SCSVMV

Department of Mathematics

COURSE MATERIAL

III BSC - ABSTRACT ALGEBRA

Dr T N KAVITHA

Abstract algebra

L	P	T	C
4	0	1	4

Unit I

Definition of groups- examples- elementary properties- equivalent definitions- cyclic groups- order of an element.

Unit II

Subgroups - Cosets and Lagrange's theorem- normal subgroups – quotient groups- homomorphism.

Unit III

Isomorphism-automorphism- Cayley's theorem- permutations – transpositions, cycles – odd and even permutations - permutation groups – symmetric group S_n

Unit IV

Rings- definition and examples- elementary properties of rings- characteristic of a ring – integral domain - Homomorphism of a rings

Unit V

subrings- ideals and quotient rings- prime ideal – maximal ideal- field of quotients of an integral domain- ordered integral domain- field-Definition and examples.

Recommended Text

I.N.Herstein. Topics in Algebra, (2nd Edn.) Wiley Eastern Ltd. New Delhi

Reference Books

1. S.Arumugam. *Modern Algebra.* Scitech Publications, Chennai.

2. J.B.Fraleigh *A First Course in Algebra* (3rd Edition) Addison Wesley, Mass. (Indian Print)

3. Lloyd R.Jaisingh and Frank Ayres,Jr. *Abstract Algebra,* (2nd Edition), Tata McGraw Hill Edition, New Delhi.

4. M.L.Santiago *Modern Algebra,* Tata McGraw Hill, New Delhi.

5. Surjeet Singh and QaziZameeruddin. *Modern Algebra*. Vikas Publishing House Pvt. Ltd. New Delhi.

ABSTRACT ALGEBRA

Unit I- Topics

Definition of groups- examples- elementary properties- equivalent definitions- cyclic groups - order of an element.

Chapter 1 : Basics of Groups

1.1 Binary operation:

A binary operation is a "way of putting two things together".

For example in the set N of natural numbers we can associate with any two elements a, b $\in$ N the unique element a + b $\in$ N. Again with any two sets, A,B $\in$ f(x) we can associate the set A $\cup$ B $\in$ f(x).

Here + in N gives rise to the function + : N $\times$ N -> N given by (a, b) -> a + b.

1.2 Definition

Let A be non - empty set. A binary operation * on A is a function *: A $\times$ A -> A. The image of an ordered pair (a, b) Ɛ A $\times$ A under * is denoted by a * b. A set A with a binary operation * defined on it is denoted by (A, *).

Examples

1. The usual addition + , is a binary operation on N, Z, Q, R and C.
2. On f(x), $\cup$,$\cap$, Δ and are binary operations
3. Let A = {0, 1, 2}. A binary operation * on A is given by 0*1 = 1*0 = 1; 0*2 = 2* 0 = 2; 1*2 = 2*1 = 0; 0*0 = 0; 1*1 = 2; 2*2 = 1.

If * is a binary operation on a finite set A containing n elements then the n^2 products a * b , a, b $\in$ A can be conveniently arranged in the form of a table containing n rows and n columns, the product a * b coming in the row along a and in the column along b. Thus the above binary operation on A is given by the table.

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Question to revise 1. Define Binary operation:

If f is a function from $G \times G \rightarrow$G,then f is said to be a binary operation on the set G.The image of the ordered pair (a,b) under the function f is denoted by a f b.

1.3 Algebraic structure

Yet despite this simplicity of description the fundamental algebraic concepts such as homomorphism, quotient construction, and the like, which play such an important role in all algebraic structures- in fact , in all of mathematics - already enter here in a pure and revealing form.

Question to revise2: Define .algebraic structure:

A non-empty set G equipped with one or more binary operation is called an algebraic structure.

Examples: (N,+) (I,+) (I,-) (R,+,^{o}) are all algebraic structure.

1.4 Semi group:

Let us consider, an algebraic system (A, *), where * is a binary operation on A. Then, the system (A, *) is said to be semi-group if it satisfies the following properties:

1. The operation * is a closed operation on set A.
2. The operation * is an associative operation.

Example:

Consider an algebraic system (A, *), where A = {1, 3, 5, 7, 9....}, the set of positive odd integers and * is a binary operation means multiplication. Determine whether (A, *) is a semi-group.

Solution:

Closure Property: The operation * is a closed operation because multiplication of two +ve odd integers is a +ve odd number.

Question to revise3. Define Semi group:

An algebraic structure (G,*) is called a semi group if the binary operation * is associative in G. i.e) if (a*b)*c=a*(b*c) $\forall a, b, c \in G$.

Chapter 2: Elementary properties of Groups

2.1 Group

Modern algebra is largely concerned with the study of abstract sets endowed with one or more binary operations. 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 (Z, +) given below

(i) Addition is an associative binary operation in Z.

(ii) The element $0 \in Z$ is such that $a + 0 = 0 + a = a$ for all $a \in Z$.
Hence 0 is the identity element with respect to addition.

(iii) Let $a \in Z$. The element $-a \in Z$ is such that $a + (-a) = (-a) + a = 0$.
Hence -a is the inverse of a.

Question to revise3.: Define Group:

The algebraic structure (G,*) is a group if the binary operation * satisfies the following postulates:

i)closure property
ii)Associative property
iii)Existence of identity
iv)Existence of inverse

2.2 Definition:

Let G be a non-empty set with a binary operation *. G is called a group if the following axioms are satisfied.

Closure Property : For any two elements a, b ∈ G ,a*b ∈ G

Associative law : For any three elements a, b, c ∈ G, a* (b*s) = (a* b)* c

Identity : For any element a ∈ G , there exists an element e ∈ G such that

a* e = e* a = a , e is called identity element in G.

Inverse : For any element a ∈G , there exists an element a' ∈ G such that a* a' = a'* a = e

a' is called inverse of a.

Note :

If the above axioms are satisfied we say that (G, *) is a group.

Examples of group

1. The set Z of all integers is a group with respect to the operation addition.
2. The set Q of all rational numbers is a group with respect to addition.
3. The set R of all real numbers is a group with respect to addition.
4. The set C of all complex number is a group with respect to addition.
5. The set of all non-zero rational numbers Q -{0) is a group with respect to multiplication.
6. The set of all non-zero real numbers R - {0) is a group with respect to multiplication.
7. The set of all non-zero complex numbers C-{0) is a group with respect to multiplication.
8. The set of all non-zero integers is not a group with respect to multiplication since integers do not possess inverse with respect to multiplication.

2.3 Properties of Group

2.3.1 Property

The identity element in a group (G, *) is unique.

Proof:

If possible, let e_1 and e_2 be two identity elements in a group (G, *)

Considering $e_1$as identity element,

$e_2 * e_1 = e_1 * e_2 = e_2$.....(1)

Considering e_2 as identity element,

$e_1 * e_2 = e_2 * e_1 = e_1$.....(2)

From (1) and (2), we have $e_1 = e_2$. Hence there can be only one identity element in a group

i.e., Identity element in a group is unique.

2.3.2 Property

The inverse of an element in a group is unique.

Solution :

Let (G, *) be a group and e be the identity element. Let a be any element in it. If possible, let and a'anda" be the inverses of a.

Then a* a' = a'* a = e

a* a" = a"* a = e

In a group, associative law is true.

i.e., a' * (a* a") = (a' * a)* a"

i.e., a'* e = e* a"

i.e., a' = a"

There is only one inverse for each element of a group. i.e., the inverse of an element in a group is unique.

2.3.3 Note : The inverse of an element is also denoted by a^{-1} .

2.3.4 Property :(Cancellation laws)

Prove that in a group, for any three elements in G ;

(i) a* b = a* c⇒ b = c (Left cancellation law)

(ii) (ii) b* a = c* a ⇒b = c (Right cancellation law)

Proof:

Let a ' be the inverse of a.

(i) a* b = a* c ⇒a'*(a*b)=a'*(a*c)

⇒(a'* a)* b = (a'* a)* c (Associative law)

⇒e* b = e* c ⇒b = c .

(ii) b* a = c* a ⇒(b* a)* a' = (c* a)* a'

⇒b*(a*a') = c*(a* a')

⇒b* e = c* e ⇒ b = c

2.3.5 Property

Let G be a group and a, b ∈ G . Show that the equations a* x = b and y*a =b have unique solution in G.

Proof :

First let us prove that there is a unique solution for the equation a* x = b . Let us suppose that there are two solutions for x in G, say x = x_1 and x = x_2. Then

a* x_1 =b and a*x_2 =b

a* x_1 = a*x_2

∴By cancellation law, $x_1 = x_2$

i.e., the solution for x is unique. Now let us find the solution.

Let a', be the inverse of a.

a* x = b⇒ a'*(a*x)= a'*b

⇒(a'* a)* x = a'*b

⇒e* x = a'*b

⇒x = a'*b

∴x = a'*b is the solution of the equation a* x = b

If $y_1$and y_2 are the solutions of y* a =b , then y_1 *a = b and y_2 *a =b

∴y_1 * a and y_2*a and ∴y_1= y_2(By Cancellation law)

Also (y* a)*a' = b* a'

y*(a* a') = b* a'

y* e = b* a'

i. e., y = b* a'

2.3.6 Property (Reversal Law)

In a group G, for any two elements a, b ∈ G , the inverse of the product is equal to the product of the inverse in the reverse order. i.e., (a*b)' = b'* a'

Proof:

For any two elements x, y ∈ G to be the inverses of each other, we have to show that

x* y = y* x = e

We want to prove b'* a' is the inverse of a* b . For this we have to prove that

(a* b)*(b' *a')= e

and (b'*a')*(a*b) = e

Now (a* b) * (b' * a')

= a*(b* b')* a' (Associative law)

= (a* e)* a'

= a* a' = e ----------(1)

Also (b'*a')*(a*b) = b' * (a'* a)* b

= b'*(e*b)

= b'* b =e ----------(2)

From (1) and (2),

b',* a', is the inverse of a* b

∴(a* b)' = b'* a'

2.3.7 Note: This result can be generalized for n elements a_1, $a_2 a_n$,∈ G ,

i.e., (a_1*a_2 * ..... * a_n)' = a'_n *a'_{n-1}……..*a'

2.3.8 Property

The inverse of an inverse of an element in a group is the element itself, i.e., (a')' = a .

Proof:

Let a'' be the inverse of a' .

Then a'* a'' =a''*a' = e ----------(1)

Since a' is the inverse of a,

a* a' = a'*a = e ----------(2)

From (1) and (2),

a'*a'' = a'*a By cancellation law, a'' = a

i. e., (a')' = a

Chapter 4: Equivalent definitions of a group

4.1.1 Definition

Let * be a binary operation defined on G. an element e ∈ G is called a left identity if e * a = a for all a ∈ G. e is called a right identity if a ∗ e = a for all a ∈ G.

4.1.2 Example

1. in C we define z ° z = |z |z . Here all elements z such that |z| = 1 are left identities.

2. In R we define a * b = ab^2 . Here 1 and -1 are right identities.

3. In N we define a * b = a. Here every element is a right identity.

4.1.3 Definition

Let * be a binary operation defined on G. Let e ∈ G be the identity element. Let a ∈ G. An element a' ∈ G is called a left inverse of a if a' * a = e. a' is called a right inverse of a if a * a' = e.

4.1.4 Note

The identity element e of a group G is both a left identity and a right identity. The inverse of any element a ∈ G is both a left inverse and a right inverse.

4.1.5 Theorem

A semigroup G contains left identity e and a left inverse a' for every a, e in G, then G is a group.

Proof

a' is a left inverse of a so that a'a = e.

let a'' be a left inverse of a' so that a''a' = e

then aa' = e(aa') [since e is left identity]

= (a''a')(aa') = a''(a'a)a' [associative]

= a'' (ea') = a''a' [since e is left identity]

= e. Hence a' is also a right inverse of a .

Also a = ea = (aa')a = a(a'a) = ae. Hence e is also a right identity.

Thus ea = a = ae and a'a = aa' = e and for all a ∈ G. Hence G is a group.

4.1.6 Theorem

A semigroup G contains right identity e and right inverse a' with respect to e for every element a, e in G, then G is a group.

The proof is similar to previous theorem.

4.1.7 Note

If G is a semigroup with respect the operation * defined on it such that there exists a left identity and a right inverse for each element, then (G, *) need not be a group.

For example, consider (R, *) where a * b = |a|b.

Clearly * is a binary operation on R^*.

Now, a * (b*c) = (a * b) * c = |a| |b| c and hence * is associative.

(-1) * a = |-1|a = a. Hence -1 is a left identity.

Now, when a < 0 ; a * (1/a) = |a|(1/a) = (-a)(1/a) = -1 and

when a > 0; a * (-1/a) = |a|(-1/a) = (a) (-1/a) = -1.

Hence if a < 0 , (1/a) is the right inverse of a and if a > 0, (-1/a) is the right inverse of a. However $(R^*, *)$ is not a group since the equation y * a = a has two solutions namely 1 and -1.

4.1.8 Theorem

Let G be semigroup such that the equation ax = b and ya = b have unique solutions for x and y in G. Then G is a group.

Proof

Let $a \in G$. Then there exists a unique $e \in G$ such that ea = a.

Now, let b be any other element in G. Then there exists a unique x in G such that ax = b

Now, eb = e(ax) = (ea)x = ax = b

eb = b for all $b \in G$ so that e is a left identity.

Let $a \in G$. Then ya = a has a unique solution a'.

a'a = e so that a' is the left inverse of a.

Hence by theorem 4.1.5, G is a group.

4.1.9 Theorem

Let G be a semigroup contains both cancellation laws. Then G is a group.

Proof

Let $G = \{ a_1, a_2, \ldots\ldots, a_n \}$

Now let $a, b \in G$

Consider the elements $aa_1, aa_2, \ldots\ldots aa_n$.

All these elements are distinct, for if $aa_r = aa_s$ then $a_r = a_s$ (by cancellation law).

Hence $aa_1, aa_2, \ldots\ldots aa_n$ are just the elements $a_1, a_2, \ldots\ldots a_n$ of G in some order and hence $aa_i = b$ for some i.

Thus the equation ax = b has a unique solution for x in G. Similarly taking the elements $aa_1, aa_2, \ldots\ldots aa_n$ we can prove that the equation ya = b has a unique solution for y in G.

Hence by previous theorem, G is a group.

4.1.10 Note

The above theorem is not true if G is infinite. For example, consider (N, +). Clearly N+ is a semigroup and both cancellation laws hold good in N. But (N, +) is not a group.

Chapter 5:Cyclic groups

5.1 Definition.

Let G be a group, and let a be any element of G. The set

$\langle a \rangle = \{ x \in G \mid x = a^n \text{ for some } n \in Z \}$

is called the **cyclic subgroup** generated by a.
The group G is called a **cyclic group** if there exists an element $a \in G$ such that $G=\langle a \rangle$.
In this case a is called a **generator** of G.

5.2 Proposition.

Let G be a group, and let $a \in G$.

(a) The set $\langle a \rangle$ is a subgroup of G.
(b) If K is any subgroup of G such that $a \in K$, then $\langle a \rangle \subseteq K$.

5.3 Proposition.

Let a be an element of the group G.
(a) If a has infinite order, and $a^k = a^m$ for integers k,m, them k=m.
(b) If a has finite order and k is any integer, then $a^k = e$ if and only if $o(a) \mid k$.
(c) If a has finite order $o(a)=n$, then for all integers k, m, we have

$a^k = a^m$ if and only if $k \equiv m \pmod n$.

Furthermore, $|\langle a \rangle|=o(a)$.

5.4 Corollaries to Lagrange's Theorem (restated):

(a) For any $a \in G$, o(a) is a divisor of |G|.
(b) For any $a \in G$, $a^n = e$, for $n = |G|$.
(c) Any group of prime order is cyclic.

5.5 Theorem. Every subgroup of a cyclic group is cyclic.

5.6 Theorem. Let G cyclic group.

(a) If G is infinite, then $G \cong \mathbf{Z}$.
(b) If $|G| = n$, then $G \cong \mathbf{Z}_n$.

5.7 Proposition.

Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$.
(a) If $m \in \mathbf{Z}$, then $\langle a^m \rangle = \langle a^d \rangle$, where $d=\gcd(m,n)$, and a^m has order n/d.
(b) The element a^k generates G if and only if $\gcd(k,n)=1$.

(c) The subgroups of G are in one-to-one correspondence with the positive divisors of n.

(d) If m and k are divisors of n, then $\langle a^m \rangle \subseteq \langle a^k \rangle$ if and only if $k \mid m$.

5.8 Definition.

Let G be a group. If there exists a positive integer N such that $a^N=e$ for all $a \in G$, then the smallest such positive integer I is called the **exponent** of G.

5.9 Lemma.

Let G be a group, and let $a,b \in G$ be elements such that ab = ba. If the orders of a and b are relatively prime, then o(ab) = o(a)o(b).

5.10 Proposition.

Let G be a finite abelian group.

(a) The exponent of G is equal to the order of any element of G of maximal order.
(b) The group G is cyclic if and only if its exponent is equal to its order.

Question to revise20. Define cyclic groups:

A group G is called cyclic if for $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. The element a is then called a generator of G.

Chapter 6: Finite and infinite groups :

A group which contains only finite number of elements is called a finite group. A group which is not finite is called an infinite group.

6.1 Order of an Group :

The number of elements in a group is called the order of the group and is denoted by O(G). In the case of a finite group the order is finite and the order of an infinite group is infinity.

6.2 Integral power of an element :

Let G be a group and a be an element of G. For any positive integer n,

a .a .a ……..n times = a"

We note $(a^1)^{-1}$= (a .a . a ……n times$)^{-1}$

= $a^{-1}, a^{-1}a^{-1}$.....n times

=$(a^{-1})^n$

Ie.,$(a^n)^{-1}=(a^{-1})^n$

Also, we define for any element a, a°= e and $a^{-n} = (a^n)^{-1} = a^{-1})^n$

6.3 Order of an element in a group :

Let G be a group and a be any element in G. If there exists a least positive integer n such that a^n = e then n is called the order of the element a. It is denoted by o(a) = n

6.4 Congruent modulo n :

Let n be a positive integer. An integer a is said to be congruent modulo n to the integer b if and only if a - b is divisible by n i.e., a - b = r n where r is an integer. This is denoted by a ≡ b (modulo n)

6.5 Example

15 ≡3 (modulo 4)

15 =1 (modulo 7)

The different numbers congruent to 0 modulo 3 are

…….- 9, - 6, -3, 0, 3, 6, 9, …….

Numbers congruent to 1 modulo 3 are

…….-11, - 8, -5, - 2, 1, 4, 7, 10,……..

Numbers congruent to 2 modulo 3 are

……. -10, - 7, -4, -1, 2, 5, 8, 11, …….

6.6 Congruent classes modulo n :

The set of all integers congruent to a (modulo n) is denoted by [a] and its called the congruent class modulo n. The distinct congruent classes modulo 3 are

[0] = {…….. -9, -6, -3, 0, 3, 6, 9…….}= {x ∈z|x = 3k; k ∈z}

[1]= {…….-11, - 8, - 5, -2, 1, 4, 7, 10…… } = {x ∈ z|x = 3k +1; k∈ z}

[2] ={…… -10,-7, -4, -1, 2, 5, 8, 11 …..}= {x ∈z|x = 3k +2, k}

[3]= [0] =[3]= [9]=…….. [-3]= [-6]=……

The set of all congruent classes modulo 3 is denoted by

Z_3 = {[0], [1], [2]}

Similarly, Z_4= {[0], [1], [2], [3]}

Z_5 = [0], [1], [2], [3], [4]}

Addition modulo n of congruent classes

6.4 Definition :

Let [a], [b] $\in Z_n$,, . The addition modulo n of these two classes is defined by

$$[a] \quad +_n [b] = \begin{cases} [a + b] \text{ if } a + b < n \\ [r] \text{ if } a + b, \ z_n \text{ and r is the positive remainder} \\ \qquad \text{when a + b is divided by n} \end{cases}$$

$[a] +_n [b] = [a + b]$ if $a + b < n$

$[r]$

E.g., $[4] +_8 [5] = [4 + 5] = [9] = [1]$

6.5 Multiplication modulo n of congruent classes

Let [a], [b] $\in Z_n$The multiplication modulo n of these two classes is defined by

$$\{[a] \cdot_n [b] = \begin{cases} [ab] \text{ if } ab < n \\ [r] \text{ if } ab \geq n \text{ where r is the positive remainder} \\ \text{when ab is divided by n} \end{cases}$$

E.g., $[4] \cdot_8 [5] = [20] = [4]$

$[6] \cdot_8 [7] = [42] = [2]$

6.6 Example

The cube roots of unity form an abelian group under ordinary multiplication.

Solution :

1	**ω**	ω^2

The		**1**	1	**ω**	ω^2	cube roots of unity are 1, **ω**, ω^2. Let G =
{1,	**ω**,	**ω**	**ω**	ω^2	1	ω^2}
		ω^2	ω^2	1	**ω**	

Since **ω** is a cube root of unity, ω^3=1

Closure law :

From the multiplication table, we see that the set G is closed under multiplication.

Associative law :

Multiplication of complex numbers is always associative.

Identity :

From the table, we see that 1 is the identity element.

Inverse :

The inverses of 1, **ω**,ω^2 are ω^2, **ω** respectively. ∴All elements of G possess inverse in G.

Commutative law :

From the multiplication table, we see that multiplication is commutative. G is an abelian group under addition.

Abelian group : A group (G, *) is called an Abelian group (or commutative group) if it also satisfies the following axiom.

Commutative law : For any two elementsa, b ∈ G , a* b = b* a

Note : A non-empty set G with a binary operation is called an abelian group if all the axioms 1 to 5 are satisfied.

6.7 Abelian group

A group G is said to be abelian if ab = ba for all a, b ∈ G. A group which is not abelian is called non abelian group.

Example

1. Z, Q, R and C under usual addition are abelian groups.
2. (f(x), Δ) is an abelian group since A Δ B = B Δ A for all A, B ∈ f(x).
3. (Z_n, ⊕) is an abelian group

Question to revise 5. Define abelian group:

A group G is said to be abelian (or) commutative if $a * b = b * a \forall a, b \in G$

Question to revise6. Show that the set N of all natural number 1,2,3,4,5….. is not a group with respect to addition.

Addition is obviously a binary composition is N
i.e) N is closed with respect to addition
Also addition of natural number is an associative operation
But there exists no natural number $e \in N$ such that
$e + a = a = a + e \quad \forall\ a \in N$
For the addition of number the number 0 is the identity and $0 \notin N$.
$\therefore$ (N, +) is not a group.

Question to revise7.

Let G be a group. Then show that $(a^{-1})^{-1} = a \ \ \forall a \in G$

Solution

If e is the identity element, we have

$a^{-1}a = e$.

$\Rightarrow (a^{-1})^{-1}a^{-1}a = (a^{-1})^{-1}e$

$\Rightarrow \left[(a^{-1})^{-1}a^{-1}\right]a = (a^{-1})^{-1}$

$\Rightarrow ea = (a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1} \Rightarrow (a^{-1})^{-1} = a$

Question to revise8. If G is a group then prove that the identity element is unique

Solution

Suppose e and e' are two identity elements of a group G.
We have $ee' = e$ if e' is an identity and $ee' = e'$ if e is an identity.
But ee' is a unique element of G. Therefore $ee' = e$ and $ee' = e' \Rightarrow e = e'$.
Hence the identity element is unique.

6.8 Infinite group

An **infinite group** is a group whose underlying set contains an infinite number of elements.

Example: (**Z**, +), the group of integers with addition, and (**R**, +), the group of real numbers with addition

6.9 Finite group

A **finite group** is a group whose underlying set is finite. Finite groups often arise when considering symmetry of mathematical or physical objects, when those objects admit just a finite number of structure-preserving transformations. Important examples of finite groups include cyclic groups and permutation groups.

Question to revise9. Define finite and infinite group:

If in a group G the underlying set G consists of a finite number of distinct element then the group is called a finite group otherwise an infinite group.

6.10 Order of an element

Definition.

If G is a group and $g \in G$, the **order** of g is the smallest positive integer n such that $g^n = 1$. If $g^n \neq 1$ for any postive integer n, then g has **infinite order**.

In this definition, "1" denotes the identity element of G, and I'm using multiplicative notation. Using additive notation, the definition would read: If G is a group and $g \in G$, the **order** of g is the smallest positive integer n such that $ng = 0$. If $ng \neq 0$ for any postive integer n, then g has **infinite order**.

Recall that the **order of a group** is the number of elements in the group; the preceding definition pertains to the **order of an element**, which is the smallest positive power of the element which equals the identity. Don't confuse the two uses of the word "order"!

Example. (Orders of elements)

This is a group of order 6:

·	1	a	a^2	a^3	a^4	a^5
1	1	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	1
a^2	a^2	a^3	a^4	a^5	1	a
a^3	a^3	a^4	a^5	1	a	a^2
a^4	a^4	a^5	1	a	a^2	a^3
a^5	a^5	1	a	a^2	a^3	a^4

Find the orders of the elements of this group.

The operation is multiplication and the identity is 1. To find the order of an element, I find the first positive power which equals 1.

1 has order 1 --- and in fact, in any group, the identity is the only element of order 1.

The element a has order 6 since $a^6 = 1$, and no smaller positive power of a equals 1.

a^2 has order 3, because

$$a^2 \neq 1, \quad (a^2)^2 = a^4 \neq 1, \quad \text{but} \quad (a^2)^3 = a^6 = 1.$$

a^3 has order 2, because

$$a^3 \neq 1, \quad \text{but} \quad (a^3)^2 = a^6 = 1.$$

a^4 has order 3, because

$a^4 \neq 1, \quad (a^4)^2 = a^8 = a^2 \neq 1, \quad \text{but} \quad (a^4)^3 = a^{12} = (a^6)^2 = 1.$

a^5 has order 6. Note that

$(a^5)^6 = a^{30} = (a^6)^5 = 1.$

You can check that no smaller positive power of a^5 gives the identity.

Example.

What is the order of $\sqrt{2}$ in $\mathbb{R}$, the group of real numbers under addition?

The element $\sqrt{2}$ has infinite order: If I take positive multiples of $\sqrt{2}$, I'll never get 0:

$\sqrt{2}, \quad 2\sqrt{2}, \quad 3\sqrt{2}, \quad \ldots$ □

Example. (The group of quaternions)

This is the group table for Q, the group of quaternions. (Notice that the way i, j, and k multiply is similar to the way the unit vectors $\hat{\imath}$, $\hat{\jmath}$, $\hat{k}$ multiply under the cross product in $\mathbb{R}^3$.)

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(a) Show that Q is not abelian.

(b) Find the orders of 1, -1, and i.

(a) Since $ij = k$ but $ji = -k$ (for instance), Q is not abelian.

(b) The identity 1 has order 1, -1 has order 2, and i has order 4:

$$i^2 = -1, \quad i^3 = -i, \quad i^4 = (i^2)^2 = (-1)^2 = 1.$$

It's no coincidence that 1, 2, and 4 are divisors of 8, the order of the group. The order of an element always divides the order of the group.

Definition.

If G is a group and $g \in G$, the **order** of g is the smallest positive integer n such that $g^n = 1$. If $g^n \neq 1$ for any postive integer n, then g has **infinite order**.

In this definition, "1" denotes the identity element of G, and I'm using multiplicative notation. Using additive notation, the definition would read: If G is a group and $g \in G$, the **order** of g is the smallest positive integer n such that $ng = 0$. If $ng \neq 0$ for any postive integer n, then g has **infinite order**.

Note

Recall that the **order of a group** is the number of elements in the group; the preceding definition pertains to the **order of an element**, which is the smallest positive power of the element which equals the identity. Don't confuse the two uses of the word "order"!

Example. (Orders of elements)

This is a group of order 6:

·	1	a	a^2	a^3	a^4	a^5
1	1	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	1
a^2	a^2	a^3	a^4	a^5	1	a
a^3	a^3	a^4	a^5	1	a	a^2
a^4	a^4	a^5	1	a	a^2	a^3
a^5	a^5	1	a	a^2	a^3	a^4

Find the orders of the elements of this group.

The operation is multiplication and the identity is 1. To find the order of an element, I find the first positive power which equals 1.

1 has order 1 --- and in fact, in any group, the identity is the only element of order 1.

The element a has order 6 since $a^6 = 1$, and no smaller positive power of a equals 1.

a^2 has order 3, because

$$a^2 \neq 1, \quad (a^2)^2 = a^4 \neq 1, \quad \text{but} \quad (a^2)^3 = a^6 = 1.$$

a^3 has order 2, because

$$a^3 \neq 1, \quad \text{but} \quad (a^3)^2 = a^6 = 1.$$

a^4 has order 3, because

$$a^4 \neq 1, \quad (a^4)^2 = a^8 = a^2 \neq 1, \quad \text{but} \quad (a^4)^3 = a^{12} = (a^6)^2 = 1.$$

a^5 has order 6. Note that

$$(a^5)^6 = a^{30} = (a^6)^5 = 1.$$

You can check that no smaller positive power of a^5 gives the identity.

Example.

What is the order of $\sqrt{2}$ in $\mathbb{R}$, the group of real numbers under addition?

The element $\sqrt{2}$ has infinite order: If I take positive multiples of $\sqrt{2}$,

I'll never get 0:

$$\sqrt{2}, \quad 2\sqrt{2}, \quad 3\sqrt{2}, \quad \ldots . \ \square$$

Example. (The group of quaternions)

This is the group table for Q, the group of quaternions. (Notice that the way i, j, and k multiply is similar to the way the unit vectors $\hat{\imath}$, $\hat{\jmath}$, $\hat{k}$ multiply under the cross product in $\mathbb{R}^3$.)

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(a) Show that Q is not abelian.

(b) Find the orders of 1, -1, and i.

(a) Since $ij = k$ but $ji = -k$ (for instance), Q is not abelian.

(b) The identity 1 has order 1, -1 has order 2, and i has order 4:

$$i^2 = -1, \quad i^3 = -i, \quad i^4 = (i^2)^2 = (-1)^2 = 1.$$

It's no coincidence that 1, 2, and 4 are divisors of 8, the order of the group. The order of an element always divides the order of the group.

However, it doesn't work the other way: 8 is obviously a divisor of 8, but there's no element of order 8 in Q.

Definition.

If G is a group with n elements and G has an element x of order n, G is said to be **cyclic** of order n.

x is called a **generator** of the cyclic group, and the cyclic group consists of all powers of x.

Thus, Q is not cyclic, since it has no elements of order 8.

It turns out the $\mathbb{Z}$ is an infinite cyclic group, since you can get every7 element by taking multiples of 1 (or -1). I'll discuss cyclic groups in more detail later.

Question to revise10. Define order of the group:
The number of elements in a finite group is called the order of the group. We shall denote the order of a group G by the symbol o(G).

Question to revise11. Find the order of each element of the multiplicative group {1, -1, i, -i }.

o(1) = 1
o(-1) = 2
o(i) = 4
o(-i) = 4

Question to revise12. Given axa = b in G. Find x.

We have a x a = b
$a^{-1}(a \times a) = a^{-1}b$
$(a^{-1}a) \times a = a^{-1} b$
$x\ a = a^{-1} b$
$(x\ a)\ a^{-1} = (a^{-1}b)\ a^{-1}$
$x\ (a\ a^{-1}) = a^{-1} b\ a^{-1}$
$x\ e = a^{-1} b\ a^{-1}$
$x = a^{-1} b\ a^{-1}$

Definition.

A group G is said to be **abelian** if ab = ba for all a, b ∈ G. In other words groups in which the binary operation is commutative.
for example, in Z, Q, R, C it is understood that the binary operation is abelian under usual addition

Question to revise13. Prove that if for every element a in a group G, a^2=e then G is an abelian group.

Let a and b be any two elements of the group G. Then ab is also an element of G.

$\therefore (ab)^2=e$
$(ab)(ab)=e$
$(ab)^{-1}=ab$
$b^{-1}a^{-1}=ab$
But $a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$
Similarly. $b^2 = e \Rightarrow bb = e \Rightarrow b^{-1} = b$
Therefore, we have ba = ab
$\therefore$ G is an abelian group.

Question to revise14.Prove that a group G is an abelian if every element of G except the identity element is of order two.

Identity element e is of order 1. But $e^2 = e$

Since every other element is of order two, $\therefore$ we have $a^2 = e \quad \forall\, a \in G$

$\therefore$ G is abelian.

Question to revise15. Show that if every element of a group G is its own inverse, then G is abelian.

Let a and b be any two elements of G.

Then ab is also an element of G.

$\therefore (ab)^{-1}=ab$ as it is given that every element is its own inverse.

Now $(ab)^{-1}=ab \Rightarrow b^{-1}a^{-1}=ab$

$ba=ab \quad (\because a^{-1}=a, b^{-1}=b)$

Thus we have $ab=ba \quad \forall a,b \in G$

$\therefore$ G is an abelian group.

What is addition modulo n?

Then **addition modulo n** on S is defined as follows. For a and b in S, take the usual sum of a and b as integers, and let r be the element of S to which the result is congruent (**modulo n**); the sum $a+b \equiv$ (mod **n**) is equal to r.

Question to revise16. Define addition modulo m:

We define a new type of addition known as "addition modulo m" and written as $a+_m b$ where a and b are any integers and m is fixed positive integer.

By definition we have, $a+_m b=r, \quad 0 \leq r < m.$ where r is the least non-negative remainder when a+b is divided by m.

Residue class

The residue classes of a function $f(x) \mod n$ are all possible values of the residue $f(x) \pmod n$. For example, the residue classes of $x^2 \pmod 6$ are $\{0, 1, 3, 4\}$, since

$0^2 \equiv 0 \pmod 6$
$1^2 \equiv 1 \pmod 6$
$2^2 \equiv 4 \pmod 6$
$3^2 \equiv 3 \pmod 6$
$4^2 \equiv 4 \pmod 6$
$5^2 \equiv 1 \pmod 6$

are all the possible residues.

A complete residue system is a set of integers containing one element from each class, so $\{0, 1, 9, 16\}$ would be a complete residue system for $x^2 \pmod 6$.

The $\phi(m)$ residue classes prime to m form a group under the binary multiplication operation (mod m), where $\phi(m)$ is the totient function (Shanks 1993) and the group is classed a modulo multiplication group.

Question to revise17. Define Residue class:

Let I be the set of integers. Let m be any fixed positive integer. If a$\in$I, then the residue class $\vec{a}$ or {a} or [a] = {x : :x$\in$I, x-a is divisible by m}

Question to revise18. Define order of an element of a group:

Suppose G is a group and the composition has been defined multiplicatively.By the order of an element a$\in$G is meant the least positive integer n, if one exists,such that a^n=e (the identity of G)

If there exists no positive integer n such that a^n=e, then we say that a is of infinite order or of zero order. We shall use the symbol o(a) to denote the order of a.

Question to revise19.Prove that if a^2=a, a$\in$G then a=e.

We have a^2=a $\Rightarrow$ aa=a

aa=ae

a=e (by left cancellation law)

Unit -I

1. Define Binary operation:
2. Define .algebraic structure:
3. Define Semi group:
4. Define Group:
5. Define abelian group:
6. Show that the set N of all natural number 1,2,3,4,5….. is not a group with respect to addition.
7. If G is a group then show that $(a^{-1})^{-1} = a \ \ \forall a \in G$
8. If G is a group then prove that the identity element is unique
9. Define finite and infinite group:
10. Define order of the group:
11. Find the order of each element of the multiplicative group {1,-1,i,-i}.
12. Given axa=b in G. Find x.
13. Prove that if for every element a in a group G, a^2=e then G is an abelian group.
14. Prove that a group G is an abelian if every element of G except the identity element is of order two.
15. Show that if every element of a group G is its own inverse, then G is abelian.
16. Define addition modulo m:
17. Define Residue class:
18. Define order of an element of a group:
19. Prove that if a^2=a, a $\in$G then a=e.
20. Define cyclic groups:

M. Tamizharasi

111862030

Abstract Algebra

10/09

Assignment - I

2 Marks

1) Define Binary operation.

If f is a function from $G \times G \to G$, then f is said to be a binary operation on the set G. The image of the ordered pair (a, b) under the function f is denoted by a f b.

Eg :* The usual addition +, is a binary operation on N, Z, Q, R and C.

* On $f(x)$, $\cup$, $\cap$, Δ are binary operations.

---

2) Define Algebraic structure.

A non-empty set G equipped with one or more binary operations is called an Algebraic structure.

Eg: $(N, +)$ $(I, +)$ $(I, -)$ $(R, +, \circ)$ are all algebraic structure.

---

3) Define Semi Group.

Let us consider, an algebraic system $(A, *)$, where * is a binary operation on A. Then the system $(A, *)$ is said to be Semi-Group if it satisfies the following properties :

* The operation * is a closed operation on set A.
* The operation * is an associative operation.

Eg: If $(a * b) * c = a * (b * c)$ $\forall$ $a, b, c \in G$.

---

4) Define Group.

The algebraic structure $(G, *)$ is a group if the binary operation $*$ satisfies the following postulates.

(i) Closure Property

(ii) Associative Property

(iii) Existence of Identity

(iv) Existence of Inverse

---

5) Define Abelian Group.

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 non-abelian group.

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

2) $(f(x), \Delta)$ is an abelian group since $A \Delta B = B \Delta A$ for all $A, B \in f(x)$.

3) $Z_n, \oplus$ is an abelian group.

---

6) Show that the set N of all natural numbers 1, 2, 3, 4.... is not a group with respect to addition.

* Addition is obviously a binary composition is N.
* ie., N is closed with respect to addition.
* Also addition of natural number is an associative operation.
* But there exists no natural number $e \in N$ such that $e + a = a = a + e \ \forall \ a \in N$.
* For the addition of number, the number 0 is the identity and $0 \notin N$.

$\therefore (N, +)$ is not a Group.

7) Let G be a group. Then show that $(a^{-1})^{-1} = a \ \forall \ a \in G$.

If e is the identity element, we have $a^{-1}a = e$.

$$\Rightarrow (a^{-1})^{-1} a^{-1} a = (a^{-1})^{-1} e$$

$$\Rightarrow [(a^{-1})^{-1} a^{-1}] = (a^{-1})^{-1}$$

$$\Rightarrow e\,a = (a^{-1})^{-1}$$

$$\Rightarrow a = (a^{-1})^{-1}$$

$$\Rightarrow (a^{-1})^{-1} = a$$

Hence proved.

---

8) If G is a group, then prove that the identity element is unique.

* Suppose e and e' are two identity elements of a group G.

* We have $ee' = e$ if e' is an identity and $ee' = e'$ if e is an identity.

* But ee' is unique element of G. Therefore $ee' = e$ and $ee' = e' \Rightarrow e = e'$.

* Hence the identity element is unique.

---

9) Define finite and infinite group.

* <u>Finite Group</u> :

A group contains only finite number of elements is called a finite group.

Eg : Finite groups include cyclic and permutation groups.

* <u>Infinite Group</u> :

A group which contains infinite number of elements is called an infinite group.

Eg: $(Z, +)$ the group of integers with addition and

$(R, +)$ the group of real numbers with addition.

10) Define Order of a Group.

* The number of elements in a group is called the order of the group and it is denoted by $O(G)$.

* In the case of a finite group the order is finite and the order of an infinite group is infinity.

---

11) Find the order of each element of the multiplication group $\{1, -1, i, -i\}$.

$$O(1) = 1$$
$$O(-1) = 2$$
$$O(i) = 4$$
$$O(-i) = 4$$

---

12) Given $axa = b$ in G. Find x.

We have $axa = b$.

$$a^{-1}(axa) = a^{-1}b.$$
$$(a^{-1}a)xa = a^{-1}b$$
$$xa = a^{-1}b.$$
$$(xa)a^{-1} = (a^{-1}b)a^{-1}$$
$$x(aa^{-1}) = a^{-1}ba^{-1}$$
$$xe = a^{-1}ba^{-1}$$
$$x = a^{-1}ba^{-1}$$

---

13) Prove that if for every element a in a group G, $a^2 = e$ then G is an abelian group.

Let a and b be any two elements of the group G. Then ab is also an element of G.

$$\therefore (ab)^2 = e$$
$$(ab)(ab) = e$$

$$(ab)^{-1} = ab$$

$$b^{-1}a^{-1} = ab$$

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

similarly,

$b^2 = e \Rightarrow bb = e \Rightarrow b^{-1} = b$

Therefore, we have $ab = ba$.

$\therefore$ G is an Abelian group.

---

14) Prove that a group G is an abelian if every element of G except the identity element is of order two.

* Identity element e is of order 1. But $e^2 = e$.
* Since every other element is of order two, $\therefore$ we have $a^2 = e \ \forall \ a \in G$.

$\therefore$ G is abelian.

---

15) Show that if every element of a group G is its own inverse, then G is abelian.

* Let a and b be any two elements of G.
* Then ab is also an element of G.
* $\therefore (ab)^{-1} = ab$ as it is given that every element is its own inverse.
* Now $(ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab$.
* $ba = ab$ $(\because a^{-1} = a, \ b^{-1} = b)$
* Thus, we have $ab = ba \ \forall \ a, b \in G$.

$\therefore$ G is an Abelian group.

16) Define Addition modulo $\overset{=}{m}$.

We define a new type of addition known as "addition modulo m" and written as $a +_m b$ where a and b are any integers and m is fixed positive integer.

By definition, we have $a +_m b = r$, $0 \leq r < m$, where r is the least non-negative remainder when $a+b$ is divided by m.

---

17) Define Residue class.

Let I be the set of integers. Let m be any fixed positive integer.

Let $a \in I$, then the residue class $\bar{a}$ or $\{a\}$ or $[a] = \{x :: x \in I, x-a \text{ is divisible by } m\}$.

Eg: The Residue classes of $x^2 \pmod 6$ are $\{0,1,3,4\}$ since

$0^2 = 0 \pmod 6$; $3^2 = 3 \pmod 6$

$1^2 = 1 \pmod 6$; $4^2 = 4 \pmod 6$

$2^2 = 4 \pmod 6$; $5^2 = 1 \pmod 6$

are all positive residues.

---

18) Define order of an element of a group.

Suppose G is a group and the composition has been defined multiplicatively. By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that $a^n = e$ (the identity of G).

If there exists no positive integer n such that $a^n = e$, then say that a is of infinite order or of zero order. We shall use the symbol $O(a)$ to denote the order of a.

---

19) Prove that if $a^2 = a$, $a \in G$, then $a = e$.

We have, $a^2 = a \Rightarrow aa = a$

$aa = ae$

$a = e$ (By left cancellation law).

---

20) Define cyclic Groups.

A group G is called cyclic if for $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. The element a is then called a generator of G.

M. Tamizharasi

111862030

10/09

Assignment - 16 Marks

1) Show that the set $\bar{I}$ of all integers $\{\ldots -4, -3, -2, -1, 0, +1, +2, +3, +4 \ldots\}$ is a group with respect to the operation of addition of integers.

To show that the integers, $\mathbb{Z}$ together with usual addition form a group, you just need to check that the 4 properties * (or axioms) of a group are satisfied.

1) There exists an <u>identity element</u> in your group that fixes every element under the given binary operation.

2) <u>Closure</u> : Given any elements a and b in the set, we need to show that $a+b$ stays in the set. Yes, given any two integers aa and bb, their sum $a+b$ is again an integer.

3) <u>Associativity</u> of the given operation. Yes, addition in $\mathbb{Z}$ is associative. ie., $(a+b)+c = a+(b+c)$.

4) <u>Existence of inverse</u> : Given any element in the set, we need to find another element (call it "a inverse") such that a and its inverse commute and their operation together give the identity element.

Yes, given $a \in \mathbb{Z}$, then $-a$ is the inverse since $a + (-a) = (-a) + a = 0$.

Since $\mathbb{Z}$ with addition satisfies 1-4 above, it is a group. Done.

2) Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = (ab)/2$.

Let A = set of all positive rational numbers.

Let a, b, c be any three elements of A.

1) <u>Closure Property</u> :

W.K.T, Product of two positive rational numbers is again a rational number.

ie., $a * b \in A \ \forall \ a, b \in A$.

2) <u>Associativity</u> :

$$(a*b)*c = [(ab)/2] * c = abc/4$$

$$a*(b*c) = a*(bc/2) = abc/4$$

3) <u>Identity</u> :

Let e be the identity element.

We have $a*e = (ae)/2$ —— (1)

By the definition of * again, $a*e = a$. —— (2)

Since e is the identity.

From (1) and (2), $(ae)/2 = a \Rightarrow e = 2$ and $2 \in A$.

∴ Identity element exists, and '2' is the identity element in A.

4) <u>Inverse</u> :

Let $a \in A$.

Let us suppose b is inverse of a.

Now, $a * b = (ab)/2$ —— (1)

(By definition of inverse). Again,

$a*b = e = 2$ —— (2) [By definition of inverse)

From (1) and (2), it follows that

$$(ab)/2 = 2 \Rightarrow b = (4/a) \in A$$

$\therefore (A, *)$ is a group.

5) commutativity:

$$a * b = (ab/2) = (ba/2) = b * a.$$

Hence, $(A, *)$ is an abelian group.

---

3) Show that the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where α is a real number forms a group under matrix multiplication.

Matrix multiplication is closer.

Matrix multiplication is associative.

The addition formulas for sin and cos yield

$$\begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) & -\sin(\alpha)\cos(\beta) - \cos(\alpha)\sin(\beta) \\ \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) & \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta) \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$$

* The rest of the group requirements are pretty immediate after this.

* That the matrix multiplication is associative is obvious as the composition of functions is associative and the matrix multiplication is the composition of two linear functions.

* The neutral element is $\mathbb{I}$ the identity matrix, and every element has an inverse as we defined the group to be all invertible matrices, and as the inverse

of a matrix is invertible, the inverse are in G.

4) Show that the set $G = \{1, \omega, \omega^2\}$ where ω is an imaginary cube root of unity is a group with respect to multiplication.

* Cube roots of unity are $(1, \omega, \omega^2)$.
* Let G be the set $(1, \omega, \omega^2)$.
* To verify whether G is a Group or not,

* **Closure :**

Clearly for all a, b belonging to G, $a * b$ also belongs to G. (illustrated in the table).

* **Associative :**

Clearly for all a, b and c belonging to G,
$a * (b * c) = (a * b) * c$.

* **Existence of Identity :**

'e' is called the identity of the group if for all a belong to G, $a * e = e = e * a$,

Now from table it is clearly evident that $e = 1$ is the identity.

* **Existence of Inverse :**

If for all a belonging to G, there exists s a b such that $a * b = e$, then b is called the inverse of a.

Clearly, Inverse of 1 is 1, Inverse of ω is ω^2 and Inverse of ω^2 is ω.

Since, all 4 properties of group are satisfied G is a group.

Also, it is evident from the table that for all a, b belonging to G, we have $a * b = b * a$.

Thus, G is commutative.

A commutative group is called as an abelian group.

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

Thus, cube roots of unity form a finite abelian group under multiplication.

---

5) Prove that the set $G = \{0, 1, 2, 3, 4, 5\}$ is a finite abelian group of order 6 with respect to addition modulo 6.

* **Addition modulo m ($+_m$):**

Let m is a positive integer. For any two positive integers a and b

$a +_m b = a + b$ if $a + b < m$

$a +_m b = r$ if $a + b \geq m$ where r is the remainder obtained by dividing $(a + b)$ with m.

Multiplication modulo p ($*_m$):

Let p is a positive integer. For any two positive integers a and b

$a *_m b = ab$ if $ab < p$.

$a *_m b = r$ if $ab \geq p$ where r is the remainder obtained by dividing (ab) with p. Ex: $3 *_5 4 = 2$, $5 *_5 4 = 0$, $2 *_5 2 = 4$.

Eg: The set $G = \{0, 1, 2, 3, 4, 5\}$ is a group with respect to addition modulo 6.

The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

* **Closure property** :

Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

* **Associativity** :

The binary operation $+_6$ is associative in G.

Eg: $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

$2 +_6 (3 +_6 4) = 2 +_6 1 = 3$.

* **Identity** :

Here, The first row of the table coincides with the toprow. The element heading that row, ie., 0 is the identity element.

* **Inverse** :

From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

Commutativity:

The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

Hence, $(G, +_6)$ is an abelian group.

---

6) P.T if G is an abelian group, then for all $a, b \in G$ and all integers n, $(ab)^n = a^n b^n$.

Proof:

* Let a and b be any two elements of G.

* Suppose n, n+1, n+2 are three consecutive integers such that

$$(ab)^n = a^n . b^n \quad \text{---- (1)}$$

$$(ab)^{n+1} = a^{n+1} . b^{n+1} \quad \text{---- (2)}$$

$$(ab)^{n+2} = a^{n+2} . b^{n+2} \quad \text{---- (3)}$$

* Equation (2) can also be written as,

$$(ab)\ (ab)^n = a . a^n . b . b^n$$

$$a . b . a^n . b^n = a . a^n . b . b^n$$

$$b . a^n = a^n . b \ [\text{by cancellation law}]$$

* Equation (3) can also be written as,

$$(ab)\ (ab)^{n+1} = a . a^{n+1} . b . b^{n+1}$$

$$a . b . a^{n+1} . b^{n+1} = a . a^{n+1} . b . b^{n+1}$$

$$b . a^{n+1} = a^{n+1} . b \ [\text{by cancellation law}]$$

$$b . a^n . a = a^n . a . b$$

$$a^n . b . a = a^n . a . b$$

$\Rightarrow ba = ab$ [by left cancellation law]

Therefore, G is an abelian group.

7) If G is a group then prove that

a) the identity element in a group is unique.

b) The Inverse of each element of a group is unique.

c) $(a^{-1})^{-1} = a$.

d) $(ab)^{-1} = b^{-1}a^{-1}$ $\forall$ $a, b \in G$.

Proof :

* We first prove (1).

By definition G has to contain at least one identity element. Suppose that both e and f are identity elements in G. We compute the product ef.

As e is an identity in G,

$$ef = f$$

On the kother hand as f is an identity in G.

$$ef = e.$$

Thus $e = ef = f$. Thus the identity is unique. Hence(1)

* Now we prove (2) :

Suppose that g is an element of G. Then g has at least one inverse by definition. Suppose that there were two elements h and k that were both inverse of g. We compute hgk (by associativity we can drop the parenthesis). On the one hand we get

$hgk = (hg)k$ by associativity

$= ek$ property of inverse

$= k$ property of identity

$$hgk = h(gk) \quad \text{by associativity}$$

$$= he \quad \text{property of inverse}$$

and

$$= h \quad \text{property of identity}$$

Thus $h = hgk = k$. Thus g has only one inverse and (2) holds.

Suppose that $x \in G$ is a solution to the equation.

$$ax = b.$$

Multiply both sides by a^{-1}. We get

$$a^{-1}(ax) = a^{-1}b.$$

By associativity the LHS is equal to

$$(a^{-1}a)x = ex = x.$$

Thus $x = a^{-1}b$. Now we check that this is indeed a solution of the equation.

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

Thus $x = a^{-1}b$ is the unique solution to the equation

$$ax = b. \quad \text{Hence (3)}$$

(4) is similar to (3) and is left as an excercise for the reader.

* <u>Now we prove (5)</u>.

Let $b = a^{-1}$ and $c = b^{-1} = (a^{-1})^{-1}$. We want to prove that $c = a$. This follows from (2), if we can show that both a and c are the inverse of b, c is by definition an inverse of b.

We check that a is also an inverse of b.

We have $ab = aa^{-1} = e$ and $ba = a^{-1}a = e$.

So a is an inverse of b. By uniqueness of the inverse $a = c$. Hence (5).

* Finally we prove (6).

Suppose $c = b^{-1}a^{-1}$. We have to check that

$$(ab)c = c(ab) = e.$$

But $(ab)c = (ab)(b^{-1}a^{-1})$ substituting for c

$= a(bb^{-1})a^{-1}$ by associativity

$= a(e)a^{-1}$ property of inverses

$= (ae)a^{-1}$ by associativity

$= aa^{-1}$ property of identity.

$= e$ property of inverses.

and

$c(ab) = (b^{-1}a^{-1})(ab)$ substituting for c

$= b^{-1}(a^{-1}a)b$ by associativity

$= b^{-1}(e)b$ property of inverses

$= (a^{-1}e)a$ by associativity

$= a^{-1}a$ property of identity

$= e$ property of inverses.

Thus c is the inverse of ab. Hence (6).

---

8) Prove that if a, b, c are any elements of G then

a) $ab = ac \Rightarrow b = c$ (Left cancellation law) and
$ba = ca \Rightarrow b = c$ (Right cancellation law).

b) Prove that the left identity is also the right identity, ie., if e is the left identity then $ae = a \ \forall \ a \in G$.

c) The left inverse of an element is also its right inverse ie., if a^{-1} is the left inverse of a, then $(a^{-1})a = e$.

Soln:

A) * First let us prove that there is a unique soln. for the eqn. $a * x = b$.

* Let us suppose that there are two solutions for x in G, say $x = x_1$ and $x = x_2$. Then

$a * x_1 = b$ and $a * x_2 = b$

$a * x_1 = a * x_2$

$\therefore$ By cancellation law, $x_1 = x_2$.

* ie., the soln. for x is unique. Now let us find the solution.

* Let a', be the inverse of a.

$a * x = b \Rightarrow a' * (a * x) = a' * b$

$\Rightarrow (a' * a) * x = a' * b$

$\Rightarrow e * x = a' * b$

$\Rightarrow x = a' * b$

* $\therefore x = a' * b$ is the solution of the eqn. $a * x = b$.

and If y_1 and y_2 are the solutions of $y * a = b$,

then $y_1 * a = b$ and $y_2 * a = b$.

$\therefore y_1 * a$ and $y_2 * a$ and $\therefore y_1 = y_2$ (By cancellation law)

* Also, $(y * a) * a' = b * a'$

$y * (a * a') = b * a'$

$y * e = b * a'$

ie., $y = b * a'$

B) A semigroup G contains left identity e and a left inverse a' for every a, e in G, then G is a group.

Proof :

* a' is a left inverse of a so that a'a = e.
* Let a'' be a left inverse of a' so that a''a' = e then aa' = e(aa') [since e is left identity]

$= (a''a')(aa') = a''(a'a)a'$ [associative]

$= a''(ea') = a''a'$ [since e is left identity]

$= e.$

* Hence a' is also a right inverse of a.
* Also a = ea = (aa')a = a(a'a). Hence e is also a right identity.
* Thus ea = a = ae and a'a = aa' = e and for all a ∈ G. Hence G is a group.
* A semigroup G contains right identity e and right inverse a' with respect to e for every element a, e in G, then G is a group.
* The proof is similar to previous theorem.

C) For any two element x, y ∈ G to be the inverses of each other, we have to show that x * y = y * x = e. and
* We want to prove b' * a' is the inverse of a * b. For this we have to prove that

$(a * b) * (b' * a') = e$

and $(b' * a') * (a * b) = e$

* Now, $(a*b)*(b'*a') = a*(b*b')*a'$ (Associative)

$= (a*e)*a'$

$= a*a' = e$ —— (1)

* Also, $(b'*a')*(a*b) = b'*(a'*a)*b$.

$= b'*(e*b)$

$= b'*b = e$ —— (2)

* From (1) and (2),

$b'*a'$, is the inverse of $a*b$.

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

---

9) If a, b are any two elements of a group G, then the eqn. $ax = b$ and $ya = b$ have unique soln. in G.

* Let $a \in G$. Then there exists a unique $e \in G$ such that $ea = a$.

* Now, $eb = e(ax) = (ea)x = ax = b$

$eb = b$ for all $b \in G$ so that e is a left identity.

* Let $a \in G$. Then $ya = a$ has a unique solution a'.

* $a'a = e$ so that a' is the left inverse of a.

* Hence G is a group.

---

10) Show that the additive group of integers modulo m, the set $G = \{0, 1 \ldots m-1\}$ of first m non-negative integers is a group, the composition being ordinary addition residue modulo m.

(OR)

Prove that the order of every element of a finite group is finite and is less than or equal to order of the group.

* Let G be a finite group and let $a \in G$, we consider all positive integral powers of a, ie., $a^1, a^2, a^3, a^4 \ldots\ldots$

* Every one of these powers must be an element of G. But G is of finite order, Hence these element cannot all be different. We may therefore suppose that $a^s = a^r$, $s > r$.

* Now, $s = a^r \Rightarrow a^s a^{-r} = a^r a^{-r}$

$$\Rightarrow a^{s-r} = a^0$$

$$\Rightarrow a^{s-r} = e$$

$$\Rightarrow a^t = e \text{ (putting } s-r = t)$$

* Since $s > r$, t is a positive integer, hence there exists a positive integer t such that $a^t = e$.

* Now, we know that every set of positive integers has atleast number. It follows that the set of all those positive integer t such that $a^t = e$ has a least member, say m, thus there exists a least positive integer m such that $a^m = e$, showing that the order of every element of a finite group is finite.

---

11) Show that

(i) The order of an element of a group is the same as that of its inverse a^{-1}.

(ii) The order of any integral power of an element a cannot exceed the order of a.

(iii) Prove that if the element a of a group G is of order n then $a^m = e$ iff n is a divison of m.

Proof :

(i) The order of an element is same as that of its inverse in a group G.

To prove : $O(a) = O(a^{-1})$ for every a in G.

* Suppose, let $O(a) = m$ and $O(a^{-1}) = n$ where m ; n is the least positive integer.

Now, $O(a) = m \Rightarrow a^m = e$.

$\Rightarrow (a^m)^{-1} = e^{-1} = e$

$\Rightarrow (a^{-1})^m = e$

$\Rightarrow O(a^{-1}) \leq m$ ie., $n \leq m$ —— (1)

Now, $O(a^{-1}) = n \Rightarrow (a^{-1})^n = e$

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

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

$\Rightarrow a^n = e$

$\Rightarrow O(a) \leq n$ ie., $m \leq n$. —— (2)

From (1) and (2), we have $n = m$, ie., $O(a) = O(a^{-1})$.

(ii) The order of any integral power of an element a cannot exceed the order of a.

Proof :

* Let G be a group and $a \in G$.

* Let $O(a) = n$ and let a^k be any integral power of a.

To prove : $O(a^k) = O(a)$

Now, $a^n = e \Rightarrow (a^n)^k = e^k$

$\Rightarrow (a^k)^n = e$ and

$\Rightarrow O(a^k)$ is finite and $\leq n$

$\Rightarrow O(a^k) \leq O(a)$.

(iii) Prove that if the element a of a group G is of order n then $a^m = e$ iff n is a divisor of m.

Proof :

Given, $O(a) = n \Rightarrow a^n = e$.

To prove : $a^m = e \Leftrightarrow n/m$.

* Now, $a^m = e$ and $O(a) = n \Leftrightarrow n \leq m$

* By division algorithm, $\exists\ q, r \in Z$ such that $m = qn + r$ with $0 \leq r < n$.

* Now, $a^m = e \Rightarrow a^{qn+r} = e$

$\Rightarrow a^{qn} a^r = e$

$\Rightarrow (a^n)^q a^r = e$

$\Rightarrow e^q a^r = e$

$\Rightarrow a^r = e$

$\Rightarrow r = 0$ [$\because O(a) = n \Rightarrow n$ is the least positive integer such that $a^n = e$].

$\therefore m = qn \Rightarrow n/m$.

* Conversely : Suppose if n/m.

To prove : $a^m = e$.

Now, $n/m \Rightarrow m = qn$ where q is any integer.

$\Rightarrow a^m = a^{qn} \Rightarrow a^m = (a^n)^q$

$\Rightarrow a^m = a^q$

$\Rightarrow a^m = e$

---

12) Prove that the orders of the elements a and bab^{-1} are the same where a, b are any two elements of a group.

Lemma :

If a and b are any two elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$ for any positive integer n.

Proof:

* Let $(bab^{-1})^n = ba^nb^{-1}$ —— (1)
* We prove (1) by induction on n.
* For $n = 1$, we have $bab^{-1} = ba^1b^{-1} = bab^{-1}$ which is true.
* Assume (1) is true for $n = k$, i.e., $(bab^{-1})^k = ba^kb^{-1}$
* Consider, $(bab^{-1})^{k+1} = ba^{k+1}b^{-1}$.

$\Rightarrow (bab^{-1})^{k+1} = (bab^{-1})^k (bab^{-1})^1$

$\Rightarrow (bab^{-1})^{k+1} = (ba^kb^{-1})(bab^{-1})$

$\Rightarrow (bab^{-1})^{k+1} = ba^k(b^{-1}b)ab^{-1}$ (By associative law in G).

$\Rightarrow (bab^{-1})^{k+1} = b.a^k(ea)b^{-1}$

$\Rightarrow (bab^{-1})^{k+1} = b(a^ka)b^{-1}$

$\Rightarrow (bab^{-1})^{k+1} = ba^{k+1}b^{-1}$

* By induction on n, (1) holds for all positive integers

Theorem:

Let G be a group and $a, b \in G$ then $O(a) = O(bab^{-1})$

Proof:

* Let $O(a) = n \Rightarrow a^n = e$ and $O(bab^{-1}) = m$
* Since, $(bab^{-1}) = ba^nb^{-1}$ (By Lemma)

$\Rightarrow (bab^{-1})^n = beb^{-1}$

$\Rightarrow (bab^{-1})^n = bb^{-1}$

$\Rightarrow (bab^{-1})^n = e$

$\Rightarrow O(bab^{-1})$ is finite and $\leq n$ ie., $m \leq n$ —— (1)

Now,

$O(bab^{-1}) = m \Rightarrow (bab^{-1})^m = e$

$\Rightarrow ba^mb^{-1} = e$

$\Rightarrow ba^mb^{-1} = bb^{-1}$ and

$\Rightarrow a^m = e$ (By cancellation law)

$\Rightarrow O(a)$ is finite and $\leq m$ ie., $n \leq m$ —— (1)

From (1) and (2), we have $n = m$.

ie., $O(a) = O(bab^{-1})$.

---

13) Prove that the order of ab is the same as that of ba where a and b are any elements of a group.

To prove:

Let G be a group and $a, b \in G$ then $O(ab) = O(ba)$.

Proof:

* From the theorem above, Let G be a group and $a, b \in G$ then $O(a) = O(bab^{-1})$.
* We have $O(a) = O(bab^{-1})$.

$\Rightarrow O(ab) = O[b(ab)b^{-1}]$

$\Rightarrow O(ab) = O[(ba)(bb^{-1})]$

$\Rightarrow O(ab) = O(ba)$

---

14) S.T if a, b are any two elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

(OR)

Let G be a group and $a, b \in G$ then G is abelian if and only if $(ab)^2 = a^2b^2$.

Soln:

* Suppose G is abelian then $ab = ba \ \forall \ a, b \in G$.
* consider $(ab)^2 = (ab)(ab)$.

$\Rightarrow (ab)^2 = a(ba)b$ [By associative law in G]

$\Rightarrow (ab)^2 = a(ab)b$ [G is abelian]

$\Rightarrow (ab)^2 = (aa)(bb)$ [By associative law in G]

$\Rightarrow (ab)^2 = a^2b^2$

* Conversely : Suppose $(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ [By associative law in G]

$\Rightarrow ba = ab$ [By cancellation law in G]

$\Rightarrow$ G is abelian.

---

15) If a group G has four element show that it must be abelian. (OR)
Prove that a group of order four is an abelian.

Soln :

* Let G be a group of order 4.
* The order of an element of a group has to divide the order of a group, n/m when $o(a)^m = e$.
* So there are two cases :

(1) either G has an element of order 4. (or)
(2) every non-identity element of G is of order 2.

Case (1) :

If G has an element of order 4, then it is cyclic and so Abelian.

case (2) :

* Let $G = \{1, a, b, c\}$ with 1 the identity element and $a^2 = b^2 = c^2 = 1$.
* Note that this means that every element is its own inverse.
* Now whatever ab is, we must have $(ab)^2 = 1$.

* It cannot be that $ab = 1$ however, because (multiplying both sides on the right by b), this would imply $a = b$ in which case the order of G would be less than 4.

* So we have $abab = 1$. Multiply by b on the right and a on the left to get $ba = ab$.

* The same argument shows $ca = ac$ and $cb = bc$, so G is Abelian in this case as well.

* To understand G a little better, note that we cannot have $ab = b$, because then $a = 1$, and we cannot have $ab = a$, because then $b = 1$, so it must be that $ab = c$.

* So our group is $G = \{1, a, b, ab\}$ with $a^2 = 1 = b^2$ and $ba = ab$. (This data implies that $(ab)^2 = 1$ as well).

* If we let $H = \{1, a\}$ and $K = \{1, b\}$, then H and K are subgroups of G, $HK = KH = G$, and $H \cap K = \{1\}$.

* Under these conditions, we write $G = H \oplus K$. Since H and K are both isomorphic to Z_2, we see that $G = Z_2 \oplus Z_2$.

* So the final result is that the only groups of order 4 (up to isomorphism) are Z_4 and $Z_2 \oplus Z_2$.

16) (i) Prove that every cyclic group is an abelian group

(OR)

Show that every cyclic group is Abelian.

Soln:

* Suppose that G is a cyclic group that is generated by the element g.
* Let x and y be arbitary elements of G. We must show that $xy = yx$.
* Since G is generated by g, there must exist integers r and s such that
* $x = g^r$, $y = g^s$. But then $xy = g^r g^s = g^{r+s} = g^s g^r = yx$

(ii) Prove that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof:

* Let G be a infinite cyclic group generated by element a. ie., $G = \langle a \rangle = \{a, a^2, a^3 \ldots a^n, \ldots\}$.
* Let $g \in G \Rightarrow n \in \mathbb{Z}$ such that $g = a^n$.
* Now, $g = (a^{-1})^{-n} = (a^{-1})^m$ where $m = -n$.
* Hence, $g = (a^{-1})^m \; \forall \; g \in G$. and

$\Rightarrow a^{-1}$ is also a generator of G.

---

17) Prove that every group of prime order is cyclic.

* Let p be a prime and G be a group such that $|G| = p$.
* Then G contains more than one element.

* Let $g \in G$ such that $g \neq e_G$.
* Then $\langle g \rangle$ contains more than one element.
* Since $\langle g \rangle \leq G$, by Lagrange's theorem,

$|\langle g \rangle|$ divides p.

* Since $|\langle g \rangle| > 1$ and $|\langle g \rangle|$ divides a prime,

$|\langle g \rangle| = p = |G|$.

* Hence, $\langle g \rangle = G$. It follows that G is cyclic.

1. Show that

   i). The order of an element of a group is the same as that of its inverse a^{-1}.

   and

   ii). The order of any integral power of an element a cannot exceed the order of a.

   iii). Prove that If the element a of a group G is of order n then $a^m = e$ iff n is a divisor of m.

Proof:

I) The order of an element is same as that of its inverse in a group G.

To prove: $O(a) = O(a^{-1})$ for every a in G.

Suppose, let $O(a) = m$ and $O(a^{-1}) = n$ where m; n is the least positive integer.

Now, $O(a) = m \Rightarrow a^m = e$

$\Rightarrow (a^m)^{-1} = e^{-1} = e$

$\Rightarrow (a^{-1})^m = e$

$\Rightarrow O(a^{-1}) \leq m$ i.e., $n \leq m$ .....(1)

Now, $O(a^{-1}) = n \Rightarrow (a^{-1})^n = e$

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

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

$\Rightarrow a^n = e$

$\Rightarrow O(a) \leq n$ i.e., $m \leq n$ .....(2)

From (1) and (2) we have $n = m$ i.e., $O(a) = O(a^{-1})$

ii) The order of any integral power of an element a cannot exceed the order of a.

Proof:

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

Let $O(a) = n$ and let a^k be any integral power of a.

To prove: $O(a^k) = O(a)$

Now, $a^n = e \Rightarrow (a^n)^k = e^k$

$\Rightarrow (a^k)^n = e$

$\Rightarrow O(a^k)$ is finite and $\leq n$ and

$\Rightarrow O(a^k) \leq O(a)$

iii).Prove that If the element a of a group G is of order n then $a^m = e$ iff n is a divisor of m.

Proof:

Given, $O(a) = n \Rightarrow a^n = e$.

To prove: $a^m = e \Leftrightarrow n|m$.

Now $a^m = e$ and $O(a) = n \Rightarrow n \leq m$

By division algorithm, $\exists$ q, r $\in$ Z such that $m = qn + r$ with $0 \leq r < n$

Now, $a^m = e \Rightarrow a^{qn+r} = e$

$\Rightarrow a^{qn} a^r = e$

$\Rightarrow (a^n)^q a^r = e$

$\Rightarrow e^q a^r = e$

$\Rightarrow a^r = e$

$\Rightarrow r = 0$ [$\because$ $O(a) = n \Rightarrow n$ is the least positive integer such that $a^n = e$]

$\therefore m = qn \Rightarrow n|m$

Conversely: Suppose if n|m. To prove: $a^m = e$.

Now, $n|m \Rightarrow m = qn$ where q is any integer

$\Rightarrow a^m = a^{qn} \Rightarrow a^m = (a^n)^q$

$\Rightarrow a^m = e^q$

$\Rightarrow a^m = e$

2. Prove that the orders of the elements a and bab^{-1} are the same where a, b are any two elements of a group.

Lemma:

If a and b are any two elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$

for any positive integer n.

Proof:

Let $(bab^{-1})^n = ba^nb^{-1}$.....(1)

We prove (1) by induction on n.

For n = 1, we have $bab^{-1} = ba^1b^{-1} = bab^{-1}$ which is true.

Assume (1) is true for n = k, i.e., $(bab^{-1})^k = ba^kb^{-1}$

Consider, $(bab^{-1})^{k+1} = ba^{k+1}b^{-1}$

$\Rightarrow (bab^{-1})^{k+1} = (bab^{-1})^k(bab^{-1})^1$

$\Rightarrow (bab^{-1})^{k+1} = (ba^kb^{-1})(bab^{-1})$

$\Rightarrow (bab^{-1})^{k+1} = ba^k(b^{-1}b)ab^{-1}$ By associative law in G.

$\Rightarrow (bab^{-1})^{k+1} = ba^k(ea)b^{-1}$

$\Rightarrow (bab^{-1})^{k+1} = b(a^ka)b^{-1}$

$\Rightarrow (bab^{-1})^{k+1} = ba^{k+1}b^{-1}$

By induction on n,(1) holds for all positive integers.

Theorem : Let G be a group and $a, b \in G$ then $O(a) = O(bab^{-1})$

Proof: Let $O(a) = n \Rightarrow a^n = e$ and $O(bab^{-1}) = m$

Since, $(bab^{-1})^n = ba^nb^{-1}$ (By lemma)

$\Rightarrow (bab^{-1})^n = beb^{-1}$

$\Rightarrow (bab^{-1})^n = bb^{-1}$

$\Rightarrow (bab^{-1})^n = e$

$\Rightarrow O(bab^{-1})$ is finite and $\leq n$ i.e., $m \leq n$ .....(1)

Now, $O(bab^{-1}) = m \Rightarrow (bab^{-1})^m = e$

$\Rightarrow ba^m b^{-1} = e$

$\Rightarrow ba^m b^{-1} = bb^{-1}$

and

$\Rightarrow a^m = e$ (By cancellation laws)

$\Rightarrow O(a)$ is finite and $\leq m$ i.e., $n \leq m$ .....(2)

From (1) and (2), we have $n = m$ i.e., $O(a) = O(bab^{-1})$

3. Prove that the order of ab is the same as that of ba where a and b are any elements of a group.

Proof:

To prove : Let G be a group and a; b Ɛ G then O(ab) = O(ba)

From the theorem above,Let G be a group and $a, b \in G$ then $O(a) = O(bab^{-1})$

we have $O(a) = O(bab^{-1})$

=> $O(ab) = O[b(ab)b^{-1}]$

=> $O(ab) = O[(ba)(bb^{-1})]$

=> O(ab) = O(ba)

4. Show that if a, b are any two elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

(or)

Let G be a group and a; b Ɛ G then G is abelian if and only if $(ab)^2 = a^2b^2$.

Solution:

Suppose G is abelian then ab = ba ∀ a; b Ɛ G.

Consider, $(ab)^2 = (ab)(ab)$

=>$(ab)^2 = a(ba)b$ By associative law in G

=> $(ab)^2 = a(ab)b$ G is abelian

$\Rightarrow (ab)^2 = (aa)(bb)$ By associative law in G

$\Rightarrow (ab)^2 = a^2b^2$

and

Conversely: suppose $(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ By associative law in G

$\Rightarrow ba = ab$ By cancellation law in G

$\Rightarrow$ G is abelian.

5. If a group G has four element show that it must be abelian.

(or) Prove that a group of order four is an abelian

Solution:

Let G be a group of order 4.

The order of an element of a group has to divide the order of the group,

n/m when $o(a)^m = e$.

so there are two cases:

(1) either G has an element of order 4

or

(2) every non-identity element of G is of order 2.

Case(1) : If G has an element of order 4, then it is cyclic and so Abelian.

Case(2): Let $G=\{1,a,b,c\}$ with 1 the identity element and $a^2= b^2= c^2= 1$.

Note that this means that every element is its own inverse.

Now whatever ab is, we must have $(ab)^2 = 1$.

It cannot be that ab=1 however, because (multiplying both sides on the right by b), this would imply a=b in which case the order of G would be less than 4.

So we have abab=1. Multiply by b on the right and a on the left to get ba=ab.

The same argument shows ca=ac and cb=bc, so G is Abelian in this case as well.

To understand G a little better, note that we cannot have ab=b, because then a=1, and we cannot have ab=a, because then b=1, so it must be that ab=c.

So our group is

G={1,a,b,ab} with $a^2=1=b^2$ and ba=ab.

(This data implies that $(ab)^2=1$ as well.)

If we let H={1,a} and K={1,b}, then H and K are subgroups of G, HK=KH=G, and H∩K={1}. Under these conditions, we write $G=H \oplus K$. Since H and K are both isomorphic to Z_2, we see that $G \cong Z_2 \oplus Z_2$.

So the final result is that the only groups of order 4 (up to isomorphism) are Z_4 and $Z_2 \oplus Z_2$.

6. i) Prove that every cyclic group is an abelian group.

Or

Show that every cyclic group is Abelian.

Solution: Suppose that G is a cyclic group that is generated by the element g.

Let x and y be arbitrary elements of G. we must show that $xy = yx$.

Since G is generated by g, there must exist integers r and s such that

$x = g^r$, $y = g^s$. But then $xy = g^r g^s = g^{r+s} = g^s g^r = yx$.

ii)Prove that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof:

Let G be a infinite cyclic group generated by element a. i.e., G =< a >= {a, a^2, a^3,……., a^n, ……..}

Let g Ɛ G => n Ɛ Z such that $g = a^n$.

Now, $g = (a^{-1})^{-n} = (a^{-1})^m$ where $m = -n$.

Hence, $g = (a^{-1})^m$ ∀ $g \in G$.

and
$\Rightarrow a^{-1}$ is also a generator of G.

7. Prove that every group of prime order is cyclic.

Let p be a prime and G be a group such that $|G| = p$. Then G contains more than one element. Let $g \in G$ such that $g \neq e_G$. Then $\langle g \rangle$ contains more than one element. Since $\langle g \rangle \leq G$, by Lagrange's theorem, $|\langle g \rangle|$ divides p.
Since $|\langle g \rangle| > 1$ and $|\langle g \rangle|$ divides a prime, $|\langle g \rangle| = p = |G|$. Hence, $\langle g \rangle = G$. It follows that G is cyclic.

SRI CHANDRASEKHARENDRA SARASWATHI VISVA MAHAVIDYALAYA

(Deemed to be University under sec. 3 of UGC Act.1956)

(Accredited with "A" Grade by NAAC)

ENATHUR, KANCHIPURAM-631561.

Lecture Notes

Compiled by Dr. T. N. Kavitha

Abstract Algebra – Unit II

SUB GROUPS

Subject Code: UM504

Course : B.Sc Mathematics

Unit - II- Abstract algebra

TOPICS: Subgroups - Cosets and Lagrange's theorem- normal subgroups – quotient group Ishomomorphism.

Chapter1 - Sub-Groups

Definition :

Let G be a group under a binary operation *. Let H be a non-empty subset of G. If H is also a group under the same binary operation *, then H is called a subgroup of G.

Remark :

The sets {e} and { G} are subgroups of G under the same binary operation. These subgroups are trivial subgroups of G or improper subgroups of G. All other subgroups of G are called non-trivial subgroups or proper subgroups of G.

Examples

{.Z, +} is a sub-group of (Q, +), (R, +) and (C, +).

2. (Q, +) is a subgroup of (R, +) and (C, +)

3. (R, +) is a subgroup of (C, +)

Properties of subgroups

Property 1

Let H be a sub-group of a group G. Prove that the identity element of subgroup H is the same as the identity element of the group.

Proof:

Let e be the identity element in G and e_1 be the identity element in H.

Let a be any element in H. Then a $\in$ G

Since a $\in$ G,a•e = a ….(1)

Since a ∈ H, a •e_1 = a …….(2)

From (1) and (2), a • e = a • e_1

∴By left cancellation law, e = e_1

Hence both H and G have the same identity element.

Property 2

Let H be a subgroup of G. Prove that the inverse of an element a ∈ H is the same as the inverse of a ∈G (Or)

The inverse of an element in a subgroup is the same as the inverse of that element in the group.

Proof :

Let a ∈ H , then a ∈ G .

Let a' and a" be the inverses of a in H and G respectively.

Then a • a' = a' • a = e ….(1)

a • a" = a" • a = e

∴a • a' = a • a"

Hence by left cancellation law, a' = a"

∴ The inverse of a in H is the same as the inverse of a in G.

Criterion for a subgroup :

In order to prove that a subset Hof a group G is a subgroup of G, we have to test whether H also satisfies the axioms of a group. Now we give two different sets of criteria for a subset to be a subgroup.

Property 3

Let H be a subset of G. H is a subgroup of G if and only if for any two elements a* b' ∈ H

Proof :

Case 1 : Condition is necessary :

Given H is a subgroup of G, we have to prove that a • b'∈ H for all a, b ∈ H .

Since H is a sub-group, for b ∈ H , we have b' ∈ H .By closure property in H,

∴condition a, b' ∈ H ⇒,a • b' ∈ H

Case 2 : Condition is sufficient :

Given for any two elements a, b ∈ H , we have a •b'∈ H . We have to prove that H is a subgroup of G.

Proof:

Given for any two elements a,b' ∈H, a. b', ∈H. Since a,a'∈H, a•a' ∈H

i.e., e ∈ H

∴Identity element exists in H.

Since e, a ∈ H, we have e• a' ∈ H i.e., a' ∈ H

∴For each element a, its inverse a' ∈ H

a, b ∈H, a.b' ∈ H

Since a, b' ∈H, a•(b')' ∈H i.e., a•b∈H

∴The set is closed.

Associative law is true in H since H is a subset of C and associative law is

true in G.

∴ H is a group and hence is a subgroup of G.

Property 4

A non-empty subset H of a group (G, *) is a group of G if' and only if

(i) a, b ∈ H ⇒a*b E H

(ii) a ∈ H ⇒a' ∈H (Or)

A non-empty subset H of a group G is a subgroup of G and only if (1) the set H is closed (2) each element of H possesses inverse in H.

Proof:

Case 1 : Conditions are necessary :

Given His a subgroup of G. To prove that conditions (1) and (2) are satisfied.

Since H is a group, by closure property, for any two elements a, b ∈ H ,

we have a.b ∈H.

∴Condition (1) is satisfied. Since His a group by inverse axiom, for a ∈ H, a' ∈ H

∴Condition (2) is satisfied.

Case 2 : Conditions are sufficient :

Given (1) a•b ∈ H for all a, b ∈H

(2) a' ∈ H for all a ∈H

To prove : H is a subgroup of G.

Condition (1) States that closure property is true in H.

(2) Associative law is true in H since it is true in G and H is a subset of G.

Since a' ∈ H for all a ∈ H and closure property is true in H, a • a' ∈ H

i.e., e ∈H . Hence identity exists in H. By condition (2) all elements in H

possess inverse in H. ∴H is a group and hence a subgroup of G.

Property 5

If H and K are subgroups of G, show that H ∩ K is a subgroup of G.

Proof:

Let a, b ∈ H ∩ K

Then a, b ∈ H and a, b ∈ K.

Since H is a subgroup of G and a, b ∈ H ,

we have a • b' ∈H (Property 3)

Since K is a subgroup of G and a, b ∈ H,

we have a • b'∈ K (Property 3)

Since a • b' ∈ H and a•b' ∈ K , we have a•b` ∈ H ∩ K

For a, b ∈ H ∩ K , we have a•b'∈H ∩ K

Hence H ∩ K is also a subgroup of G.

Property 6

Let G be a group and a e G then H = { a^n | n ∈ Z} is a subgroup of G.

Proof:

a^n∈H for all n ∈Z

a ∈ H since 1 ∈ Z

∴H is non-empty. Also since a ∈ G and G is a group.

a^n∈G for all n ∈Z

∴ H is non-empty subset of G.

$Let_x = a^r$ and y = a^s for some integers r, s $\in$Z . Then x, y $\in$ H.

Now x• y^{-1} = $a^r(a^s)^{-1}=a^r a^{-s}=a^{r-s}$ and r - s $\in$Z

x. $y^{-1} \in$ H and hence H is a sub-group of G.

Example

Show that in S_3 the group of symmetries of the equilateral triangle, the set

H =(R_0 , R_{120} R_{240} is a subgroup.

Solution :

+	R_0	R_{120}	R_{240}
R_0	R_0	R_{120}	R_{240}
R_{120}	R_{120}	R_{240}	R_0
R_{240}	R_{240}	R_0	R_{120}

From the above table we see that the set is closed and the set operation is binary.

Associative law :

The composition of functions is always associative.

Identity :

R_0 is the identity element

Inverse :

The inverse of R_0 isR_0

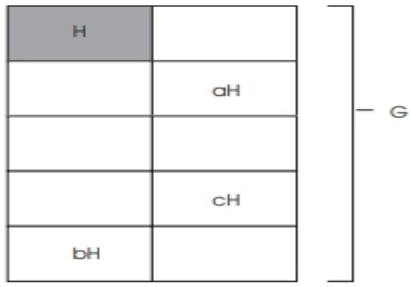
The inverse of R_{120} is R_{240}

The inverse of R_{240} is R_{120}

∴H = {$R_0 R_{120} R_{240}$ } is a group. Since H is a subset of S_3 , H is a subgroup of S_3

Chapter2 - Coset

If H is a subgroup of G, you can break G up into pieces, each of which looks like H:



These pieces are called cosets of H, and they arise by "multiplying" H by elements of G.

Definition.

Let G be a group and let H < G. A left coset of H in G is a subset of the form

gH = {gh | h ∈ H} for some g ∈ G.

The element g is a representative of the coset gH. The collection of left cosets is denoted G/H.Likewise, a right coset is a subset of the form

Hg = {hg | h ∈ H} for some g ∈ G.

The set of right cosets is denoted H\G.

Thus, the left coset *gH* consists of *g* times everything in *H*; *Hg* consists of everything in *H* times *g*.

Example. (Listing the elements of cosets)

(a) List the elements of U_{28} and the elements of the cyclic subgroup generated by 9.

(b) List the elements of the cosets of (9) in U_{28}.

(a) U_{28} = {1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27}.

$$(9) = \{1, 9, 25\}.$$

(b) The subgroup is always a coset. I'll list that first:

$$(9) = \{1, 9, 25\}.$$

Take an element of U_{28} which is not in the subgroup — say 3. Multiply the subgroup by the element:

$$3 \cdot (9) = 3 \cdot \{1, 9, 25\} = \{3 \cdot 1, 3 \cdot 9, 3 \cdot 25\} = \{3, 27, 19\}.$$

Take an element of U_{28} which is not in either of the two known cosets — say 5. Multiply the subgroup by the element:

$$5 \cdot (9) = 5 \cdot \{1, 9, 25\} = \{5 \cdot 1, 5 \cdot 9, 5 \cdot 25\} = \{5, 17, 13\}.$$

Notice that all the cosets have 3 elements — the same as the number of elements in the subgroup.

At this point, there are only 3 elements which aren't in any of the known cosets. These elements make

up the last coset: $\{11, 15, 23\}$. You can check that

$$11 \cdot (9) = \{11, 15, 23\}.$$

3 represents the coset $3 \cdot \langle 9 \rangle$, but a given coset can be represented by any of its elements. For example,

$$19. (9) = 19. \{1, 9, 25\} = \{19 .1, 19. 9, 19. 25\} = \{19, 3, 27\} = 3 \cdot (9).$$

Example. (Listing the elements of cosets)

List the elements of the cosets of 2Z in Z.

Z/2Z consists of two cosets: the even numbers 2Z and the odd numbers. Explicitly,

0 + 2Z = {. . . ,−4,−2, 0, 2, 4, . . .} and 1 + 2Z = {. . . ,−3,−1, 1, 3, . . .}. Notice that when the operation in the group is +, a coset of a subgroup H is written a + H.

Example. (Listing the elements of cosets)

List the elements of the cosets of the subgroup {1,−1} of the group of quaternions.

Here is the table for the group of quaternions:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Consider the subgroup {1,−1}. Its cosets are

1 · {1,−1} = {1,−1}, (−1) · {1,−1} = {−1, 1} = {1,−1},

i · {1,−1} = {i,−i}, (−i) · {1,−1} = {−i, i} = {i,−i},

j · {1,−1} = {j,−j}, (−j) · {1,−1} = {−j, j} = {j,−j},

k · {1,−1} = {k,−k}, (−k) · {1,−1} = {−k, k} = {k,−k}.

There are four distinct cosets. Notice that 2 · 4 = 8. This is a special case of Lagrange's theorem:

The order of a subgroup times the number of cosets of the subgroup equals the order of the group.

Example. (Identifying a set of cosets with another set)

Show that the set of cosets R / Z can be identified with S1, the group of complex numbers of modulus 1 under complex multiplication.

The cosets R / Z are $x + Z$ where $0 \leq x < 1$.

Thus, there is one coset for each number in the half-open interval [0, 1).

On the other hand, you can "wrap" the half-open interval around the circle S1 in the complex plane:

Use $f(t) = e^{2it}$, $0 \leq t < 1$. It's easy to show this is a bijection by constructing an inverse using the logarithm.

Thus, there is a bijection from the set of cosets R/Z to the circle S1.

In fact, this is an example of an **isomorphism** of groups.

Theorem. Let G be a group and let H < G. The left cosets of H in G form a partition of G.

Proof.

we need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.

Let $g \in G$. Since $1 \in H$, it follows that $g \cdot 1 = g$ is in gH. This shows that every element of G lies in some coset of H, so the union of the cosets is all of G.

Next, suppose aH and bH are two cosets of H, and suppose they are not disjoint. I must show they're identical: aH = bH. As usual, I can show two sets are equal by showing that each is contained in the other.

Since aH and bH are not disjoint, I can find an element $g \in aH \cap bH$.

Write $g = ah_1 = bh_2$ for $h_1, h_2 \in H$. Then $a = bh_2h_1^{-1}$

Now let $ah \in aH$. Then $ah = bh_2h_1^{-1} h$.

1

The element on the right is in bH, since it is b times something in H. Therefore,

$ah \in bH$, and $aH \subset bH$.

By symmetry, $bH \subset aH$, so $aH = bH$.

Theorem. Any two left cosets have the same number of elements.

Proof.

Let H be a subgroup of a group G, and let $a, b \in G$. I must show that aH and bH have the same number of elements. By definition, this means that I must construct a bijective map from aH to bH.

An element of aH looks like ah, for some $h \in H$. So it is tempting to simply define

$f : aH \to bH \quad$ by $\quad f(ah) = bh.$

But how do you know this is well-defined? How do you know that the same element of aH might not be expressed as both ah and ah′, where h and h′ are different elements of H?

Fortunately, this can't happen; if $ah = ah'$, then

$$a^{-1}ah = a^{-1}ah', \text{ so } h = h'.$$

Thus, it's legitimate for me to define a function f as above.

Likewise, I can define $g : bH \to aH$ by

$$g(bh) = ah \text{ for } bh \in bH.$$

This is well-defined, just as f was.

Since f and g are clearly inverses, f (or g) is a bijection, and aH and bH have the same number of elements.

Definition. If G is a group and $H < G$, $|G/H|$ is called the **index** of H in G, and is denoted $(G : H)$.

The way we've defined it, the index of H in G is the number of left cosets of H. It turns out that this is the same as the number of right cosets.

Theorem. (Lagrange's theorem) Let G be a finite group and let H be a subgroup of G. Then (G : H) = $\frac{|G|}{|H|}$

Proof.

The cosets of H partition G into (G : H) pieces, and each piece contains |H| elements. So the total number of elements in the (G : H) pieces is (G : H) · |H|, but this is all of G:

(G : H) · |H| = |G|.

Now divide both sides by |H|.

Note that this result implies that the order of a subgroup divides the order of the group. Thus, a group of order 14 could have subgroups of order 1, 2, 7, or 14, but could not have a subgroup of order 5.

Example. (A specific example of Lagrange's theorem) Verify Lagrange's theorem for the subgroup H = {0, 3} of Z_6.

The cosets are

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

Notice there are 3 cosets, each containing 2 elements, and that the cosets form a partition of the group.

Example. (A specific example of Lagrange's theorem) List the elements of the cosets of $\langle h(2,2) \rangle$ in $Z_4 \times Z_6$.

First, list the elements of the subgroup:

$\langle (2,2) \rangle$ = {(0, 0), (2, 2), (0, 4), (2, 0), (0, 2), (2, 4)}.

The subgroup is a coset.

The subgroup has 6 elements and the group has 24. By Lagrange's theorem, there are 4 cosets.

(1, 1) isn't in the subgroup; add it to the subgroup:

$(1, 1) + \langle(2,2)\rangle = \{(1, 1), (3, 3), (1, 5), (3, 1), (1, 3), (3, 5)\}$.

(2, 1) isn't in either of the known cosets; add it to the subgroup:

$(2, 1) + \langle(2,2)\rangle = \{(2, 1), (0, 3), (2, 5), (0, 1), (2, 3), (0, 5)\}$.

The remaining elements make up the fourth coset. I can find them by noting that (1, 2) isn't in the three known cosets, so the fourth coset is represented by (1, 2):

$(1, 2) + \langle(2,2)\rangle = \{(1, 2), (3, 4), (1, 0), (3, 2), (1, 4), (3, 0)\}$.

Notice that there are 4 cosets, each containing 6 elements, and the cosets form a partition of the group.

Corollary. Every group of prime order is cyclic.

Proof.

Suppose G is a group of order p, where p is prime. Let g $\in$ G, g 6= 1. hgi is a subgroup of G, and since g $\neq$ 1, |(g)| $\neq$ 1.

But |(g)| divides |G| by Lagrange's theorem, and the only positive numbers which divide |G| = p are 1 and p. Therefore, |(g)| = p, which means that (g) is all of G. That is, G is cyclic with generator g.

For example, this means that the only group of order 17 is the cyclic group of order 17.

I noted earlier that the number of left cosets equals the number of right cosets; here's the proof.

Proposition.

Let G be a group, H < G. The set of left cosets G/H may be put in 1-1 correspondence with the set of right cosets H\G.

Proof.

Define $Ø : G/H \to H\backslash G$ by $Ø(gH) = Hg^{-1}$. I need to show Ø- is well-defined.

Suppose aH = bH. Then $a = a \cdot 1 \in aH = bH$, so a = bh for some $h \in H$. Then

$Ø(aH) = Ha^{-1} = H(bh)^{-1} = Hh^{-1}b^{-1} = Hb^{-1} = Ø(bH)$.

Next, define $\chi : H\backslash G \to G/H$ by $\chi(Hg) = g^{-1}H$. A computation similar to the one I just did shows is well Ø defined. χ and are inverses, so either one gives a bijection of G/H with H\G.

While there are the same number of left and right cosets, the left and right cosets may be different as sets. In fact, if the left and right cosets are the same as sets, the subgroup is said to be **normal**. It's a very important condition on a subgroup, since it will allow us to turn the set of left (or right) cosets into a **quotient group.**

Example.

(A subgroup whose left and right cosets are different) List the elements of the left cosets and the right cosets of the subgroup {id, (1 2)} of S_3.

The left cosets are

{id, (1 2)}, (1 3){id, (1 2)} = {(1 3), (1 2 3)}, (2 3){id, (1 2)} = {(2 3), (1 3 2)}.

The right cosets are

{id, (1 2)}, {id, (1 2)}(1 3) = {(1 3), (1 3 2)}, {id, (1 2)}(2 3) = {(2 3), (1 2 3)}.

The left and right cosets aren't the same, though there are the same number of left and right cosets.

Chapter 3 Lagrange's Theorem

Proposition

Let H *be a subgroup of* G *with* $g \in G$ *and define a map* $\phi: H \to gH$ *by* $.\phi(h)=gh$. *The map* ϕ *is bijective; hence, the number of elements in* H *is the same as the number of elements in* gH.

Proof:

We first show that the map ϕ is one-to-one.

Suppose that $\phi(h_1)=\phi(h_2)$ for elements $h_1, h_2 \in H$.

We must show that $h_1=h_2$, but $\phi(h_1)=gh_1$ and $\phi(h_2)=gh_2$. So $,gh_1=gh_2$, and by left cancellation $.h_1=h_2$. To show that ϕ is onto is easy. By definition every element of gH is of the form gh for some $h \in H$ and $\phi(h) = gh$.

Theorem : Lagrange.

Let G *be a finite group and let* H *be a subgroup of* .G. *Then* $|G| / |H| = [G:H]$ *is the number of distinct left cosets of* H *in* G. *In particular, the number of elements in* H *must divide the number of elements in* G.

Proof

The group G is partitioned into [G:H] distinct left cosets. Each left coset has |H| elements; therefore, $|G|=[G:H]|H|$.

Corollary

Suppose that G *is a finite group and* $.g \in G$. *Then the order of* g *must divide the number of elements in* G.

Corollary

Let $|G|=p$ *with* p *a prime number. Then* G *is cyclic and any* $g \in G$ *such that* $g \neq e$ *is a generator.*

Proof

Let g be in G such that .g≠e. Then by Corollary 6.11, the order of gg must divide the order of the group. Since |⟨ g⟩ |>1, it must be p.. Hence, g generates .G.

Corollary

Let |G|=p| with p a prime number. Then G is cyclic and any g∈G such that g≠e is a generator.

Proof

Let g be in G such that g≠e. Then by Corollary ,

Corollary : ***Suppose that*** G ***is a finite group and*** .g∈G. ***Then the order of*** g ***must divide the number of elements in*** G.

the order of g must divide the order of the group. Since |⟨ g⟩ | >1, it must be p. Hence, g generates G.

Corollary

Let H *and* K *be subgroups of a finite group* G *such that* G⊃H⊃K.. *Then* [G:K]=[G:H][H:K].

Proof

Observe that

[G:K] = |G| / |K| = |G| / |H| · |H| / |K| = [G:H][H:K]..

Remark : The converse of Lagrange's Theorem is false.

The group A4 has order 12; however, it can be shown that it does not possess a subgroup of order 6. According to Lagrange's Theorem, subgroups of a group of order 12 can have orders of either 1,2, 3, 4, or 6. However, we are not guaranteed that

subgroups of every possible order exist. To prove that A4 has no subgroup of order 6, we will assume that it does have such a subgroup H and show that a contradiction must occur. Since A4 contains eight 3-cycles, we know that H must contain a 3-cycle. We will show that if H contains one 3-cycle, then it must contain more than 6 elements.

Proposition.

The group A_4 *has no subgroup of order* 6.

Proof

Since $[A_4:H] = 2$, there are only two cosets of H in A_4. In as much as one of the cosets is H itself, right and left cosets must coincide; therefore, $gH=Hg$ or $gHg^{-1}=H$ for every $g \in A_4$.. Since there are eight 3-cycles in A_4, at least one 3-cycle must be in H. Without loss of generality, assume that (123) is in H. Then (123)-1=(132) must also be in H. Since $ghg^{-1} \in H$ for all $g \in A_4$ and all $h \in H$ and

(124)(123)(124)-1=(124)(123)(142)=(243)

(243)(123)(243)-1=(243)(123)(234)=(142)

we can conclude that H must have at least seven elements

(1),(123),(132),(243),(243)−1=(234),(142),(142)−1=(124).

Therefore, A_4 has no subgroup of order 6.

Theorem

Two cycles τ and μ in Sn have the same length if and only if there exists a $\sigma \in$ Sn such that $\mu=\sigma\tau\sigma-1$.

Proof

Suppose that

$\tau=(a1,a2,\ldots,ak)$

$\mu=(b1,b2,\ldots,bk)$

Define σ to be the permutation

$\sigma(a1)=b1$

$\sigma(a2)=b2$

$\vdots$

$\sigma(ak)=bk$

Then $\mu=\sigma\tau\sigma-1$.

Conversely, suppose that $\tau=(a1,a2,\ldots,ak)$ is a k-cycle and $\sigma \in Sn$. If $\sigma(ai)=b$ and $\sigma(a(imodk)+1)=b'$, then $\mu(b)=b'$. Hence,

$\mu=(\sigma(a1),\sigma(a2),\ldots,\sigma(ak))$.

Since σ is one-to-one and onto, μ is a cycle of the same length as τ.

Chapter 4 - Normal subgroups

Definition A subgroup H of the group G is called a **normal** subgroup if

$ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Proposition Let H be a subgroup of the group G. The following conditions are equivalent:

(1) H is a normal subgroup of G;

(2) aH = Ha for all $a \in G$;

(3) for all $a,b \in G$, abH is the set theoretic product (aH)(bH);

(4) for all $a,b \in G$, $ab^{-1} \in H$ if and only if $a^{-1}b \in H$.

Example Any subgroup of index 2 is normal.

Factor groups

Proposition Let N be a normal subgroup of G, and let $a,b,c,d \in G$.
If $aN = cN$ and $bN = dN$, then $abN = cdN$.

Theorem If N is a normal subgroup of G, then the set of left cosets of N forms a group under the coset multiplication given by $aNbN = abN$ for all $a,b \in G$.

Definition If N is a normal subgroup of G, then the group of left cosets of N in G is called the **factor group** of G determined by N. It will be denoted by G/N.

Example . Let N be a normal subgroup of G. If $a \in G$, then the order of aN in G/N is the smallest positive integer n such that $a^n \in N$.

Chapter 5- Quotient groups

Now that we've learned a bit about quotients, we should build more examples.

Integers mod n, Again
When N is a normal subgroup of a group G, the ***quotient group*** G/N is obtained by "*collapsing the elements of N to the identity.*" More precisely, the set G/N is

defined as the set of equivalence classes where two elements g, h are considered equivalent if the cosets gN and hN are the same.

By far the most well-known example is G = Z, N = nZ, where n is some positive integer and the group operation is addition. Then G/N is the additive group Z*n* of integers modulo n. So the quotient group construction can be viewed as a generalization of modular arithmetic to arbitrary groups. In fact, the quotient group G/N is read "*G* mod N."

Definition

The quotient G/H is a well-defined set even when H is not normal.

Let G be a group and H a subgroup. Then G/H is the set of left cosets, gH = { gh : h ∈ H }, as g runs over the elements of G.

This set is used in the proof of Lagrange's theorem, for instance. In fact, the proof of Lagrange's theorem establishes that if G is finite, then |G/H| = |G|/|H|.

Note that $g1\ H = g2\ H \Leftrightarrow H = g_1^{-1}\ g_2\ H \Leftrightarrow g_1^{-1}\ g_2 \in H.$

If N is normal, then the set G/N has a natural group structure; because

Ng2 = g2 N

.(g1N)(g2N) = g1g2NN = g1g2N.

This gives a formula for multiplying cosets. Another way to express this formula is as follows:

If N is a normal subgroup of G, then the function $\pi: G \to G/N$ given by $\pi(g) = gN$ is a group homomorphism.

Representatives and Notation

The definition of the quotient group uses cosets, but they are somewhat unwieldy to work with. It is often easier to denote the coset gN by the notation $\bar{g}$; then $\bar{g}_1\bar{g}_2 = \overline{g_1 g_2}$ as expected. The important point is that this is true no matter which representatives g1 ,g2 are chosen: if $\bar{g_1}' = \bar{g_1}$ and $\bar{g_2}' = \bar{g_2}$, then $g_1' g_2' = g_1 n_1 g_2 n_2 = g_1 g_2 (g_2^{-1} n_1 g_2) n_2) \in g_1 g_2 N$, so $\bar{g}_1'\bar{g}_2' = \overline{g_1 g_2}$. Another way to say this is as follows: the coset containing the product of two coset representatives is independent of the choice of representatives.

This is not true if N is not normal.

Let $G = S_3$, the symmetric group on three symbols. Let H be the two-element subgroup generated by the transposition (12). Then G/H consists of three cosets:

H={id,(12)}

(13)H={(13),(123)}

(23)H={(23),(132)}.

Since H is not normal, it does not inherit the group structure from G; in other words, the product of two coset representatives will land in a coset that is not independent of the choice of representatives.

For example, taking $\mathrm{id} \in H$ and $(13) \in (13)H$, the product of these two representatives is (13), which is in .(13)H. But instead taking $(12) \in H$ and $(13) \in (13)H$, we find $(12)(13) = (132) \in (23)H$.

Example: Integers mod 6

When $G = Z$ (with group law given by addition) and $N = 6Z$, the quotient G/N is the set of cosets of N. The coset representatives that are usually chosen are $0,1,2,3,4,5$. So for instance the coset $1+6Z$ is abbreviated $\bar{1} \in Z6$, and

$Z6 = \{0,1,2,3,4,5\}$.

The addition in $Z6$ is as expected: $\bar{a} + \bar{b} = \overline{a+b}$. If $a + b > 6$, subtracting 6 will give the coset representative in the range $\{0,1,2,3,4,5\}$. For example, $\bar{3} + \bar{5} = \bar{8} = \bar{2}$. Here $\bar{8} = \bar{2}$ because $8-2 \in 6Z$, so $8 + 6Z = 2 + 6Z$.

First Isomorphism Theorem

The three fundamental isomorphism theorems all involve quotient groups. The most important and basic is the first isomorphism theorem; the second and third theorems essentially follow from the first. Here are some examples of the theorem in use.

(First Isomorphism Theorem) A group homomorphism $\phi : G \to H$ induces an isomorphism $\phi : G/\ker(\phi) \to \text{im}(\phi)$ defined naturally by $\bar{\Phi}(\bar{g}) = \phi(g)$.

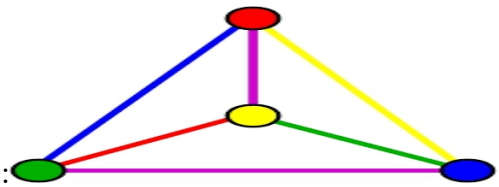
The complex numbers z such that $|z| = 1$ form a group under multiplication. Call this group C (for unit circle). Show that $R/Z \cong C$, where R and Z denote the additive groups of real numbers and integers, respectively.

Consider the function $\phi : R \to C$ given by $\phi(r) = e^{2\pi ir}$. Then ϕ is clearly surjective, because every complex number with absolute value 11 can be written as $e^{i\theta}$ for some real number \thetaθ (by Euler's formula). The kernel of \phiϕ is the set of real numbers r such that ,$e^{2\pi ir} = 1$, i.e. $\cos(2\pi r) = 1$ and $\sin(2\pi r) = 0$. This happens if and only if rr is an integer, so $\ker(\phi) = Z$.

The result follows directly from the first isomorphism theorem.

Another example of the first isomorphism theorem is an appealingly nontrivial example of a non-abelian group and its quotient.

Consider the symmetric group S_4 on four symbols. It permutes the vertices of this tetrahedron

: 

Disjoint pairs of edges are preserved. [1]There are three pairs of disjoint edges: the two purple edges, the blue/green pair, and the red/yellow pair. Any permutation of the vertices will permute the edges in such a way as to move these pairs onto each other. For instance, a transposition of the red and yellow vertices will fix the purple edge pair, but the red/yellow pair will swap places with the blue/green pair.

So any permutation in S4 will have an associated permutation of these three objects (the edge pairs). This gives a function $\phi : S4 \rightarrow S3$. It is a homomorphism (essentially tautologically, since the group operation on both sides is just composition of functions). Its kernel V4 has four elements in it, consisting of the identity and the three double transpositions. (Any double transposition will fix both edges in one pair, and will swap the edges in the other two pairs. For example, swapping the yellow and red vertices and then swapping the blue and green vertices will leave the purple edge pair unchanged, but will swap the blue and green edges, and the yellow and red edges. The three pairs stay in the same place, even though the two edges in some pairs may have switched places.) And it is not hard to show that ϕ is surjective.

So the first isomorphism theorem gives an isomorphism $\phi :S4 / V4 \cong S3$.

Chapter 6- Group homomorphisms

3.7.1. Definition Let G_1 and G_2 be groups, and let $\theta : G_1 \to G_2$ be a function. Then θ is said to be a **group homomorphism** if

$\theta(ab) = \theta(a)\,\theta(b)$ for all $a,b \in G_1$.

Example 3.7.1. (Exponential functions for groups) Let G be any group, and let a be any element of G. Define $\theta : \mathbf{Z} \to G$ by $\theta(n) = a^n$, for all $n \in \mathbf{Z}$. This is a group homomorphism from **Z** to G.
If G is abelian, with its operation denoted additively, then we define $\theta : \mathbf{Z} \to G$ by $\theta(n) = na$.

Example 3.7.2. (Linear transformations) Let V and W be vector spaces. Since any vector space is an abelian group under vector addition, any linear transformation between vector spaces is a group homomorphism.

3.7.2. Proposition If $\theta : G_1 \to G_2$ is a group homomorphism, then

(a) $\theta(e) = e$;

(b) $(\theta(a))^{-1} = \theta(a^{-1})$ for all $a \in G_1$;

(c) for any integer n and any $a \in G_1$, we have $\theta(a^n) = (\theta(a))^n$;

(d) if $a \in G_1$ and a has order n, then the order of $\theta(a)$ in G_2 is a divisor of n.

Example 3.7.4. (Homomorphisms defined on cyclic groups) Let C be a cyclic group, denoted multiplicatively, with generator a. If $\theta : C \to G$ is any group homomorphism, and $\theta(a) = g$, then the formula $\theta(a^m) = g^m$ must hold. Since every element of C is of

the form a^m for some integer m, this means that θ is completely determined by its value on a.

If C is infinite, then for an element g of any group G, the formula $\theta(a^m) = g^m$ defines a homomorphism.

If $|C|=n$ and g is any element of G whose order is a divisor of n, then the formula $\theta(a^m) = g^m$ defines a homomorphism.

Example 3.7.5. (Homomorphisms from $\mathbf{Z}_n$ to $\mathbf{Z}_k$) Any homomorphism $\theta : \mathbf{Z}_n \to \mathbf{Z}_k$ is completely determined by $\theta([1]_n)$, and this must be an element $[m]_k$ of $\mathbf{Z}_k$ whose order is a divisor of n. Then the formula $\theta([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$, defines a homomorphism. Furthermore, every homomorphism from $\mathbf{Z}_n$ into $\mathbf{Z}_k$ must be of this form. The image $\theta(\mathbf{Z}_n)$ is the cyclic subgroup generated by $[m]_k$.

3.7.3 Definition Let $\theta : G_1 \to G_2$ be a group homomorphism. Then

$\{ x \in G_1 \mid \theta(x) = e \}$

is called the **kernel** of θ, and is denoted by $\ker(\theta)$.

3.7.4 Proposition Let $\theta : G_1 \to G_2$ be a group homomorphism, with $K = \ker(\theta)$.

(a) K is a normal subgroup of G.

(b) The homomorphism θ is one-to-one if and only if $K = \{e\}$.

3.7.6 Proposition Let $\theta : G_1 \to G_2$ be a group homomorphism.

(a) If H_1 is a subgroup of G_1, then $\theta(H_1)$ is a subgroup of G_2.

If θ is onto and H_1 is normal in G_1, then $\theta(H_1)$ is normal in G_2.

(b) If H_2 is a subgroup of G_2, then

$\theta^{-1}(H_2) = \{ x \in G_1 \mid \theta(x) \in H_2 \}$

is a subgroup of G_1.

If H_2 is normal in G_2, then $\theta^{-1}(H_2)$ is normal in G_1.

3.8.6. Proposition Let N be a normal subgroup of G.

(a) The natural projection mapping $\pi : G \to G/N$ defined by $\pi(x) = xN$, for all $x \in G$, is a homomorphism, and $\ker(\pi) = N$.

(b) There is a one-to-one correspondence between subgroups of G/N and subgroups of G that contain N. Under this correspondence, normal subgroups correspond to normal subgroups.

Example If m is a divisor of n, then $\mathbf{Z}_n / m\mathbf{Z}_n \cong \mathbf{Z}_m$.

3.8.8. Theorem [Fundamental Homomorphism Theorem] Let G_1, G_2 be groups. If $\theta : G_1 \to G_2$ is a group homomorphism with $K = \ker(\theta)$, then

$G_1/K \cong \theta(G_1)$.

3.8.9. Definition The group G is called a **simple** group if it has no proper nontrivial normal subgroups.

QUESTION AND ANSWER FOR PRACTICE

1. Define subgroup
   A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a induced composition in H and for this induced composition H itself is a group.
2. Define improper subgroup:
   A subgroup containing only one element is identity element {e} and G are known as improper (or) trivial subgroups.
3. Define proper subgroup
   A subgroup other than {e} and G are known as proper subgroup.
4. Give two examples of a subgroup
   Multiplication group {1,-1} is a subgroup of the group {1,-1,i,-i}.
   The addition group of even integers is a subgroup of the addition group of all integers.
5. Give an example in which H is a subset of a group G and H^{-1}=H but H is not a subgroup of G
6. Prove that if H is any subgroup of G then $HH = H$
   Let h_1, h_2 be any element of HH where $h_1 \in H, h_2 \in H$. Since H is a subgroup of G , therefore
   $h_1 \, h_2 \in H \Rightarrow h_1 h_2 \in H$
   $\therefore HH \subseteq H$
   Now let h be any element of H. Then we can write $h = he$ where e is the identity of G. Now $he \in HH$, since $h \in H, e \in H$. Thus $H \subseteq HH$
   Hence HH = H.
7. Define right coset
   Suppose G is a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G generated by a.
8. If G is the additive group of integers and H is the subgroup of G obtained on multiplying the elements of G by 3 then find the right coset decomposition of G with respect to H.
   $G = H \cup (H+1) \cup (H+2)$.
9. Define index of a subgroup in a group
   If H is a subgroup of a group G, the number of distinct right(left) cosets of H in G is called the index of H in G and is denoted by $i_G(H)$
10. State Lagrange's theorem
    The order of each subgroup of a finite group is a divisor of the order of the group.
11. Define Normal subgroup

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

12. Define improper normal subgroup

Every group G possesses at least two normal subgroups namely G itself and the subgroup consisting of the identity element e alone. These are called improper subgroups.

13. Define simple group.

A group having no proper normal subgroups is called a simple group.

14. Show that every subgroup of an abelian group is normal.

Let G be abelian group and H be. a subgroup of G. Let x be any element of G and h any element of H, we have $xhx^{-1} = xx^{-1}h = eh = h \in H$. Thus $x \in G, h \in H \Rightarrow xhx^{-1} \in H$. Hence H is normal in G.

15. Define normalizer of an element of a group.

If $a \in G$, then N(a), the normalizer of a in G is the set of all those element of G which commute with a. Symbolically $N(a) = \{x \in G : \text{ax} = \text{xa}\}$.

16. Define Quotient group

If G is a group and H is a subgroup of G then the set of cosets of H in G is a group with respect to multiplication of cosets. It is called the Quotient group G/H in H.

17. Show that every quotient group of an abelian group is abelian

Let G be an abelian group and H be a subgroup of G. Then H is normal subgroup of G. If $a, b \in G$ then Ha, Hb are any two elements of G/H. We have,

$$(Ha)(Hb) = Hab = Hba$$
$$= (Hb)(Ha)$$

.

Therefore G/H is abelian.

18.Define onto homomorphism of groups

A mapping f from a group G onto a group G' is said to be a homomorphism of G onto G' if $f(ab) = f(a)f(b) \forall \text{a, b} \in \text{G}$. Also then G' is said to be a homomorphic image of G.

19.If f is a homomorphism of a group G into a group G' then $f(e) = e'$ where e is the identity of G and e' is the identity of G'

Let $a \in G$. Then $f(a) \in G'$. We have

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

Now G' is a group . Therefore

$$f(a)e' = f(a)f(e)$$
$$\Rightarrow e' = f(e)$$
$$f(ab) = f(a)f(b) \forall \text{a, b} \in \text{G}$$

20. Define kernel of a Homomorphism

If f is a homomorphism of a group G into a group G', then the set K of all those elements of G which are mapped by f onto the identity e' of G' is called the kernel of the homomorphism f.

Thus if f is a homomorphism of G into G', then K is the kernel of f if

$K = \{x \in G : f(x) = e'$ is the identity of G′

All the best

Unit-II

1. Define subgroup
   A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a induced composition in H and for this induced composition H itself is a group.

2. Define improper subgroup:
   A subgroup containing only one element is identity element {e} and G are known as improper (or) trivial subgroups.

3. Define proper subgroup
   A subgroup other than {e} and some element in G are known as proper subgroup.

4. Give two examples of a subgroup
   Multiplication group H= {1,-1} is a subgroup of the group G={1,-1,i,-i}.

x	1	-1
1	1	-1
-1	-1	1

   The addition group of even integers is a subgroup of the addition group of all integers.
   INTEGERS Z = I = { ……-4, -3, -2, -1,0,1, 2, 3, 4,……}
   EVEN INTEGERS= {……..-6, -4, -2, 0, 2, 4, 6,……..}

5. Give an example in which H is a subset of a group G and H^{-1}=H but H is not a subgroup of G

6. Prove that if H is any subgroup of G then $HH = H$
   Let h_1, h_2 be any element of HH where $h_1 \in H, h_2 \in H$.
   Since H is a subgroup of G , therefore
   $h_1 \, h_2 \in H \Rightarrow h_1 h_2 \in H$
   $\therefore HH \subseteq H$ --------(1)
   Now let h be any element of H. Then we can write $h = he$ where e is the identity of G. Now $he \in HH$, since $h \in H, e \in H$.
   Thus $H \subseteq HH$ -----(2)
   Hence HH = H.

7. Define right coset
   Suppose G is a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G generated by a.

Example:
G= {-1,1,i, -i} group
H= {1,-1} subgroup
1 Ɛ G
H.1 = RIGHT COSET = {1.1 , -1.1}= Ha

8. If G is the additive group of integers and H is the subgroup of G obtained on multiplying the elements of G by 3 then find the right coset decomposition of G with respect to H.
   $G = H \cup (H+1) \cup (H+2)$.
9. Define index of a subgroup in a group
   If H is a subgroup of a group G, the number of distinct right(left) cosets of H in G is called the index of H in G and is denoted by $i_G(H)$

10. State Lagrange's theorem

The order of each subgroup of a finite group is a divisor of the order of the group.

O(G)/O(H)

11. Define Normal subgroup

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

12. Define improper normal subgroup

Every group G possesses at least two normal subgroups namely G itself and the subgroup consisting of the identity element e alone. These are called improper normal subgroups.

13. Define simple group.

A group having no proper normal subgroups is called a simple group.

14. Show that every subgroup of an abelian group is normal.

Let G be abelian group and H be a subgroup of G. Let x be any element of G and h any element of H, we have $xhx^{-1} = xx^{-1}h = eh = h \in H$.

Thus $x \in G, h \in H \Rightarrow xhx^{-1} \in H$. Hence H is normal in G.

15. Define normalizer of an element of a group.

If $a \in G$, then N(a), the normalizer of a in G is the set of all those element of G which commute with a. Symbolically $N(a) = \{x \in G : \text{ax} = \text{xa}\}$.

16. Define Quotient group

If G is a group and H is a subgroup of G then the set of cosets of H in G is a group with respect to multiplication of cosets. It is called the Quotient group G/H in H.

17. How that every quotient group of an abelian group is abelian

Let G be an abelian group and H be a subgroup of G. Then H is quotient group of G. If $a, b \in G$ then Ha, Hb are any two elements of G/H. We have,

$$(Ha)(Hb) = Hab = Hba$$
$$= (Hb)(Ha)$$

Therefore G/H is abelian.

18.Define onto homomorphism of groups

A mapping f from a group G onto a group G' is said to be a homomorphism of G onto G' if $f(ab) = f(a)f(b) \forall a, b \in G$. Also then G' is said to be a homomorphic image of G.

17. I

f f is a homomorphism of a group G into a group G' then $f(e) = e'$ where e is the identity of G and e' is the identity of G'

Let $a \in G$. Then $f(a) \in G'$. We have

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

Now G' is a group . Therefore

$$f(a)e' = f(a)f(e)$$
$$\Rightarrow e' = f(e)$$
$$f(ab) = f(a)f(b) \forall a, b \in G$$

18. D

efine kernel of a Homomorphism

If f is a homomorphism of a group G into a group G', then the set K of all those elements of G which are mapped by f onto the identity e' of G' is called the kernel of the homomorphism f.

Thus if f is a homomorphism of G into G', then K is the kernel of f if

$K = \{x \in G : f(x) = e'$ is the identity of G'

1.Prove that

i) **The identity of a subgroup in the same as that of the group.**

ii) **The inverse of any element of a subgroup in the same as the inverse of the same regarded as an element of the group.**

iii) **The order of any element of a subgroup is the same as the order of the element regained as a member of the group.**

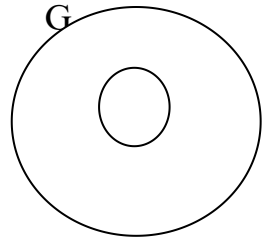
i) Let H be a sub-group of a group G. Prove that the identity element of subgroup H is the same as the identity element of the group G.

Proof:

Let e be the identity element in G and e_1 be the identity element in H.

Let a be any element in H. Then a ε G

Since a ε G, a•e = a ….(1)



Since a ε H, a •e_1= a …….(2)

From (1) and (2), a • e = a • e_1

∴By left cancellation law, e = e_1

Hence both H and G have the same identity element.

II) **Property 2**

Let H be a subgroup of G. Prove that the inverse of an element a ε H is the same as the inverse of a ε G (Or)

The inverse of an element in a subgroup is the same as the inverse of that element in the group.

Proof :

Let a ε H , then a ε G .

Let a' and a" be the inverses of a in H and G respectively.

Then a • a' = a' • a = e ….(1)

a • a" = a" • a = e ----(2)

∴a • a' = a • a"

Hence by left cancellation law, a' = a"

∴ The inverse of a in H is the same as the inverse of a in G.

III) Lemma.

Suppose that G is a group containing an element g with $g^n = e$.

There is a unique group homomorphism f : Zn -> G such that f(1) = g. In particular every group of order n with an element of order n is isomorphic to Zn.

Proof.

Suppose that f : Zn -> G is a homomorphism such that f(1) = g.

Then for a = 0, 1,……, n-1, f(a +n 1) = f(a).f(1) = f(a)g. Thus we can see inductively that

$f(a) = g^a$ for all a Ɛ Zn. Thus if f exists then it is unique.

We now see how to construct f. We define $f(a) = g^a$ for all a Ɛ Zn and we must prove that this defines a homomorphism.

That is we must show that g^{a+nb} = f(a+n b) and g^{a+b} = f(a)f(b) are equal for all a, b ε Zn.

Since a+b - (a+n b) = kn for some integer k and $g^n = e$, we see that

$$g^{a+b}g^{-(a+n\,b)} = (g^n)^k = e^k = e:$$

Thus $g^{a+b} = g^{a+nb}$ as claimed.

Suppose now that G has order n and g Ɛ G has order n.

By the previous part there is a homomorphism f : Zn -> G such that f(a) = g^a for each a Ɛ Zn.

Suppose that f(a) = f(b) for a, b Ɛ Zn. Then f(b - $_n$ a) = $g^{a.-nb}$ = e thus a = b else g would have order strictly smaller than n. It follows that ker f = {e} and | Im f| has n elements and so must be the whole of G. Thus f is an isomorphism.

2.A non-empty subset H of a group G is a subgroup of G iff

(i) $a \in H, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$ **where a^{-1} is the inverse of a in G.**

Or

Theorem: Let H be a nonempty subset of a group G. H is a subgroup of G iff (i) H is closed under the operation in G and (ii) every element in H has an inverse in H.

Proof.

Properties (i) and(i i) are, respectively, the closure and inverse axioms of a group.

Associativity holds in H, since it holds already in G.

We only need to verify that e Ɛ H.

But (i) and(i i) together imply that e = aa^{-1} Ɛ H. Therefore, H is a group.

Or

Suppose H is a subgroup of G, then H must be closed with respect to composition a in G, i.e. a∈H, b∈H⇒a∘ b∈H.

Let a ɛH and a^{-1} be the inverse of a in G.

Then the inverse of a in H is also a^{-1}.

As H itself is a group, each element of H will possess inverse in it,

i.e. $a \in H \Rightarrow a^{-1} \varepsilon H$.

Thus the condition is necessary. Now let us examine the sufficiency of the condition

(i) Closure Axiom: $a \in H, b \in H \Rightarrow a \circ b \in H$. Hence the closure axiom is satisfied with respect to the operation .

(ii) Associative Axiom: Since the elements of H are also the elements of G, the composition is associative in H also.

(iii) Existence of Identity: The identity of the subgroup is the same as the identity of the group because $a \varepsilon H, a^{-1} \in H \Rightarrow a \circ a - 1 \in H \Rightarrow e \in H$. The identity e is an element of H.

(iv) Existence of Inverse: Since $a \in H \Rightarrow a^{-1} \in H, \forall a \in H$. Therefore each element of H possesses an inverse.

The H itself is a group for the composition $\circ$ in G. Hence H is a subgroup.

3.Prove that a necessary and sufficient condition for a non- empty subset H of a group G to be subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.

Proof: The condition is necessary.

Suppose H is a subgroup of G and let $a \varepsilon H, b \varepsilon H$.

Now each element of H must possess an inverse because H itself is a group.

$$b \in H \Rightarrow b^{-1} \varepsilon H$$

Also H is closed under the composition ∘ in G. Therefore

$$a\varepsilon H, b^{-1} \in H \Rightarrow a \circ b^{-1} \varepsilon H$$

The condition is sufficient. If it is given that $a\varepsilon H, b^{-1} \in H \Rightarrow a \circ b^{-1} \varepsilon H$ then we have to prove that H is a subgroup.

(i) Closure Property: Let $a, b \varepsilon H$ then $b \in H \Rightarrow b-1 \varepsilon H$ (as shown above). Therefore by the given condition:

$$a\varepsilon H, b^{-1} \in H \Rightarrow a \circ (b^{-1})^{-1} \in H \Rightarrow a \circ b \in H$$

Thus H is closed with respect to the composition ∘ in G.

(ii) Associative Property: Since the elements of H are also the elements of G, the composition is associative in H.

(iii) Existence of Identity: Since

$$a\varepsilon H, a^{-1} \in H \Rightarrow a \circ a^{-1} \in H \Rightarrow e \in H$$

(iv) Existence of Inverse: Let $a \varepsilon H$, then

$$e \in H, a \in H \Rightarrow e \circ a{-}1 \in H \Rightarrow a^{-1} \varepsilon H$$

Then each element of H possesses an inverse.

Hence H itself is a group for the composition ∘ in group G.

4. Prove that if H_1 and H_2 are two subgroup of a group G then $H_1 \cap H_2$ is also a subgroup of G.

Proof: Let H1 and H2 be any two subgroups of G.

Then $H1 \cap H2 \neq \phi$ because at least the identity element e is common in both H1 and H2.

Now to prove that $H1 \cap H2$ is a subgroup of G, it is sufficient to show that $a \in H1 \cap H2$, $b \in H1 \cap H2 \Rightarrow a.b^{-1} \in H1 \cap H2$, $\circ$ being a composition in G.

Since

$a \in H1 \cap H2 \Rightarrow a \varepsilon H1$ and $b \varepsilon H2$ and $b \varepsilon H1 \cap H2 \Rightarrow H1b \in H1 \cap H2 \Rightarrow H1$ and $b \in H2$ and H1, H2 are subgroups of G we see that

$a \in H1, b \in H1 \Rightarrow a \circ b^{-1} \in H1$ and similarly $a \in H2, b \in H2 \Rightarrow a \circ b^{-1} \in H2$

Thus,

$a \circ b^{-1} \in H1, a \circ b^{-1} \in H2 \Rightarrow a \circ b^{-1} \in H1 \cap H2$

which establishes that $H1 \cap H2$ is a subgroup of G

5. Prove that if a, b are any two element of a group G and H any subgroup of G $a \in Hb \Leftrightarrow Ha = Hb$ **and** $a \in bH \Leftrightarrow aH = bH.$

(OR)

Prove that any two right (left) co-set of a subgroup are other disjoint or identical.

Proof.

we need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.

Let g ε G. Since 1 ε H, it follows that g · 1 = g is in gH. This shows that every element of G lies in some coset of H, so the union of the cosets is all of G.

Next, suppose aH and bH are two cosets of H, and suppose they are not disjoint. I must show they're identical: aH = bH. As usual, I can show two sets are equal by showing that each is contained in the other.

Since aH and bH are not disjoint, I can find an element $g \in aH \cap bH$.

Write $g = ah_1 = bh_2$ for $h_1, h_2 \in H$. Then $a = bh_2h_1^{-1}$

Now let $ah \in aH$. Then $ah = bh_2h_1^{-1} h$.

The element on the right is in bH, since it is b times something in H. Therefore,

$ah \in bH$, and $aH \subset bH$.

By symmetry, $bH \subset aH$, so $aH = bH$.

UNIT 3 - Abstract Algebra

Chapter1 - Isomorphism of groups

Definition. Let G_1 and G_2 be groups, and let $\theta : G_1 \to G_2$ be a function. Then θ is said to be a **group isomorphism** if

(i) θ is one-to-one and onto and

(ii) $\theta(ab) = \theta(a)\,\theta(b)$ for all $a,b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and this is denoted by $G_1 \cong G_2$.

Proposition. Let $\theta : G_1 \to G_2$ be an isomorphism of groups.

(a) If a has order n in G_1, then $\theta(a)$ has order n in G_2.

(b) If G_1 is abelian, then so is G_2.

(c) If G_1 is cyclic, then so is G_2.

Isomorphism theorems; automorphisms

Theorem. [First Isomorphism Theorem] Let G be a group with normal subgroups N and H such that $N \subseteq H$. Then H/N is a normal subgroup of G/N, and $(G / N) / (H / N) \cong G / H$.

Theorem. [Second Isomorphism Theorem] Let G be a group, let N be a normal subgroup of G, and let H be any subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and

$(HN) / N \cong H / (H \cap N)$.

Theorem. Let G be a group with normal subgroups H, K such that HK=G and $H \cap K = \{e\}$. Then

$G \cong H \times K$.

Proposition. Let G be a group and let $a \in G$. The function $i_a : G \to G$ defined by $i_a(x) = axa^{-1}$ for all $x \in G$ is an isomorphism.

Definition. Let G be a group. An isomorphism from G onto G is called an **automorphism** of G.

An automorphism of G of the form i_a, for some $a \in G$, where $i_a(x) = axa^{-1}$ for all $x \in G$, is called an **inner automorphism** of G. The set of all automorphisms of G will be denoted by Aut(G) and the set of all inner automorphisms of G will be denoted by Inn(G).

Proposition. Let G be a group. Then Aut(G) is a group under composition of functions, and Inn(G) is a normal subgroup of Aut(G).

Definition. For any group G, the subset

$Z(G) = \{ x \in G \mid xg = gx \text{ for all } g \in G \}$ is called the **center** of G.

Proposition. For any group G, we have $\text{Inn}(G) \cong G/Z(G)$.

Example. $\text{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$ and $\text{Inn}(\mathbf{Z}) = \{e\}$

Example. $\text{Aut}(\mathbf{Z}_n) \cong \mathbf{Z}_n^{\times}$

Lemma : Let G and H be two cyclic groups of the same order. Then G and H are isomorphic.

Proof.

Let a be a generator of G and let b be a generator of H. Define a map $\varphi: G \longrightarrow H$ as follows. Suppose that $g \in G$. Then $g = a^i$ for some i, then send g to $g^i = b^i$.

We first have to check that this map is well-defined. If G is infinite, then so is H and every element of G may be uniquely represented in the form a^i. Thus the map is automatically well-defined in this case.

Now suppose that G has order k, and suppose that $g = a^j$.

We have to check that $b^i = b^j$.

As $a^i = a^j$, $a^{i-j} = e$ and k must divide $i - j$. In this case $b^{i-j} = e$ as the order of H is equal to k and so $b^i = b^j$. Thus φ is well-defined.

The map $H \longrightarrow G$ defined by sending b^i to a^i is clearly the inverse of φ. Thus φ is a bijection.

Now suppose that $g = a^i$ and $h = a^j$. Then $gh = a^{i+j}$ and the image of this element would be b^{i+j}.

On the other hand, the image of a^i is b^i and the image of a^j is b^j and the product of the images is $b^i b^j = b^{i+j}$.

Here is a far more non-trivial example.

Lemma The group of real numbers under addition and positive real numbers under multiplication are isomorphic.

Proof. Let G be the group of real numbers under addition and let H be the group of real numbers under multiplication.

Define a map $\varphi: G \longrightarrow H$ by the rule $\varphi(x) = e^x$. This map is a bijection, by the well-known results of calculus. We want to check that it is a group isomorphism. Suppose that x and $y \in G$. Then multiplying in G, we get $x + y$. Applying φ we get e^{x+y}.

On the other hand, applying φdirectly we get e^x and e^y. Multiplying together we get $e^x e^y = e^{x+y}$.

Definition : Let G be a group. An isomorphism of G with itself is called an automorphism.

Definition-Lemma . Let G be a group and let $a \in G$ be an element of G.

Define a map $\varphi: G \longrightarrow G$

by the rule

$$\phi(x) = axa^{-1}.$$

Then ϕ is an automorphism of G.

Proof. We first check that ϕ is a bijection.

Define a map

$$\psi\colon G \longrightarrow G$$

by the rule

$$\psi(x) = a^{-1}xa.$$

Then

$$\begin{aligned}\psi(\phi(x)) &= \psi(axa^{-1}) \\ &= a^{-1}(axa^{-1})a \\ &= (a^{-1}a)x(a^{-1}a) \\ &= x.\end{aligned}$$

Thus the composition of φ and ψ is the identity. Similarly the composition of ψ and φ is the identity. In particular φ is a bijection.

Now we check that φ is an isomorphism.

$\varphi(x)\varphi(y) = (axa^{-1})(aya)$

$= a(xy)a^{-1}$

$= \varphi(xy).$

Thus φ is an isomorphism.

Chapter3 - Cayley's theorem

Theorem. (Cayley's Theorem) Let G be a group. Then G is isomorphic to a subgroup of a permutation group. If moreover G is finite, then so is the permutation group, so that every finite group is a subgroup of Sn, for some n.

Proof.

Let H = A(G), the permutations of the set G.

Define a map $\varphi\colon G \longrightarrow H$

by the following rule. Given a $\in$ G, send it to the permutation $\sigma = \varphi(a)$,

$\sigma\colon G \longrightarrow G$, defined as follows $\sigma(g) = ag$, for any $g \in G$.

Note that σ is indeed a permutation, that is, σ is a bijection. In fact the inverse of σ is the map that sends g to $a^{-1}g$.

I claim that φ is an isomorphism onto its image. We first check that φ is an injection. Suppose that a and b are two elements of G. Let σ and τ be the two corresponding elements of A(G). If σ = τ , then σ and τ must have the same effect on elements of G. Look at their effect on e, the identity,

$$a = ae = \sigma(e) = \tau(e) = be = b.$$

Thus φ(a) = φ(b) implies a = b and φ is injective. Thus φ is certainly a bijection onto its image. Now we check that φ(ab) = φ(a)φ(b). Suppose that σ = φ(a) and τ = φ(b) and ρ = φ(ab). We want to check that ρ = στ . This is an equation that involves permutations, so it is enough to check that both sides have the same effect on elements of G. Let g ∈ G. Then

$$\sigma(\tau(g)) = \sigma(bg) =$$
$$a(b(g)) = (ab)g =$$
$$\rho(g).$$

Thus φ is an isomorphism onto its image.

In practice Cayley's Theorem is not in itself very useful. For example, if G = D3 then G is isomorphic to S3. But if we were to apply the machinery behind Cayley's Theorem, we would exhibit G as a subgroup of S6, a group of order 6! = 720.

One exception to this is the example of trying to construct a group G of order 4. We have already shown that there are at most two groups of order four, up to isomorphism. One is cyclic of order 4. The multiplication table of the other, if it is indeed a group, we decided was

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

.

In fact the only thing left to show is that this rule of multiplication is associative.

The idea is to find a subgroup H of Sn, whose multiplication table is precisely the one given. The clue to finding H is given by Cayley's Theorem. For a start Cayley's Theorem shows that we should take n = 4.

Now the four permutations of G determined by the multiplication table are

$$\begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} \quad \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} \quad \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} \quad \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}.$$

Replacing letters by numbers, in the obvious way, we get

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

This reduces to

$$H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Now it is easy to see that this subset is in fact a subgroup. In fact the square of any element is the identity and the product of any two elements is the third. Thus H is a subgroup of S4. Now H is a group of order 4, which is not cyclic. Thus there are at least two groups of order 4, up to isomorphism.

Chapter3 - Permutation

Permutations

Definition. Let S be a set. A function σ :S->S is called a **permutation** of S if σ is one-to-one and onto.
The set of all permutations of S will be denoted by Sym(S).
The set of all permutations of the set { 1, 2, ..., n } will be denoted by S_n.

Proposition shows that the composition of two permutations in Sym(S) is again a permutation. It is obvious that the identity function on S is one-to-one and onto. Proposition 2.1.8 shows that any permutation in Sym(S) has an inverse function that is also one-to-one and onto. We can summarize these important properties as follows:

(i) If $\sigma, \tau \in$ Sym(S), then $\sigma\tau \in$ Sym(S);
(ii) $1_S \in$ Sym(S);
(iii) if $\sigma \in$ Sym(S), then $\sigma^{-1} \in$ Sym(S).

Definition. Let S be a set, and let $\sigma \in$ Sym(S). Then σ is called a **cycle of length k** if there exist elements $a_1, a_2, ..., a_k \in S$ such that

$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$, and

$\sigma(x)=x$ for all other elements $x \in S$ with $x \neq a_i$ for $i = 1, 2, ..., k$.

In this case we write $\sigma = (a_1,a_2,...,a_k)$.

We can also write $\sigma = (a_2,a_3,...,a_k,a_1)$ or $\sigma = (a_3,...,a_k,a_1,a_2)$, etc. The notation for a cycle of length k can thus be written in k different ways, depending on the starting point. The notation (1) is used for the identity permutation.

Cycles

Definition. Let $\sigma = (a_1,a_2,...,a_k)$ and $\tau = (b_1,b_2,...,b_m)$ be **cycles** in Sym(S), for a set S. Then σ and τ are said to be **disjoint** if $a_i \neq b_j$ for all i,j.

Proposition. Let S be any set. If σ and τ are disjoint cycles in Sym(S), then $\sigma\tau = \tau\sigma$.

Theorem. Every permutation in S_n can be written as a product of disjoint cycles. The cycles that appear in the product are unique.

Definition. Let $\sigma \in S_n$. The least positive integer m such that $\sigma^m = (1)$ is called the **order** of σ.

Proposition. Let $\sigma \in S_n$ have order m. Then for all integers j,k we have

$\sigma^j = \sigma^k$ if and only if $j \equiv k \pmod m$.

Proposition. Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its cycles.

Transposition

Definition. A cycle (a_1,a_2) of length two is called a **transposition**.

Proposition. Any permutation in S_n, where $n \geq 2$, can be written as a product of transpositions.

Theorem. If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even in both cases or odd in both cases.

Definition. A permutation σ is called **even** if it can be written as a product of an even number of transpositions, and **odd** if it can be written as a product of an odd number of transpositions.

Chapter4- Permutation groups

Permutation groups

Definition. The set of all permutations of a set S is denoted by Sym(S).
The set of all permutations of the set $\{1,2,...,n\}$ is denoted by S_n.

Proposition. If S is any nonempty set, then Sym(S) is a group under the operation of composition of functions.

Theorem. Every permutation in S_n can be written as a product of disjoint cycles. The cycles that appear in the product are unique.

Proposition. If a permutation in S_n is written as a product of disjoint cycles, then its order is the least common multiple of the lengths of its cycles.

symmetric group

Definition. Any subgroup of the **symmetric group** Sym(S) on a set S is called a **permutation group** or **group of permutations**.

Theorem. (Cayley) Every group is isomorphic to a permutation group.

Definition. Let $n > 2$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n.

We can describe the nth dihedral group as

$D_n = \{ a^k, a^k b \mid 0 \leq k < n \}$,

subject to the relations $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$.

Theorem. If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even in both cases or odd in both cases.

Odd Even permutation

Definition. A permutation is called **even** if it can be written as a product of an even number of transpositions, and **odd** if it can be written as a product of an odd number of transpositions.

Proposition. The set of all even permutations of S_n is a subgroup of S_n.

Definition. The set of all even permutations of S_n is called the **alternating group** on n elements, and will be denoted by A_n.

Practice question and answer- Unit- III - Abstract algebra

1. Define into isomorphism of groups

   A mapping f from a group G into a group G' is a homomorphism of G into G' and f is one-one, then f is an isomorphism of G into G'.

2. Define onto isomorphism of groups

   A mapping f from a group G onto a group G' is a homomorphism of G into G' and f is one-one, then f is an isomorphism of G onto G'.

3. Define endomorphism

A homomorphism of a group into itself is called an endomorphism.

4. Define automorphism of a group
   An isomorphic mapping of a group G onto itself is called an automorphism of G.
5. Show that the mapping f: $I \to I$ such that $f(x) = -x \forall x \in I$ is an automorphism of the additive group of integers I.

6. Define permutation
   Suppose S is a finite set having n distinct elements. Then a one-one mapping of S onto itself is called a permutation of degree n. The number of elements in a finite set S is known as the degree of permutation.

7. Give an example of two permutations of degree 4.
   $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ are permutations of degree 4.

8. When will you say two permutations of degree n are equal?
   Two permutations f and g of degree n are equal if we have $f(a) = g(a)\ \forall \text{a} \in \text{S}$ where $S = \{a_1, a_2, ..., a_n\}$

9. Define symmetric set of permutations of degree n.
   If S is a finite set having n distinct elements, then we shall have $n!$ distinct arrangements of the elements of S. Therefore there will be $n!$ distinct permutations of degree n. If P_n be the set consisting of all permutations of degree n then the set P_n will have $n!$ distinct elements. This set P_n is called the symmetric set of permutations of degree n.

10. Define identity permutation
    If I is a permutation of degree n such that I replaces each element by the element itself. I is called the identity permutation of degree n.

11. Define product or composite of two permutations
    The product of or composite of two permutations f and g of degree n denoted by fg, is obtained by first carrying out the operation defined by f and then g.

12. Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ be two permutations of degree 5. Then find fg.
    $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$
13. Give an example that multiplication of permutations is not commutative.
    Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\text{g} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutations of degree 3.
    Then $\text{fg} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\text{gf} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ obviously $\text{fg} \neq \text{gf}$
    . .

14. Define cyclic permutation

    Suppose f is a permutation of degree n on a set having n distinct elements. Let it be possible to arrange m elements of the set S in a row in such a way that the f-image of each element in the row is the element which follows it, the f-image of the last element is the first element and the remaining n-m elements of the set S are left unchanged by f. Then f is called a cyclic permutation or a cycle of length m or an m cycle.

15. Write down the cycle representation for the permutation given below:

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

    $(1\ \ 2\ \ 4\ \ 3)$

16. If $(1\ \ 3\ \ 4\ \ 2\ \ 6)$ is a cycle of length 5 then find the permutation of degree 9 on a set S consisting of the elements 1,2,3,…,9.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

17. Write the following permutation as the product of disjoint cycles.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$$

18. Define Transpositions

    A cycle of length two is called a transposition.

19. Define even permutation

    A permutation is said to be an even permutation if it can be expressed as a product of an even number of transpositions; otherwise it is said to be an odd permutation.

20. Whether the following permutation is a even permutation

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

    We can write f=(1 2)(1 3)(1 2). The number of transpositions is 3.i.e, odd. Therefore f is an odd permutation.

21. The necessary and sufficient condition for a homomorphism f of a group G into a group G' with kernel K to be an isomorphism of G into G' is that K={e}.

Proof

Let G be a group, and let $K \subset G$ be a subgroup

we claim that K is the kernel of some homomorphism $\varphi: G \to G$ if and only if K is normal, and G/K is isomorphic to a subgroup K' of G.

Indeed, if Let G be a group, and let $K \subset G$ be a subgroup.

we claim that K is the kernel of some homomorphism $\varphi: G \to G$ if and only if K is normal, and G/K is isomorphic to a subgroup K' of G.

If $K = \ker(\varphi)$ for some Homomorphism $\varphi: G \to G$, then K is normal and by the first isomorphism theorem, $G/K \cong \operatorname{im}(\varphi)$, which is a subgroup of G.

On the other hand, if G/K is isomorphic to the subgroup K' of G, then the composition of the projection $G \to G/K$ with the isomorphism from G/K to

K' and the inclusion $K' \hookrightarrow G$ gives a homomorphism from G to G with kernel K.

Unit- III

1. Define into isomorphism of groups
   A mapping f from a group G into a group G' is a homomorphism of G into G' and f is one-one, then f is an isomorphism of G into G'.
2. Define onto isomorphism of groups
   A mapping f from a group G onto a group G' is a homomorphism of G into G' and f is one-one, then f is an isomorphism of G onto G'.
3. Define endomorphism
   A homomorphism of a group into itself is called an endomorphism.
4. Define automorphism of a group
   An isomorphic mapping of a group G onto itself is called an automorphism of G.
5. Show that the mapping f: $I \to I$ such that $f(x) = -x \forall x \in I$ is an automorphism of the additive group of integers I.

6. Define permutation
   Suppose S is a finite set having n distinct elements. Then a one-one mapping of S onto itself is called a permutation of degree n. The number of elements in a finite set S is known as the degree of permutation.
7. Give an example of two permutations of degree 4.
   $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ are permutations of degree 4.
8. When will you say two permutations of degree n are equal?
   Two permutations f and g of degree n are equal if we have
   $f(a) = g(a) \forall \text{a} \in \text{S}$ where $S = \{a_1, a_2, ..., a_n\}$
9. Define symmetric set of permutations of degree n.
   If S is a finite set having n distinct elements, then we shall have $n!$ distinct arrangements of the elements of S. Therefore there will be $n!$ distinct permutations of degree n. If P_n be the set consisting of all permutations of degree n then the set P_n will have $n!$ distinct elements. This set P_n is called the symmetric set of permutations of degree n.
10. Define identity permutation
    If I is a permutation of degree n such that I replaces each element by the element itself. I is called the identity permutation of degree n.
11. Define product or composite of two permutations
    The product of or composite of two permutations f and g of degree n denoted by fg, is obtained by first carrying out the operation defined by f and then g.
12. Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ be two permutations of degree 5. Then find fg.

$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$

13. Give an example that multiplication of permutations is not commutative.

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ be two permutations of degree 3. Then f

$fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $gf = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ obviously $fg \neq gf$

14. Define cyclic permutation

Suppose f is a permutation of degree n on a set having n distinct elements. Let it be possible to arrange m elements of the set S in a row in such a way that the f-image of each element in the row is the element which follows it, the f-image of the last element is the first element and the remaining n-m elements of the set S are left unchanged by f. Then f is called a cyclic permutation or a cycle of length m or an m cycle.

15. Write down the cycle representation for the permutation given below:

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

(1 2 4 3)

16. If (1 3 4 2 6) is a cycle of length 5 then find the permutation of degree 9 on a set S consisting of the elements 1,2,3,…,9.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$

17. Write the following permutation as the product of disjoint cycles.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$

18. Define Transpositions

A cycle of length two is called a transposition.

19. Define even permutation

A permutation is said to be an even permutation if it can be expressed as a product of an even number of transpositions; otherwise it is said to be an odd permutation.

20. Whether the following permutation is a even permutation

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

21.

We can write f=(1 2)(1 3)(1 2). The number of transpositions is 3.i.e, odd. Therefore f is an odd permutation.

Unit-III

1. The necessary and sufficient condition for a homomorphism f of a group G into a group G' with kernel K to be an isomorphism of G into G' is that K={e}.

Proof

Let G be a group, and let K⊂G be a subgroup. I claim that K is the kernel of some homomorphism φ:G→G if and only if K is normal, and G/K is isomorphic to a subgroup K′ of G. Indeed, if K=ker(φ) for some homomorphism φ:G→G, then K is normal and by the first isomorphism theorem, G/K≅ im(φ), which is a subgroup of G. On the other hand, if G/K is isomorphic to the subgroup K′ of G, then the composition of the projection G→G/K with the isomorphism from G/K to K′ and the inclusion K′↪ G gives a homomorphism from G to G with kernel K.

2. Show that additive group of integers $G = \{...,-3,-2,-1,0,1,2,3,...\}$ is isomorphic to the additive group $G' = \{...,-3m,-2m,-1m,0,1m,2m,3m,...\}$ where m is any fixed integer not equal to zero.

Proof. Let G = (a) = $\{a^n : n \in I\}$ is a cyclic group and I = {0, ±1, ±2, ±3, …} is an additive group of integers. We define a map $f : G \to I$ by $f(a^n) = n \ \forall\ a^n \in G$. Clearly f is well defined. Now, $\forall\ a^n, a^m \in G$, suppose that $f(a^n) = f(a^m) \Rightarrow n = m \Rightarrow a^n = a^m$ $\Rightarrow$ f is one-one. Also for each $n \in I\ \exists\ a^n \in G$ such that $f(a^n) = n \Rightarrow$ f is onto. Finally, $f(a^n a^m) = f(a^{n+m}) = n + m = f(a^n) + f(a^m) \Rightarrow$ f is homomorphism. Hence G ≅ I.

3. Let f be an isomorphic mapping of a group G into a group G' . Then prove that
   i)The f image of the identity e of G is the identity of G'i.e, f(e) is the identity of G'.
   ii)The f image of the inverse of an element a of G is the inverse of the f-image of a ie.,$f(a^{-1}) = [f(a)]^{-1}$
   iii)The order of an element a of G is equal to the order of its image f(a).

Proof. Let $a = \phi(e)$, where e is the identity in G. Then

$$\begin{aligned} a &= \phi(e) \\ &= \phi(ee) \\ &= \phi(e)\phi(e) \\ &= aa. \end{aligned}$$

Thus $a^2 = a$. Cancelling we get $a = f$, the identity in H. Hence (1).

Let $b = a^{-1}$.

$$\begin{aligned} f &= \phi(e) \\ &= \phi(ab) \\ &= \phi(a)\phi(b), \end{aligned}$$

and

$$\begin{aligned} f &= \phi(e) \\ &= \phi(ba) \\ &= \phi(b)\phi(a). \end{aligned}$$

But then $\phi(b)$ is the inverse of $\phi(a)$, so that $\phi(a^{-1}) = \phi(a)^{-1}$. Hence (2).

Lemma : Let G and H be two cyclic groups of the same order. Then G and H are isomorphic.

Proof.

Let a be a generator of G and let b be a generator of H. Define a map φ: G $\longrightarrow$ H as follows. Suppose that g $\in$ G. Then $g = a^i$ for some i, then send g to $g^i = b^i$.

We first have to check that this map is well-defined. If G is infinite, then so is H and every element of G may be uniquely represented in the form a^i. Thus the map is automatically well-defined in this case.
Now suppose that G has order k, and suppose that $g = a^j$.

We have to check that $b^i = b^j$.

As $a^i = a^j$, $a^{i-j} = e$ and k must divide i − j. In this case $b^{i-j} = e$ as the order of H is equal to k and so $b^i = b^j$. Thus φ is well-defined.

The map H $\longrightarrow$ G defined by sending b^i to a^i is clearly the inverse of φ. Thus φ is a bijection.

Now suppose that $g = a^i$ and $h = a^j$. Then $gh = a^{i+j}$ and the image of this element would be b^{i+j}.

On the other hand, the image of a^i is b^i and the image of a^j is b^j and the product of the images is $b^i b^j = b^{i+j}$.

---

4. Show that the multiplicative group G= {1,-1,i,-i} is isomorphic to the permutation group.

By Cayley's theorem the regular permutation group G' is isomorphic to G consists of the following four permutations f_1, f_2, f_3, f_4.

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1.(-1) & 1.i & 1.(-i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix} = 1$$

$$\begin{pmatrix} 1 & -1 & i & -i \\ (-1)(1) & (-1)(-1) & (-1)i & (-1)(-i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix} = (1-1)(i-i)$$

$$f_3 = \begin{pmatrix} 1 & -1 & i & -i \\ i(1) & -i(-1) & ii & i(-1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix} = (1\, i\, -1\, -i)$$

$$f_4 = \begin{pmatrix} 1 & -1 & i & -i \\ (-i)(1) & (-i)(-1) & (-i)i & (-i)(-i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix} = (1\, -i\, -1\, i)$$

5. State and prove Fundamental theorem on homomorphism of groups.

23.1. **Proof of the fundamental theorem of homomorphisms (FTH)**

We start by recalling the statement of FTH introduced last time.

1

Theorem (FTH). *Let G, H be groups and $\varphi : G \to H$ a homomorphism. Then*

$$G/\mathrm{Ker}\,\varphi \cong \varphi(G). \qquad (***)$$

Proof. Let $K = \mathrm{Ker}\,\varphi$ and define the map $\Phi : G/K \to \varphi(G)$ by

$$\Phi(gK) = \varphi(g) \text{ for } g \in G.$$

We claim that Φ is a well defined mapping and that Φ is an isomorphism. Thus we need to check the following four conditions:

(i) Φ is well defined
(ii) Φ is injective
(iii) Φ is surjective
(iv) Φ is a homomorphism

For (i) we need to prove the implication "$g_1K = g_2K \Rightarrow \Phi(g_1K) = \Phi(g_2K)$."

So, assume that $g_1K = g_2K$ for some $g_1, g_2 \in G$. Then $g_1^{-1}g_2 \in K$ by Theorem 19.2, so $\varphi(g_1^{-1}g_2) = e_H$ (recall that $K = \mathrm{Ker}\,\varphi$). Since $\varphi(g_1^{-1}g_2) = \varphi(g_1)^{-1}\varphi(g_2)$, we get $\varphi(g_1)^{-1}\varphi(g_2) = e_H$. Thus, $\varphi(g_1) = \varphi(g_2)$, and so $\Phi(g_1K) = \Phi(g_2K)$, as desired.

For (ii) we need to prove that "$\Phi(g_1K) = \Phi(g_2K) \Rightarrow g_1K = g_2K$." This is done by taking the argument in the proof of (i) and reversing all the implication arrows.

(iii) First note that by construction $\mathrm{Codomain}(\Phi) = \varphi(G)$. Thus, for surjectivity of Φ we need to show that $\mathrm{Range}(\Phi) = \Phi(G/K)$ is equal to $\varphi(G)$. This is clear since

$$\Phi(G/K) = \{\Phi(gK) : g \in G\} = \{\varphi(g) : g \in G\} = \varphi(G).$$

(iv) Finally, for any $g_1, g_2 \in G$ we have

$$\Phi(g_1K \cdot g_2K) = \Phi(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \Phi(g_1K)\Phi(g_2K)$$

where the first equality holds by the definition of product in quotient groups. Thus, Φ is a homomorphism.

So, we constructed an isomorphism $\Phi : G/\mathrm{Ker}\,\varphi \to \varphi(G)$, and thus $G/\mathrm{Ker}\,\varphi$ is isomorphic to $\varphi(G)$. □

6. Show that $a \to a^{-1}$ is an automorphism of a group G iff G is abelian.

Solutions: Suppose α is an automorphism. Let $x, y \in G$. We want to show that $xy = yx$. Applying the property of automorphism to $(xy)^{-1}$:

$$\alpha(xy)^{-1}) \overset{\text{definition of } \alpha}{=} ((xy)^{-1})^{-1} = xy,$$

but also

$$\alpha((xy)^{-1}) = \alpha(y^{-1}x^{-1}) \overset{\text{autom.}}{=} \alpha(y^{-1})\alpha(x^{-1}) = (y^{-1})^{-1}(x^{-1})^{-1} = yx.$$

Thus, $xy = yx$. Conversely, suppose G is abelian. To prove that α is an automorphism, we need two facts:

(1) WTS α is a bijection. It is sufficient to exhibit an inverse for α. In fact, we will show that α is its own inverse. Let $x \in G$, then

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

Thus, $\alpha \circ \alpha =$ identity and α has an inverse so is a bijection.

(2) WTS α preserves the operation. Let $x, y \in G$. Then

$$\alpha(xy) = (xy)^{-1} = y^{-1}x^{-1} \overset{\text{abelian}}{=} x^{-1}y^{-1} = \alpha(x)\alpha(y),$$

as required.

7. If H be a normal subgroup of a group G and K a normal subgroup of G containing H, then G/K ≅ (G/H)(K/H).

Theorem (Third Isomorphism Theorem). *Let $K \subset H$ be two normal subgroups of a group G.*

Then

$$G/H \simeq (G/K)/(H/K).$$

Proof. Consider the natural map $G \longrightarrow G/H$. The kernel, H, contains K. Thus, by the universal property of G/K, it follows that there is a homomorphism $G/K \longrightarrow G/H$.

This map is clearly surjective. In fact, it sends the left coset gK to the left coset gH. Now suppose that gK is in the kernel. Then the left coset gH is the identity coset, that is, $gH = H$, so that $g \in H$. Thus the kernel consists of those left cosets of the form gK, for $g \in H$, that is, H/K. The result now follows by the first Isomorphism Theorem. □

8. Let G be a group and let H be any subgroup of G. If N is any normal subgroup of G, then

$HN / N \cong H /(H \cap N)$.

Second Isomorphism Theorem

The **second isomorphism theorem** relates two quotient groups involving products and intersections of subgroups.Let G be a group, let H be a subgroup, and let N be a normal subgroup. Then HN = \{hn : h Ɛ H, n Ɛ N\} is a subgroup of G, and $HN/N \simeq H/(H \cap N)$.

Let S_3 be the symmetric group on three letters. Let H be the subgroup generated by the transposition , and let N be the subgroup generated by the transposition.

Then the second isomorphism theorem gives an isomorphism $HN/N \simeq H/(H \cap N)$, where $HN = \{hn : h \in H, n \in N\}$.

Now $H \cap N = \{1\}$, so the right side has order 2. So the left side has order 2. Now |N|=2 and |HN/N|=2, so |HN|=4. But Lagrange's theorem says that |HN| must divide $|S_3|$, which is 6.

I. As defined above, HN is not a subgroup of S_3, so Lagrange's theorem does not apply.
II. The order of a quotient G/K of finite groups is not always equal to |G|/|K|.
III. N is n

---

9. Prove that a cyclic group G with generator of finite order n is isomorphic to the multiplicative group of n nth roots of unity.

Proof

Let G_1 and G_2 be cyclic groups, both of finite order k.

Let $G_1 = \langle a \rangle, G_2 = \langle b \rangle$.

Then, by the definition of a cyclic group:

$$|a| = |b| = k$$

Also, by definition:

$$G_1 = \{a^0, a^1, \ldots, a^{k-1}\}$$

and:

$$G_2 = \{b^0, b^1, \ldots, b^{k-1}\}$$

Let us set up the obvious bijection:

$$\phi : G_1 \to G_2 : \phi(a^n) = b^n$$

The next task is to show that ϕ is an isomorphism.

Note that $\phi(a^n) = b^n$ holds for all $n \in \mathbb{Z}$, not just where $0 \leq n < k$, as follows:

Let $n \in \mathbb{Z} : n = qk + r, 0 \leq r < k$, by the Division Theorem.

Then, by Element to Power of Remainder:

$$a^n = a^r, b^n = b^r$$

Thus:

$$\phi(a^n) = \phi(a^r) = b^r = b^n$$

Now let $x, y \in G_1$.

Since $G_1 = \langle a \rangle$, it follows that:

$$\exists s, t \in \mathbb{Z} : x = a^s, y = a^t$$

Thus:

$$\begin{aligned}
\phi(xy) &= \phi\left(a^s a^t\right) \\
&= \phi\left(a^{s+t}\right) \\
&= b^{s+t} \\
&= b^s b^t \\
&= \phi(a^s)\,\phi\left(a^t\right) \\
&= \phi(x)\,\phi(y)
\end{aligned}$$

So ϕ is a homomorphism.

As ϕ is bijective, ϕ is an isomorphism from G_1 to G_2.

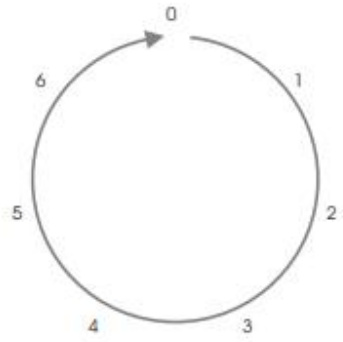
Thus $G_1 \cong G_2$ and the result is proved.

10. Show that a cyclic group G with a generator of finite order n is isomorphic to the additive group of residue classes modulo n.

$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of 1 (or of -1). For instance, $117 = 117 \cdot 1$.
(Remember that "$117 \cdot 1$" is really shorthand for $1 + 1 + \cdots + 1$ — 1 added to itself 117 times.)
In fact, it is the only infinite cyclic group up to **isomorphism**.
Notice that a cyclic group can have more than one generator.
If n is a positive integer, $\mathbb{Z}_n$ is a cyclic group of order n generated by 1.
For example, 1 generates $\mathbb{Z}_7$, since

$$\begin{aligned}
1 + 1 &= 2 \\
1 + 1 + 1 &= 3 \\
1 + 1 + 1 + 1 &= 4 \\
1 + 1 + 1 + 1 + 1 &= 5 \\
1 + 1 + 1 + 1 + 1 + 1 &= 6 \\
1 + 1 + 1 + 1 + 1 + 1 + 1 &= 0
\end{aligned}$$

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.



a cyclic group of order 7

Notice that 3 also generates $\mathbb{Z}_7$:

$$\begin{aligned} 3+3 &= 6 \\ 3+3+3 &= 2 \\ 3+3+3+3 &= 5 \\ 3+3+3+3+3 &= 1 \\ 3+3+3+3+3+3 &= 4 \\ 3+3+3+3+3+3+3 &= 0 \end{aligned}$$

The "same" group can be written using multiplicative notation this way:

$$\mathbb{Z}_7 = \{1, a, a^2, a^3, a^4, a^5, a^6\}.$$

In this form, a is a generator of $\mathbb{Z}_7$.
It turns out that in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group.
On the other hand, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate. □

(OR)

1. Prove that the set P_n of all permutations on n symbols is a finite group of order $n!$ with respect to composite of mapping as the operation. For $n \leq 2$, this group is abelian and for n > 2 it is always non-abelian.

Let $S=\{a_1, a_2, a_3, \ldots, a_n\}$ be a finite set having n distinct elements. Thus there are n! permutations possible on S. If Pr denotes the set of all permutations of degree n then the multiplication of permutation on Pn satisfies the following axioms.

Closure Axiom: Let f, g∈Pn, then each of them is one-one mapping of S onto itself and therefore their composite mapping (g◦ f) is a one-one mapping of S onto itself. Thus (g◦ f) is a permutation of degree n on S, i.e.

$$f, g \in Pn \Rightarrow fg \in Pn$$

This shows that P_n is closed under multiplication.

Associative Axiom: Since the product of two permutations on a set S is nothing but the product of two one-one onto mappings on S and the product of mapping is associative, the product of permutations also obeys the associative law. Hence

$$f, g, h \in Pn \Rightarrow (fg)h = f(gh)$$

Identity Axiom: Identity permutation $I \in P_n$ is the identity of multiplication in P_n because

$$If = fI = f \forall f \in P_n$$

Inverse Axiom: Let $f \in P_n$ then f is one-one mapping, hence it is investible. Hence f^{-1}, the inverse mapping of f is also one-one and onto. Consequently,f^{-1} is also a permutation in P_n.

$$f^{-1}f = ff^{-1} = I$$

Thus the symmetric set P_n of all permutations of degree n defined on a finite set forms a finite group of order $n!$ with respect to the composite of permutations as the composition.

Commutative Axiom: If we consider the symmetric group (P_1, O) of permutations of degree 1 with respect to permutation product 0, then it consists of a single permutation, namely the identity permutation I. Since $I O I = I$, (P_1, O) is an abelian group. If we consider the symmetric group (P2,0) of all permutations of degree 2, i.e. the group of all permutations defined on a set of two elements (a_1, a_2), then

$$P_2 = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}, \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \right\}$$

Now

$$\begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix} 0 \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

and

$$\begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} 0 \begin{pmatrix} a_1 & a_2 \\ a_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & a_1 \\ a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$$

Therefore an operation having commutative (P_2, O) is an abelian group of order 2. But when $n>2$ then the permutation product is not necessarily commutative. Hence (P_n, O) is not necessarily an abelian group.

2. State and prove Cayley's theorem

Cayley's Theorem:
Every group is isomorphic to a permutation group.

Proof: Let G be a finite group of order n. If $a \in G$, then $\forall x \in G$, $ax \in G$. Now consider a function from G into G, defined by

$$f_a(x) = ax \quad \forall x \in G$$

For $x, y \in G, f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$. Therefore, the function f_a is one-one.

The function f_a is also onto because if x is any element of then there exists an element $a^{-1}x$ such that

$$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x$$

Thus f_a is one-one from G onto G. Therefore, f_a is a permutation on G. Let G' denote the set of all such one-to-one functions defined on G corresponding to every element of G, i.e. $G' = \{f_a : a \in G\}$

Now, we show that G' is a group with respect to the product of functions.

(i) Closure Axiom: Let $f_a, f_b \in G'$ where $a, b \in G$, then

$$(f_a \circ f_b)x = f_a[f_b(x)] = f_a(bx) = a(bx) = (ab)x = f_{ab}(x) \quad \forall x \in G$$

Since $ab \in G$, therefore $f_{ab} \in G'$ and thus G' is closed under the product of functions.

(ii) Associative Axiom: Let $f_a, f_b, f_c \in G'$ where $a, b, c \in G$, then

$$f_a \circ (f_b \circ f_c) = f_a \circ f_{bc} = f_a(bc) = f(ab)c = f_{ab} \circ f_c = (f_a \circ f_b) \circ f_c$$

The product of functions is associative in G'.

(iii) Identity Axiom: If e is the identity element in G, then f_e is the identity of G' because $\forall f_x \in G'$ we have $f_e \circ f_x = f_{ex} = f_x$ and $f_x \circ f_e = f_{xe} = f_x$.

(iv) Inverse Element: If a^{-1} is the inverse of a in G, then $f_{a^{-1}}$ is the inverse of f_a in G' because $f_{a^{-1}} \circ f_a = f_{a^{-1}a} = f_e$ and $f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e$

Hence G' is a group with respect to the composite of functions denoted by the symbol $\circ$.

Now consider the function g and G into G′ defined by $g(a)=fa \forall a \in G$.
g is one-one because for $a,b \in G$.

$$g(a)=g(b) \Rightarrow fa=fb \Rightarrow fa(x)=fb(x)$$

$$\Rightarrow ax=bx \Rightarrow a=b, \forall x \in G$$

g is onto because if $fa \in G'$ then for $a \in G$, we have $g(a)=fa$
g preserves composition in G and G′ because if $a,b \in G$ then

$$g(ab)=fab=fa \circ fb=g(a) \circ g(b)$$

Hence $G \cong G'$.

3. If f and g are two disjoint cycles then fg=gf i.e, the product of disjoint cycles is commutative.

Theorem 1: The product of disjoint cycles is commutative.

Proof: Let f and g be any two disjoint cycles, i.e. there is no element common in two when they are expressed in one row notation. Therefore, the elements permuted by f are invariant under g and the elements permuted by g are invariant under f.
Hence $f \circ g=g \circ f$ the product of disjoint cycles is commutative.

4. Prove that every permutation can be expressed as a product of disjoint cycles.

Proof: Let the given permutation ff be denoted by the usual two row symbol within a bracket. Let aa be any element in the first row and bb the element in the second row exactly beneath aa, i.e. $f(a)=b$f(a)=b. Similarly, let $f(b)=c$f(b)=c. Continuing this process, an element 1 may be found in the upper row such that its ff image is aa. Then $a,b,c,\ldots 1$a,b,c,…1 is one circular permutation. If there are additional elements a',b',a′,b′,, etc., in the original permutation ff, follow the above process to obtain another cycle $(a',b',c',\ldots,1')$(a′,b′,c′,…,1′). Even now, if some element or elements are left in the original permutation this procedure can be repeated to the extent that all the elements of ff are exhausted. In this way the original permutation can be put as the product of disjoint cycles.

5. Prove that every cycle can be expressed as a product of transpositions in infinitely many ways.

Proof: To prove the above result, we shall first show that every cycle can be expressed as a composite of transpositions. Let us consider a cycle $(a_1,a_2,\ldots,a_n)$(a1,a2,…,an) then

$$(a_1,a_2,\ldots,a_n)=(a_1a_n)(a_1a_{n-1})\ldots(a_1a_2)\text{(a1, a2, ⋯, an) = (a1an) (a1an − 1) ⋯ (a1a2)}$$

We have already proved that every permutation can be expressed as a composition of disjoint cycles. Therefore in the light of the two results stated above, every permutation can be expressed as a product of transpositions.

6. Prove that if a permutation f is expressed as a product of transpositions then the number of transpositions is either always even or always odd.

Proof: Let us consider the polynomial A in distinct symbols $x_1, x_2, \ldots, x_n$. It is defined as the product of $\frac{1}{2n(n-1)}$ factor of the form $x_i - x_j$ where $i < j$.

Thus

$$A = \prod_{i \leqslant j=1}^{n} (x_i - x_j)$$

$$\begin{aligned} A = {} & (x_1-x_2)(x_1-x_3)(x_1-x_4)\cdots(x_1-x_n) \\ & (x_2-x_3)(x_2-x_4)(x_2-x_5)\cdots(x_2-x_n) \\ & (x_3-x_4)\cdots(x_3-x_n)\cdots\cdots\cdots(x_{n-1}-x_n) \end{aligned}$$

Now consider any permutation P on n symbol $1, 2, 3, \ldots, n$. By AP we mean the polynomial obtained by permuting the subscript $1, 2, 3, \ldots, n$of the x_i as prescribed by P.

For example, taking $n = 4$, we have

$$A = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$$

If $P(1342)$, then

$$AP = (x_3 - x_1)(x_3 - x_4)(x_3 - x_2)(x_1 - x_4)(x_1 - x_2)(x_4 - x_3)$$

In particular if $P = (12)$, we have

$$AP = (x_2 - x_1)(x_2 - x_3)(x_2 - x_4)(x_1 - x_3)(x_1 - x_4)(x_3 - x_4) = -A$$

This shows that the effect of a transposition on A is to change the sign of A.

In general, a transposition (i, j), $i < j$ has the following effects on A.
(i) Any factor which involves neither the suffix i nor j remains unchanged.
(ii) The single factor $(x_i - x_j)$ changes its sign.
(iii) The remaining factors which involve either the suffix i or j but not both can be grouped into pairs of products, $\pm(x_m - x_i)(x_m - x_j)$ where $m \neq i$ or j and such a product remains unaltered when x_i and x_j are interchanged.

Hence the net effect of transposition i, j on A is to change its sign, i.e. A operated upon by transposition (i, j)gives $-A$.

Now the permutation P is considered a product of s transposition when operated upon A and gives $(-1)^s A$ so that $AP = (-1)^s A$ and is considered a product of t transposition when it gives $(-1)^t A$ so that $AP = (-1)^t A$.

Hence

$$(-1)^s A = (-1)^t A$$

$$(-1)^s = (-1)^t$$

Now this equation will hold only if s and t are either both even or both odd. Hence this completes the theorem.

7. Of the n! permutations on n symbols, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd nd

Proof: Let the even permutations be $e_1, e_2, \ldots, e_m$e1,e2,…,em and the odd permutations be $o_1, o_2, \ldots, o_k$o1,o2,…,ok. Then $m+k=n!$m+k=n!

Now let t be any transposition. Since t is evidently an odd permutation, we see that $te_1, te_2, \ldots, te_m$ are odd permutations and that $to_1, to_2, \ldots, to_k$ are even permutations. Since an odd permutation is never an even permutation, we have for any $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots, k$. Furthermore, if $te_i = te_j$, then $e_i = e_j$ by cancellation law. Similarly $to_i \neq to_j$ if $i \neq j$.

It follows that all of the m even permutations must appear in the list $to_1, to_2, \ldots, to_k$, which are all distinct so that their number is m. Similarly, all of the k odd permutations must be in the list $te_1, te_2, \ldots, te_m$, which are all distinct as shown above and their number of k.

Hence $m = k = \frac{1}{2n!}$

8. Show that the alternating set A_n of all even permutations of degree n forms a finite group of order $\frac{n!}{2}$ with respect to permutation multiplication.
9. Show that the set P_n of all permutations on three symbols 1,2,3 is a finite non-abelian group of order 6 with respect to permutation multiplication as composition.
10. i) If $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ then find AB and BA.

    ii) Find the inverse of the permutation $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

    iii) Decompose the following permutation into transpositions

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

iv) Examine whether the following permutation is even or odd:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$$

M. Tamizharasi

111862030

Abstract Algebra.

16 Marks

1) Let G be a group, and let $K \subset G$ be a subgroup.

I claim that K is the kernel of some homomorphism $\phi : G \to G$ if and only if K is normal, and G/K is isomorphic to a subgroup K' of G.

Indeed, if $K = \ker(\phi)$ for some homomorphism $\phi : G \to G$, then K is normal and by the first isomorphism theorem, $G/K = \text{im}(\phi)$, which is a subgroup of G.

On the other hand, if G/K is to isomorphic to the subgroup K' of G, then the composition of the projection $G \to G/K$ with the isomorphism from G/K to K' and the inclusion $K' \to G$ gives a homomorphism from G to G with kernel K.

---

2) Let $G = (a) = \{a^n : n \in I\}$ is a cyclic group and $I = \{0, \pm 1, \pm 2, \dots\}$ is an additive group of integers.

We define a map $f : G \to I$ by $f(a^n) = n \ \forall \ a^n \in G$.

Clearly, f is well defined. Now, $\forall\ a^n, a^m \in G$, suppose that $f(a^n) = f(a^m) \Rightarrow n = m \Rightarrow a^n = a^m$

$\Rightarrow f$ is one - one.

Also for each $n \in I$ $\exists$ $a^n \in G$. such that

$f(a^n) = n \Rightarrow$ f is onto.

Finally, $f(a^n a^m) = f(a^{n+m}) = n+m = f(a^n) + f(a^m)$

$\Rightarrow$ f is homomorphism.

Hence $G \cong I$.

---

3) Proof :

(i) Let $a = \phi(e)$, where e is the identity in G.

Then, $a = \phi(e)$

$= \phi(ee) = \phi(e)\,\phi(e)$

$= aa$

Thus $a^2 = a$. Cancelling we get $a = f$, the identity in H. Hence (i).

(ii) Let $b = a^{-1}$.

$f = \phi(e)$

$= \phi(ab) = \phi(a)\,\phi(b)$

and $f = \phi(e)$

$= \phi(ba) = \phi(b)\,\phi(a)$

But then $\phi(b)$ is the inverse of $\phi(a)$, so that $\phi(a^{-1}) = \phi(a)^{-1}$. Hence (2).

(iii) As $f(a) = a'$ then we have $f(a.a) = f(a).f(a)$ $= a'.a' = a'^2$ and in general we can write it as

$$f(a^n) = a^m.$$

But $f(a^n) = f(e) = e'$, by using the statement of the known theorem, therefore $a^m = e'$. Also $a'^m \neq e'$ for $m < n$ ie., $o(a') = n$.

---

4) By Cayley's Theorem, the regular permutation group G_1' is isomorphic to G_1 consists of the following four permutations f_1, f_2, f_3, f_4.

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1.(-1) & 1.i & 1.(-i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix} = 1$$

$$f_2 = \begin{pmatrix} 1 & -1 & i & -i \\ (-1)(1) & (-1)(-1) & (-1)i & (-1)(i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix} = (1\,-1)(i\,-i)$$

$$f_3 = \begin{pmatrix} 1 & -1 & i & -i \\ i(1) & -i(-1) & i.i & i(-1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix} = (1\,i\,-1\,-i)$$

$$f_4 = \begin{pmatrix} 1 & -1 & i & -i \\ (-i)(1) & (-i)(-1) & (-i)i) & (-i)(-i) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix} = (1\,-i\,-1\,i)$$

5) **Theorem:**

Let G, H be a groups and $\phi : G \to H$ a homomorphism. Then

$$G / \ker \phi \cong \phi(G).$$

Proof:

Let $k = \ker \phi$ and define the map $\phi : G/k \to \phi(G)$ by $\phi(gk) = \phi(g)$ for $g \in G$.

(i) ϕ is well defined

(ii) ϕ is injective

(iii) ϕ is surjective

(iv) ϕ is a homomorphism.

For (i),

we need to prove the implication.

" $g_1 k = g_2 k \Rightarrow \phi(g_1 k) = \phi(g_2 k)$ ".

So assume that $g_1 k = g_2 k$ for some $g_1, g_2 \in G$. Then $g_1^{-1} g_2 \in k$ by the thm, so $(g_1^{-1} g_2) \in H$. (recall that $k = \ker \phi$).

Since $\phi(g_1^{-1} g_2) = \phi(g_1)^{-1} \phi(g_2)$, we get

$$\phi(g_1)^{-1} \phi(g_2) = e_H.$$

Thus $\phi(g_1) = \phi(g_2)$ and so $\phi(g_1 k) = \phi(g_2 k)$, as desired.

For (ii),

we need to prove that

"$\phi(g_1 k) = \phi(g_2 k) \Rightarrow g_1 k = g_2 k$".

This is done by taking the argument in the proof of (i) and reversing all the multiplication arrows.

(iii) First note that the construction codomain (ϕ) = $\phi(G)$. Thus, surjectivity of ϕ we need to show that Range (ϕ) = $\phi(G/k)$ is equal to $\phi(G)$.

This is clear,

$$\phi(G/k) = \{\phi(gk) : g \in G\}$$

$$= \{\phi(g) : g \in G\} = \phi(G).$$

(iv) Finally, for any $g_1, g_2 \in G$ we have

$$\phi(g_1 k \cdot g_2 k) = \phi(g_1 g_2 k) = \phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$

$= \phi(g_1 k)\,\phi(g_2 k)$ where the first equality holds by the definition of product in quotient groups.

This ϕ is a homomorphism.

So, we constructed an isomorphism

$\phi : G/\ker\phi \to \phi(G)$ and thus $G/\ker\phi$ is isomorphic to $\phi(G)$.

UNIT 4 - Rings

Introduction to Rings in Algebra

The concept of a group has its origin in the set of mappings or permutations of a set unto itself. So far we have considered sets with one binary operation only. But rings are the motivation which arises from the fact that integers follow a definite pattern with respect to addition and multiplication. Thus we now aim at studying rings which are algebraic systems with two suitably restricted and related binary operations.

Definition

An algebraic structure $(R,+,\times)$ where R is a non-empty set and $+$ and $\times$ are defined operations in R is called a ring if for all a,b,c in R, the following axioms are satisfied:

R1: $(R,+)$ is an abelian group.

(i) $a + b \in R$ [Closure Law for Addition]

(ii) $(a + b) + c = a + (b + c)$ [Associative Law of Addition]

(iii) $a + 0 = a = 0 + a \ \forall \ a \in R$ [Existence of Additive Identity]

(iv) $a + (-a) = -a + a = 0 \ \forall \ a \in R$ [Existence of Additive Inverse]

(v) $a + b = b + a \ \forall \ a \in R$ [Commutative Law of Addition]

R2: $(R, \times)$ is a semi group.

(i) $a \cdot b \in R$ [Closure Law for Multiplication]

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ [Associative Law of Multiplication]

R3: Multiplication is left as well as right distributive over addition, i.e.
$a \cdot (b+c)=a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$

Examples of Rings

Example 1:

A Gaussian integer is a complex number a+ib, where a and b are integers. Show that the set J(i) of Gaussian integers forms a ring under the ordinary addition and multiplication of complex numbers.

Solution:

1

Let $a1+ib1$ and $a2+ib2$ be any two elements of $J(i)$, then

$(a1 + ib1) + (a2 + ib2) = (a1 + a2) = i(b1 + b2) = A + iB$

and

$(a1 + ib1) \cdot (a2 + ib2) = (a1a2 - b1b2) + i(a1b2 + b1a2) = C + iD$

These are Gaussian integers and therefore J(i) is closed under addition as well as the multiplication of complex numbers. Addition and multiplication are both associative and commutative compositions for complex numbers.

Also, multiplication distribution with respect to addition. The additive inverse of $a + ib \in J(i)$ is $(-a) + (-b)i \in J(i)$ as

$(a + ib) = (-a) + (-b)I = (a - a) + (b - b)i = 0 + 0i = 0$

The Gaussian integer $1+0 \cdot i$ is the multiplicative identity. Therefore, the set of Gaussian integers is a commutative ring with unity.

Example 2: Prove that the set of residue **{0, 1, 2, 3, 4}** modulo **5** is a ring with respect to the addition and multiplication of residue classes (**mod 5**).

Solution: Let **R = {0, 1, 2, 3, 4}.** Addition and multiplication tables for given set **R** are:

+ mod 5	**0**	**1**	**2**	**3**	**4**	**mod 5**	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**4**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**2**	**3**	**4**	**0**	**1**	**0**	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**0**	**1**	**2**	**0**	**2**	**4**	**1**	**3**
3	**3**	**4**	**0**	**1**	**2**	**3**	**0**				
4	**4**	**0**	**1**	**2**	**3**	**4**					

From the addition composition table the following is clear:

(i) Since all elements of the table belong to the set, it is closed under addition (**mod 5**).

(ii) Addition (**mod 5**) is always associative.

(iii) $0 \in R$ is the identity of addition.

(iv) The additive inverse of the elements **0, 1, 2, 3, 4** are **0, 4, 3, 2, 1** respectively.

(v) Since the elements equidistant from the principal diagonal are equal to each other, the addition (**mod 5**) is commutative. From the multiplication composition table, we see that **(R, .)** is a semi group, i.e. following axioms hold good.

(vi) Since all the elements of the table are in **R**, the set **R** is closed under multiplication (mod 5).

(vii) Multiplication (**mod 5**) is always associative.

(viii) The multiplication (**mod 5**) is left as well as right distributive over addition (**mod 5**).

Hence $(R,+,\cdot)$ is a ring.

ELEMENTARY PROPERTIES OF RING

If R is a ring, then for all a,b are in R.

(a) $a \cdot 0 = 0 \cdot a = a$
(b) $a(-b) = (-a)\, b = -(ab)$
(c) $(-a)(-b) = ab$

Proof:

(a) We know that $a0 = a(0 + 0) = a0 + a0 \quad \forall\ a \in R$ [using distributive law]

Since R is a group under addition, applying the right cancellation law,
$a0 = a0 + a0 \Rightarrow a + a0 = a0 + a0 \Rightarrow a0 = 0$

Similarly, $0a = (0 + 0)\, a = 0a + 0a \ \forall a \in R$ [using distributive law]
$\therefore 0+0a=0a+0a$ [because$0=0a+0a$]

Applying right cancellation law for addition, we get $0 = 0a$ i.e. $0a = 0$

Thus $a0 = 0a = 0$

(b) To prove that $a(-b) = -ab$ we should show that $ab = a(-b) = 0$

We know that $a[b + (b)] = a0 = 0$ because $b + (-b) = 0$ with the above result **(a)**
$ab+a(-b)=0$[by distributive law]
$\therefore a(-b) = -(ab)$

Similarly, to show $(-a)b = -ab$, we must show that $ab + (-a)b = 0$

But $ab + (-a)b = [a + (-a)]\, b = 0b = 0$
$\therefore -(a)\, b = -(ab)$ hence the result.

(c) Proving $(-a)(-b) = ab$ is a special case of forgoing the article. However its proof is given as:
$(-a)(-b) = -[a(-b)] = [-(ab)] = ab$

This is because $-(-x) = x$ is a consequence of the fact that in a group, the inverse of the inverse of an element is the element itself.
This is because $-(-x) = x$ is a consequence of the fact that in a group, the inverse of the inverse of an element is the element itself.

Special Types of Rings

1. Commutative Rings

A ring R is said to be a commutative if the multiplication composition in R is commutative,

i.e. $ab=ba \forall a,b \in R$

2. Rings With Unit Element

A ring R is said to be a ring with unit element if R has a multiplicative identity, i.e. if there exists an element R denoted by 1, such that

$1 \cdot a=a \cdot 1 \forall a \in R$

The ring of all $n \times n$ matrices with element as integers (rational, real or complex numbers) is a ring with unity. The unity matrix

$I_n=[100\cdots\ 0010\cdots\ 0001\cdots\ 0\vdots\ \vdots\ \vdots\ \ddots\ \vdots\ 000\cdots\ 1]$ is the unity element of the ring.

3. Rings With or Without Zero Divisors

While dealing with an arbitrary ring R, we may find elements a and b in R, where neither of which is zero and their product may be zero. We call such elements divisors of zero or zero divisors.

Definition:

A ring element $a(\neq 0)$ is called a divisor of zero if there exists an element $b(\neq 0)$ in the ring such that either
$ab = 0$ or $ba = 0$

We also say that a ring R is without zero divisors if the product of no two non-zero elements of the same is zero, i.e. if
$ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$ or both $a = 0$ and $b=0$

Cancellation Laws in a Ring

Cancellation Laws in a Ring

We say that cancellation laws hold in a ring R if
$ab = bc\ (a \neq 0) \Rightarrow b = c$ and $ba = ca\ (a \neq 0) \Rightarrow b = c$ where a,b,c are in R.

Thus in a ring with zero divisors, it is impossible to define a cancellation law.

Theorem:

A ring has no divisor of zero if and only if the cancellation laws holds in R.

Proof:

Suppose that R has no zero divisors. Let a,b,c be any three elements of R such that $a\neq 0, ab=ac$.

Now $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0 \Rightarrow b - c = 0$

[because R is without zero divisor and $a \neq 0$] $\Rightarrow b = c$

Thus the left cancellation law holds in R. Similarly, it can be shown that the right cancellation law also holds in R.

Conversely, suppose that the cancellation law holds in R. Let $a, b \in R$ and if possible let $ab = 0$ with $a \neq 0, b \neq 0$ then $ab = a \cdot 0$ (because $a \cdot 0 = 0$).

Since $a \neq 0, ab = a \cdot 0 \Rightarrow b = 0$

Hence we get a contradiction to our assumption that $b \neq 0$ and therefore the theorem is established.

Division Ring

A ring is called a division ring if its non-zero elements form a group under the operation of multiplication.

Pseudo Ring

A non-empty set R with binary operations + and × satisfying all the postulates of a ring except right and left distribution laws is called pseudo ring if

$(a+b) \cdot (c+d) = a \cdot c + a \cdot d + b \cdot c + b \cdot d$

for all $a,b,c,d \in R$

Integral Domain in Rings

Integral Domain: A commutative ring with unity is said to be an integral domain if it has no zero-divisors. Alternatively a commutative ring R with unity is called an integral domain if for all $a, b \in R$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Examples:

(i) The set II of integers under usual addition and multiplication is an integral domain for any two integers a,b, $ab = 0 \Rightarrow a = 0$ or $b = 0$.

(ii) Consider a ring $R=\{0,1,2,3,4,5,6,7\}$ under the addition and multiplication modulo 8. This ring is commutative but it is not an integral domain because $2 \in R, 4 \in R$ are two non-zero elements such that $2 \cdot 4 \equiv 0 \pmod 8$.

(iii) The ring of complex numbers C is an integral domain.

Let $J(i) = \{a + ib : a , b \in I\}$. It is easy to prove that J(i) is a commutative ring with unity. The zero element is $0 + 0i$ and unit element is $1 + 0i$. Also this ring is free from zero-divisor because the product of two non-zero complex numbers cannot be zero. Hence J(i) is an integral domain.

Euclidean Ring

An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a non-negative integer, to be denoted by d(a), such that:

(i) For all a, b $\in$ R, both non-zero, $d(a) \leqslant d(ab)$,

(ii) For any a, b $\in$ R, both non-zero, there exist q, r $\in$ R such that a = qb + r when either r = 0 or d(r) < d(b).

Note: The set of integers Z depends on the property of division algorithm. This property is also known as the Euclidean algorithm, which is used to find the greatest common divisors. This property is mostly satisfied for rings, and as such we can say that such type of rings are called Euclidean rings.

2. The above axioms ensure that the arithmetic in a ring R is "more or less" the familiar one: To be on the safe side let us mention the following rules:

   $0 \cdot a = 0 = a \cdot 0$ holds, since

   $a = 1 \cdot a = (1 + 0)a = a + 0 \cdot a$ and $(-1)a = a(-1) = -a$ follows from $0 = (1 + (-1))a = a + (-1)a$. But there is no cancellation rule for the multiplication, since there may be nontrivial "zero divisors",

   i.e. elements $a \in R \setminus \{0\}$, such that $ab = 0$ for some $b \neq 0$, and it can happen that $1 + \ldots + 1 = 0$.

   So we should actually derive all computation rules we use from the ring axioms!

Example

1. The sets $R = Z, Q, R, C$ with the usual addition and multiplication of integers resp. rational, real or complex numbers are rings.
2. If M is any set and R a ring, so is the set

$$R^M := \{f : M \to R\}$$

of all R-valued maps on M with the argument wise addition and multiplication of functions:

$$(f + g)(x) := f(x) + g(x),\ (fg)(x) := f(x)g(x).$$

Commutative rings, in general

The examples to keep in mind are these: the set of integers **Z**; the set $\mathbf{Z}_n$ of integers modulo n; any field F (in particular the set **Q** of rational numbers and the set **R** of real numbers); the set F[x] of all polynomials with coefficients in a field F. The axioms are similar to those for a field, but the requirement that each nonzero element has a multiplicative inverse is dropped, in order to include integers and polynomials in the class of objects under study.

Definition Let R be a set on which two binary operations are defined, called addition and multiplication, and denoted by + and ·. Then R is called a **commutative ring** with respect to these operations if the following properties hold:

(i) Closure: If $a,b \in R$, then the sum $a+b$ and the product $a \cdot b$ are uniquely defined and belong to R.

(ii) Associative laws: For all $a,b,c \in R$,

$a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) *Commutative laws:* For all $a,b \in R$,

$a+b = b+a$ and $a \cdot b = b \cdot a$.

(iv) *Distributive laws:* For all $a,b,c \in R$,

$a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$.

(v) *Additive identity:* The set R contains an **additive identity element**, denoted by 0, such that for all $a \in R$,

$a+0 = a$ and $0+a = a$.

(vi) *Additive inverses:* For each $a \in R$, the equations

$a+x = 0$ and $x+a = 0$

have a solution $x \in R$, called the **additive inverse** of a, and denoted by -a.
The commutative ring R is called a **commutative ring with identity** if it contains an element 1, assumed to be different from 0, such that for all $a \in R$,

$a \cdot 1 = a$ and $1 \cdot a = a$.

In this case, 1 is called a **multiplicative identity element** or, more generally, simply an **identity element.**

As with groups, we will use juxtaposition to indicate multiplication, so that we will write ab instead of $a \cdot b$.

Example ($\mathbf{Z}_n$) The rings $\mathbf{Z}_n$ form a class of commutative rings that is a good source of examples and counterexamples.

Definition Let S be a commutative ring. A nonempty subset R of S is called a **subring** of S if it is a commutative ring under the addition and multiplication of S.

Proposition Let S be a commutative ring, and let R be a nonempty subset of S. Then R is a subring of S if and only if

(i) R is closed under addition and multiplication; and
(ii) if $a \in R$, then $-a \in R$.

Definition Let R be a commutative ring with identity element 1. An element $a \in R$ is said to be **invertible** if there exists an element $b \in R$ such that $ab = 1$. The element a is also called a **unit** of R, and its multiplicative inverse is usually denoted by a^{-1}.

Proposition Let R be a commutative ring with identity. Then the set $R^\times$ of units of R is an abelian group under the multiplication of R.

An element e of a commutative ring R is said to be **idempotent** if $e^2 = e$. An element a is said to be **nilpotent** if there exists a positive integer n with $a^n = 0$.

Definition Let R and S be commutative rings. A function θ:R->S is called a **ring homomorphism** if

$\theta(a+b) = \theta(a) + \theta(b)$ and $\theta(ab) = \theta(a)\theta(b)$ for all $a,b \in R$.

A ring homomorphism that is one-to-one and onto is called an **isomorphism**. If there is an isomorphism from R onto S, we say that R is **isomorphic** to S, and write $R \cong S$. An isomorphism from the commutative ring R onto itself is called an **automorphism** of R.

Proposition

(a) The inverse of a ring isomorphism is a ring isomorphism.

(b) The composition of two ring isomorphisms is a ring isomorphism.

Proposition Let θ: R -> S be a ring homomorphism. Then

(a) $\theta(0) = 0$;

(b) $\theta(-a) = -\theta(a)$ for all a in R;

(c) if R has an identity 1, then $\theta(1)$ is idempotent;

(d) $\theta(R)$ is a subring of S.

Definition Let θ: R -> S be a ring homomorphism. The set $\{ a \in R \mid \theta(a) = 0 \}$ is called the **kernel** of θ, denoted by $\ker(\theta)$.

Proposition Let θ : R -> S be a ring homomorphism.

(a) If $a, b \in \ker(\theta)$ and $r \in R$, then $a + b$, $a - b$, and ra belong to $\ker(\theta)$.

(b) The homomorphism θ is an isomorphism if and only if $\ker(\theta) = \{0\}$ and $\theta(R) = S$.

Example Let R and S be commutative rings, let ϕ : R -> S be a ring homomorphism, and let s be any element of S. Then there exists a unique ring homomorphism Φ : R[x] -> S such that $\Phi(r) = \phi(r)$ for all $r \in R$ and $\Phi(x) = s$, defined by

$$\Phi(a_0 + a_1x + \ldots + a_mx^m) = \phi(a_0) + \phi(a_1)s + \ldots + \phi(a_m)s^m.$$

Proposition Let R and S be commutative rings. The set of ordered pairs (r,s) such that $r \in R$ and $s \in S$ is a commutative ring under componentwise addition and multiplication.

Definition Let R and S be commutative rings. The set of ordered pairs (r,s) such that $r \in R$ and $s \in S$ is called the **direct sum** of R and S.

Example The ring $\mathbf{Z}_n$ is isomorphic to the direct sum of the rings $\mathbf{Z}_k$ that arise in the prime factorization of n. This describes the structure of $\mathbf{Z}_n$ in terms of simpler rings, and is the first example of what is usually called a ``structure theorem." This structure theorem can be used to determine the invertible, idempotent, and nilpotent elements of $\mathbf{Z}_n$ and provides an easy proof of our earlier formula for the Euler phi-function in terms of the prime factors of n.

Definition Let R be a commutative ring with identity. The smallest positive integer n such that (n)(1) = 0 is called the **characteristic** of R, denoted by char(R). If no such positive integer exists, then R is said to have **characteristic zero**.

Ideals and factor rings

Definition Let R be a commutative ring. A nonempty subset I of R is called an **ideal** of R if

(i) $a \pm b \in I$ for all $a,b \in I$, and

(ii) $ra \in I$, for all $a \in I$ and $r \in R$.

Proposition Let R be a commutative ring with identity. Then R is a field if and only if it has no proper nontrivial ideals.

Definition Let I be a proper ideal of the commutative ring R. Then I is said to be a **prime ideal** of R if for all $a,b \in R$ it is true that $ab \in I$ implies $a \in I$ or $b \in I$.
The ideal I is said to be a **maximal ideal** of R if for all ideals J of R such that $I \subseteq J \subseteq R$, either J = I or J = R.

For an ideal I of a commutative ring R, the set { a+I | a∈R } of cosets of I in R (under addition) is denoted by R/I. By Theorem 3.8.4, the set forms a group under addition. The next theorem justifies calling R/I the **factor ring** of R modulo I.

Theorem If I is an ideal of the commutative ring R, then R/I is a commutative ring, under the operations (a+I) + (b+I) = (a+b) + I and (a+I)(b+I) = ab + I, for all $a,b \in R$.

Proposition Let I be an ideal of the commutative ring R.

(a) The natural projection mapping π: R -> R/I defined by $\pi(a) = a+I$ for all $a \in R$ is a ring homomorphism, and $\ker(\pi) = I$.

(b) There is a one-to-one correspondence between the ideals of R/I and the ideals of R that contain I.

Theorem [Fundamental Homomorphism Theorem for Rings] Let θ:R->S be a ring homomorphism. Then R/ker(θ) is isomorphic to θ(R).

Integral domains

Definition A commutative ring R with identity is called an **integral domain** if for all a,b $\in$ R, ab = 0 implies a = 0 or b = 0.

The ring of integers **Z** is the most fundamental example of an integral domain. The ring of all polynomials with real coefficients is also an integral domain, but the larger ring of all real valued functions is not an integral domain.

The cancellation law for multiplication holds in R if and only if R has no nonzero divisors of zero. One way in which the cancellation law holds in R is if nonzero elements have inverses in a larger ring; the next two results characterize integral domains as subrings of fields (that contain the identity 1).

Theorem Let F be a field with identity 1. Any subring of F that contains 1 is an integral domain.

Theorem Let D be an integral domain. Then there exists a field F that contains a subring isomorphic to D.

Theorem Any finite integral domain must be a field.

Proposition An integral domain has characteristic 0 or p, for some prime number p.

Proposition Let I be a proper ideal of the commutative ring R with identity.

(a) The factor ring R/I is a field if and only if I is a maximal ideal of R.
(b) The factor ring R/I is a integral domain if and only if I is a prime ideal of R.
(c) If I is maximal, then it is a prime ideal.

Definition Let R be a commutative ring with identity, and let a $\in$ R. The ideal

Ra = { x ∈ R | x = ra for some r ∈ R }is called the **principal ideal** generated by a.
An integral domain in which every ideal is a principal ideal is called a **principal ideal domain**.

Example (**Z** is a principal ideal domain) theorem shows that the ring of integers **Z** is a principal ideal domain. Moreover, given any nonzero ideal I of **Z**, the smallest positive integer in I is a generator for the ideal.

Theorem Every nonzero prime ideal of a principal ideal domain is maximal.

Example (Ideals of F[x]) Let F be any field. Then F[x] is a principal ideal domain, since by the ideals of F[x] have the form I = <f(x)>, where f(x) is the unique monic polynomial of minimal degree in the ideal. The ideal I is prime (and hence maximal) if and only if f(x) is irreducible. If p(x) is irreducible, then the factor ring F[x] / <p(x)> is a field.

Example (Evaluation mapping) Let F be a subfield of E, and for any element u ∈ E define the evaluation mapping θ_u: F[x] -> E by $\theta_u(g(x)) = g(u)$, for all g(x) ∈ F[x]. Since $\theta_u(F[x])$ is a subring of E that contains 1, it is an integral domain, and so the kernel of θ_u is a prime ideal. Thus if the kernel is nonzero, then it is a maximal ideal, so F[x] / ker(θ_u) is a field, and the image of θ_u is a subfield of E.

Unit- IV

1. Define Ring

Suppose R is a non-empty set equipped with two binary operations called addition and multiplication denoted by '+' and '.'respectively. i.e,)for all $a,b \in R$ we have $a+b \in R$ and $a \cdot b \in R$. Then the algebraic is structure (R,+,.) is called a ring, if the following postulates are satisfied:

1.Addition is associative,i.e,

$(a+b)+c = a+(b+c) \forall a,b,c \in R$.

2.Addition is commutative,i.e, a+b=b+a $a+b = b+a \forall a,b \in R$

3. There exists an element denoted by 0 in R such that $0+a = a \forall a \in R$

4. To each element a in R there exists an element –a in R such that $(-a)+a = 0$

5.Multiplication is associative, i.e, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \forall a,b,c \in R$.

6. Multiplication is distributive with respect to addition, i.e., for all a,b,c in R

$a \cdot (b+c) = a \cdot b + a \cdot c$

and $(b+c) \cdot a = b \cdot a + c \cdot a$

2. When will you say ring is a ring with unity.

If a ring possesses multiplicative identity then it is a ring with unity.

3. Give an example of a ring with unity

The set Q of all rational numbers is ring with unity.

4. Define commutative ring

If in a ring R, the multiplication composition is also commutative ie., if we $a \cdot b = b \cdot a \forall a,b \in R$ then R is called a commutative ring.

have

5. Prove that if R is a ring, then for all $a \in R$, $a0 = 0a = 0$.

$a0 = a(0+0)$

$= a0 + a0$

Therefore $0 + a0 = a0 + a0$. Now R is a group with respect to addition, therefore applying right cancellation law for addition in R we get $0 = a0$.

Similarly we have

$0a = (0+0)a$

$= 0a + 0a$

Therefore $0 + 0a = 0a + 0a$

Applying right cancellation law for addition in R we get $0 = 0a$

6. Give an example of a Ring with unity

The set I of all integers is a ring with unity, the addition and multiplication of integers as the two ring compositions.

7. Give an example of a Ring with out unity

The set 2I of all even integers is a commutative ring with out unity, the addition and multiplication of integers being the two ring compositions.

8. Define zero divisor

A non-zero element of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$ such that either $ab = 0$ or ba = 0

9. Define ring without zero divisors

A ring R is without zero divisors if the product of no two non-zero elements of R is zero, i.e., if $ab = 0 \Rightarrow a = 0$ orb = 0

10. Give an example of a ring without zero divisors

The ring of integers is a ring without zero divisors.

The product of two non-zero integers cannot be equal to the zero integer.

11. Define Integral domain

A ring is called an integral domain if it (i) is commutative, (ii) has unit element, (iii) is without zero divisors.

12. Show that the set of integers is an integral domain

The set of integers is a commutative ring with unity. Also I does not possess zero divisors because if a and b are integers such that $ab = 0$, then either a or b must be zero.

Therefore the set of integers is an integral domain.

13. Define characteristic of a ring

ith zero element 0 and suppose there exists a positive integer n such that $na = a + a + ...$ upto n terms $= 0$ for every $a \in R$. The smallest such positive integer n is called the characteristic of the ring R. If there exists no such positive integer, then R is said to be of characteristic zero or infinite.

14. Give an example of two rings whose characteristic is zero.

    1. The ring of integers
    2. The ring of rational numbers.

15. Show that the ring of integers modulo 6 has characteristic 6.

In the ring of integers modulo 6, we have $6x = 0$ for every x in the ring . Obviously no integer smaller than 6 satisfies this property. For instance, 5 cannot be the characteristic, since $5(2) = 4$ in I_6 and $4 \neq 0$.

Therefore the ring of integers modulo 6 has characteristic 6.

16. Define onto homomorphism of rings

A mapping f from a ring R onto a ring R' is said to be a homomorphism of R onto if

i) $f(a+b) = f(a) + f(b) \forall a, b \in R$

ii) $f(ab) = f(a)f(b)$ for all a, b ∈ R ring R'

17. If f is a homomorphism of a ring R into a ring R' then $f(-a) = -f(a) \forall a \in R$.

Let a be any element of R. Then $-a \in R$. We have $0' = f(0) = f[a + (-a)] = f(a) + f(-a)$.

Therefore $f(-a)$ is the additive inverse of $f(a)$ in the ring Thus $f(-a) = -f(a)$.

18. Define Kernel of a ring homomorphism

If f is a homomorphism of a ring R into a ring R' then the set of all those elements of R which are mapped onto the zero element of R' is called the kernel of the homomorphism f.

19. Show that every homomorphic image of a commutative ring is commutative.

Let R be a commutative ring. Let f be a homomorphic mapping of R onto a ring R'.

Then R' is a homomorphic image of R.

Let a', b' be any two elements of R' . Then $f(a) = a', \text{f(b)} = \text{b}'$ for some $a, b \in R$ because f is onto R'.

20. If R is a ring with unit element 1 and ϕ is a homomorphism of R into R' prove that $\phi(1)$ is the unit element of R'.

Since ϕ is a homomorphism of R onto R' therefore R' is a homomorphic image of R. If 1 is the unit element of R, then $\phi(1) \in R'$. Let a' be any element of R'. Then $a' = \phi(a)$ for some $a \in R$ since ϕ is onto R'. We have

$\phi(1)a' = \phi(1)\phi(a) = \phi(1a) = \phi(a) = a'$

And $a'\phi(1) = \phi(a)\phi(1) = \phi(a1) = \phi(a) = a'$

Therefore $\phi(1)$ is the unity element of R'.

Unit-IV- REVISION

1. If R is a ring then for all $a,b,c \in R$
   i) $a0 = 0a = 0$
   ii) a (-b)=-(ab)=(-a)b
   iii) $(-a)(-b) = ab$
   iv) $a(b-c) = ab - ac$
   v) $(b-c)a = ba - ca$

A *ring* R is an abelian group with a multiplication operation $(a, b) \to ab$ that is associative and satisfies the distributive laws: $a(b+c) = ab+ac$ and $(a+b)c = ab+ac$ for all $a, b, c \in R$. We will always assume that R has at least two elements, including a multiplicative identity 1_R satisfying $a1_R = 1_R a = a$ for all a in R. The multiplicative identity is often written simply as 1, and the additive identity as 0. If a, b, and c are arbitrary elements of R, the following properties are derived quickly from the definition of a ring; we sketch the technique in each case.

(1) $a0 = 0a = 0$ $[a0 + a0 = a(0+0) = a0; 0a + 0a = (0+0)a = 0a]$

(2) $(-a)b = a(-b) = -(ab)$ $[0 = 0b = (a+(-a))b = ab+(-a)b$, so $(-a)b = -(ab)$; similarly,

$$0 = a0 = a(b+(-b)) = ab + a(-b), \text{ so } a(-b) = -(ab)]$$

(3) $(-1)(-1) = 1$ [take $a = 1, b = -1$ in (2)]

(4) $(-a)(-b) = ab$ [replace b by $-b$ in (2)]

(5) $a(b-c) = ab - ac$ $[a(b+(-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac]$

(6) $(a-b)c = ac - bc$ $[(a+(-b))c = ac + (-b)c) = ac - (bc) = ac - bc]$

(7) $1 \neq 0$ [If $1 = 0$ then for all a we have $a = a1 = a0 = 0$, so $R = \{0\}$, contradicting the assumption that R has at least two elements]

(8) The multiplicative identity is unique [If $1'$ is another multiplicative identity then $1 = 11' = 1'$]

2. Show that the set I of all integers is a ring with respect to addition and multiplication of integers as the two ring composition.

$(\mathbf{Z}_n, \oplus, \odot)$ 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 $b \oplus c \equiv (b + c) \pmod{n}$.

Hence $a \odot (b \oplus c) \equiv a(b + c) \pmod{n}$.

Also $a \odot b \equiv ab \pmod{n}$ and

$a \odot c \equiv ac \pmod{n}$ so that

$(a \odot b) \oplus (a \odot b) \equiv (ab + ac) \pmod{n}$.

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.

3. Show that the set R of all real numbers is a ring with respect to addition and multiplication of real numbers as the two ring compositions.

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 distributative laws are consequences of the corresponding properties in $\mathbf{R}$. Hence R is a ring.

4. Prove that the set Q of all rational numbers is a commutative ring with unity, the addition and multiplication of rational numbers being the two ring compositions.

Let Q be the set of all symbols of the form $a_0+a_1i+a_2j+a_3k$ where $a_0, a_1, a_2, a_3 \in \mathbf{R}$. Two such symbols $a_0 + a_1i + a_2j + a_3k$ and $b_0 + b_1i + b_2j + b_3k$ are defined to be equal iff $a_i = b_i, i = 0, 1, 2, 3$. We now make Q into a ring by defining $+$ and $\cdot$ as follows.

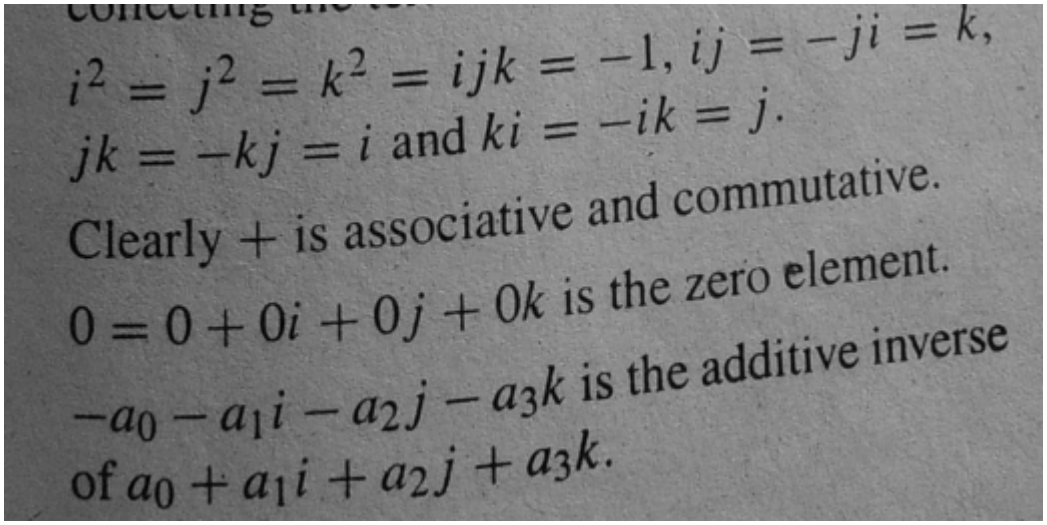
For any $x = a_0 + a_1i + a_2j + a_3k$ and $y = b_0 + b_1i + b_2j + b_3k$,

$$\begin{aligned} x + y &= (a_0 + a_1i + a_2j + a_3k) \\ &\quad + (b_0 + b_1i + b_2j + b_3k) \\ &= (a_0 + b_0) + (a_1 + b_1)i \\ &\quad + (a_2 + b_2)j + (a_3 + b_3)k \text{ and} \end{aligned}$$

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

The formula for the product comes from multiplying the two symbols formally and collecting the terms using the relations

$ii = k$.

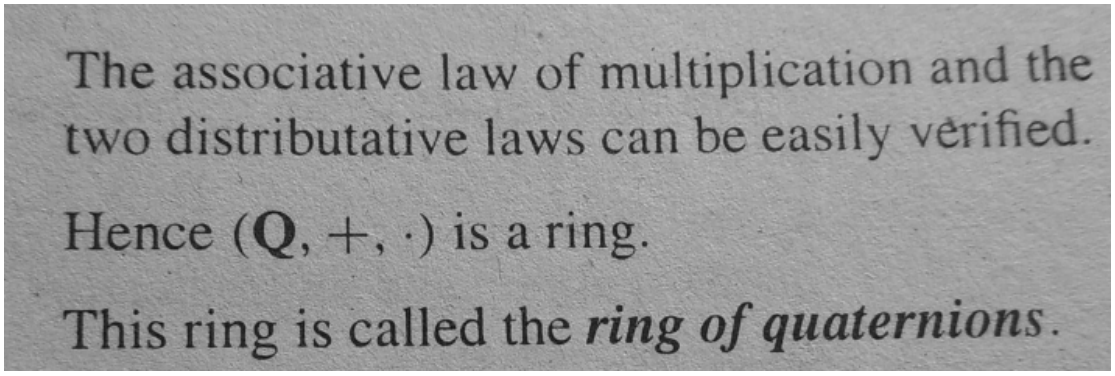


$$i^2 = j^2 = k^2 = ijk = -1,\ ij = -ji = k,$$
$$jk = -kj = i \text{ and } ki = -ik = j.$$

Clearly $+$ is associative and commutative.

$0 = 0 + 0i + 0j + 0k$ is the zero element.

$-a_0 - a_1 i - a_2 j - a_3 k$ is the additive inverse of $a_0 + a_1 i + a_2 j + a_3 k$.



The associative law of multiplication and the two distributative laws can be easily verified.

Hence $(\mathbf{Q}, +, \cdot)$ is a ring.

This ring is called the ***ring of quaternions***.

5. Show that the set M of all $n \times n$ matrices with their elements as real numbers(rational numbers, complex numbers, Integers) is a non-commutative ring with unity, with respect to addition and multiplication of matrices.

Let $M_2(\mathbb{Z})$, $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$ and $M_2(\mathbb{C})$ denote the sets of 2×2 matrices with entries, respectively, in the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. Addition and multiplication can be defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \oplus \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+b & b+f \\ c+g & d+h \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

with a, b, c, d, e, f, g, h in, respectively $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. The matrices

$$0_R = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

are then, respectively, additive identity elements and multiplicative identity elements of R. Note however that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

so multiplication in R is not commutative in general. Thus, each of these sets is a non-commutative ring with identity.

6. Prove that the set $R = \{0,1,2,3,4\}$ is a commutative ring with respect to $+_6$ *and* $\times_6$ as the two ring compositions.

Solution: Let **R = {0, 1, 2, 3, 4}.** Addition and multiplication tables for given set **R** are:

+ mod 5	**0**	**1**	**2**	**3**	**4**	**. mod 5**	**0**	**1**	**2**	**3**	**4**

0	**0**	**1**	**2**	**3**	**4**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**2**	**3**	**4**	**0**	**1**	**0**	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**0**	**1**	**2**	**0**	**2**	**4**	**1**	**3**
3	**3**	**4**	**0**	**1**	**2**	**3**	**0**	**3**	**1**	**4**	**2**
4	**4**	**0**	**1**	**2**	**3**	**4**	**0**	**4**	**3**	**2**	**1**

From the addition composition table the following is clear:

(i) Since all elements of the table belong to the set, it is closed under addition (**mod 5**).

(ii) Addition (**mod 5**) is always associative.

(iii) $0 \in R$ is the identity of addition.

(iv) The additive inverse of the elements **0, 1, 2, 3, 4** are **0, 4, 3, 2, 1** respectively.

(v) Since the elements equidistant from the principal diagonal are equal to each other, the addition (**mod 5**) is commutative.From the multiplication composition table, we see that **(R, .)** is a semi group, i.e. following axioms hold good.

(vi) Since all the elements of the table are in **R**, the set **R** is closed under multiplication (mod 5).

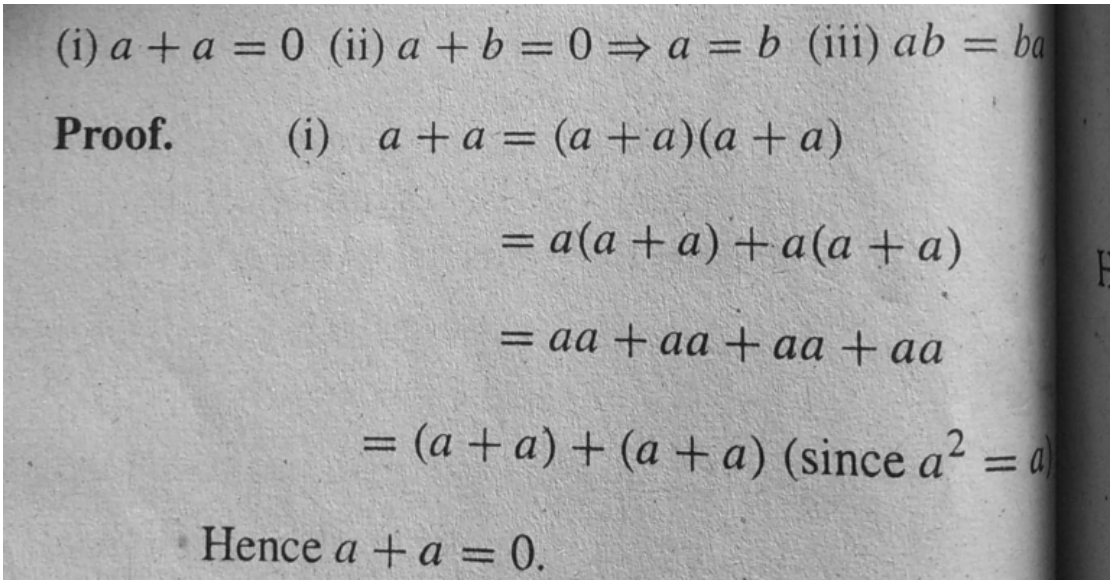
(vii) Multiplication (**mod 5**) is always associative.

(viii) The multiplication (**mod 5**) is left as well as right distributive over addition (**mod 5**).

Hence (R,+, .) is a ring.

7. If a,b are any elements of a ring R, Prove that
   i) $-(-a) = a$
   ii)
   iii) $-(a+b) = -a-b$
   iv) $-(a-b) = -a+b$
8. If two operations $*$ and $\circ$ on the set I of integers are defined as follows: $a * b = a + b - 1$, $a \circ b = a + b - ab$ Prove that the system $(I, *, \circ)$ is a commutative ring with identity.
9. Prove that the set M of 2 x 2 matrices over the field of real numbers is a ring with respect to addition and multiplication. Is it a commutative ring with unity element? Find the zero element.

10. If R is a ring such that $a^2=a$ for every $a \in R$. Prove that
    i) $a+a=0$ for every $a \in R$
    ii) $a+b=0$ implies $a=b$
    iii) R is commutative ring



(i) $a+a=0$ (ii) $a+b=0 \Rightarrow a=b$ (iii) $ab=ba$

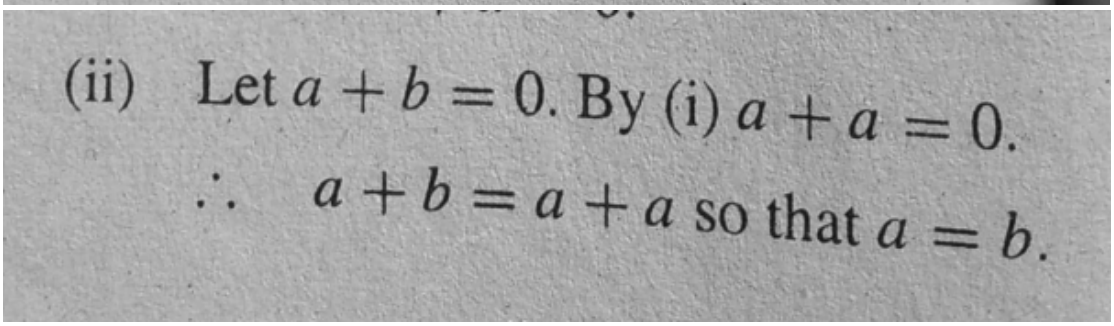
Proof. (i) $a+a=(a+a)(a+a)$

$=a(a+a)+a(a+a)$

$=aa+aa+aa+aa$

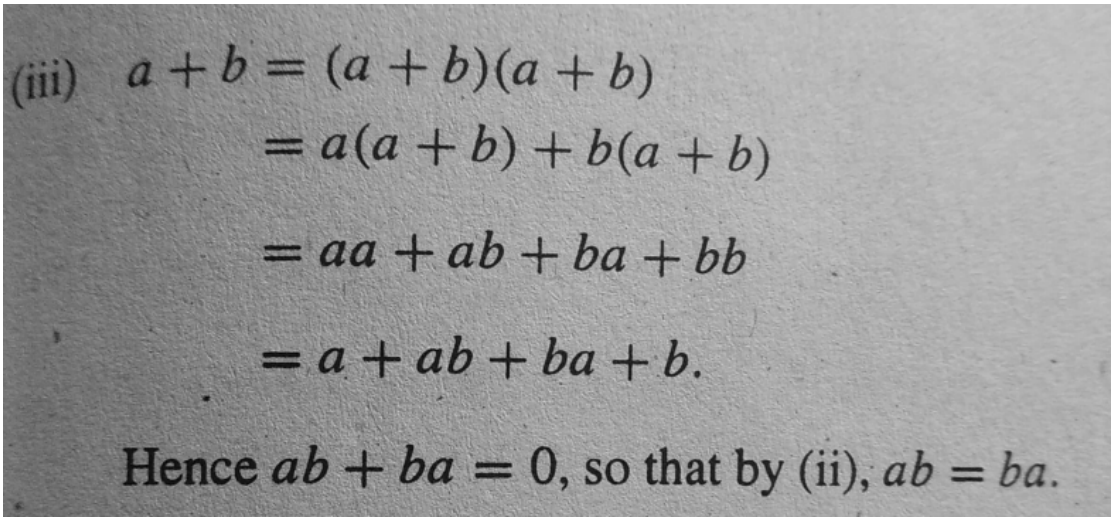
$=(a+a)+(a+a)$ (since $a^2=a$)

Hence $a+a=0$.



(ii) Let $a+b=0$. By (i) $a+a=0$.

$\therefore \quad a+b=a+a$ 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), $ab=ba$.

(OR)

1. Prove that a ring R is without zero divisors if and if the cancellation laws hold in R.
2. Show that the set of all integers is an integral domain with respect to addition and multiplication.

3. Define a ring and an integral domain. Give an example of a ring which is not an integral domain.
4. Give an example each of which is
   i) a non-commutative ring
   ii) ring without zero divisors
   iii) division ring
   iv) a ring which is not an integral domain
5. Show that the characteristic of a ring with unity is 0 or $n > 0$ according as the unity element 1 regarded as a member of the additive group of the ring has the order zero or n.
6. Show that the set of all real numbers of the form $a + b\sqrt{2}$ with a and b as integers is an integral domain with respect to ordinary addition and multiplication.
7. Prove that the characteristic of an integral domain is 0 or $n > 0$ according as the order of any non-zero element regarded as a member of the additive group of integral domain is either 0 or n.
8. Prove that each non-zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order.
9. Prove that the characteristic of an integral domain is either 0 or a prime number.
10. If f is a homomorphism of a ring R into ring R' then

    i) $f(0) = 0'$, where 0 is the zero element of the ring R and $0'$ is the zero element of R'.

    ii) $f(-a) = -f(a) \forall a \in R$ be a homomorphic mapping of a ring R into a ring R.

UNIT 5- SUBRINGS

Definition Let S be a commutative ring. A nonempty subset R of S is called a **subring** of S if it is a commutative ring under the addition and multiplication of S.

Definition Let R be a commutative ring. A nonempty subset I of R is called an **ideal** of R if

(i) $a \pm b \in I$ for all $a, b \in I$, and
(ii) $ra \in I$, for all $a \in I$ and $r \in R$.

Subrings and ideals

These are the concepts which play the same role as subgroups and normal subgroups in group theory.

Definition

A **subring** S of a ring R is a subset of R which is a ring under the same operations as R.

Equivalently: **The criterion for a subring**
A non-empty subset S of R is a subring if $a, b \in S \Rightarrow a - b, ab \in S$.

So S is *closed under subtraction and multiplication*.

Exercise: Prove that these two definitions are equivalent.

Remark

Using the above criterion makes it easy to check that something is a ring by showing that it is a subring of something else since one does not need to check associativity or distributivity.

Examples

1. The *even integers* $2\mathbf{Z}$ form a subring of $\mathbf{Z}$.
   More generally, if n is any integer the set of all multiples of n is a subring $n\mathbf{Z}$ of $\mathbf{Z}$.
   The odd integers do not form a subring of $\mathbf{Z}$.
2. The subsets $\{0, 2, 4\}$ and $\{0, 3\}$ are subrings of $\mathbf{Z}_6$.
3. The set $\{a + bi \in \mathbf{C} \mid a, b \in \mathbf{Z}\}$ forms a subring of $\mathbf{C}$.
   This is called the ring of **Gaussian integers** (sometimes written $\mathbf{Z}[i]$) and is important in Number Theory.

4. The set $\{a + b\sqrt{5} \mid a, b \in \mathbf{Z}\}$ is a subring of the ring **R**.
5. The set $\{x + y\sqrt{5} \mid x, y \in \mathbf{Q}\}$ is also a subring of **R**.
6. The set of real matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ forms a subring of the ring of *all* 2 × 2 real matrices.

An *ideal* is a special kind of subring.

Definition

A subring I of R is a **left ideal** if $a \in I, r \in R \Rightarrow ra \in I$.

So I is *closed under subtraction and also under multiplication on the left by elements of the "big ring"*.

A **right ideal** is defined similarly.

A **two-sided ideal** (or just an **ideal**) is both a left and right ideal.
That is, $a, b \in I, r \in R \Rightarrow a - b, ar, ra \in I$.

Remark

These subsets are related to the *ideal numbers* that Eduard Kummer (1810 to 1893) defined to "restore the uniqueness of factorisation" in the rings used for proving cases of Fermat's last theorem.

Examples

1. Examples 1) and 2) of subrings are also ideals, while examples 3), 4), 5) and 6) are not.
2. In *any* ring R the subsets $\{0\}$ and R are both two-sided ideals. If R is a field these are the only ideals.
   Proof
   Note that if the identity 1 is in an ideal then the ideal is the whole ring. But if a field element $a \neq 0$ is in an ideal, so is $a^{-1}a$ and so 1 is in too.□
3. The set of real matrices of the form $\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}$ forms a *left ideal* of the ring of *all* 2 × 2 real matrices while those of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ form a *right ideal* of this ring.
   This ring does not have any proper non-trivial two-sided ideals.

4. The set of all polynomials over any ring with 0 "constant" coefficient form an ideal.
   Proof
   Such a polynomial is of the form $xq(x)$ for some polynomial $q(x)$ and it is easy to verify the ideal condition for these.□
5. The set of all polynomials in $\mathbf{Z}[x]$ whose coefficients are all *even* is an ideal. So is the set of those with even constant coefficient.

Here is a very important way of making ideals.

Definitions

Let R be a commutative ring with identity. Let S be a subset of R. The **ideal generated by** S is the subset $< S > = \{r_1s_1 + r_2s_2 + ... + r_ks_k \in R \mid r_1 , r_2 , ... \in R, s_1 , s_2 , ... \in S, k \in \mathbf{N}\}$.

In particular, if S has a single element s this is called the **principal ideal generated by** s.

That is, $< s > = \{rs \mid r \in R\}$.

Remarks

1. It is easy to see that the above does define an ideal.
2. If the ring is not commutative then the above defines a *left* ideal. It is easy to modify the definition to get a right ideal or a two-sided ideal. If the ring does not have an identity then in general S will not be a subset of $< S >$.
3. In general, the "thing" generated by a subset is the smallest "thing" containing the subset. So you can talk about the subgroup of a group generated by a subset or the subring of a ring generated by a subset, ...

Examples

1. The ideal $2\mathbf{Z}$ of $\mathbf{Z}$ is the *principal ideal* $< 2 >$.
2. Example 4 above (the polynomials in $\mathbf{R}[x]$ with 0 constant term) is the principal ideal $< x >$.
3. The set of all polynomials in $\mathbf{Z}[x]$ whose coefficients are all *even* is the principal ideal $< 2 >$.
   The set of all polynomials with even constant coefficient is the ideal $< 2, x >$ and is *not* principal.

4. The set of polynomials in $\mathbf{R}[x, y]$ with zero constant coefficient is the ideal $< x, y >$ and is not principal.
5. For any commutative ring with identity, the trivial ideal $\{0\}$ is the principal ideal $< 0 >$ and the whole ring is the principal ideal $< 1 >$.

Remark

We will see later that in the rings $\mathbf{Z}$ and $\mathbf{R}[x]$ *every* ideal is principal.

Unit -V

1. Define subring
   Let R be a ring. A non-empty subset S of the ring R is said to be a subring of R is S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.
2. Define improper subrings
   The subrings $\{0\}$ and R are known as improper subrings of R.
3. Define proper subrings
   The subrings of R other than $\{0\}$ and R are known as proper subrings of R.
4. State the necessary and sufficient condition for a non-empty subset S of a ring R to be a subring of R.
   i). $a \in S, b \in S \Rightarrow a - b \in S$
   ii). $a \in S, b \in S \Rightarrow ab \in S$
5. Show that the set of integers is a subring of the ring of rational numbers.
6. Define an ordered integral domain.

   An integral domain (D,+,.) is said to be ordered if D contains a subset D_+ such that

   i) D_+ is closed with respect to addition and multiplication as defined on D.
   ii) $\forall a \in D$ one and only one of a=0, $a \in D_+, -a \in D_+$ holds.

   The elements of D_+ are called positive elements of D, all other non-zero elements of D are called negative elements of D.
7. Define left ideal
   A non empty subset S of a ring R is said to be a left ideal of R if:
   i) S is a subgroup of R with respect to addition
   ii) $rs \in S \; \forall r \in R, \forall s \in S$
8. Define right ideal
   A non empty subset S of a ring R is said to be a right ideal of R if:
   S is a subgroup of R with respect to addition
   $sr \in S \; \forall r \in R, \forall s \in S$
9. Define ideal
   A non empty subset S of a ring R is said to be an ideal (also two sided ideal)
   i) S is a subgroup of R under addition. i.e., S is a subgroup of the additive group of R.
   ii) $rs \in S$ and $sr \in S$ for every $r \in R$ and for every $s \in S$.
10. Define proper ideal
    An ideal of R other than the two ideals 0 and R are known as proper ideal of R.
11. Show that the set of integers is only a subring but not an ideal of the ring of rational numbers (Q,+,.)

    The product of a rational number and an integer is not necessarily an integer.

    For example, $3 \in I, \frac{2}{5} \in Q$ but $(2/5).3 = 6/5 \notin I$

Therefore I is not an ideal of the ring of rational numbers.

12. Define field of Quotients
    If D is a commutative ring with out zero divisors, then we shall see that it can be embedded in a field F i.e, there exists a field F which contains a subset D' isomorphic to D. We shall construct a field F with the help of elements of D and this field F will contain a subset D' such that D is isomorphic to D'. This field F is called the field of Quotients of D.
13. Define Quotient ring
    Suppose R is an arbitrary ring and S is an ideal in R. Then S is a subgroup of the additive abelian group of R. The cosets of S in R are called the residue classes of S in R. We denote the set of all residue classes of S in R by the symbol $R/S.$ Thus $R/S. = \{S + a : a \in R\}$.
14. If an ideal U of a ring R contains a unit of R then U =R.
    Let R be a ring with unity element 1. Let u be a unit of R Then u is an inversible element of R i.e, u^{-1} exists . Let $u \in U$. Since U is an ideal, therefore
    $u \in U, u^{-1} \in R \Rightarrow uu^{-1} \in U \Rightarrow 1 \in U$.
    Now let x be any element of R. Then $x \in R, 1 \in \mathrm{U} \Rightarrow \mathrm{x1} \in \mathrm{U} \Rightarrow \mathrm{x} \in \mathrm{U}$
    Therefore $R \subseteq U$.
    Also $U \subseteq R$ as U is an ideal of R. Hence U=R.

15. Define Maximal Ideal

    An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if when ever U is an ideal of R such that $S \subseteq U \subseteq R$, then either $R = U$ or $S = U$.

16. Define Prinicipal ideal
    An ideal S of a ring R is said to be a prinicipal ideal if there exists an element $a \in S$ such that any ideal T of R containing a also contains S i.e, S= (a).
17. Define Prime ideal
    Let R be a ring and S is an ideal in R. Then S is said to be a prime ideal of R if
    $ab \in S, \mathrm{ab} \in \mathrm{R}$ implies that either a or b is in S.
18. Define Field
    A ring R with atleast two elements is called a field if it,
    i) is commutative
    ii) has unity
    iii) is such that each non zero element possesses multiplicative inverse.
19. Define Division ring
    A ring R with atleast two elements is called division ring if it
    i) has unity
    ii) is such that each non zero element possesses multiplicative inverse.
20. Give an example of integral domain but not field.
    The ring of all integers is an integral domain and it is not a field. The only invertible elements of the ring of integers are 1 and -1.

Practice questions in Unit-V

1. Prove that necessary and sufficient condition for a non-empty subset S of a ring R to be a subring of R are
   i). $a \in S, b \in S \Rightarrow a - b \in S$
   ii). $a \in S, b \in S \Rightarrow ab \in S$
2. Prove that the intersection of two subrings is a subring.
3. Prove that an arbitrary intersection of subrings is a subring.
4. Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2 x 2 matrices with integral elements.
5. Prove that the intersection of two ideals of R is an ideal of R.
6. Show that S is an ideal of $S + T$ where S is any ideal of ring R, and T any subring of R.
7. Let ϕ be a homomorphic mapping of a ring R into a ring R'. Let S' be the homomorphic image of R in R'. Then S' is a subring of R'.
8. If f is a homomorphism of a ring R into a ring R' with kernel S, then S is an ideal of R.
9. Prove that a commutative ring with zero divisors can be embedded in a field.
10. Suppose R is a ring, S an ideal of R. Let f be a mapping from R to R|S defined by $f(a) = S + a \forall a \in R$. Then prove that f is an homomorphism of R onto R/S..

(OR)

1. State and prove fundamental theorem on homomorphism of rings
2. Prove that an ideal S of the ring of integers I is maximal if and only if S is generated by some prime integer.
3. Let R be a commutative ring and S an ideal of R, Then the ring of residue classes R / S is an integral domain if and only if S is a prime ideal.
4. Let S_1, S_2 be ideals of a ring R and let $S_1 + S_2 = \{s_1 + s_2 : s_1 \in S_1, s_2 \in S_2\}$ .Then $S_1 + S_2$ is an ideal of R generated by $S_1 \cup S_2$
5. Let R be a commutative ring with unity and a,b be two non-zero elements of R. Then $(a) = (b)$ iff $a \mid b$ and b | a .
6. Let R be a ring with unit element, R not necessarily commutative, such that the only right ideals of R are (0) and R. Prove that R is a division ring.
7. Show that the set of all rational numbers is a field.
8. Show that the set of real numbers is a field.
9. Show that every field is an integral domain.
10. Show that every finite integral domain is a field.