

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

Examples

1. ($\mathbf{Z}, +$) is a cyclic group. 1 is a generator of this group. -1 is also a generator of this group. Thus a cyclic group can have more than one generator.
2. ($n\mathbf{Z}, +$) is a cyclic group, n and $-n$ are generators of this group.
3. ($\mathbf{Z}_8, \oplus$) is a cyclic group. 1,3,5,7 are all generators of this group.
4. ($\mathbf{Z}_n, \oplus$) is a cyclic group for all $n \in \mathbf{N}$; 1 is a generator of this group. In fact if $m \in \mathbf{Z}_n$ 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 the group $G = (\mathbf{Z}_7, -\{0\}, \odot)$, 3 and 5 are both generators. Here 2 is not a generator of G since $(2) = \{2,4,1\} \neq G$.

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

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

Exercises

Determine which of the following groups are cyclic. If it is cyclic find all the generators of the group.

1. ($6\mathbf{Z}, +$).
2. (Q, +).
3. The set of all n^{th} roots of unity under multiplication.
4. The group of symmetries of an equilateral triangle.
5. The group of symmetries of a rectangle.
6. The group of symmetries of a square.
7. $\{2^n/\text{n} \in Z\}$ under usual multiplication.
8. ($\mathbf{Z}, \oplus$)
9. ($\mathbf{R}^*, \cdot$)
10. $(Z_{11} - (0), \odot)$
11. $G = (e, p_1, p_2, p_3, p_4)$ where

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$
$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$
$$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$
$$p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \text{ and}$$
$$p_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Answers. 1, 3,7,8,10 and 11 are cyclic.

Theórem 3.22. 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 $r, s \in \mathbf{Z}$.

Hence $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$.

$\therefore$ G is abelian.

Theorem 3.23. 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 a generator of H.

Let $b \in H$. Then $b = a^n$ for some $n \in \mathbf{Z}$.

Let $n = mq + r$ where $0 \leq r < m$.

Then $b = a^n = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$.

$$\therefore\ a^r = (a^m)^{-q} b \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Now, $a^m \in H$. Since H is a subgroup, $(a^m)^{-q} \in H$.

Also $b \in H$.

By (1), $a^r \in II$ and $0 \leq r < m$.

But m is the least positive integer such that $a^n \in H$.

$\therefore$ $r = 0$. Hence $b = a^n = a^{qm} = (a^m)^q$.

$\therefore$ Every element of H is a power of a^m.

$\therefore$ $H = (a^m)$ and hence H is cyclic

Exercises

1. Prove that if a is a generator of a cyclic group G then a^{-1} is also a generator of G.
2. Prove that any subgroup of $(\mathbf{Z}, +)$ is of the form $n\mathbf{Z}$ for some integer n.

3. Find the number of elements in the following cyclic subgroups.

(a) $\langle 2 \rangle$ in $(\mathbf{Z}_{18}, \oplus)$

(b) (18) in $(\mathbf{Z}_{30}, \oplus)$

(c) $\langle 5 \rangle$ in $(\mathbf{Z}_{80}, \oplus)$

(d) $\langle i \rangle$ in $\mathbf{C}^*$

4. Show that every proper subgroup of V_4 is cyclic. (However V_4 is not cyclic).

UNIT II

3.7. Order of an Element

1. Consider the group S_3 given in 3.4

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$p_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_2.$$

$$p_1^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

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

In this case 3 is the least positive integer such that $p_1^3 = e$. Also $\langle p_1 \rangle = \{e, p_1, p_2\}$ is a subgroup of S_3 of order 3.

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

Definition. 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.

Note.

1. In example 1, p_1 is of order 3 and 2 is of infinite order in example 2.
2. In $(\mathbf{C}^*, \cdot)$, i is an element of order 4.

Exercises

1. Show that in any group G, e is the only element of order 1.
2. Find the order of -1 and 3 in $(Z, +)$.
3. Find the order of -1 and 3 in $(\mathbf{R}^*, \cdot)$.
4. Find the order of -1 and $-i$ in $(\mathbf{C}^*, \cdot)$.
5. zFind the order of 2 and 3 in $(\mathbf{Z}_8, \oplus)$.
6. Show that in V_4 the order of every element other than the identity is 2 .
7. Show that in $(\mathbf{Z}, +)$ the order of every element other than 0 is infinite.
8. Show that in $(\wp(S), \Delta)$ the order of every element other than Φ is 2 .
9. Show that in $(\mathbf{C}^*, \cdot)$ for every positive integer n there exists an element of order n.

Answers.

2. Infinite
3. Order of -1 is 2 and order of 3 is infinite
4. Order of -1 is 2 and Order of –i is 4
5. Order of 2 is 4 and Order of 3 is 8

Theorem 3.24. 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 $\langle a \rangle = \{e, a, a^2, \ldots, 2^{n-1}\}$ which is of order n.

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

Theorem 3.25. 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. The converse of the above theorem is not true. (ie) if G is a group in which every element is of finite order then the group G need not be finite.

Example. If S is any infinite set, then $(\wp(S), \Delta)$ is an infinite group. In this group $A \Delta A = \Phi$ for every $A \in \rho(S)$ so that the order of every element other than Φ is 2 .

Theorem 3.26. Let G be a group and a be an element of order n in G. Then $a^m = e$ iff n divides m.

Proof. Suppose $n \mid m$. Then $m = nq$ where $q \in \mathbf{Z}$.

$$\therefore\ a^m = a^{nq} = (a^n)^q = e^q = e.$$

Conversely, let $a^m = e$.

Let $m = nq + r$ where $0 \leq r < n$.

$\therefore\ a^m = a^{nq+r} = a^{nq}a^r = ea^r = a^r$.

$\therefore\ a^r = e$ and $0 \leq r < n$.

Now, since n is the smallest positive integer such that $a^n = e$, we have $r = 0$. Hence $m = nq$.

Therefore $n \mid m$.

Theorem 3.27. 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 $a^n = e$.

$\therefore\ (a^{-1})^n = (a^n)^{-1} = e^{-1} = e$.

Now, if possible let $0 < m < n$ and $(a^{-1})^m = e$.

$\therefore\ (a^m)^{-1} = e$. Hence $a^m = e$ which contradicts the definition of the order of a. Thus n is the least positive integer such that $(a^{-1})^n = e$.

$\therefore$ The order of a^{-1} is n.

(ii) We shall first prove that for any positive integer r.

$$(b^{-1}ab)^r = b^{-1}a^r b \ldots\ldots\ldots\ldots\ldots (1)$$

(1) is trivialy true if $r = 1$,

Now, suppose that (1) is true for $r = k$ so that $(b^{-1}ab)^k = b^{-1}a^k b$.

Then

$$\begin{aligned}(b^{-1}ab)^{k+1} &= (b^{-1}ab)^k (b^{-1}ab).\\ &= (b^{-1}a^k b)(b^{-1}ab).\\ &= b^{-1}a^{k+1}b.\end{aligned}$$

Hence by induction (1) is true for all positive integers.

Now, let a be an element of order n. Then $a^n = e$.

$$\begin{aligned}\therefore\ (b^{-1}ab)^n &= b^{-1}a^n b \text{ (by (1))}\\ &= b^{-1}eb = e\end{aligned}$$

Now, if possible, let $0 < m < n$ and $(b^{-1}ab)^m = e$.

$\therefore b^{-1}a^m b = e$. Hence $a^m = e$ 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)

$$order\ of\ \ ab = \text{ the order of } a^{-1}(ab)a \text{ (by (ii))}$$
$$= \text{ the order of } ba.$$

Theorem 3.28. 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 $n \mid sm$.

$\therefore\ kd \mid ldm$. Hence $k \mid lm$

But k and l are relatively prime.

Hence k/m so that $m \geq k$.

Thus k is the least positive integer such that $(a^s)^k = e$.

$\therefore$ order of $a^s = k = n/d$.

Corollary 1. The order of any power of a cannot exceed the order of a.

Corollary 2. 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 3. Let G be a finite cyclic group of order n generated by an element a. a^s is a generator of G iff 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.

Example. Consider the group ($\mathbf{Z}_{12}$,$\oplus$).

$\phi(12) = 4$. Hence the group has exactly 4 generators and they are 1,5,7 and 11 .

Solved Problems

Problem 1. If G is a finite group with even number of elements then G contains at least one element of order 2.

Solution. 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 $S = \{a/a \in G, a \neq a^{-1}\}$.

Clearly $a \in S \Rightarrow a^{-1} \in S$ 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 $a \notin S \cup \{e\}$. Clearly $a = a^{-1}$.

Problem 2. The order of a permutation p is the l.c.m. of the lengths if its disjoint cycles.

Solution. Let $p = c_1 c_2 \ldots, c_r$ 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, $e = p^m = (c_1 c_2 \ldots c_r)^m = {c_1}^m c_2^m \ldots c_r^m$.

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, $c_1^m = c \Rightarrow l_1 \mid m$ 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 $l_1, l_2, \ldots, l_r$.

$\therefore$ 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 3. 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 $a^m = a^n \Rightarrow a^{m-n} = e$.

$\therefore$ Order of a is finite.

$\therefore$ $G = \langle a \rangle$ is a finite group (by theorem 3.24)

Exercises

1. Show that a group G of order n is cyclic iff G contains an element of order n.
2. Find the number of generators of the cyclic groups of orders 8,24 and 60.
3. Let p and q be prime numbers. Find the number of generators of Z_{pq}.
4. Find the number of generators of Z_p, where p is prime.

5. Find two elements a, b in a group such that

(a) order of $ab \neq$ (order of a) (order of b).

(b) order of $ab =$ (order of a) (order of b).

6. Find the order of the following permutations.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

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

(c) $(12345)(67)(1657)$

(d) (12) (23) (345) (1456).

Answers.

2. 4 ,8 and 16

6. (a) 4 (b) 4 (c) 7 (d) 6

3.8. Cosets and Lagrange's Theorem

Definition. Let H be a subgroup of a group G. Let $a \in G$. Then the set $aH = \{ah/h \in H\}$ is called the left coset of H defined by a in G.

Similarly $Ha = (ha/h \in H)$ is called the right coset of H defined by a.

Examples.

1. Let us determine the left cosets of ($\mathbf{5Z}, +$) in $(\mathbf{Z}, +)$. Here the operation is + .

$0 + 5\mathrm{Z} = 5\mathrm{Z}$ is itself a left coset.

Another left coset is $1 + 5Z = \{1 + 5n/n \in \mathrm{Z}\}$. We notice that this left coset contains all integers having remainder 1 when divided by 5 .

Similarly

$$2 + 5\mathbf{Z} = \{2 + 5n/n \in \mathbf{Z}\}$$
$$3 + 5\mathbf{Z} = \{3 + 5n/n \in \mathbf{Z}\}.$$
$$\text{and } 4 + 5\mathbf{Z} = \{4 + 5n/n \in \mathbf{Z}\}.$$

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

2. Consider $(\mathbf{Z}_{12},\oplus)$. Then $H = \{0,4,8\}$ is a subgroup of G.

The left cosets of H are given by

$$0 + H = \{0,4,8\} = H$$
$$1 + H = \{1,5,9\}$$
$$2 + H = \{2,6,10\}$$
$$\text{and } 3 + H = \{3,7,11\}$$

We notice that

$$4 + H = \{4,8,0\} = H. \text{ and}$$
$$5 + H = \{5,9,1\} = 1 + H \text{ etc.}$$

Exercises.

1. Find all the left cosets of $(n\mathbf{Z}, +)$ in $(\mathbf{Z}, +)$.
2. Find all the left cosets of $\{0,3,6,9\}$ in $(\mathbf{Z}_{12},\oplus)$.
3. Find all the left cosets of $\{1,6\}$ in $(\mathbf{Z}_7 - \{0\},\odot)$.

Theorem 3.29. Let G be a group and l 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 $a = ae \in aH$.

$\therefore\ a \in H$.

(ii) Let $aH = bH$.

$\therefore\ a^{-1}(aH) = a^{-1}(bH)$.

$\therefore\ H = (a^{-1}b)H$.

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

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

Then $a^{-1}bH = H$ (by).

$\therefore\ aa^{-1}bH = aH$ and hence $bH = aH$.

(iii) Let $a \in bH$. Then $a = bh$ for some $h \in H$.

$\therefore\ a^{-1} = (bh)^{-1} = h^{-1}b^{-1} \in Hb^{-1}$.

Converse can be similarly 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 $h_2 \in H$

$\therefore\ x = (bh_2)h_1) = b(h_2h_1) \in bH$.

$\therefore\ aH \subseteq bH$.

Now, let $x \in bH$. Then $x = bh_3$ for some $h_3 \in H$.

Also from (1), $b = ah_2^{-1}$.

$\therefore\ x = ah_2^{-1}h_3 \in aH$.

$\therefore\ bH \subseteq aH$. Hence $aH = bH$.

Conversely, let $aH = bH$.

Then $a = ae \in aH$.

$\therefore\ a \in bH$.

Theorem 3.30. 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, $aH \cap bH \neq \Phi$.

$\therefore$ There exists an element $c \in aH \cap bH$.

$\therefore\ c \in aH$ and $c \in bH$.

$\therefore\ aH = cH$ and $bH = cH$ (by (iv) of Theorem 3.29).

$\therefore\ aH = bH.$

(ii) Let $a \in G$. Then $a = ae \in aH$.

$\therefore$ Every element of G belongs to a left coset of H.

$\therefore$ The union of all the left cosets of H is G.

(iii) 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.

Note 1. This theorem shows that the collection of all left cosets forms a partition of the group.

Note 2. The above result is true if we replace left cosets by right cosets. In what follows, the results we prove for left cosets are also true for right cosets.

Remark. 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, $a^{-1}a = e \in H$. Hence $a \sim a$.

Hence $\sim$ is reflexive.

$$a \sim b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H.$$
$$\Rightarrow b^{-1}a \in H \Rightarrow b \sim a.$$

$\therefore\ a \sim b \Rightarrow b \sim a.$

Hence $\sim$ 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.

Thus $\sim$ 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. This gives another proof of Theorem 3.30.

Theorem 3.31. 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 $f(aH) = Ha^{-1}$.

To prove f is well defined.

Now $aH = bH. \Rightarrow a^{-1}b \in H$

$\Rightarrow a^{-1} \in Hb^{-1}$

$\Rightarrow Ha^{-1} = Hb^{-1}$

Therefore f is well defined.

To prove f is $1-1$.

Now

$f(aH) = f(bH)$

$\Rightarrow Ha^{-1} = Hb^{-1}$

$\Rightarrow a^{-1} \in Hb^{-1}$

$\Rightarrow a^{-1} = hb^{-1}$ for some $h \in H$.

$\Rightarrow a = bh^{-1}$

$\Rightarrow a \in bH$

$\Rightarrow aH = bH$.

Therefore f is 1-1

To prove f is onto.

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. 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. In $(\mathbf{Z}_8, \oplus)$, $H = \{0,4\}$ 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 $[\mathbf{Z}_8 : H] \times |H| = 4 \times 2 = 8 = |\mathbf{Z}_8|$.

Exercises

1. Find the index of $(nZ, +)$ in $(Z, +)$.
2. Find the index of $(8Z, +)$ in $(2Z, +)$.
3. Find the index of $\{0,3,6,9\}$ in $(Z_{12}, \oplus)$.
4. Find the index of $\{1,6\}$in$(Z_7 - \{0\}, \odot)$
5. Determine which of the following statements are true and which are false

Let G be a group and H a subgroup of G, Then

(a) H itself is a left coset of H.

(b) The identity element belongs to every left coset of H.

(c) Every element of H belongs to at least one left coset of H.

(d) Every element of H belongs to exactly one left coset of H.

(e) The number of left cosets of H is the same as the number of right cosets of H.

(f) If $b \in Ha$ then $Ha = Hb$.

(g) If $c \in Ha \cap Hb$ then $Ha = Hb = Hc$.

(h) $a \in H$ if and only if $aH = H$.

Answers.

5. (a) T (b) F (c) T (d) T

(e) T (f) T (g) T (h) T

Theorem 3.32. (Lagrange's theorem) Let G be a finite group of order n and H be any 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 3.30, these r left cosets are mutually disjoint, they have the same number of elements namely m and their union is G.

$\therefore\ n = rm$. Hence m divides n.

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

Note 1. Lagrange's theorem has many important applications in group theory.

Example. A group G of order 8 cannot have subgroups of order 3,5,6 or 7 . In fact any proper subgroup of G must be of order 2 or 4 .

Note 2. Any group of prime order has no proper subgroups.

Note 3. The converse of Lagrange's theorem is false. (i.e) If G is a group of order n and m divides n, then G need not have a subgroup of order m.

Example.1 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.

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.

Exercises.

1. Can a group of order 12 contain a subgroup of order 8?
2. Show that the converse of Lagrange's theorem is true in V_4.
3. Show that the converse of Lagrange's theorem is true in any finite cyclic group.

Theorem 3.33. 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 the cyclic group $\langle a \rangle$.

Now, by Lagrange's theorem the order of the subgroup $\langle a \rangle$ divides the order of G. Hence $m \mid n$.

Theorem 3.34. 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 Theorem 3.33 order of a divides p.

$\therefore$ 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 3.35. Let G be a group of order n. Let $a \in G$ then $a^n = c$.

Proof. Let the order of a be m. Then m divides n.

Hence $n = mq$.

$\therefore\ a^n = a^{mq} = (a^m)^q = c^q = c$.

Theorem 3.36 (Euler's theorem) If n is any integer and $(a, n) = 1$ then $a^{\phi(n)} \equiv 1(\mathrm{mod} n)$.

((n) is the number of positive integers less than n relatively prime to n)

Proof. Let $G = \{m/m < n$ 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 $a \equiv r(\mathrm{mod} n)$.

Since $(a, n) = 1$ we have $(n, r) = 1$ so that $r \in G$.

$\therefore\ r^{\phi(n)} = 1$ (by Theorem 3.35).

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

Also $a^{\phi(n)} \equiv r^{\phi(n)}(\mathrm{mod} n)$ so that

$a^{\phi(n)} \equiv 1(\mathrm{mod} n)$ (since ' $\equiv$ ' is transitive).

Theorem 3.37 (Fermat's theorem) Let p be a prime number and a be any integer relatively prime to p. Then $a^{p-1} \equiv 1(\mathrm{mod} p)$.

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

Theorem 3.38. A group G has no proper subgroups if it is a cyclic group of prime order.

Proof. Suppose G is a group of prime order. Then it follows from Lagrange's theorem that 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 $\langle a^p \rangle$ is a subgroup of order q and hence is a proper subgroup of G which is a contradiction.

Hence n is prime.

$\therefore$ G is a cyclic group of prime order.

Solved problems

Problem 1. 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. $[G:A] = \frac{|G|}{|A|}$ (by Lagrange's theorem)

$$[G:B] = \frac{|G|}{|B|}$$

$$\text{and } [B:A] = \frac{|B|}{|A|}$$

$$\therefore \ [G:B][B:A] = \frac{|G|}{|B|}\frac{|B|}{|A|} = \frac{|G|}{|A|} = [G:A].$$

Problem 2. 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.

$\therefore$ By Lagrange's theorem, $|A \cap B|$ divides $|A|$ and $|B|$. But by hypothesis $|A|$ and $|B|$ have no common divisors.

$\therefore$ $|A \cap B| = 1$. Hence $A \cap B = \{e\}$.

Problem 3. Let H and K be two subgroups of G of finite index in G. Prove that $H \cap K$ is a subgroup of finite index in G.

Solution. By theorem 3.19 $H \cap K$ is a subgroup of G.

Let $[G:H] = m$ and $[G:K] = n$.

We claim that for any $a \in G, (H \cap K)a = Ha \cap Ka$

Clearly, $H \cap K \subseteq H$ and K

$(H \cap K)a \subseteq Ha$ and Ka.

$(H \cap K)a \subseteq Ha \cap Ka$ ... ... (1)

Now, let $x \in Ha \cap Ka$. Then $x \in Ha$ and $x \in Ka$

$\Rightarrow x = ha$ for some $h \in H$ and $x = ka$ for some $k \in K$.

$\therefore ha = ka \Rightarrow h = k \Rightarrow h \in H \cap K \Rightarrow x \in (H \cap K)a.$

$\therefore Ha \cap Ka \subseteq (H \cap K)a$.....(2)

From (1) and (2) we have

$(H \cap K)a = Ha \cap Ka.$

Every right coset of $H \cap K$ in G is the intersection of a right coset of H and a right coset of K.

Also since $[G:H] = m$, the number of right cosets of H in G is m.

Similarly the number of right cosets of K in G isn. Hence the number of right cosets of $H \cap K$ in G is at most mn.

$\therefore [G:H \cap K] \leq mn.$

$\therefore H \cap K$ is a subgroup of finite index in G.

Problem 4. Let H and K be two finite subgroups of a group G. Then

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

Proof. Let $L = H \cap K$. Since H and K are subgroups of G, L is also a subgroup of G and $L \subseteq H$ and $L \subseteq K$.

Now, let $Lx_1, Lx_2, \ldots, Lx_m$ be the distinct right cosets of L in K so that

$K = Lx_1 \cup Lx_2 \cup \cdots \cup Lx_m$.....(1)

$m = [K:L] = \frac{|K|}{|L|} = \frac{|K|}{|H \cap K|}$.....(2)

From (1)

$$HK = H(Lx_1) \cup H(Lx_2) \cup \cdots \cup H(Lx_m)$$
$$= HLx_1 \cup HLx_2 \cup \cdots \cup HLx_m \quad (\text{since } L \subseteq H).....(3)$$

We claim that the cosets $Hx_1, Hx_2, \ldots, Hx_m$ are distinct.

Suppose $Hx_i = Hx_j$.

$\Rightarrow x_i x_j^{-1} \in H.$

Also $x_i, x_j \in K$ and hence $x_i x_j^{-1} \in K$.

$\Rightarrow x_i x_j^{-1} \in H \cap K = L.$

$\Rightarrow Lx_i = Lx_j$ which is a contradiction since the cosets $Lx_1, Lx_2, \ldots, Lx_m$ are distinct.

Thus, from (3) we have:

$|HK| = |Hx_1| + |Hx_2| + \cdots + |Hx_m| = m|H|$

$$= \frac{|K|}{|H \cap K|}|H| \quad (by(2))$$

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

Problem 5. 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 $H \cap K = e$. $|H \cap K| = 1$.

$|HK| = \frac{|H||K|}{|H \cap K|} = |H||K|$ (by Problem 4)

$> \sqrt{|G|}, \sqrt{|G|} = |G|$.

$\therefore |HK| > |G|$ which is a contradiction

$\therefore H \cap K \neq e$.

Exercises

1. Show that any group of order 17 is cyclic.
2. Show that any infinite group has proper subgroups.
3. Prove that in an infinite cyclic group all the subgroups other than ({e}) are infinite.

3.9. Normal Subgroups and Quotient Groups

Definition. A subgroup H of G is called a **normal subgroup** of G if aH=Ha for all aϵ G..

Examples

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 3.39 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 xϵ aH. Then x=ah for some hϵ H (since G is abelian)

$\therefore x \in Ha$. Hence $aH \subseteq Ha$.

Similarly $Ha \subseteq aH$.

$\therefore aH = Ha$ and hence H is a normal subgroup of G.

Examples

(i). $n\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$.

(ii) Every subgroup of $(\mathbb{Z}, \oplus)$ is normal.

(iii) Since any cyclic group is abelian any subgroup of a cyclic group is normal.

Theorem 3.40 Let H be a subgroup of index 2 in a group G. Then H is a normal subgroup of G.

Proof. If aϵ H then H=aH=Ha.

If $a \notin H$, then aH is a left coset different from H. Hence H∩ aH=Φ

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

Theorem 3.41 Let N be a subgroup of G. Then the following are equivalent:

(i) N is a normal subgroup of G.

(ii) $aN = Na$ for all $a \in G$.

(iii) $aNa^{-1} \subseteq N$ for all $a \in G$.

(iv) $aNa^{-1} = N$ for all $a \in N$ and $a \in G$.

Proof. (i) ⇒ (ii)

Suppose N is a normal subgroup of G.

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

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

(ii) ⇒ (iii) and (iii) ⇒ (iv) are obvious.

(iv) ⇒ (i).

Suppose that $aNa^{-1} = N$ for all $n \in N$ and $a \in G$.

We claim that $aN = Na$.

Let $x \in aN$. Then

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

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

$\therefore aN \subseteq Na.$ $\ldots(1)$

Now, let $x \in Na$. Then

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

$x = a(a^{-1}na) \in aN \quad \ldots(2)$

From (1) and (2) we get $aN = Na$.

Hence N is a normal subgroup of G.

Solved Problems

Problem 1 Prove that the intersection of two normal subgroups of a group G is a normal subgroup of G.

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 $axa^{-1} \in K$.

$\therefore axa^{-1} \in H \cap K$).

Hence $H \cap K$ is a normal subgroup of G.

Problem 2 The centre H of a group G is a normal subgroup of G.

Solution. The centre H of G is given by

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

Now let $x \in H$ and $a \in G$. Hence $ax = xa$.

$\therefore axa^{-1} = x \in H$.

Hence H is a normal subgroup of G.

Problem 3 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,

$$\begin{aligned} xy^{-1} &= (ah_1a^{-1})(ah_2a^{-1})^{-1} \\ &= (ah_1a^{-1})(ah_2^{-1}a^{-1}) \\ &= a(h_1h_2^{-1})a^{-1} \in aHa^{-1} \end{aligned}$$

$\therefore aHa^{-1}$ is a subgroup of G.

Problem 4 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 ∈ G. Then by solved problem 3, aHa^{-1} is also a subgroup of G.

We claim that$|H| = |aHa^{-1}| = m$.

Now, consider $f: H \to aHa^{-1}$ defined by $f(h) = aha^{-1}$.

To prove f is 1-1.

$f(h_1) = f(h_2) \Rightarrow ah_1a^{-1} = ah_2a^{-1} \Rightarrow h_1 = h_2$.

Hence f is 1-1.

To prove f is onto

Let $x = aha^{-1} \in aHa^{-1}$.

Then $f(h) = x$. Thus f is a bijection.

$|H| = |aHa^{-1}| = m$.

But H is the only subgroup of G of order m.

$\Rightarrow aHa^{-1} = H$. Hence aH = Ha.

∴ H is a normal subgroup of G.

Problem 5. 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 $axa^{-1} \in H \cap N$.

∴ H ∩ N is a normal subgroup of H.

Example. Give an example to shows that H ∩ 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 6. 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 $n \in N$.

But $hN = Nh$ (since N is normal).

$x \in Nh$. Hence $HN \subseteq NH$.

Similarly $NH \subseteq HN$.

$\therefore$ HN = NH. Hence HN is a subgroup of G.

Problem 7. M and N are normal subgroups of a group G such that M $\cap$ N = {e}. Show that every element of M commutes with every 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 $a \in M$, so that $aba^{-1}b^{-1} \in M$.

Again, since $b \in N$ and N is normal, $aba^{-1} \in N$.

Also $b^{-1} \in N$, so that $aba^{-1}b^{-1} \in N$.

Thus $aba^{-1}b^{-1} \in M \cap N = e$.

$\therefore aba^{-1}b^{-1} = e$, so that ab = ba.

Exercises.

1. If A is normal in G and B a subgroup of G such that $A \subseteq B \subseteq G$, then prove that A is a normal subgroup of B.
2. Show that a subgroup of index 3 need not be normal.

Definition. Let G be a group and N be a subgroup of G. Denote by G/N the set of all right cosets of N in G. Thus G/N={Na: aϵG}

Theorem 3.42. A subgroup N of G is normal iff 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 $NaNb = N(aN)b = N(Na)b$ (since $aN = Na$)

$= NNb = Nab$ (since $NN = N$)

$= Nab$

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.

$\therefore NaNb = Nab$

Now, we prove that N is a normal subgroup of G.

Let $a \in G$ and $n \in N$. Then

$ana^{-1} = eana^{-1} \in NaNa^{-1} = Naa^{-1} = N$.

$\therefore ana^{-1} \in N$.

Hence N is a normal subgroup of G.

Theorem 3.43. 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 theorem 3.42 the operation given by $NaNb = Nab$ is a well-defined binary operation in G/N.

Now, let $Na, Nb, Nc \in G/N$.

Then

$Na(NbNc) = Na(Nbc) = N(ab)c = (NaNb)Nc$.

$\therefore (NaNb)Nc = Na(NbNc)$.

Hence the binary operation is associative.

$Ne = N \in G/N$ and

$NaNe = Nae = Na = NeNa$.

$\therefore Ne$ is the identity element.

Also $NaNa^{-1} = Naa^{-1} = Ne = Na^{-1}Na$.

$\therefore Na^{-1}$ is the inverse of Na.

Hence G/N is a group.

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

Example $3\mathbb{Z}$ 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.

Exercises

1. Find the order of the following quotient groups:

(a) $\frac{\mathbb{Z}_6}{3}$

(b) $\mathbb{Z}_{60}/(5)$

2. Compute S_n/A_n.

3. Compute $V_4/\langle e, a\rangle$.

UNIT III

3.10. Isomorphism

Definition. 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

Example. $(Z_3, \oplus)$ 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

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

(i) f is a bijection

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

Two groups $\boldsymbol{G}$ and $\boldsymbol{G'}$ 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 3.44. Isomorphism is an equivalence relation among groups.

Proof. For any group $G, i_G: G \to G$ is clearly an isomorphism. $i(xy) = xy$

Hence $G \cong G$. Therefore, the relation is reflexive.

Now, let $G \cong G'$ and let $f: G \to G'$ be an isomorphism. TP: $G' \cong G$

Then f is a bijection. $f(xy) = f(xy)f(y)$

$\therefore$ $f^{-1}: G' \to G$ is also a bijection.

Now, let $x', y' \in G'$. TP:- $f^{-1}(x'y') = \propto y$

Let $f^{-1}(x') = x$ and $f^{-1}(y') = y$.

Then $f(x) = x'$ and $f(y) = y'$.

$\therefore\ f(xy) = f(x)f(y) = x'y'$.

$\therefore\ f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$.

Hence f^{-1} is an isomorphism.

Thus $G' \cong G$ and hence the relation is symmetric.

Now, let $G \cong G'$ and $G' \cong G''$

Then there exist 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

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

$(g \circ f')(xy) = (g \circ f)(x)(g \circ f)(y)$.

Hence $g \circ f$ is an isomorphism.

Thus $G \cong G''$ and hence the relation is transitive.

$\therefore$ Isomorphism is an eguivalence relation among groups.

Examples

1. $(\mathrm{Z}, +) \cong (2\mathrm{Z}, +)$.

Consider $f: Z \to 2Z$ 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 $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \, a \in \mathbf{R}^* \right\}$.

G is a group under matrix multiplication.

We claim that $G \cong (\mathbf{R}^*, \cdot)$.

Consider $f: G \to \mathbf{R}^*$ given by $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$.

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 $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore\ f(AB) = ab = f(A)f(B)$.

Hence f is an isomorphism.

3. $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

Consider $f: \mathbf{R} \to \mathbf{R}^+$given by $f(x) = e^x$.

Clearly f is a bijection.

Also $f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$.

Hence f is an isomorphism.

4. $\mathbf{G} = \mathbf{R} - (-1)$ is a group under $*$ defined by $a * b = a + b + ab$. We claim that $G \cong (\mathbf{R}^*, \cdot)$.

Consider $f: G \to \mathbf{R}^*$ given by $f(x) = x + 1$.

Clearly f is a bijection.

$$\begin{aligned} f(x * y) &= f(x + y + xy) \\ &= x + y + xy + 1 \\ &= (x + 1)(y + 1) \\ &= f(x)f(y) \end{aligned}$$

Hence f is an isomorphism.

Example. $(\mathbf{Z}_n, \oplus)$ is a group.

Let G denote the set of all n^{th} roots of unity G is a group under usual multiplication.

We claim that $(\mathbf{Z}_n, \oplus) \cong G$.

Consider $f: \mathbf{Z}_n \to G$ given by $f(m) = \omega^n$ where $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$.

Clearly f is a bijection.

Let $a, b \in \mathbf{Z}_n$. Let $a + b = qn + r$ where $0 \le r \le n$.

Then $a \oplus b = r$. Hence

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

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

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

Hence f is an isomorphism.

Exercises

1. Show that $G = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \, a \in \mathbf{R}\right\}$ is : group under matrix addition and prove that $G \cong (\mathbf{R}, +)$.

2. Show that $G = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \text{ ad } a^2 + b^2 \neq 0\right\}$ is a group under matrix mult plication and $G \cong (\mathbf{C}^*, \cdot)$.

3. Let $f_a : \mathbf{R} \to \mathbf{R}$ be the function defined b ! $f_a(x) = x + a$. Then $G = (f_a / a \in \mathbf{R})^{\text{is}}$ group under composition of functions. Show that $G \cong (\mathbf{R}, +)$.

Theorem 3.45. 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 indentity.

(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 $f(a) = a'$.

$\therefore a'f(e) = f(a)f(e) = f(ae) = f(a) = a'$.

Similarly $f(e)a' = a'$

$\therefore \; f(e) = e'$.

(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, $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$.

$\therefore \; f(a)f(a^{-1}) = f(a^{-1})f(a) = e'$.

$\therefore \; [f(a)]^{-1} = f(a^{-1})$.

Remark. 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 this additional property. This is seen in the following three theorems.

Theorem 3.46. 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 3.47. 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, $[f(a)]^n = f(a) \ldots \ldots f(a)$ ($f(a)$ written n times

$= f(a^n)$ (since f is an isomorphism)
$= f(e)$
$= e'$

Now, if possible, let m be a positive integer such that $0 < m \leqslant n$ 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.

$\therefore$ n is the least positive integer such that $[f(a)]^n = e'$.

$\therefore$ The order of $f(a)$ is n.

Theorem 3.48. Let $f: G \to G'$ be an isomorphism. If 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.

Remark. To-prove that two groups G and G' are isomorphic/we exhibit a bijection $f: G \to G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$. If two groups G and G' are not isomorphic, then no such bijection exists. But in general it is not easy to try every possible bijection and find out whether it has the above property or not except when there is no bijection. In this case it is obvious that the groups are not isomorphic.

Examples.

1. ($\mathbf{Z}_4$,$\oplus$) and S_3 are not isomorphic since $\mathbf{Z}_4$ contains 4 elements and S_3 contains 6 elements and therefore there exists no bijection from $\mathbf{Z}_4$ to S_3.

2. The groups ($\mathbf{Z}_6$,$\oplus$) and S_3. Both groups contain 6 elements. We note that $\mathbf{Z}_6$ is abelian whereas S_3 is non-abelian. Hence by theorem 3.46 these two groups are not isomorphic. Thus in this case we conclude that the two groups are not isomorphic by showing that one group has an algebraic property which the other group does not have.

3. Consider ($\mathbf{Z}$, $+$) and ($\mathbf{Q}+$). These two groups are not isomorphic since ($\mathbf{Z}, +$) is cyclic and ($Q, +$) is not cyclic

Problem 1. Show that ($\mathbf{R}^*$,$\cdot$) is not isomorphic to ($\mathbf{R}, +$).

Solution. In $(\mathbf{R}, +)$ every element other than 0 is of infinite order. But in ($\mathbf{R}^*$,$\cdot$) there exists an element (other than 1) of finite order. For example, -1 is of order 2 in ($\mathbf{R}^*$,$\cdot$). Hence we cannot find an isomorphism from ($\mathbf{R}^*$,$\cdot$) to ($\mathbf{R}, +$). (by theorem 3.47).

Problem 2. Show that $(\mathbf{Z}_4,\oplus)$ is not isomorphic to V_4.

Solution. In $\mathbf{Z}_4$, 1 is an element of order 4. B$_{U_4}V_4$ every element other than e is of order 2 . Hence, two groups are not isomorphic.

This can also be proved by noticing that $\mathbf{Z_4}$ is cycles and V_4 is not cyclic.

Problem 3. If G is a group and G' is a set with a bines operation and there exists a one-one mapping f from f onto G' such that $f(ab) = f(a)f(b)$ for all $a, b \in c$ then show that G' is also a group.

Solution. Let $a, b, c \in G'$.

Since $f: G \to G'$ is a bijection, there exist $a, b, c \in G$ such that

$f(a) = a'; f(b) = b'; f(c) = c'$.

Since G is a group, $(ab)c = a(bc)$.

$\therefore\ f[(ab)c] = f[a(bc)]$.

$\therefore\ f(ab)f(c) = f(a)f(bc)$ (by hypothesis).

$\therefore\ [f(a)f(b)]f(c) = f(a)[f(b)f(c)]$.

$\therefore\ (a'b')c' = a'(b'c')$.

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, then exists $a \in G$ such that $f(a) = a'$.

Now, $ae = ea = a$.

$\therefore\ f(ae) = f(ea) = f(a)$.

$\therefore\ f(a)f(e) = f(e)f(a) = f(a)$.

$\therefore\ a'f(e) = f(e)a' = a'$.

$\therefore\ f(e)$ is the identity in G'.

Let $a' \in G'$. Since $f: G' \to G'$ is a bijection, the exists $a \in G$ such that $f(a) = a'$.

Now, $aa^{-1} = a^{-1}a = e$.

$\therefore\ f(aa^{-1}) = f(a^{-1}a) = f(e)$.

$\therefore\ f(a)f(a^{-1}) = f(a^{-1})f(a) = f(e)$.

$\therefore\ a'f(a^{-1}) = f(a^{-1})a' = f(e)$.

$\therefore\ f(a^{-1})$ is the inverse of a' in G'.

Hence G' is a group.

Problem 4. 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 $f(x^{-1}y^{-1}) = f(x^{-1})f(y^{-1})$. (since f is an isomorphism).

$\therefore\ (x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$.

$\therefore\ (y^{-1})^{-1}(x^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$.

$\therefore\ yx = xy$.

sHence G is abelian.

Conversely, suppose G is abelian.

Clearly $f: G \to G$ given by $f(x) = x^{-1}$ is a bijection.

Now, $f(\text{xy}) = ((xy)^{-1}) = y^{-1}x^{-1} = x^{-1}y^{-1}$ = f(x)f(y)

$\therefore\ f$ is an isomorphism.

Exercises

1. Show that any two groups of order 2 are isomorphic.
2. Show that any two groups of order 3 are isomorphic.
3. Show that any proper subgroup of $(\text{Z}, +)$ is isomorphic to ($\mathbf{Z}, +$). (Hint: Any proper subgroup of 77)

4. Show that $(\mathbf{Q}, +)$ is not isomorphic to $(\mathbf{Q}^*, \cdot)$.
5. Show that $(\mathbf{C}, +)$ is not isomorphic to $(\mathbf{C}^*, \cdot)$.
6. Let $f: G \to G'$ be an isomorphism. Then if H is a subgroup of G, $f(H)$ is a subgroup of G'.
7. Prove that for any positive integer n, $(\mathbf{Z}/n\mathbf{Z}) \cong \mathbf{Z}_n$.

Theorem 3.49. Any infinite cyclic group G is isomorphic to $(\mathbf{Z}, +)$.

Proof. Let G be an infinite cyclic group with generator a. Then $G = \{a^n / n \in \mathbf{Z}\}$.

Define $f: Z \to G$ 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, $f(n+m) = a^{n+m} = a^n a^n \overset{\neq m}{=} f(n)f(m)$.

Hence f is an isomorphism.

Corollary. Any two infinite cyclic groups are isomorphic to each other.

Note. Let G and G' be two infinite cyclic groups. By theorem 3.49, $G \cong (\mathbf{Z}, +)$ and $(\mathbf{Z}, +) \cong G'$. Thus $G \cong G'$ (since $\cong$ is an equivalence relation).

Theorem 3.50. Any finite cyclic group of order n is isomorphic to $(\mathbf{Z}_n, \oplus)$.

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

Define $f: \mathbf{Z}_n \to G$ by $f(r) = a^r$.

Clearly f is a bijection.

Now, let $r, s \in \mathbf{Z}_n$. Let $r \oplus s = t$. Then $r + s = qn + t$, where $0 \leq t < n$.

$$\therefore\ f(r \oplus s) = a^{r \oplus s} = a^t \ldots\ldots\ldots\ldots\ldots (1)$$

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

From (1) and (2), we get $f(r \oplus s) = f(r)f(s)$.

Hence f is an isomorphism.

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

Theorem 3.51 (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. Let G be a finite group of order n. Let $a \in G$.

Define $f_a: G \to G$ by $f_a(x) = ax$.

Now, f_a is $1-1$, since $f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$.

Let $y \in G$. Then $f_a(a^{-1}y) = a(a^{-1}y) = y)$. Thus f_a is onto.

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 $f_a, f_b \in G'$. Then $(f_a o\ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$

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 $\to \boldsymbol{G'}$ 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. .

$$\text{Also } \phi(ab) = f_{ab} = f_a \circ f_b = \phi(a) \circ \phi(b)$$

Hence ϕ is an isomorphism.

Example. Consider the group $G = \{e, a, b\}$ whose multiplication table is 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 permut. tion group $G' = \{f_e, f_a, f_b\}$ were

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

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

Examples.

1. Any group G has atleast one automorphism namely i_G.
2. The map $f: \mathbf{R}^* \to \mathbf{R}^*$ defined by $f(a) = a^{-1}$ is an automorphism.

Clearly f is a bijection.

Also $f(ab) = (ab^{-1})^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$

More generally if G is abelian, $f: G \to C$ defined by $f(a) = a^{-1}$ is an automorphism.

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

$$\begin{aligned}\phi(z+w) &= (\overline{z+w}) \\ &= \bar{z} + \bar{w} \\ &= \phi(z) + \phi(w)\end{aligned}$$

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

For, let $x, y \in G$. Then

$$\begin{aligned}\phi_a(x) = \phi_a(y) &\Rightarrow axa^{-1} = aya^{-1} \\ &\Rightarrow x = y \text{(by cancellation law)}\end{aligned}$$

$\therefore$ ϕ_a is $1-1$.

Also $\phi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = exe = x.$

Hence $a^{-1}xa$ is the pre-image of x under ϕ_a.

Also

$$\begin{aligned}\phi_a(xy) &= axya^{-1} \\ &= (axa^{-1})(aya^{-1}) \\ &= \phi_a(x)\phi_a(y)\end{aligned}$$

Thus ϕ_a is an automorphism of G.

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

Definition. 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 3.52. 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.

$\therefore$ f and g are isomorphisms of G to itself.

$\therefore f \circ g$ is an isomorphism of G to itself (Theorem 3.44).

$f \circ g \in$ Aut G.

$f \in$ Aut $G \Rightarrow f^{-1} \in$ Aut G (Theorem 3.44).

Clearly composition of functions is associative.

Hence Aut G is a group.

(ii) Let $\phi_a, \phi_b \in I(G)$. Then

$$\begin{aligned}(\phi_a\phi_b)(x) &= \phi_a(bxb^{-1}) \\ &= a(bxb^{-1})a^{-1} \\ &= (ab)x(ab)^{-1} \\ &= \phi_{ab}(x)\end{aligned}$$

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 ϕ_{a-1}.

$\therefore$ $I(G)$ 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

$$(\alpha\phi_a\alpha^{-1})(x) = \alpha\phi_a\left(\alpha^{-1}(x)\right) = \alpha(a\alpha^{-1}(x)a^{-1}) = \alpha(a)\alpha\alpha^{-1}(x)\alpha(a^{-1})$$

$$= \alpha(a)x[\alpha(a)]^{-1} = \phi_{\alpha(a)}(\mathrm{x}) \in I(G).$$

Therefore $\alpha\phi_a\alpha^{-1} = \phi_{\alpha(a)} \in I(G)$.

Hence $I(G)$ is a normal subgroup of Aut G.

Theorem 3.53. 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 iff $f(a)$ 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 (i) Let G be a finite cyclic group of order n. Then order of a is n. By theorem 3.46$f(a)$ is also an element of order n and hence $f(a)$ is a generator of $\boldsymbol{G}$.

Case (ii) 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 $G = \langle a\rangle$.

$\therefore \quad x = f(a^n) = [f(a)]^n \in H.$

$\therefore \quad f(G) \subseteq H.$

Now, let $x \in H$. Then $x = [f(a)]^n$ for some n.

$\therefore \quad x = f(a^n)$. Hence $x \in f(G)$.

$\therefore \quad H \subseteq f(G)$. 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 preimage a^n under f. Hence f is onto.

Now, to prove f is $1-1$.

Case (i) G is finite.

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

Case (ii) G is infinite.

Let $x, y \in G$ and let $x = a^n, y = a^m$ and $n \geq m$.

Now,

$$\begin{aligned} f(x) = f(y) &\Rightarrow f(a^n) = f(a^m) \\ &\Rightarrow [f(a)]^n = [f(a)]^m \\ &\Rightarrow [f(a)]^{n-m} = e \\ &\Rightarrow n - m = 0 \end{aligned}$$

(since $f(a)$ is an element of finite order)

$$\begin{aligned} &\Rightarrow n = m \\ &\Rightarrow a^n = a^m \\ &\Rightarrow x = y \end{aligned}$$

Hence f is $1-1$. Thus f is an automorphism.

Note. 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 example if $x \in G$ is any element then $x = a^n$ for some integer n and hence $f(x) = f(a^n) = [f(a)]^n$.

Example. Consider $(\mathbf{Z}_4, \oplus)$. Here 1 is a generator of this cyclic group.

If $f(1) = 3$, then

$$f(2) = f(1 \oplus 1) = f(1) \oplus f(1) = 3 \oplus 3 = 2$$
$$f(3) = f(2 \oplus 1) = f(2) \oplus f(1) = 2 \oplus 3 = 1 \text{ and}$$
$$f(0) = f(3 \oplus 1) = f(3) \oplus f(1) = 1 \oplus 3 = 0$$

Theorem 3.54. The number of automorphisms of a cyclic group of order n is $\phi(n)$.

Proof. Let G be a cyclic group of order n. Let $a \in C$ 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 3 of Theorem 3.28). Hence the number of automorphisms of a cyclic group of order n is $\phi(n)$.

Solved problems

Problem 1. Construct the group of automorphisms of $(\mathbf{Z}_4, \oplus)$.

Solution. 1 and 3 are the only 2 generators of Z_4. Hence there are only 2 automorphisms of $\mathbf{Z_4}$, say f and g. They are given by $f(1) = 1$ and $g(1) = 3$.

Hence Aut $G = \{f, g\} \cong \mathbf{Z}_2$.

Problem 2. Construct the group of automorphisms of ($\mathbf{Z}, +$).

Solution. 1 and -1 are the only 2 generators of Z . Hence there are only 2 automorphisms of $\mathbf{Z}$ 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 $\mathbf{Z} = \{f, g\} \cong \mathbf{Z}_2$.

Problem 3. Let G be a finite abelian group of order n and let m be a positive integer relatively prime 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,

$$\begin{aligned} f(x) = f(y) &\Rightarrow x^m = y^m \\ &\Rightarrow x^{mu} = y^{mu} \\ &\Rightarrow x = y \end{aligned}$$

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 $f(xy)=(xy)^m=x^m y^m=f(x)f(y)$

Hence f is an isomorphism.

Problem 4. Show that Aut $\mathbf{Z}_8 \cong \mathbf{V}_4$.

Solution. The generators of $\mathbf{Z}_8$ are 1,3,5,7. The four different automorphisms of $\mathbf{Z}_8$ are f_1, f_2, f_3, f_4 given by $f_1(1) = 1; f_2(1) = 3; f_3(1) = 5; f_4(1) = 7$.

We shall now compute $f_2 \circ f_3$.

$$(f_2 \circ f_3)(1) = f_2(f_3(1)) = f_2(5)$$
$$= f_2(1 \oplus 1 \oplus 1 \oplus 1 \oplus 1)$$
$$= f_2(1) \oplus f_2(1) \oplus f_2(1) \oplus f_2(1) \oplus f_2(1)$$
$$= 3 \oplus 3 \oplus 3 \oplus 3 \oplus 3$$
$$= 7 = f_4(1)$$

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 $\mathbf{Z}_8$ 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 $Z_8 \cong V_4$.

Exercises

1. Compute the group of automorphisms of $(\mathbf{Z}_{12}, \oplus)$ and show that Aut $\mathbf{Z}_{12} \cong$ Aut $\mathbf{Z}_8$.
2. Show that in a group G every inner automorphism is identity iff G is abelian.
3. Prove that a subgroup H of G is a normal subgroup iff $\phi_a(H) = H$ for every inner automorphism ϕ_a'.
4. Represent $\mathbf{Z}_4$ and V_4 as groups of permutations.

3.11. Homomorphisms

Example. Let n be any given positive integer.

Let $x \in \mathbf{Z}$ and $x = qn + r$, where $0 \leq r < n$.

We define $f(x) = r$.

f is a mapping from $(\mathbf{Z}, +)$ to $(\mathbf{Z}_n, \oplus)$.

We claim that $f(a + b) = f(a) \oplus f(b)$ for all $a, b \in \mathbf{Z}$.

Let $a = q_1 n + r_1, 0 \leq r_1 < n$ so that $f(a) = r_1$

and $b = q_2 n + r_2, 0 \leq r_2 < n$ so that $f(a) = r_2$.

Let $r_1 + r_2 = q_3 n + r_3, 0 \leq r_3 < n$ so that $r_1 \oplus r_2 = r_3$.

$\therefore\ a + b = (q_1 + q_2 + q_3)n + r_3$.

$\therefore\ f(a + b) = r_3$.

Also $f(a) \oplus f(b) = r_1 \oplus r_2 = r_3$.

$\therefore f(a + b) = f(a) \oplus f(b)$.

Note that f is not an isomorphism since f is not $1 - 1$.

Definition. A map f from 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 homorphism and a bijective homomorphism is an isomorphism.

Examples

1. $f: (\mathrm{Z}, +) \to (\mathrm{Z}, +)$ 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. $f: (\mathbf{R}^*, \cdot) \to (\mathbf{R}^+, \cdot)$ defined by $f(x) = |x|$ is a homomorphism.

For, $f(xy) = |xy| = |x||y| = f(x)f(y)$.

This homorphism 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. $f:(\mathbf{Z},+)\to(\mathbf{C}^*,\cdot)$ given by $f(n)=i^n$ is a homomorphism.

For, $f(m+n)=i^{m+m}=i^n i^m=f(n)f(m)$.

Note that f is neither $1-1$ nor onto.

5. $f:(\mathbf{R}\times\mathbf{R},+)\to(\mathbf{R},+)$ 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 homomorphism.

For, $f(ab)=Nab=NaNb=f(a)f(b)$. f is called the canonical homomorphism from G to G/N. Note that f is onto.

Definition. 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. 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 3.55. 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 no. empty.

Now, let $x,y\in f(H)$.

Then $x=f(a)$ and $y=f(b)$ where $a,b\in H$.

$$\therefore xy^{-1} = f(a)[f(b)]^{-1}$$
$$= f(a)f(b^{-1}) = f(ab^{-1}).$$

Now, since H is a subgroup of $G, ab^{-1} \in H$.

$\therefore\ xy^{-1} = f(ab^{-1}) \in f(H)$.

$\therefore\ f(H)$ 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 $G, bab^{-1} \in H$.

$\therefore\ f(bab^{-1}) \in f(H)$.

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

$\therefore\ yxy^{-1} \in f(H)$. 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 $f(a), f(b) \in H'$.

$\{f(a)[f(b)]^{-1} \in H'$

$f(ab^{-1}) \in H'$

(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 $f(G), f(a)f(x)[f(a)]^{-1} \in H'$.

$\therefore\ f(axa^{-1}) \in H'$.

Hence $axa^{-1} \in f^{-1}(H')$.

Thus $f^{-1}(H')$ is normal in G.

Examples

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

Let $K = \{x / x \in \mathbf{Z}, f(x) = 0\}$.

Clearly $K = n\mathbf{Z}$ which is a normal subgroup of $\mathbf{Z}$.

2. Consider the homomorphism

$f:(\mathbf{R}^*,\cdot) \to (\mathbf{R}^+,\cdot)$ which is given by $f(x) = |x|$.

Let $K = \{x/x \in \mathbf{R}^*, f(x) = 1\}$.

Clearly $K = \{1,-1\}$ which is a normal subgroup of $(\mathbf{R}^*,:)$.

Definition. Let f : G → G' be a homomorphism. Let K = {x/x ϵ G, f(x) = e'} . Then K is called the kernel of f and is denoted by ker f .

Theorem 3.56. Let f : G → G' be a homomorphism. Then the kernel K of f is a normal subgroup of G .

Proof. Since f(e) = e', e ϵ K and hence K ≠ Φ .

Now, let x, y ϵ K . Then f(x) = e' = f(y) .

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = e'(e')^{-1} = e'.$$

Thus $xy^{-1} \in K$. Hence K is a subgroup of G .

Now, let xϵ K and a ϵ G .

Then

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

Therefore $axa^{-1} \in K$. Hence K is a normal subgroup of G .

Theorem 3.57. (Fundamental theorem of homomorphism)

Let f : G → G' be an epimorphism. Let K be the kernel of f. Then G/K ≅ G'.

Proof. Define ϕ: G/K → G' by ϕ (Ka) = f(a).

Step (i) ϕ is well defined.

Let Kb = Ka. Then b ϵ Ka.

Hence b = ka where k ϵ K.

Now, f(b) = f(ka) = f(k)f(a)= e'f(a) = f(a).

Therefore ϕ (Kb) = f(b) = f(a) = ϕ (Ka).

Hence ϕ (Ka) = ϕ (Kb).

Step (ii) ϕ is 1-1.

For ϕ (Ka) = ϕ (Kb) ⟹ f(a) = f(b)⟹ $f(a)[f(b)]^{-1} = e'$⟹ f(ab^{-1}}) = e'.⟹ ab^{-1} ϵ K.

⟹a ϵ Kb⟹ Ka = Kb.

Step (iii) ϕ is onto.

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

Hence ϕ (Ka) = f(a) = a'.

Step (iv) ϕ is a homomorphism.

ϕ (KaKb) = ϕ (Kab) = f(ab) = f(a)f(b)= ϕ (Ka) ϕ (Kb).

Thus ϕ is an isomorphism from G/K onto G'.

Therefore G/K ≅ G'.

Solved problems

Problem 1. Let $f: G \to G'$ be a homomorphism. Then f is $1-1$ iff ker $f = e$.

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

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. Let G be any group and H be the centre 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.

we claim that $\ker f = H$.

$$a \in \ker f \Leftrightarrow f(a) = \phi_e. \Leftrightarrow \phi_a = \phi_e \Leftrightarrow \phi_a(x) = x \text{ for all } x \in G$$
$$\Leftrightarrow axa^{-1} = x \text{ for all } x \in G$$
$$\Leftrightarrow ax = xa \text{ for all } x \in G$$
$$\Leftrightarrow a \in H.$$

Hence $\ker f = H$.

∴ By the fundamental theorem of homomorphism $G/H \cong I(G)$.

Problem 3. Show that $\mathbf{R}^*/\{1, -1\} \cong \mathbf{R}^+$.

Solution. Consider $f: \mathbf{R}^* \to \mathbf{R}^+$ defined by $f(x) = |x|$.

Clearly f is an epimorphism and $\ker f = \{1, -1\}$.

Hence by the fundamental theorem of homomorphism $\mathbf{R}^*/\{1, -1\} \cong \mathbf{R}^+$.

Problem 4. 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 be a generator of G. Then $f(a)$ is a generator of G'. (by theorem 3.48).

Hence G' is cyclic.

Problem 5. Show that the map $f: (\mathbf{C}, +) \to (\mathbf{R}, +)$ defined by $f(x + iy) = y$ is an epimorphism and $\ker f = \mathbf{R}$. Deduce that $\mathbf{C}/\mathbf{R} \cong \mathbf{R}$.

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, $\ker f = \{x + iy / f(x + iy) = 0\} == \{x + iy / y = 0\} = \mathrm{R}$.

By the fundamental theorem of homomorphism $\mathbf{C}/\mathbf{R} \cong \mathbf{R}$.

Exercises

1. Determine which of the following maps are homomorphism. If it is a homomorphism, find the kernel.

(a) $f: (\mathbf{Z}, +) \to (1, -1)$ given by $f(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$

(b) $f: \mathbf{R}^* \to \mathbf{R}^*$ given by $f(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases}$

(c) $f: (\mathbf{R} \times \mathbf{R}, +) \to (\mathbf{R}, +)$ given by $f(x, y) = y$.

(d) $f: (\mathbf{Z}, +) \to (\mathbf{R}^*, \cdot)$ given by $f(x) = 3^x$.

(e) $f: S_n \to (1, -1)$ given by $f(p) = \begin{cases} 1 & \text{if } p \text{ is an even permutation} \\ -1 & \text{if } p \text{ is an odd permutation.} \end{cases}$

(f) $f: \mathbf{R} \to \mathbf{C}$ given by $f(x) = e^{ix}$.

(g) $f: (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ given by $f(n) = 2n$.

(h) $f: \mathbf{R}^* \to \mathbf{R}^*$ given by $f(x) = -x$.

(i) $f: \mathbf{Z_6} \to \mathbf{Z}_2$ given by $f(x) =$ remainder of x when x is divided by 2 .

(j) $f: \mathbf{C}^* \to \mathbf{R}^*$ given by $f(z) = |z|$.

(k) $f: (\mathbf{R}, +) \to (\mathbf{R}, +)$ given by $f(x) = x + 2$.

2. Determine which of the following statements are true and which are false.

(a) Any isomorphism is a homomorphism.

(b) Any homomorphism is an isomorphism.

(c) An infinite group cannot be homomorphic to a finite group.

(d) Homomorphism pri res the order of an element.

(e) Any homomorphism f is a monomorphism iff $kerf$ is $\{e\}$.

Answers.

1. (a) Yes. $\ker f = 2\mathbf{Z}$.

(b) Yes. $\ker f = \mathbf{R}^+$.

(c) Yes. $\ker f = \mathbf{R} \times \{0\}$.

(d) Yes. $\ker f = \{0\}$.

(e) Yes. $\ker f = A_n$.

(f) No

(g) Yes. $\ker f = \{0\}$.

(h) No

(i) Yes. $\ker f = \{0,2,4\}$.

(j) Yes. $\ker f = \{z / z \in \mathbf{C} \text{ and } |z| = 1\}$.

(k) No.

2. (a) T (b) F (c) F (d) F (e) T .

UNIT IV

Rings

4.1. Definition and examples

Definition. A nonempty set R together with two binary operations denoted by " + " and "." and called addition and multiplication which satisfy the following axioms is called a ring.

(i) $(R, +)$ is an abelian group.

(ii) ". " 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. 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

1. ($\mathbf{Z}, +, \cdot$); ($\mathbf{Q}, +, \cdot$); ($\mathbf{R}, +, \cdot$); ($\mathbf{C}, +, .$) are all rings.
2. ($2\mathrm{Z}, +,$) is a ring.
3. Let $R = \{a + b\sqrt{2}/a, b \in \mathbf{Z}\}$.

Clearly R is an abelian group under usual addition.

Let $a + b\sqrt{2}$ and $c + d\sqrt{2} \in R$. Then

$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \in R$

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 $R = \{a + ib/a, b \in \mathbf{Z}\}$. 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.
5. $\{0\}$ with binary operations ' + ' and ' $\cdot$ ' defined as $0 + 0 = 0$ and $0.0 = 0$ is a ring. This is called the null ring.
6. In $\mathbf{R} \times \mathbf{R}$ we define $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac, bd)$. Here ($\mathbf{R} \times \mathbf{R}, +$) is an abelian group. The identity is $(0,0)$ and the inverse of (a, b) is $(-a, -b)$.

$$(a,\mathrm{b})[(\mathrm{c},\mathrm{d})+(\mathrm{e},\mathrm{f})] = (a,b)(c+e,d+f)$$
$$= (ac+ae,bd+bf)$$
$$= (ac,bd)+(ae,bf)$$
$$= (a,b)(c,d)+(a,b)(e,f)$$

Similarly, $[(a,b)+(c,d)](e,f) = (a,b)(e,f)+(c,d)(e,f)$.

Hence ($\mathbf{R}\times\mathbf{R},+,\cdot$) 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. $(\mathbf{Z}_n,\oplus,\odot)$ is a ring, for, we know that $(\mathbf{Z}_n,\oplus)$ is an abelian group and $\odot$ is an associative binary operation.

We now prove the distributive laws.

Let $a,b,c\in\mathbf{Z}_n$.

Then $b\oplus c\equiv(b+c)(\mathrm{mod}n)$.

Hence $a\odot(b\oplus c)\equiv a(b+c)(\mathrm{mod}n)$.

Also $a\odot b\equiv ab(\mathrm{mod}\ n)$ and $a\odot c\equiv ac(\mathrm{mod}\ n)$ so that

$(a\odot b)\oplus(a\odot b)\equiv(ab+ac)(\mathrm{mod}\ n)$.

Since $a\odot(b\oplus c)$ and $(a\odot b)\oplus(a\odot c)\in\mathbf{Z}_n$, 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 $(\mathbf{Z}_n,\oplus,\odot)$ is a ring.

9. $(\wp(S),\Delta,\cap)$ is a ring. We know that $(\wp(S),\Delta)$ is an abelian group (refer example 12 of section 3.1).

Also $\cap$ is an associative binary operation on $\wp(S)$.

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 $(\wp(S),\Delta,\cap)$ is a ring.

10. $M_2(\mathrm{R})$ 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 ring.

Example. Let A be any abelian group. Let Hom (A) be the set of all endomorphisms of A. Let $f,g\in \mathrm{Hom}(A)$. 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 $f,g\in \mathrm{Hom}(A)$.

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 $f+g\in \mathrm{Hom}(A)$.

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 $\mathrm{Hom}(A)$.

Now, let $f\in \mathrm{Hom}(A)$. 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 $f \circ g \in \text{Hom}(A)$.

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

Thus Hom (A) is a ring.

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

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

Then

$$A + B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R.$$
$$AB = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+ac) & ac-bd \end{pmatrix} \in R.$$

Clearly matrix addition is commutative and $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ 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.

Exercises

1. Prove that the set of all real numbers of the form $a + b\sqrt{3}$ where $a, b \in \mathbf{Q}$ under usual addition and multiplication is a ring.
2. Determine which of the following statements are true and which are false.

(a) The set of all even integers is a ring under usual addition and multiplication

(b) The set of all odd integers is a ring under usual addition and multiplication.

(c) In any ring addition is commutative

(d) The non-zero elements of a ring form a group under multiplication.

Answers. 2.(a) T (b) F (c) T (d) F

4.2. Elementary properties of rings

Theorem 4.1. 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) $a0 = a(0+0) = a0 + a0$.

$\therefore a0 = 0$. (by cancellation law in $(R, +)$)

Similarly $0a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a0 = 0$.

$\therefore a(-b) = -(ab)$.

Similarly, $(-a)b = -(ab)$.

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

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

Solved problems

Problem 1. 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) (since $a^2 = a$)

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

Note. A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$.

For example ($\wp(S), \Delta, \cap$) is a Boolean ring.

Problem 2. 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

.	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.

$$\begin{aligned} cb &= (b + d)b && \text{(from addition table)} \\ &= bb + db \\ &= b + b && \text{(from multiplication table)} \\ &= a && \text{(from addition table)} \end{aligned}$$

Now, $cc = c(b + d) = cb + cd = a + a = a$.

$bc = (\hat{b} + d)c = cc + dc = a + \mathrm{c} = c$.

$bd = b(b + c) = bb + bc = b + c = d$.

$dd = (b + c)d = bd + cd = d + a = d$.

Hence the completed table for multiplication is

.	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

Exercises

1. Given any positive integer n show that there exists a ring with n elements.
2. Prove by induction that $a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n$.

4.4. Types of rings

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

Examples

1. The familiar rings Z, Q, R are all commutative. The following are examples of noncommutative rings.
2. Let F denote the set of all functions from **R** to R. We define $(f + g)(x) = f(x) + g(x)$ and $f \cdot g = f \circ g$. Then ($F, +, \cdot$) is noncommutative ring.
3. The ring of quaternions given in example 13 of 4.1 is a non-commutative ring since $ij = k$ and $ji = -k$.
4. $M_2(\mathrm{R})$ is a non-commutative ring.

Exercises Determine which of the rings given in section 4.1 are commutative. section 4.1 are commutative.

Answers 1,2,3,4,5,6,7,8,9,11,14 are commutative rings.

Definition. Let R be a ring. We say that R is a ring with identity if there exists 1 belongs to R such that $a1 = 1a = a$ for all a belongs to R

Examples

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

Exercises Determine which of the rings given in section 4.1 are rings with identity.

Answers. 1,3,4,6,8,9,10,11,12,13 and 14 are rings with identity.

Note. 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 multiplicative identity is not 0 .

Theorem 4.2. 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. 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}.

Examples.

1. In $(\mathbf{Z}, +, \cdot)$,1 and -1 are units.
2. In $M_2(\mathbf{R})$, all the non-singular matrices are units.
3. In $\mathbf{Q}, \mathbf{R}$ and $\mathbf{C}$ every non-zero element is a unit.

Theorem 4.3. 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 hence $a \in U \Rightarrow a^{-1} \in U$.

Hence U is a group under multiplication.

Exercises. Find all the units in the rings given in section 4.1

Answers.

1. In $\mathbf{Z}$, 1 and -1 are units; $\mathbf{Q}^*, \mathbf{R}^*$ and $\mathbf{C}^*$ are the units in $\mathbf{Q}, \mathbf{R}$ and $\mathbf{C}$ respectively.
2. Nil
3. 1 and -1
4. $1, i, -1, -i$.
5. Nil
6. $\mathbf{R}^* \times \mathbf{R}^*$.
7. Nil.
8. $\{a/a \in \mathbf{Z}_n$ and $(a, n) = 1\}$.
9. S.
10. All non-singular matrices.
11. All bijections.
12. All automorphisms

13. Q^*

14. R^*.

Definition. 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 element $a \in R$, there exists a multiplicative inverse $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Thus, in a skew field the non-zero elements form a group under multiplication.

Definition. 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

1. **Q**, **R** and **C** are fields under usual addition and multiplication.

2. Let p be a prime. Then $(Z_p, \oplus, \odot)$ is field.

Proof. ($\mathbf{Z}_p, \oplus, \odot$) is a ring (by example 8 of 4.1)

Also since p is prime $(Z_p - \{0\}, 0)$ is an abelian group. (refer example 23 of 3.1).

Hence $(Z_p, \oplus, \odot)$ is a field.

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

Proof. Let $A, B \in M$.

Let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$ Then

$$A + B = \begin{pmatrix} a+b & b+d \\ -\bar{b} - \bar{d} & \bar{a} + \bar{c} \end{pmatrix}$$

$$= \begin{pmatrix} a+c & b+d \\ -(b+d) & \overline{a+c} \end{pmatrix} \in M.$$

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.

$\begin{pmatrix} -a & -b \\ \bar{b} & -\bar{a} \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$

Hence M is an abelian group und addition.

Now,

$$AB = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix}$$
$$= \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \overline{ac} \end{pmatrix}$$

which is of the form $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$.

Hence M is closed under matrix multipletioni.

Further matrix multiplication is associnic and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ is the multiplicare identity.

Now, let $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ be a non-zen matrix in M.

Then either $a \neq 0$ or $b \neq 0$ so that either $|a| > 0$ or $|b| > 0$.

Hence $|A| = a\bar{a} + b\bar{b} = |a|^2 + |b|^2 > 0$

Thus A is a non-singular matrix and hence br an inverse and $A^{-1} \in M$. Thus M is a skew field. Also since matrix multiplication is ad commutative, M is not a field.

4. Let Q be the ring of quarternions given is example 13 of section 4.1. Q is a skew field but not a field.

Proof. We have proved that $(Q, +, \cdot)$ is : ring.

$1 = 1 + 0i + 0j + 0k$ is the identity elemest Let $x = a_0 + a_1 i + a_2 j + a_3 k$ be a non-zero element in Q.

Then not all of 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. $(Z_i +.)$ is a commutative ring with identity but not a field since 1 and -1 are the only non-zero elements which have inverses.

Theorem 4.4. In a skew field R,

(i) $ax = ay, a \neq 0 \Rightarrow x = y$ (cancellation laws in ring)

(ii) $xa = ya, a \neq 0 \Rightarrow x = y$

(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 $x = 0$, then clearly $ax = 0$.

Conversely let $ax = 0$ and $a \neq 0$.

$\therefore\ ax = a0$.

$\therefore\ x = 0$ by (i).

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

Example

1. Consider the ring ($\mathbf{R} \times \mathbf{R}, +, \cdot$) where ' + ' and '. ' are defined by

$$(a, b) + (c, d) = (a + c, b + d) \text{ and}$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

$\mathbf{R} \times \mathbf{R}$ 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. 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

1. In the ring $\mathbf{R} \times \mathbf{R}$, $(1,0)$ 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 $Z_{12}, 3$ 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 4.5. A ring R has no zero-divisors iff cancellation law is valid in R.

Proof. Let R be a ring without zero-divisors.

Let $ax = ay$ and $a \neq 0$.

$\therefore\ ax - ay = 0$. Hence $a(x - y) = 0$ and $a \neq 0$.

$\therefore\ x - y = 0$ (since R has no zero-divisors).

$\therefore\ x = y$. Thus, cancellation laws 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 4.6. 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. The converse of the above result is not true. (ie.) a is not a zero-divisor does not imply a is a unit.

For example, in **Z,** 2 is not a zero-divisor and 2 is not a unit.

Definition. A commutative ring with identity having no zero-divisors is called in integral domain.

Thus, in an integral domain $\boldsymbol{ab = 0} \Rightarrow$ either $\boldsymbol{a = 0}$ 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

1. **Z** is an integral domain.
2. nZ where $n > 1$ is not an integral domain since the ring nZ does not have an identity.
3. $\mathbf{Z}_{12}$ is not an integral domain since 4 is a zerodivisor in Z_{12}.
4. Z_7 is an integral domain.

Theorem 4.7.Z_n is an integral domain iff n is prime.

Proof. Let Z_n be an integral domain.

We claim that n is prime. Suppose n is not prime.

Then $n = pq$ where $I < p < n$ and $I < q < n$.

Clearly $p \odot q = 0$.

Hence p and q are zero-divisors.

$\therefore$ $\mathbf{Z}_n$ is not an integral domain which is a contradiction. Hence n is prime.

Conversely, suppose n is prime. Let $a, b \in \mathbf{Z}_n$.

Then $a \odot b = 0 \Rightarrow ab = qn$ where $q \in Z_n$.

$\Rightarrow n \mid ab$
$\Rightarrow n \mid q$ or $n \mid b$ (since n is prime)
$\Rightarrow a = 0$ or $b = 0$.

$\therefore$ Z_n has no zero-divisors.

Also $\mathbf{Z}_n$ is a commutative ring with identity.

Hence Z_n is an integral domain.

Theorem 4.8. Any field F is an integral domain.

Proof. It is enough if we prove that F has no zerodivisors.

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. The converse of the above theorem is not true

(ie) An integral domain need not be a field.

For example, $\mathbf{Z}$ is an integral domain but not a field.

Theorem 4.9. Let R be a commutative ring with identity 1 . Then R is an integral domain iff 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 4.10. Let R be a commutative ring with identity. Then R is an integral domain iff cancellation law is valid in R.

Proof. The result is an immediate consequence of Theorem 4.5.

Theorem 4.11. 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 $R = (0,1, a_1, a_2, \dots, \dots, a_n)$.

Consider $\{a1, aa_1, aa_2, \dots \dots, aa_n\}$.

By Theorem 4.9 all these elements are non-zero and all these elements are distinct by Theorem 4.10.

Hence $aa_i = 1$ for some $a_i \in R$

since R is commutative, $aa_i = a_i a = 1$ so that $a_i = a^{-1}$. Hence R is a field.

Remark. 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 4.12.Z_n is a field iff n is prime.

Proof. By theorem 4.7, $\mathbf{Z}_n$ is an integral domain iff n is prime.

Further Z_n is finite. Hence the result follows from Theorem 4.11.

Theorem 4.13. 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 4.11 it is a field. So we prove the existence of identity.

Let $R = \{0, a_1, \dots \dots, a_n\}$.

Let $a \in R$ and $a \neq 0$.

Then the elements $aa_1, aa_2, \dots \dots, aa_n$, are distinct and non-zero.

$\therefore\ aa_i = a$ 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.

$\therefore a_i b = a_i(aa_j) = (a_i a)a_j = aa_j = b$.

Thus $a_i b = ba_i = b$.

Since $b \in R$ is arbitrary, a_i is the identity of R.

Hence the theorem.

Solved problems

Problem 1. Prove that the set F of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbf{Q}$ is a field under the usual addition and multiplication of real numbers.

Solution. Obviously, $(F, +)$ is a 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 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 (ii) $a = 0$ and $b \neq 0$, then $a^2 - 2b^2 = -2b^2 \neq 0$.

Case (iii) $a \neq 0$ 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, $a/b \in \mathbf{Q}$ and $\sqrt{2} \notin \mathbf{Q}$. This is a contradiction.

Hence $a^2 - 2b^2 \neq 0$.

$$\therefore \frac{1}{a + b\sqrt{2}} = \left(\frac{a}{a^2 - 2b^2}\right) - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in F$$

and is the inverse of $a + b\sqrt{2}$.

Hence F is a field.

Problem 2. Give examples of

a finite commutative ring with identity which is not an integral domain.

a finite non-commutative ring.

an infinite non-commutative ring with identity.

an infinite ring having no identity.

Solution.

$A = (Z_4, \oplus, \odot)$ 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.

Consider the set $M_2(Z_3)$ of all matrices with entries from \mathbf{Z}_3. Clearly $M_2(Z_3)$ 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 $M_2(Z_3)$ is non-commutative.

$M_2(R)$ is an infinite non-commutative ring with identity $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.

(2Z, +, .) is an infinite ring with no identity.

Problem 3. Prove that the only idempotent 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 zero-divisors $a(a-1)=0 \Longrightarrow a=0$ or $a-1=0$

Problem 4. 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 $a^{n-1} = 1$ (by Theorem 3.35). Therefore $a^n = a$.

Problem 5. 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 6. 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 $m, n \in Z$.

Now, $xy = mana = (a + a + \ldots. + a)\ (a + a + \ldots\ldots + a)$

$= mna^2 = nma^2 = na\ ma = yx$

Hence R is a commutative ring.

Now, let R be a ring with 7 elements.

Then $(R, +)$ is a group of order 7. $|R| = 7$

Hence $(R, +)$ is cyclic.

Hence R is commutative.

Problem 7. Let R and R' be rings and $f : R \to R'$ be an isomorphism. Then

(i) R is commutative $\Longrightarrow R'$ is commutative.

(ii) R is ring with identity $\Longrightarrow R'$ is a ring with identity.

(iii) R is an integral domain R' is an integral domain.

(iv) R is a field $\Longrightarrow R'$ 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)

$= f(b)f(a)$

$= b'a'$

Therefore 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 hence $f(1)$ is the identity element in R' .

Therefore 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"ϵ R' and let a'b' = 0 .

Since f is onto there exist a, b'ϵ R such that f(a) = a' and f(b) = b' .

a'b' = 0$\Longrightarrow$ f(a)f(b) = 0

$\Longrightarrow$f(ab) = 0

$\Longrightarrow$ab = 0 (since f is 1-1)

$\Longrightarrow$ a = 0 or b = 0 (since R is an integral domain)

$\Longrightarrow$ f(a) = 0 or f(b) = 0.

$\Longrightarrow$ a' = 0 or b' = 0.

Therefore R' is an integral domain.

(iv) We need to prove that every non-zero element in R' has an inverse. Let a"ϵ R' and a' $\neq$ 0.

Then there exists a'ϵ 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 8. Prove that the only isomorphism f :Q$\rightarrow$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.

f(n) = f(1 + 1 +… + 1) (written n times)

= f(1) + f(1) +…. + f(1) (written n times)

= 1 + 1 +…. + 1 (written n times)

= n.

Now, if n is a negative integer, let n = -m where m 'ϵN.

Then f(n) = f(-m) = -f(m) = -m = n

Thus for any integer n, f(n) = n.

Now, let a 'ϵ Q. Then a = p/q where p, q 'ϵ Z.

Hence $f(a) = f(p/q) = f(pq^{-1}) = f(p)f(q^{-1}) = f(p)[f(q)]^{-1} = pq^{-1} = p/q = a$.

Exercises

1. Give examples of

(a) a commutative ring with zero. divisors.

(b) a non-commutative ring with zero. divisors.

(c) an integral domain which is not a field.

(d) a skew field which is not a field.

(e) a commutative ring with identity which is not an integral domain.

2. Prove that a ring R is commutative iff for all $a, b \in R, (a+b)^2 = a^2 + 2ab + b^2$.

4.5. Characteristic of a ring

Let R be a ring. Then $(R, +)$ is a group. For any $a \in R$ we have $na = a + a + \cdots + a$ (written n times).

Note. For the ring $\mathbf{Z}_6$ we have $6a = 0$ for all $a \in \mathbf{Z}_6$.

Definition. 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

1. Z_6 is a ring of characteristic 6 . In general $\mathbf{Z}_n$ is a ring of characteristic n.
2. $\mathbf{Z}$ is a ring of characteristic zero, since there is no positive integer n such that na $= 0$ for all $a \in \mathbf{Z}$.
3. $M_2(\mathbf{R})$ is a ring of characteristic zero.
4. $(\wp(S), \Delta, \cap)$ is a ring of characteristic 2 , since $2A = A\Delta A = \Phi$ for all $A \in \wp(S)$.
5. Any Boolean ring is of characteristic 2 (refer solved problem 1 of 4.2).

Theorem 4.14. 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, $na = a + a + \cdots + a(n \text{ times})$

$$= 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a$$
$$= (1 + 1 + \cdots + 1)a.$$
$$= 0 \cdot a$$
$$= 0.$$

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 4.15. 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.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, q are both less than n, this contradicts the definition of the characteristic of D.

Hence n is a prime number.

Corollary. The characteristic of any field is either 0 or a prime number.

Proof. Since every field is an integral domain the result follows.

Note.

1. The characteristic of an arbitrary ring need not be prime. For example $\mathbf{Z}_6$ 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.

Example. The ring ($\wp(S), \Delta, \cap$) is of characteristic 2 but it is 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 $\wp(S)$.

Theorem 4.16. 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 the characteristic of D we have $pa = 0$.

Hence $n \mid p$. 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. The above result is not true for an arbitrary ring. For example the characteristic of the ring $\mathbf{Z}_6$ is 6 whereas the order of $2 \in \mathbf{Z}_6$ is 3 .

Exercises

1. Prove that any integral domain of characteristic zero is infinite.
2. Show that the characteristic of $M_2(Z_3)$ is 3 .
3. Give an example of an infinite ring of characteristic not zero.
4. In a field of characteristic p show that $(a \pm b)^p = a^p \pm b^p$.
5. Let a, b be arbitrary elements of a ring a whose characteristic is 2 and let $ab = ba$

Then show that $(a + b)^2 = a^2 + b^2 = (a - b)^2$.

6. Determine which of the following are true and which are false.

(a) $n\mathbf{Z}$ is of characteristic n.

(b) The characteristic of any ring is either 0 or a prime number.

(c) The characteristic of $\mathbf{Q}$ is zero.

(d) The characteristic of any finite ring is not zero.

(e) The characteristic of any field is zero.

Answers.

6. (a) F (b) F (c) T (d) T (e) F .

4.6. Subrings

Definition. A non-empty subset S of a ring $(R, +, .)$ is called a subring if S itself is a ring under the same operations as in R.

Examples

1. 2Z is a subring of Z.
2. $\mathbf{Z}$ is a subring of $\mathbf{Q}$.
3. $\mathbf{Q}$ is a subring of $\mathbf{R}$.
4. $\mathbf{R}$ is a subring of $\mathbf{C}$.

5. The set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a subring of $\boldsymbol{M_2(\mathbf{R})}$.
6. $\{0\}$ and R are subrings of any ring R. They are called the trivial subrings of R.
7. $S = \{a + b\sqrt{2}/a, b \in \mathbf{Q}\}$ is a subring of $\mathbf{R}$.
8. $\{0,2\}$ is a subring of $\mathbf{Z}_4$.

Theorem 4.17. A non-empty subset S of a ring R is a subring iff $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$.

Proof. Let S be a subring of R. Then $(S, +)$ is a subgroup of (R,+).

Hence, $a, b \in$ S $\Longrightarrow$ a-b ϵ S.

Also since S itself is a ring abϵ S.

Conversely, let S be a non-empty subset of R such that a, bϵ S$\Longrightarrow$ a-bϵ S and abϵ S.

Then $(S, +)$ is a subgroup of $(R, +)$.

Also S is closed under multiplication.

The associative and distributive laws are consequences oi the corresponding laws in R.

Hence S is a subring.

Solved problems

Problem 1. Let X be any set and let F be the set of all finite subsets of X. Then F is a subring of $(\rho(X), \Delta, \cap)$.

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 2. Let R be a ring with identity. Then $S = (n \cdot 1/n \in \mathbf{Z})$ is a subring of R.

Solution. Let $a, b \in S$. Then $a = n \cdot 1$ and $b = m \cdot 1$ for some $n, m \in \mathbf{Z}$.

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. Given 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 $a, b \in \mathbf{R}$. Then R is a ring under matrix addition and multiplication .

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,

$$\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} ac & 0 \\ bd & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

$\Rightarrow ac = a$ and $ad = b \Rightarrow c \neq 1$ 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 $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ has $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as identity.

(b) 2 Z is a subring of Z. Z has 1 as the identity but 2 Z doesnot have an identity.

(c) $M_2(\mathbf{R})$ is a ring with the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ The subring $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} / a \in \mathbf{R}\right\}$ has the identity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

(d) Example given in (c).

(e) Q is a field. Z is a subring of Q but Z is not a field.

Theorem 4.18. 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 $a - b$ and $ab \in A$ and B.

$\therefore\ a - b$ and $ab \in A \cap B$.

$\therefore\ A \cap B$ is subring of R (by Theorem 4.17).

Note.

1. The union of the two subrings of a ring need not be a subring.

2. The union of two subrings of a ring is again a subring iff one is contained in the other (proof as in theorem 3.20).

Definition. A non-empty subset S of a field $(F, +, \cdot)$ is called a subfield if S itself is a field under the same operations as in F.

Example.

1. $\mathbf{Q}$ is a subfield of $\mathbf{R}$
2. $\mathbf{R}$ is a subfield of $\mathbf{C}$.

Theorem 4.19. A non-empty subset S of a field F is a subfield iff

(i) $a, b \in S \Rightarrow a - b \in S$ and

(ii) $a, b \in S$ and $b \neq 0 \Rightarrow ab^{-1} \in S$.

The proof follows by applying Theorem 3.17 to the groups $(F, +)$ and $(F - (0), .)$.

Exercises

1. Prove that every subgroup of $(Z, +)$ is a subring of the ring of integers. (Hint: Any subgroup of $\mathbf{Z}$ is $n\mathbf{Z}$ for some n).
2. Prove that every subgroup of $(\boldsymbol{Z}_n, \oplus)$ is a subring of $(\mathbf{Z}_n, \oplus, \odot)$.
3. Find all the subrings of $\mathbf{Z}_8, \mathbf{Z}_{12}$ and $\mathbf{Z}_{13}$.

4.7. Ideals

Definition. 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 coincide.

Examples

1. In any ring, $R, \{0\}$ and R are ideals. They called improper ideals of R.
2. $\mathbf{2Z}$ is an ideal of $\mathbf{Z}$.

Proof. Let $a, b \in \mathbf{2Z}$. Then $a - b \in \mathbf{2Z}$. Let $a \in 2Z$ and $b \in Z$. Then ab is even and hence

ab∈ $2Z$. Thus $2Z$ is an ideal of Z.

In general $n\mathbf{Z}$ is an ideal of $\mathbf{Z}$

3. In $M_2(\mathbb{R})$ the set S 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 $B \in M_2(\mathbf{R})$.

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 $Ra = \{xa/x \in R\}$ 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. 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 (a).

Note. If R is a commutative ring with identity 1 then $a = a.1 \in (a)$. This may not be true if the ring R does not have an identity.

Example. Consider the ring 2 Z . Here $(4) = \{0, \pm,8, \pm16, \pm24, ...1\}$ and $4 \notin (4)$.

Remark.

(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.

Example.

$\mathbf{Z}$ is a subring of $\mathbf{Q}$ but $\mathbf{Z}$ is not an ideal of $\mathbf{Q}$ since $I \in \mathbf{Z}$ and $\frac{1}{2} \in \mathbf{Q}$ but $I \cdot \frac{1}{2} = \frac{1}{2} \notin Z$.

Theorem 4.20. Let R be a ring with identity 1 . If I is an ideal of R and $I \in I$, then $I = \mathbf{R}$.

Proof. Obviously $I \subseteq R$. Now, let $r \in R$.

Since $I \in I, r \cdot 1 = r \in I$. Thus $R \subseteq I$.

Hence $R = I$.

Theorem 4.21. Let F be any field. Then the only ideals of F are $\{0\}$ and F.

(ie.,) A field has no proper ideals.

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 theorem 4.20, $I = F$.

Theorem 4.22. Let R be a commutative ring with identity. Then R is a field iff R has no proper ideals.

Proof. If R is a field, by theorem 4.21, 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 element 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, $a = a \cdot 1 \in aR$.

$\therefore aR \neq \{0\}$. Since R has no proper ideals, $aR = R$.

Hence there exists $x \in R$ such that $ax = 1$.

Thus x is the inverse of a. Hence R is a field.

Definition. An integral domain R is said to be a principal ideal domain (PID) if every ideal of R is a principal ideal.

Examples

1. $\mathbf{Z}$ is a principal ideal domain since any ideal of $\mathbf{Z}$ is of the form $n\mathbf{Z}$.

2. Any field F is a principal ideal domain since the only ideals of F are (0) and (1) = F (by theorem 4.21).

Exercises

1. Show that intersection of two left ideals of a ring R is again a left ideal of R. Prove similar results for right ideals and ideals.

2. Let I_1 and I_2 be two ideals of R. Let $I_1 + I_2 = \{a + b/a \in I_1, b \in I_2\}$. Show that $I_1 + I_2$ is an ideal of R.

3. Determine which of the following statements are true and which are false.

(a) A subring of a commutative ring is commutative.

(b) A subring of a ring with identity is again a ring with identity.

(c) The identity element of a subring is the same as the identity element a the ring.

(d) The set of all non-singular 2 × d matrices is a subring of $M_2(\mathbf{R})$.

(e) Every subring of a ring R is an ideal of R.

(f) Every ideal of a ring R is a subring dR.

(g) $\mathbf{Z}$ is an ideal of $\mathbf{R}$.

(h) $\mathbf{Q}$ is an ideal of $\mathbf{R}$.

(i) $\{0,2\}$ is an ideal of $\mathbf{Z}_4$.

(j) $\{0,1\}$ is an ideal of $\mathbf{Z}_4$.

(k) In a commutative ring every left ideal is a right ideal.

(l) $\mathbf{R}$ has no proper ideals.

(m) $\mathbf{Q}$ is a principal ideal domain.

(n) Z is a principal ideal domain.

Answers.

3. (a) T (b) F (c)F (d) F (e) F (f) T (g)F (h) F (i) T (j) F (k) T (l) T (m) T

(n) T .

UNIT V

4.3. Isomorphism

Definition. 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 we write $R \approx R'$.

Note. 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

1. $f: \mathbf{C} \to \mathbf{C}$ defined by $f(z) = \bar{z}$ is an isomorphism. For, clearly f is a bijection.

Also

$$\begin{aligned} f(z_1 + z_2) &= \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \\ &= f(z_1) + f(z_2), \text{ and} \\ f(z_1 z_2) &= \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} = f(z_1) f(z_2). \end{aligned}$$

2. Let $\mathbf{C}$ 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 $a, b \in \mathbf{R}$. Then S is a ring under matrix addition and matrix multiplication. Refer example 14 in 4.1. Now the mapping $f: \mathbf{C} \to S$ 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 $y = c + id$.

Similarly, $f(xy) = f(x)f(y)$.

3. The groups $(\mathbf{Z},+)$ and $(2\mathbf{Z},+)$ are isomorphic under the map $f: \mathbf{Z} \to 2\mathbf{Z}$, given by $f(x) = 2x$.

However f is not an isomorphism of the ring $(Z,+)$ to $(2Z,+,\cdot)$ 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 $(\mathbf{Z},+,\cdot)$ and $(2\mathbf{Z},+,\cdot)$ (verify).

Exercises

1. In $\mathbf{2Z}$ we define $\boldsymbol{a} * \boldsymbol{b} = \frac{1}{2}\boldsymbol{ab}$. Show that $(2Z_t+,*)$ is a ring isomorphic to $(Z,+,\cdot)$.
2. Let S be the set of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ where $a \in \mathbf{R}$. Show that $f: \mathbf{R} \to s$ given by $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is an isomorphism.
3. Verify whether $f: \mathbf{R} \to \mathbf{R}$ given by $f(x) = -x$ is an isomorphism.

4.8. 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 $(R,+)$.

$R/I = \{I + a/a \in R\}$ is a group under the operation defined by

$(I + a) + (I + b) = I + (a + b)$.

To make R/I a ring, define a multiplication in $R/I$by $(I + a)(I + b) = I + ab$.

But we have to prove that this multiplication is well defined (ie.,) it is independent of the choice of the representatives from the casets. We shall prove that this happens iff I is an ideal.

Theorem 4.23. 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 iff I is an ideal of R.

Proof. Let I be an ideal of R.

To prove multiplication is well defined,

let $I + a_I = I + a$ and $I + b_I = I + b$.

Then $a_1 \in I + a$ and $b_1 \in I + b$.

$a_1 = i_1 + a$ and $b_1 = i_2 + b$ where $i_1, i_2 \in I$.

Hence $ab_1 = (i_1 + a)(i_2 + b) = i_1 i_2 + i_1 b + a i_2 + ab$.

Now since I is an ideal we have $i_1 i_2, i_1 b, a i_2 \in I$.

Hence $a_1 b_1 = i_3 + ab$ where $i_3 = i_1 i_2 + i_1 b + a i_2 \in I$. $\therefore a_1 b_1 \in I + ab$.

Hence $I + ab = I + a_1 b_1$.

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, $I + \text{ir} = (I + i)(I + r) = (I + 0)(I + r) = I + 0r = I$.

$\therefore$ ir $\in I$. Similarly, $ri \in I$.

Hence I is an ideal.

Definition. 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

1. The subset $I = \{0,3\}$ of $\mathbf{Z}_6$ is an ideal

$Z_6/I = \{I, I + 1, I + 2\}$ is a ring isomorphic to Z_3.

Here $\mathbf{Z}_6$ is not an integral domain but the quotient ring $\mathbf{Z}_6/I$ is an integral domain.

2. The subset $p\mathbf{Z}$ where p is prime is an ideal of the ring $\mathbf{Z}$.

$\mathbf{Z}/p\mathbf{Z} = (p\mathbf{Z}, p\mathbf{Z} + 1 \ldots \ldots, p\mathbf{Z} + (p - 1))$. It is easy to see that the ring $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{Z}_p$. Here Z is an integral demain but not a field whereas Z/pZ is a field.

Exercises

1. Determine which of the following statements are true and which are false.

Let R be a ring and I an ideal of R. Then,

(a) R is commutative $\Rightarrow$ R/I is commutative.

(b) R/I is commutative $\Rightarrow$ R is commutative.

(c) R is a ring with identity $\Rightarrow$ R/I is a ring with identity.

(d) R/I is a ring with identity $\Rightarrow$ R is a ring with identity.

(e) R is an integral domain $\Rightarrow$ R/I is an integral domain.

(f) R/I is an integral domain $\Rightarrow$ R is an integral domain.

(g) R is a field $\Rightarrow$ R/I is a field.

(h) R/I is a field $\Rightarrow$ R is a field.

Answers.

1. (a) T (b) F (c) T (d) F (e) F (f) F (g) F (h) F

4.9. Maximal and prime ideals

Definition. 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** properly containing $M. M \subseteq U \subseteq R \Rightarrow U = M$

Examples

1. (2) is a maximal ideal in **Z**. For, let U be an ideal properly containing (2).

$\therefore$ U contains an odd integer say, $2n + 1$.

$\therefore$ $1 = (2n + 1) - 2n \in U$.

$\therefore$ $U = \mathbf{Z}$ (by theorem 4.20).

Thus there is no proper ideal of **Z** properly containing (2). Hence (2) is a maximal ideal of **Z**.

2. Let p be any prime. Then (p) is maximal ideal in **Z**.

Let U be any ideal of **Z** such that $(p) \subseteq U$. Since every ideal of **Z** is a principal ideal $U = (n)$ for some $n \in \mathbf{Z}$.

Now, $p \in (p) \subseteq U \Rightarrow p \in U = (n)$.

$\therefore$ $p = nm$ for some integer m.

Since p is prime either $n = 1$ or $n = p$.

Suppose $n = 1$. Then $U = \mathbf{Z}$.

Suppose $n = p$. Then $U = (p)$.

$\therefore$ There is no proper ideal of **Z** properly containing (p). Hence (p) is a maximal ideal in **Z**.

3. (4) is not a maximal ideal in **Z**. For, (2) is proper ideal of **Z** properly containing (4).

Theorem 4.24. Let R be a commutative ring identity. An ideal M of R is maximal iff R/M_{ij} 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 such 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 $m = 0a + m \in U$.

$\therefore$ $M \subseteq U$.

Also $a = 1a + 0 \in U$ and $a \notin M$.

$\therefore$ $M \neq U$.

$\therefore$ U is an ideal of R properly containing M.

But M is a maximal ideal of R.

$\therefore$ $U = R$. Hence $1 \in U$.

$\therefore$ $1 = ba + m$ for some $b \in R$.

Now, M+1=M+ba+m=M+ba (since m∈M)

= (M+b)(M+a)

Hence $M + b$ is the inverse of $M + a$.

Thus every non-zero element of R/M h inverse.

Hence R/M is a field.

Conversely, suppose R/M is a field.

Let U be any ideal of R properly containing M.

$\therefore$ There exists an element $a \in U$ such that $a \notin M$.

$\therefore$ $M + a$ is a non-zero element of R/M.

Since R/M is a field $M + a$ has an inverse, say $M + b$.

$\therefore (M + a)(M + b) = M + 1$.

$\therefore$ $M + ab = M + 1$.

$\therefore$ $1 - ab \in M$.

But $M \subseteq U$. Hence $1 - ab \in U$.

Also $a \in U \Rightarrow ab \in U$.

$\therefore$ $1 = (1 - ab) + ab. \in U$. Thus $1 \in U$.

$\therefore$ $U = R$. Thus there is no proper ideal of R properly containing M. Hence M is a maximal ideal in R.

Definition. Let R be a commutative ring. An ideal $P \neq R$ is called a prime ideal if $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

Examples

1. Let R be an integral domain. Then (0) is a prime ideal of R.

For, $ab \in (0) \Rightarrow ab = 0$

$\Rightarrow a = 0$ or $b = 0$(since R is an I.D.)
$\Rightarrow a \in (0)$ or $b \in (0)$.

2. (3) is a prime ideal of **Z**.

For, $ab \in (3) \Rightarrow ab = 3n$ for some integer n.

$\Rightarrow 3 \mid ab$
$\Rightarrow 3 \mid a$ or $3 \mid b$
$\Rightarrow a \in (3)$ or $b \in (3)$.

$\therefore$ (3) is a prime ideal.

Note. In fact for any prime number p, the ideal (p) is a prime ideal in **Z**.

(4) is not a prime ideal in **Z** since $2 \times 2 \in (4)$. But $2 \notin (4)$.

Theorem 4.25. 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.

$\therefore$ R/P is 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 $P + ab = P$.

$\therefore$ $(P + a)(P + b) = P$.

$\therefore$ $P + a = P$ or $P + b = P$. (since R/P has no zero-divisors)

$\therefore\ a \in P$ or $b \in P$.

$\therefore\ P$ is a prime ideal of R.

Corollary. 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.

$\therefore\ R/M$ is a field. (by theorem 4.24)

$\therefore R/M$ is an integral domain. (by theorem 4.8)

$\therefore\ M$ is a prime ideal. (by theorem 4.25)

Note. The converse of the above statement is not true. For example, (0) is a prime ideal of **Z** but not a maximal ideal of **Z**.

Exercises

1. Prove that in **Z**, (6) is not a maximal ideal.
2. Prove that for any composite number n, the ideal (n) is not a maximal ideal of **Z**.
3. Prove that (n) is a maximal ideal in **Z** iff n is a prime number.
4. Prove that (4) is a maximal ideal but not a prime ideal in the ring of even integers.
5. Find all prime ideals and maximal ideals of $\mathbf{Z}_{12}$.
6. Let R be a finite commutative ring with identity. Prove that every prime ideal of R is a maximal ideal of R.

Answers.

5.(2) and (3) are prime ideals and also maximal ideals.

4.10. Homomorphism of rings

Definition. 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.

1. Obviously an isomorphism of a ring is a homomorphism and a $1-1$, onto homomorphism is an isomorphism.
2. Condition (i) of ring homomorphism says that f is a group homomorphism from the additive group ($R, +$) to the additive group ($R', +$).

Examples

1. $f: R \to R'$ defined by $f(a) = 0$ for all $a \in R$ is obviously a homorphism. 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. $f: \mathbf{Z} \to \mathbf{Z}_n$ defined by $f(x) = r$ where $x = qn + r, 0 \leq r < n$ is a homomorphism.

For, let $a, b \in \mathbf{Z}$.

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 ring homomorphism. Φ is called the natural homomorphism.

$$\Phi(x+y) = I + (x+y)$$
$$= (I+x) + (I+y)$$
$$= \Phi(x) + \Phi(y).$$

$$\Phi(xy) = I + xy$$
$$= (I+x)(I+y)$$
$$= \Phi(x)\Phi(y).$$

Hence Φ is a ring homomorphism.

Theorem 4.26. Let R and R' be rings and $f: R \to R'$ tee 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 a 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) follow from Theorem 3.55

(iii) Since S is a subring of R, $(S, +)$ is a subgroup of $(R, +)$.

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 $a, b \in S$.

$\therefore\ a'b' = f(a)f(b) = f(ab) \in f(S)$.

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 $a'r' \in f(S)$.

Let $r' = f(r)$ 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 $f(a), f(b) \in S'$.

$\therefore\ f(ab) = f(a)f(b) \in S'$ (since S' is a subring of R).

$\therefore\ ab \in f^{-1}(S')$.

Hence $f^{-1}(S')$ is a subring of R.

(vi) Proof is similar to that of (v).

(vii) Let R be a ring with identity l. 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 $f(R)$.

(viii) Proof is left to the reader.

Definition. The kernel K of a homomorphism f of a ring R to a ring R' is defined by $\{a/a \in R$ and $f(a) = 0\}$.

Theorem 4.27. 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 4.26, K is an ideal of R.

Theorem 4.28. (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 $R/K \approx R'$.

Proof. Define $\Phi: R/K \to R'$ by $\Phi(K + a) = f(a)$.

(i) To prove Φ is well defined,

Let $K + b = K + a$. Then $b \in K + a$.

$\therefore\ b = k + a$ where $k \in K$.

$$\therefore f(b) = f(k + a) = f(k) + f(a)$$
$$= 0 + f(a) = f(a)$$

$\therefore\ \Phi(K + b) = f(b) = f(a) = \Phi(K + a)$

(ii) To prove Φ is 1-1

$\phi(K + a) = \phi(K + b) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a) - f(b) = 0$

$\Rightarrow f(a) + f(-b) = 0$

$\Rightarrow f(a - b) = 0$

$\Rightarrow a - b \in K$

$\Rightarrow a \in K + b$

$\Rightarrow K + a = K + b$

(iv) To prove Φ is onto

Let $c' \in R'$. Since f is omo, there exists $a \in R$ such that $f(a) = a'$. Hence $\phi(K + a) = f(a) = a'$.

(iv) To prove Φ is homomorphism

$$\begin{aligned}\Phi[(K + a) + (K + B] &= \Phi[K + (a + b)] \\ &= f(a + b) \\ &= f(a) + f(b) \text{ (since f is homomorphism)} \\ &= \Phi(K + a) + \Phi(K + b).\end{aligned}$$

and $\Phi[(K + a)(K + b)] = \Phi(K + ab)$= f(ab)= f(a) f(b)= Φ(K + a)Φ(K + b)

Hence Φ is an isomorphism.

Hence $\frac{R}{K} \cong R'$

Solved Problems

Problem 1. The homomorphic image of an integral domain need not be an integral domain.

Solution. $f: \mathbf{Z} \to \mathbf{Z}$ defined by $f(a) = r$ where $a = 4q + r, 0 \leq r < 4$ is a homomorphism of Z_4 onto Z_4. Here Z is an integral domain and Z_4 is not me instral damain since 2 $\odot 2 = 0$

Problem 2. Any homomorphism of a field to itself is either one-one or maps every element to 0 **Solution.** Let F be a field and $f: F \to F$ be a by-omophism. Let K be the kernel of f. Then K is an ideal of F. By theorem 4.21, $K = \{0\}$ or $K = F$.

If $K = [0]$ then f is $1 - 1$.

If $K = F$. then $f(a) = 0$ for all $a \in F$.

Exercises

1. If R, R', R'' are rings and if $f: R \to R'$ and $g: R' \to R''$ are homomorphisms, then $g \circ f: R \to R''$ is a homomorphism.
2. Let R, R' be rings and $f: R \to R'$ be a epimorphism. Then if R is a skew field, so is R'.
3. Determine which of the following are homomorphisms. If so find the kernel.

(a) $f: \mathbf{C} \to \mathbf{C}$ defined by $f(z) = \bar{z}$

(b) $f: \mathbf{Z} \to \mathbf{Z}$ defined by $f(a) = 2a$.

(c) Let $R = (m + n\sqrt{2}/m, n \in \mathbf{Z})$. R is a ring under usual addition and multiplication.

Define $f: R \to R$ by $f(m + n\sqrt{2}) = m - n\sqrt{2}$.

(d) $f: \mathbf{C} \to M_2(\mathbf{R})$ defined by $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

(e) $f: \mathbf{Z} \to \mathbf{Z}_n, f$ as defined in example 4 of section 4.10.

(f) $f: \mathbf{Z} \to \mathbf{Z}$ defined by $f(x) = x^2 + 3$

4. Determine which of the following are true and which are false.

(a) Every homomorphism is an isomorphism.

(b) Every isomorphism is a homomorphism.

(c) A homomorphism is 1-1 iff its kernel is $\{0\}$.

(d) In a ring homomorphism, identity element is mapped into identity.

(e) A homomorphic image of an integral domain is an integral domain.

(f) A homomorphic image of a skewfield is a skewfield.

(g) Homomorphic image of a field is a field.

(h) If $f: R \to R'$ is a homomorphism and R is commutative then R' is commutative.

Answers.

3. (a) $\text{Ker} f = \{0\}$ (b) Not a homomorphism

(c) $\text{Ker} f = \langle 0 \rangle$ (d) $\text{Ker} f = \{0\}$

(e) $\text{Ker} f = n\mathbf{Z}$ (f) Not a homomorphism.

4. (a) F (b) T (c) T (d) F (e) F (f) F (g) F (h) F .

4.11. Field of quotients of an integral domain

The construction of the quotient field of an integral domain :

Every element of $\mathbf{Q}$ can be expressed as a quotient p/q where $p, q \in \mathbf{Z}$ and $q \neq 0$. Further the two fractions $2/3$ and $4/6$ represent the same rational number.

In general, two fractions a/b and c/d. where $b, d \neq 0$ represent the same rational number iff $ad = bc$. Also $(a/b) + (c/d) = (ad + bc)/bd$ and $(a/b)(c/d) = ac/bd$. The elements of $\mathbf{Z}$ can be thought of as fractions of the form $a/1$.

The construction of the field of quotients F of an integral domain D is carried out in the following four stages

(i) Specify the elements of F.

(ii) Define addition and multiplication in F.

(iii) Show that F is a field under these operations.

(iv) D can be embedded in F.

Stage (i) Let D be an integral domain.

Let $S = \{(a,b)/a,b \in D \text{ and } b \neq 0\}$.

The ordered pair (a,b)can be represent as a formal quotient a/b.

For example, if $D = \mathbf{Z}$, the pair $(1,2)$ will eventually represent the fraction $1/2$.

Definition. Two elements (a,b) and $(c,d) \in S$ are defined to be equivalent iff $ad = bc$. If (a,b) is equivalent to (c,d) we write $(a,b) \sim (c,d)$.

Lemma 1. $\sim$ is an equivalence relation in S.

Proof. Let $(a,b) \in S$.

$(a,b) \sim (a,b)$ since $ab = ba = ab$.

Hence $\sim$ is reflexive.

Now, $(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b)$.

Hence $\sim$ is symmetric.

Now, let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

Now to prove that $(a,b) \sim (e,f)$ we must prove that $af = be$.

Case (i) Let $c = 0$. Now, $ad = bc$ and $cf = de$.

$\therefore\ ad = 0$ and $de = 0$.

But $d \neq 0$. Hence $a = 0$ and $e = 0$.

$\therefore\ af = be = 0$.

Case(ii) Let $c \neq 0$.

We have $ad = bc$ and $cf = de$.

$\therefore\ adcf = bcde$.

$\therefore\ af = be$ (by cancellation law)

$\therefore\ \sim$ is transitive.

Hence $\sim$ is an equivalence relation on S.

Consider the equivalence class containing (a,b). Let it be denoted by $\frac{a}{b}$.

Let $F = \left\{\frac{a}{b} / (a, b) \in S\right\}$.

Stage (ii) Let $\frac{a}{b}, \frac{c}{d} \in F$.

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Since D is an integral domain and $b, d \neq 0$, we have $bd \neq 0$.

$\therefore \frac{ad + bc}{bd}$ and $\frac{ac}{bd} \in F$.

Lemma 2. Addition and multiplication defined above are well defined.

Proof. Let $(a_1, b_1) \in \frac{a}{b}$ and $(c_1, d_1) \in \frac{c}{d}$.

$a_1 b = b_1 a$ and $c_1 d = d_1 c$.....(1)

$a_1 bdd_1 = b_1 add_1$ and $c_1 dbb_1 = d_1 cbb_1$

$(a_1 d_1 + b_1 c_1)bd = (ad + bc)b_1 d_1$

$\frac{ad + bc}{bd} = \frac{a_1 d_1 + b_1 c_1.}{b_1 d_1}$

$\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}$

$\therefore$ Addition is well defined.

Also from (1), $a_1 bc_1 d = b_1 ad_1 c$.

$\therefore (ac, bd) \sim (a_1 c_1, b_1 d_1)$.

$\therefore \frac{a}{b} \cdot \frac{c}{d} = \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}$.

$\therefore$ Multiplication is well defined.

Lemma 3. Stage (iii) F is a field with the addition and multiplication defined above.

Proof. It can easily be verified that addition is commutative and associative.

$\frac{0}{1}$ is the zero of F and $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

$\therefore (F, +)$ is an abelian group.

Clearly multiplication is commutative and associative. $\frac{1}{1}$ is the identity of F.

If $\frac{a}{b}$ is a non-zero element of F, then $a \neq 0$.

$\therefore \frac{b}{a} \in F$ and is the inverse of $\frac{a}{b}$.

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+de}{df}\right)$$
$$=\frac{acf+ade}{bdf}$$
$$=\frac{acfb+adeb}{bdfb}$$
$$=\frac{ac}{bd}+\frac{ae}{bf}$$
$$=\frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}$$

$\therefore$ F is a field.

Stage The field F contains a subring R which is isomorphic to D.

Lemma 4. The map $f: D \to F$ given by $f(a)=\frac{a}{1}$ is an isomorphism of D onto $f(D)$.

Proof. Let $a, b \in D$.

Then $f(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=f(a)+f(b)$ and

$f(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}=f(a)f(b)$.

To prove f is 1-1.

$$f(a)=f(b) \Rightarrow \frac{a}{1}=\frac{b}{1}$$
$$\Rightarrow (a,1)\sim(b,1)$$
$$\Rightarrow a1=1b$$
$$\Rightarrow a=b.$$

$\therefore$ f is an isomorphism.

Thus we have proved the following.

Theorem 4.29. Any integral domain D can be embeded in a field F and every element of F can be espersed as a quotient of two elements of D.

Definition. The field F which we have constructed above is called the field of quotients of D.

Theorem 4.30. The field of quotients F of an integral domsin D is the smallest field containing D.

(ie.,) If F is any other field containing D then F' contains a subfield isomorphic to F.

Proof. Let $a, b \in D$ and $b \neq 0$.

Then $a, b \in F'$ and since F' is a field $ab^{-1} \in F'$. Now, let F be the quotient field of D.

We define $f: F \to F'$ by $f\left(\frac{a}{b}\right) = ab^{-1}$.

f is well defined; for, let $(a_1, b_1) \sim (a, b)$.

Then $a_1 b = b_1 a$. Hence $a_1 b_1^{-1} = ab^{-1}$,

To prove f is 1-1

$f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right) \Rightarrow ab^{-1} = cd^{-1} \Rightarrow ad = bc \Rightarrow a/b = c/d$

Now, let $a/b, c/d \in F$.

Then $f\left[\left(\frac{a}{b}\right) + \left(\frac{c}{d}\right)\right] = f[(ad + bc)/bd] = (ad + bc)(bd)^{-1} = (ad + bc)d^{-1}b^{-1}$

$$= ab^{-1} + cd^{-1} = f(a/b) + f(c/d)$$

Also, $f[(a/b)(c/d)] = f[(ac)/(bd)] = (ac)(bd)^{-1} = acd^{-1}b^{-1} = ab^{-1} \cdot cd^{-1}$

$$= f(a/b)f(c/d)$$

Thus F is isomorphically embedded in F'.

Solved problems

Problem 1. Describe the quotient field of the integral domain $D = \{a + b\sqrt{2}/a, b \in \mathbf{Z}\}$.

Solution. The set of real numbers R is a field containing the given integral domain D.

Hence by theorem 4.30, R contains a subfield isomorphic to the field of quotiens of D.

This subfield is precisely the set of all real numbers of the form $(a + b\sqrt{2})/(c + d\sqrt{2})$

where $c + d\sqrt{2} \neq 0$.

$(a + b\sqrt{2})/(c + d\sqrt{2})$ is of the form $p + q\sqrt{2}$ where p and q are rational numbers.

Thus the quotient field of D is $\{p + q\sqrt{2}/p.q \in \mathbf{Q}\}$.

Problem 2. If D and D' are isomorphic integral domains then their quotient fields are also isomorphic.

Solution. Let $f: D \to D'$ be an isomorphism. Let F and F' be the quotient fields of D and D' respectively. Consider $\Phi: F \to F'$ given by $\Phi(a/b) = f(a)/f(b)$. Φ is an isomorphism of F onto F'

Exercises

1. Show that the field of quotients of any field is itself.

2. Let R be a ring which may or may not have a unit element. In $\mathbf{Z} \times R$ we define $(n, r) + (m, s) = (n + m, r + s)$ and $(n, r)(m, s) = (nm, mr + ns + rs)$ [Notice that since m and n are integers mr and ns are meaningful]. Prove that S is a ring with identity and R can be embedded in S. [This shows that any ring can be embedded in a ring with identity].

3. Determine which of the following statements are true and which are false.

(a) **R** is a field of quotients of **R**.

(b) **Q** is a field of quotients of **Z**.

(c) **R** is a field of quotients of **Z**.

(d) If D is any field then the field of quotients of D is isomorphic to D.

Answers.

3. (a) T (b) T (c) F (d) T .

Study Learning Material Prepared by

Dr. A. MALLIKA M.Sc. , M.Phil., Ph.D

ASSISTANT PROFESSOR

DEPARTMENT OF MATHEMATICS

SADAKATHULLAH APPA COLLEGE(AUTONOMOUS)

TIRUNELVELI -627011

TAMILNADU, INDIA