SEMESTER - V

CORE IX MODERN ALGEBRA - I

UNIT-I :

Group Theory: Definition of Group, Examples of groups, some preliminary lemmas and Subgroups - Definition - Lemmas - Theorem [Lagrange's, Euler and format] - Examples. (Sections 2.1 to 2.4).

UNIT-II :

Group theory (continuation): A counting principle - Normal Sub groups and quotient groups and Homomorphism - Definitions - Lemmas - Theorems - Examples. (Sections 2.5 to 2.7)

UNIT-III :

Group Theory (continuation): Automorphism, Cayley's theorem and permutation groups - definition - Lemmas - Theorems - Examples. (Sections 2.8 - 2.10).

UNIT-IV :

Ring Theory: Definition and Examples of Rings, Some Special classes of Rings, Homomorphisms, ideals and Quotient Rings and more ideals and Quotient rings - Definition - Lemmas - theorem - Examples Sections (3.1-3.5)

UNIT-V :

Ring theory (continuation):- The field of quotient of an integral domain, Euclidean Rings, A particular Euclidean ring and polynomial rings - Definition - Lemmas -

theorems - Examples - polynomials over the rational field. polynomial rings over the commutative rings.
(Sections 3.6 - 3.11).

TEXT BOOKS :-

1). I.N. Herstein, Topics in Algebra, John wiley. New York, 1975.

REFERENCE BOOKS:

1) Mathematics for Degree Students (B.Sc IIIy years). Dr. U.S. Rana, S. chand, 2012.

2) A first course in Modern Algebra, A.R. Vasistha, Krishna prakasan Mandhir, 9 Shivaji road, Meerut (up), 1988.

3). Modern algebra, M.L. Santiago, Tata Mc Graw Hill New Delhi, 1994.

4). Modern Algebra, K. Viswanartha Naik, Emerald Publishers, 135, Anna Salai, Chennai 1988.

UNIT-I

Group Theory.

1) **Set:**

A collection of well-defined object.

---

2) **Binary operation:**

Let G be a non empty set the binary operation is a function from $G \times G$ to S.

If $*$ is a binary operation then

$* : G \times G \to G$

i.e $\forall\ a, b \in G$, if $a * b \in G$ then $*$ is a binary on G.

Example:

Addition is a binary operation on the set of natural numbers i.e $(N, +)$

But $(N, -)$ is not a Binary operation on N.

EX: For $4 \in N, 7 \in N, \to 4-7 = -3 \notin N$

---

3. **One-one (or) injective:**

A function $f: A \to B$ is $\underset{1-1}{\text{one to one}}$ is distinct element in A have distinct images in B under f.

* If f is 1-1 if $x, y \in A$ and $x \neq y$ then $f(x) \neq f(y)$.

i.e if $f(x) = f(y)$, then $x = y$.

---

4. **onto (surjective).**

If the mapping f is called onto, if the range of f is equal to co-domain B.

Thus if f is onto then every element of B has Pre-image in A.

* If $f: A \to B$ is one-one onto then f is called bijection.

i,e if f is bijection, then every element of B has exactly one preimage in A.

Ex:

1) $f: Z \to R$, $f(x) = 2x \quad \forall x \in Z$

It is 1-1 and not onto

2) $f: R \to R$, $f(x) = 2x \quad \forall x \in R$

It is 1-1 and onto.

---

5. Definition :- Group

A non empty set of elements G is said to form a group if in G there is defined a binary operation, called the product and denoted by ., such that

1) closure property

i,e $\forall a, b \in G \Rightarrow a, b \in G$

2) Associativity

i,e $\forall a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$

3) Existence of Identity

There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$

The element e is identity.

4). Existence of inverse

For every $a \in G$, there exists an element $a^{-1} \in G$, $\ni a * a^{-1} = a^{-1} * a = e$

---

6. Definition :- Abelian group (or) commutative group.

A Group G is said to be abelian if for every $a, b \in G$, $a * b = b * a$.

* A group which is not abelian is called non abelian group.

---

7. Order of the group :

The number of elements in a finite group is called the order of the group.

* If in G, consists of a finite number of distinct elements then the group is called finite group.

* Otherwise is called an infinite group.

---

8. Definition :- Symmetric group:

For any arbitary non empty set S, we defined as to be the set of all one-to-one mappings of the set S onto itself is called an symmetric group of degree n (The set S contains n elements).

2.2.) Some examples of Groups:-

1) Let G consist of the integers $0, \pm 1, \pm 2$, where we mean by $a.b$ for $a.b \in G$, is defined by $a * b = a + b$ Then satisfies

the postulates of the group.

2). $G = \{1, -1\}$. under the multiplication of real numbers Then G is an abelian group of order 2.

3). Let $G = S_3$, i.e Symmetric group of degree 3, the group of all 1-1 mappings of the set $\{x_1, x_2, x_3\}$ onto it self. under the product the G is a group of order 6

($S_3 = \{x_1, x_2, x_3\}$, 3! elements). order = 6.

4). The set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $a, b, c, d \in R$ is a group under matrix addition. It is abelian group.

5). The set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $a, b, c, d \in R$ is a not a group under multiplication.

Because inverse exist if $|A| \neq 0$

For ex: The matrix $A = \begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix}$ has no inverse. Since $|A| = 0$

6). Let G be the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a, b, c, d \in R \ni ad - bc \neq 0$ under the multiplication G is a group.

i) closure: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{pmatrix}$

The entires of 2×2 matrices are real and also we see that

$(aw+by)(cx+dy) - (ax+bz)(cw+dy) \neq 0$

(closure is True).

(or) $(aw+by)(cx+dz) - (ax+bz)(cw+dy)$

$= (ad-bc)(aw+dy) \neq 0.$

ii) The associative law of multiplication holds in matrices.

iii) Existence of identity.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$$

Since $|I| = 1 \neq 0$.

iv) Inverse:

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $ad - bc \neq 0$

we have to find A^{-1} to see that

$$A^{-1} = \frac{1}{|A|} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

i.e $$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$A A^{-1} = A^{-1} A = I$$

It is easy to see that G is an infinite non abelian group.

2.3. Some preliminary Lemmas :-

1) Lemma : 2:3:1

If G is a group then

i) The identity element of G is unique.

ii) Every $a \in G$ has a unique inverse in G.

iii) For every $a \in G$, $(a^{-1})^{-1} = a$

iv) For all $a.b \in G$, $(a.b)^{-1} = b^{-1}a^{-1}$

Proof:

i) Suppose e and f are two identity elements of a group G1 we have for every $a \in G_1$,

$$a \cdot e = a = e \cdot a \rightarrow ①$$

$$a \cdot f = a = f \cdot a \rightarrow ②$$

From ① & ② we see that

$$a \cdot e = e \cdot a = a \cdot f = f \cdot a$$

$$\Rightarrow e = f$$

The identity is unique.

ii) Let 'a' be any element of a group G. and Let 'e' be the identity element.

Suppose x and y are two inverses of 'a'

i,e $x \cdot a = e = a \cdot x$ and $y \cdot a = e = a \cdot y$

we have $x(a \cdot y) = x \cdot e = x \rightarrow ①$

$$(xa) \cdot y = e \cdot y = y \rightarrow ②$$

From ① & ② we see that $x = y$

The inverse is unique.

iii) If e is the identity element

we have $a^{-1} \cdot a = e$

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

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

By using Left cancellation law.

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

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

(or)

We have $a^{-1}a = e$

Multiplying both sides on the left by $(a^{-1})^{-1}$

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

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

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

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

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

iv) Suppose a and b are elements of G.

If a^{-1} and b^{-1} are inverses of a and b respectively.

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

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

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

By the definition of inverse, we have

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

Lemma : 2:3:2

5m

(or)

2m

(v)

Given a, b in the group G. Then the equations $a.x = b$ and $y.a = b$ have unique solution for x and y in G. In particular the two cancellation laws.

$a.u = a.w$ implies $u = w$

and $u.a = w.a$ implies $u = w$ hold in G.

Proof:

$$a \in G \Rightarrow \exists\ a^{-1} \in G \ni a^{-1} a = e = a a^{-1}$$

where e is the identity element

Now $a \cdot u = a \cdot w \Rightarrow a^{-1}(a \cdot u) = a^{-1}(a \cdot w)$

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

$\Rightarrow e \cdot u = e w$

$\Rightarrow u = w$

Also $u \cdot a = w \cdot a \Rightarrow (u \cdot a) a^{-1} = (w \cdot a) a^{-1}$

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

$\Rightarrow u \cdot (e) = w \cdot (e)$

$\Rightarrow u = w.$

---

1) Order of an element of a group :-

If G is a group and $a \in G$, the order of a is the least positive integer m such that

$a^m = e$ i.e $O(a) = m$.

* If no such positive integer exists we say that 'a' is of infinite order.

* In any group the identity element e is of order one.

Example :

1) Let us find the order of each element of the multiplicative group $\{1, -1, i, -i\}$

Since 1 is the identity element.

$$o(1) = 1$$

Now $(-1)^1 = -1$, $(-1)^2 = (-1)(-1) = 1$

$$\therefore \quad o(-1) = 2$$

Again $(i)^1$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

$$\therefore \quad o(i) = 4$$

$(-i)^1 = -i$, $(-i)^2 = (-i)(-i) = -1$

$(-i)^3 = (-i)(-i)(-i) = -i$

$(-i)^4 = 1 \Rightarrow o(-i) = 4$

Notes :

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

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

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

We have $a^2 = a \Rightarrow a.a = a$ [by left cancellation law].

$\Rightarrow a.a = a.e$

$\Rightarrow a = e$

3) Prove that if G is an abelean group, then for all $a, b \in G$ and all integers n, $(a.b)^n = a^n . b^n$.

Proof:

Case (i) :- If $n=0$

we have $(a.b)^0 = e$

$a^0 . b^0 = e.e = e$

$\therefore (a.b)^0 = a^0 . b^0$

case (ii) :- If , $n>0$

If $n=1$, then $(a.b)^1 = a.b = a^1 . b^1$.

Now suppose $n=k$, $(a.b)^k = a^k . b^k$

Then $(a.b)^{k+1} = (a.b)^k . (a.b)$

$= a^k (b^k . a) b$ [$\because$ G is abelian]

$= a^k (a . b^k) b$

$= (a^k . a)(b^k . b)$

$(a.b)^{k+1} = a^{k+1} . b^{k+1}$

Hence by mathematical induction for all $n>0$,

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

Case (iii) :- If $n<0$

Let $n=-m$, where m is +ve integer

Then $(ab)^n = (ab)^{-m} = [(ab)^m]^{-1} = [a^m . b^m]^{-1}$

$= [b^m . a^m]^{-1}$ [$\because$ G is abelian $(ab)^{-1} = b^{-1} a^{-1}$].

$= (a^m)^{-1} (b^m)^{-1}$

$= a^{-m} b^{-m} = a^n . b^n$

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

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

Proof:

Let a and b be any two elements of the group G.

Then $ab \in G$.

$\therefore (ab)^2 = e$

$\Rightarrow (ab)(ab) = e$

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

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

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

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

$\therefore$ from (1), we get $ba = ab$

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

$\therefore$ G is abelian.

---

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

Proof:

Let a & b be any element of G.

Then $ab \in G$

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

Since given that every element is its own inverse

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

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

$\Rightarrow ba = ab$

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

$\Rightarrow$ G is abelian.

---

6. Show that if a, b or any two elements of a group G, then $(ab)^2 = a^2b^2$ iff G is abelian.

Proof:

Suppose G is abelian.

Then $(ab)^2 = (ab)(ab)$

$= a(ba)b$ [$\because$ G is abelian $\Rightarrow ab = ba$]

$= a(ab)b$

$= (aa)(b.b)$

$= a^2b^2$

conversely,

Let a, b be any two elements of G.

Then $(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$ [by left cancellation law]

$\Rightarrow a(ba)b = a(ab)b$

$\Rightarrow (ba)b = (ab)b$ [by Right cancellation law].

$\Rightarrow ba = ab$

$\Rightarrow$ G is abelian.

---

7. If G is a group $\ni (ab)^m = a^m b^m$ for three consecutive integers m for all $a, b \in G$, show that G is abelian.

Proof:

Let a, b be any two elements of G suppose m, m+1, m+2, are three consecutive integers

$\exists\ (ab)^m = a^m b^m$

$(ab)^{m+1} = a^{m+1} b^{m+1}$

$(ab)^{m+2} = a^{m+2} b^{m+2}$

We have

$(ab)^{m+2} = (ab)^{m+1}(ab)$

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

$\Rightarrow a\, a^{m+1} b^{m+1} b = a\, a^m b^m b\, ab$

$\Rightarrow a^{m+1} b^{m+1} = a^m b^m ba$ [by using left & right cancellation laws]

$\Rightarrow (ab)^{m+1} = (ab)^m ba$

$\Rightarrow (ab)^m (ab) = (ab)^m ba$ [by left cancellation law]

$\Rightarrow ab = ba$

$\Rightarrow G$ is abelian.

Definition: (cyclic groups):-

A Group G is called cyclic, if ~~the~~ for some $a \in G$, 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.

Corollary:1

If G is a finite group and $a \in G$ then $O(a) / O(G)$

Proof:

If G is a finite Group.

Let $a \in G$, TO Sow $O(a) / O(G)$

Let $H = \{\ldots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3 \ldots\}$ be the Subset of G consisting of all integral powers of a.

Then we know that H is a Subgroup of G Now, we Shall Show that H contains only $O(a)$ distinct elements and that they are $a, a^2, a^3, \ldots a^{O(a)} = e$

Suppose that it have fewer number of elements, then $a^i = a^j$ for some integers $0 \leq i < j < O(a)$.

Then $a^{j-i} = e$

Thus there exists integer $j-i$ less than $O(a)$. Such that $a^{j-i} = e$.

But $O(a)$ is the least Positive integer $\exists\ a^{O(a)} = e$.

$a^i \neq a^j$

$\therefore a, a^2, a^3 \ldots a^{O(a)} = e$ are all distinct elements of H and $O(H) = O(a)$.

Thus the cyclic subgroup H generates by a has O(a) elements.

By using Lagrange's Theorem, $O(a) / O(G)$

Corollary : 2

If G is a finite group and $a \in G$, then $a^{O(G)} = e$.

Proof:

We know that for any $a \in G$, than $O(a) / O(G)$ [By corollary 1].

Thus $O(G) = m\ O(a)$

$\therefore a^{O(G)} = a^{m\ O(a)}$

$= (a^{O(a)})^m = e^m$

$a^{O(G)} = e.$

Note:

The Euler ϕ- function, $\phi(n)$ is defined for all integers n.

$\phi(1) = 1$

For $n > 1$. $\phi(n)$ = number of positive integers less than n and relatively prime to n.

For example,

$\phi(18) = 4$

Since 1, 3, 5, 7 are the numbers less than 8 which are relatively prime to e.

Corollary : 3 (Euler's theorem):

If n is a positive integer and 'a' is relatively prime to n, then $a^{\phi(n)} \equiv 1 \mod n$.

Proof:

For any integer x,

Let $[x]$ denote the residue class of the set of integers mod n.

Let $G = \{[a] : a$ is an integer relatively prime to $n\}$.

The residue classes of G is a group w.r.to multiplication and $O(G) = \phi(n)$.

The identity element of this group is the residue class $[1]$.

We have. $[a] \in G$

$\Rightarrow [a]^{O(G)} = [1]$ [Note that $[a][b] = [ab]$]

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

$\Rightarrow [a][a] \ldots\ldots [a]$ upto $\phi(n)$ times $= [1]$

$\Rightarrow [a.a. \ldots$ upto $\phi(n)$ times$] = [1]$

$\Rightarrow [a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} = 1 \pmod n$.

Corollary 4: (Fermat's theorem)

If p is a prime Number and 'a' is any integer, then $a^p = a \pmod p$.

Proof:

Let G be the set of non zero residue classes of integers module p.

If p is a prime Number, then w.r. to multiplication of residue classes G is a group of Order P-1.

Now suppose a is any Integer relatively prime to p, then by using Euler's theorem.

$$a^{P-1} \equiv 1 \bmod P$$

$\Rightarrow a^{P-1} - 1$ is divisible by p

$\Rightarrow a(a^{P-1} - 1)$ is divisible by p.

$\Rightarrow a^P - a$ is divisible by p.

$\Rightarrow a^P = a \bmod p$.

If on the other hand, 'a' is not relatively prime to p.

i.e p is a divisor of a.

We must have $p \mid a$, so that $a \equiv 0 \bmod p$.

Hence $0 \equiv a^P \equiv a \bmod p$.

Corollary: 5

If G is a finite group whose Then is a prime Number P, then G is cyclic Group.

Proof:

First we claim that G has no nontrivial subgroup H.

If G is a finite group whose Orde is a prime number P, (i.e) $O(G) = P$ and if the only divisors of P are 1 and P.

For O(H) must divide O(G) having only two possibilities.

namely $O(H) = 1$ (or) $O(H) = P$.

The first of these implies that $H = (e)$. and the second implies that $H = G$.

Suppose now that $a \neq e \in G$.

Let $H = (a)$ is a cyclic subgroup of G and $O(H) = O(a)$

By using Lagrange's theorem, [$\because a \neq e \Rightarrow O(a) \geq 2$ $\because H \neq e$]

$O(H)$ must be a divisor of P.

But p is prime and $O(H) \geq 2$

Hence $O(H) = P$.

$H = G$ This says that G is cyclic and that every element in G is a power of a.

Examples of

1. The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

We can write $G = \{i, i^2, i^3, i^4\}$

Thus G is a cyclic group and i is a generator.

Also we can write $G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$

Thus $-i$ is also a generator of G.

2. The multiplicative group $\{1, \omega, \omega^2\}$ is cyclic. The generators are ω and ω^2.

3. The group $G = (\{0, 1, 2, 3, 4, 5\}, +_6)$ is cyclic. This group is generated by 1. Another generated is 5.

We see that

$1 = 1$

$1^2 = 1 +_6 1 = 2$

$5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$1^3 = 1 +_6 1^2 = 3$ $\quad$ $5^3 = 5 +_6 5^2 = 3$

$1^4 = 1 +_6 1^3 = 4$ $\quad$ $5^4 = 5 +_6 5^3 = 2$

$1^5 = 1 +_6 1^4 = 5$ $\quad$ $5^5 = 5 +_6 5^4 = 1$

$1^6 = 1 +_6 1^5 = 0$ $\quad$ $5^6 = 5 +_6 5^5 = 0$

4. $G = \{1, -1\}$ it is a cyclic group with generator -1.

5. $(Z_8, \cdot_8)$ is a cyclic group whose generators are $\{1, 3, 5, 7\}$.

$[\because \phi(8) = 4]$

6. $(Z_n, +_n)$ is a cyclic group all $n \in Z$. The number of integers less than 'n' and relatively prime to n.

7. $(Z, +)$, $(2Z, +)$, $(nZ, +)$ are cyclic group.

8. A cyclic group can have more than one generator.

9. Every cyclic group is an abelian group.

10. A Subgroup of a cyclic group is cyclic.

11. If 'a' is a generator of G, then it is inverse a^{-1} is also a generator.