Centre for Distance and Online Education

Punjabi University, Patiala

Class : B.A. III (Mathematics) **Semester : 5**

Paper : I (Abstract Algebra) **Unit : I**

Medium : English

Lesson No.

Department website : www.pbidde.org

B.A. / B.Sc. (MATHEMATICS) Semester - V

PAPER-I: ABSTRACT ALGEBRA

Maximum Marks: 50 **Pass Percentage: 35%**
Maximum Time: 3 Hrs

INSTRUCTIONS FOR THE PAPER SETTER

The question paper will consist of three sections A, B and C. Sections A and 8 will have four questions each from the respective sections of the syllabus and Section C will consist of one compulsory question having eight short answer type questions covering the entire syllabus uniformly. Each question in sections A and B will be of 7.5 marks and Section C will be of 20 marks.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt five questions in all selecting two questions from each of the Section A and B and compulsory question of Section C.

Section-A

Groups: Definition, Examples, Subgroups, Counting principle, Lagrange's theorem, Normal subgroups, Quotient groups, Homomorphisms, Fundamental theorem of homomorphism and related theorems, Cyclic groups.

Section-B

Rings: Definition and examples of rings, Elementary properties of rings, Subrings, Homomorphism, Ideals and quotient rings, Field of quotient of integral domain, Division rings, Euclidean rings, Principal ideals, Examples.

RECOMMENDED BOOKS:

1. Textbook on Algebra and Theory of Equations by Chandrika Prasad, Pothishala Pvt. Ltd.
2. I. N. Hernstein : Topics in Algebra
3. Linear Algebra by Schaum Outline Series
4. Surjeet Singh and QaziZameeruddin :Moden Algebra (Relevant Portion)

B.A. PART–III **MATHEMATICS : PAPER I**
(SEMESTER - V) **ABSTRACT ALGEBRA**

LESSON NO. 1.1 **AUTHOR : DR. CHANCHAL**

Last updated on May, 2023

GROUPS – I

1.1.1 Objectives: During study in this lesson, the students would be able to understand the concept of groups and its various properties. Various theorems and results concerning groups will be discussed with proofs accordingly.

1.1.2 Introduction to Groups :

A non empty set G, together with a binary composition * is said to form a group, if it satisfies the following postulates

(i) Associativity: $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$

(ii) Existence of Identity: $\exists$ an element $e \in G$, such that $a * e = e * a = a$ for all $a \in G$, where e is called identity element of G.

(iii) Existence of Inverse: For every $a \in G$, $\exists\, a' \in G$ (depending upon a) such that $a * a' = a' * a = e$. Here, a' is called inverse of a

Remarks : (i) Since * is a binary composition on G, therefore for all $a, b \in G$, $a * b$ is a unique member of G. This property is called closure property.

(ii) If, in addition to the above postulates, G also satisfies the commutative law i.e. $a * b = b * a$ for all $a, b \in G$, then G is called an abelian group or a commutative group.

(iii) We will use the symbol 'e' for identity of a group and 'a^{-1}' for the inverse of an element 'a' of the group. Further, instead of denoting the composition as 'a * b' we will simply write 'ab' (which does not mean multiplication of 'a' and 'b'.)

(iv) If the set G is finite (i.e., has finite number of elements) it is called a finite group otherwise it is called an infinite group.

(v) **Order of a group :** It is defined as the number of elements in the finite group. It is denoted by o(G) or $|G|$.

1.1.3 Examples

Example 1 : The set Z of integers forms an abelian group w.r.t the usual addition of integers.

It is easy to verify the postualtes in the definition of a group as sum of two integers is a unique integer (thus closure holds). Associativity of addition is known to us. 0 (zero) will be identity and negatives will be the respective inverse elements. Commutativity again being obvious.

Example 2 : Similarly, sets Q of rationals, R of real numbers would also form abelian groups w.r.t. addition.

Example 3 : Set of integers, w.r.t. usual multiplication does not form a group, although closure, associativity, identity conditions hold.

Note : 2 has no inverse w.r.t. multiplication as there does not exist any integer a s.t., 2. a = a.2 = 1.

Example 4 : The set G of all +ve irrational numbers together with 1 under multiplication does not form a group as closure does not hold, because $\sqrt{3}\,.\,\sqrt{3} = 3 \notin G$, however other conditions in the definition of a group are satisfied here.

Example 5 : Let G be the set {1, –1}. Then it forms an abelian group under multiplication. It is again easy to check the properties.

I would be identity and each element is its own inverse.

Example 6 : Set of all 2 × 2 matrices over integers under matrix addition would be another example of an abelian group.

Example 7 : Set of all non zero complex numbers forms a group under multiplication defined by

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

Here, 1 = 1 + i.0 will be identity,

and $\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ will be inverse of a + ib.

Note : a + ib is non-zero means that both a & b are not zero. Thus $a^2 + b^2 \neq 0$.

Example 8 : The set G of all nth roots of unity, where n is a fixed positive integer forms an abelian group under usual multiplication of complex numbers.

We know that complex number z is an nth root of unity if $z^n = 1$ and there exist exactly n distinct roots of unity.

In fact the roots are given by $e^{2\pi ir/n}$

where r = 1, 2, ..., n and $e^{ix} = \cos x + i \sin x$.

If $a, b \in G$ be any two members, then $a^n = 1$, $b^n = 1$ thus $(ab)^n = a^n b^n = 1$.

$\Rightarrow$ ab is an nth root of unity

$\Rightarrow$ $ab \in G \Rightarrow$ closure holds.

Associativity of multiplication is true in complex numbers.

Again, since 1.a = a . 1 = a, 1 will be identity.

Also for any $a \in G, \frac{1}{a}$ will be its inverse as $\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = 1$.

So, inverse of $e^{2\pi ir/n}$ is $e^{2\pi i(n-r)/n}$ and identity is $e^{2\pi i0/n} = 1$

Commutativity is obvious. Therefore, G is an abelian group.

In particular if n = 3, then G = $\{1, \omega, \omega^2\}$

In order to prove it an abelian group, we use the concept of composition table. We form the composition table using $\omega^3 = 1$ as given below :

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

(i) Closure Property : Since all the elements in composition table are elements of G, so G is closed under multiplication.

(ii) Associalivity : Since the elements of G are complex numbers and multiplication of complex numbers is associative, so multiplication is associative in G.

(iii) Existence of identity : Since 2nd row is same as the first row, ∴ 1 is left identity, Also 2nd column is same as the first column, ∴ 1 is the right identity. So 1 is the identity of G.

(iv) Existence of inverse : Here each row (column) of the composition table contains identity element 1 once and only once. So the element left to 1 is the left inverse of the element above 1. Similarly the element above 1 is the right inverse of element left to 1.

Thus we see that

$$1.1 = 1 = 1.1 \text{ so } 1^{-1} = 1.$$

Also $\omega . \omega^2 = 1 = \omega^2.\omega$, so $\omega^{-1} = \omega^2$ and $(\omega^2)^{-1} = \omega$.

(v) Abelian : Since the entries in the composition table are symmetrical about the principal diagonal.

Hence G is an abelian group under multiplication.

Example 9 : (i) Let G = {± 1, ± i, ± j, ± k}. Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1, ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

then G forms a group. G is not abelian as ij ≠ ji.

This is called the **Quaternion Group**.

(ii) If set G consists of the eight matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \text{where } i = \sqrt{-1}$$

then G forms a non abelian group under matrix multiplication. (Compare with part (i)).

Example 10 : Let G = {(a, b) | a, b rationals, a ≠ 0}. Define * on G by

$$(a, b) * (c, d) = (ac, ad + b)$$

Closure follows as a, c ≠ 0 ⇒ ac ≠ 0

$$\begin{aligned} [(a, b) * (c, d)] * (e, f) &= (ac, ad + b) * (e, f) \\ &= (ace, acf + ad + b) \\ (a, b) * [(c, d) * (e, f)] &= (a, b) * (ce, cf + d) \\ &= (ace, acf + ad + b) \end{aligned}$$

proves associativity.

(1, 0) will be identity and (1/a, –b/a) will be inverse of any element (a, b).

G is not abelian as

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$

$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

1.1.4 Elementary Properties of a Group

Lemma : In a group G,

(1) Identity element is unique.

(2) Inverse of each $a \in G$ is unique.

(3) $(a^{-1})^{-1} = a$, for all $a \in G$, where a^{-1} stands for inverse of a.

(4) $(ab)^{-1} = b^{-1} a^{-1}$ for all $a, b \in G$ (Reversal Law)

(5) $ab = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$ for all $a, b, c \in G$

(called the cancellation laws).

Proof : (1) Suppose e and e' are two elements of G which act as identity.

Then, since $e \in G$ and e' is identity,

$$e'e = ee' = e \qquad .... (1)$$

and as $e' \in G$ and e is identity

$$e'e = ee' = e' \qquad ..... (2)$$

(1) and (2) $\Rightarrow e = e'$

which proves the uniqueness of identity in a group.

(2) Let $a \in G$ be any element and let a' and a" be two inverse elements of a, then

$$aa' = a'a = e$$

$$aa'' = a''a = e$$

Now $a' = a'e = a'(aa'') = (a'a)\, a'' = ea'' = a''$.

Hence, inverse of an element is unique. (By associativity)

(3) Since a^{-1} is inverse of a

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

which also implies a is inverse of a^{-1}

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

(4) We have to prove that inverse of $b^{-1} a^{-1}$ for which we show

$$(ab)\,(b^{-1} a^{-1}) = (b^{-1} a^{-1})\,(ab) = e.$$

Now
$$\begin{aligned}(ab)\,(b^{-1} a^{-1}) &= [(ab)\, b^{-1}]\, a^{-1} \\ &= [(a(bb^{-1})]\, a^{-1} \quad \text{(By associativity)} \\ &= (ae)\, a^{-1} = aa^{-1} = e\end{aligned}$$

Similarly $(b^{-1} a^{-1})\,(ab) = e$

and thus the result follows.

(5) Let $ab = ac$, then

$$\begin{aligned}b &= eb = (a^{-1} a)\, b \\ &= a^{-1}(ab) = a^{-1}(ac) \\ &= (a^{-1} a)\, c = ec = c\end{aligned}$$

Thus $ab = ac \Rightarrow b = c$

which is called the left cancellation law.

Similarly, one can prove the right cancellation law.

Example 11 : Let X = {1, 2, 3} and let S_3 = A(X) be the group of all permutations on X. Consider f, g, h ∈ A(X), defined by

$f(1) = 2$, $f(2) = 3$, $f(3) = 1$

$g(1) = 2$, $g(2) = 1$, $g(3) = 3$

$h(1) = 3$, $h(2) = 1$, $h(3) = 2$

Then, it is easy then to verify that fog = goh

But $f \neq h$.

(b) If we consider the group in example 10, we find

$$(1, 2) * (3, 4) = (3, 6) = (3, 0) * (1, 2)$$

But $(3, 4) \neq (3, 0)$

Hence we notice, cross cancellations may not hold in a group.

Theorem 1 : For elements a, b in a group G the equations ax = b and ya = b have unique solutions for x and y in G.

Proof : Now ax = b

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

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

or $x = a^{-1}b$

which is the required solution of the equation ax = b.

Suppose $x = x_1$ and $x = x_2$ are two solutions of this equation, then

$ax_1 = b$ and $ax_2 = b$

$\Rightarrow$ $ax_1 = ax_2$

$\Rightarrow$ $x_1 = x_2$ by left cancellation

Showing that the solution is unique.

Similarly $y = ba^{-1}$ will be unique solution of the equation ya = b.

Theorem 2 : A non empty set G together with a binary compositioon '.' is a group if and only if

(1) a(bc) = (ab)c for all a, b, c ∈ G

(2) For any a, b ∈ G, the equations ax = b and ya = b have solutions in G.

Proof : If G is a group, then (1) and (2) follow by definition and previous theorem. Conversely, let (1) and (2) hold. To show G is a group, we need to prove existence of identity and inverse (for each element).

Let a ∈ G be any element.

By (2), the equation ax = a

ya = a

have solutions in G.

Let x = e and y = f be the solutions.

Thus $\exists\, e, f \in G$, s.t., $ae = a$

$fa = a$

Let now $b \in G$ be any element then again by (2) $\exists$ some x, y in G s.t.,

$ax = b$

$ya = b.$

Now $ax = b \Rightarrow f. (a. x) = f . b$

$\Rightarrow (f . a) . x = f . b$

$\Rightarrow a . x = f . b$

$\Rightarrow b = f . b$

Again $y.a = b \Rightarrow (y . a) . e = b. e$

$\Rightarrow y . (a . e) = b . e$

$\Rightarrow y . a = be$

$\Rightarrow b = be$

thus we have $b = fb$ ... (i)

$b = be$ ... (ii)

for any $b \in G$

Putting $b = e$ in (i) and $b = f$ in (ii) we get

$e = fe$

$f = fe$

$\Rightarrow$ $e = f.$

Hence $ae = a = fa = ea$

i.e., $\exists\, e \in G$, s.t., $ae = ea = a$

$\Rightarrow$ e is identity.

Again, for any $a \in G$, and (the identity) $e \in G$, the equations $ax = e$ and $ya = e$ have solutions.

Let the solutions be $x = a_1$, and $y = a_2$

then $aa_1 = e$, $a_2a = e$

Now $a_1 = ea_1 = (a_2a)\, a_1 = a_2\, (aa_1) = a_2e = a_2.$

Hence $aa_1 = e = a_1a$ for any $a \in G$

i.e., for any $a \in G$, $\exists$ some $a_1 \in G$ satisfying the above relations $\Rightarrow$ a has an inverse. Thus each element has inverse and, by definition, G forms a group.

1.1.5 Semi-Groups and Monoids

Definition : A non empty set G together with a binary composition '.' is called a semi-group if

$$a . (b . c) = (a . b) . c \text{ for all } a, b, c \in G$$

Obviously, every group is a semi-group. But the converse is not true follows by considering the set N of natural numbers under addition.

Remark : Cancellation law may not hold in a semi-group.

Consider M, the set of all 2 × 2 matrices over integers under matrix multiplication, which forms a semi-group.

If we take $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$

then clearly $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

But $B \neq C$.

Set of natural numbers under addition is an example of a semi-group in which cancellation laws hold.

Theorem 3 : A finite semi-group in which cancellation laws hold is a group.

Proof : Let G = $\{a_1, a_2, ..., a_n\}$ be a finite semi-group in which cancellation laws hold.

Let $a \in G$ be any element, then by closure property

$aa_1, aa_2, ..., aa_n$

are all in G.

Suppose any two of these elements are equal

say, $aa_i = aa_j$ for some $i \neq j$

then $a_i = a_j$ by cancellation

But $a_i \neq a_j$ as $i \neq j$

Hence no two of $aa_1, aa_2, ..., aa_n$ can be equal.

These being n in number, will be distinct members of G (Note of (G) = n).

Thus if $b \in G$ be any element then

$b = aa_i$ for some i

i.e., for $a, b \in G$ the equation $ax = b$ has a solution $(x = a_i)$ in G.

Similarly, the equation $ya = b$ will have a solution in G.

G being a semi-group, associativity holds in G.

Hence G is a group (by theorem 2).

Theorem 4 : A finite semi-group is a group if and only if it satisfies cancellation laws.

Proof : Follows by previous theorem.

Definition (Monoid) : A non empty set G together with a binary composition '.' is said to form a monoid if

(i) $a(bc) = (ab)c \ \forall\ a, b, c \in G$

(ii) $\exists$ an element $e \in G$ s. t., $ae = ea = a \ \forall\ a \in G$

e is then called identity of G. It is easy to see that e is unique.

So all groups are monoids and all monoids are semi-groups.

Notation : Let G be a group with binary composition '.'. If $a \in G$ be any element then by closure property $a . a \in G$. Similarly $(a . a) . a \in G$ and so on.

It would be very convenient to denote a . a by a^2 and a . (a . a) or (a . a) . a by a^3 and so on. Again $a^{-1}.a^{-1}$ would be denoted by a^{-2}. And since $a.a^{-1} = e$, it would not be wrong to denote $e = a^0$. It is now a simple matter to understand that

$$a^m . a^n = a^{m+n}, (a^m)^n = a^{mn}$$

where m, n are integers.

In case the binary composition of the group is denoted by +, we will talk of sums and multiples in place of products and powers. Thus here $2a = a + a$, and $na = a + a + \ldots + a$ (n times), if n is +ve integer. In case n is –ve integer then $n = -m$, where m is +ve and we define $na = -ma = (-a) + (-a) + \ldots + (-a)$ m times.

1.1.6 Problems

Problem 1 : If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \leq r \leq n$, s.t., $a^r = e$.

Solution : Since $o(g) = n$, G has n elements.

Let $a \in G$ be any elements. By closure property $a^2, a^3, \ldots$.all belong to G.

Consider $e, a, a^2, \ldots..a^n$

These are n + 1 elements (all in G). But G contains only n elements.

$\Rightarrow$ at least two of these elemnts are equal. If any of $a, a^2, \ldots..,a^n$ eqyaks e, out result is proved. If not then $a^i = a^j$ for some i, i, $1 \leq i, j \leq n$. Without any loss of generality, we can take $i > j$

then $a^i = a^j$

$\Rightarrow a^i. a^{-j} = a^j. a^{-j}$

$\Rightarrow a^{i-j} = e$ where $1 \leq i - j \leq n$.

Problem 2 : Show that a finite semi-group in which cross cancellation holds is an abelian group.

Solution : Let G be the given finite semi-group. Let $a, b \in G$ be any elements, Since G is a semi-group, by associativity

$a(ba) = (ab)a$

By cross cancellation then $ba = ab \Rightarrow$ G is abelian.

Since G is abelian, cross cancellation laws become the cancellation laws. Hence G is a finite semi-group in which cancellation laws hold.

thus G is a group.

Problem 3 : If G is a group in which $(ab)^i = a^ib^i$ forthree consecutive integers i and any a, b and G, then show htat G is abelian.

Solution : Let n, n + 1, n + 2 be three consecutive integers for which the given condition holds. Then for any a, b $\in$ G,

$(ab)^n = a^n b^n$ ..(1)

$(ab)^{n+1} = a^{n+1} b^{n+1}$ ...(2)

$(ab)^{n+2} = a^{n+2} b^{n+2}$ ...(3)

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

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

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

$\Rightarrow ba^{n+1} = a^{n+1} b$ (using cancellation) ...(4)

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

gives $(ab)(ab)^n + a^{n+1} b^{n+1}$

i.e., $(ab)(a^n b^n) = a^{n+1} b^{n+1}$

$\Rightarrow ba^n = a^n b$

$\Rightarrow ba^{n+1} = a^n ba$

$\Rightarrow a^{n+1} b = a^n ba$ (4)

$\Rightarrow ab = ba.$

Hence G is abelian.

Problem 4 : Let G be a semi-group, Suppose $\exists$ e $\in$ G, s.t., ae = a for all a $\in$ G and for each a $\in$ G, $\exists$ a' $\in$ G, s.t., aa' = e. Show that G is a group.

Solution : We first show that G satisfies the right cancellation law.

Let ac = bc

As given $\exists$ c' $\in$ G, s.t., cc' = e

(ac)c' = (bc)c'

$\Rightarrow$ a(cc') = b(cc')

$\Rightarrow$ ae = be $\Rightarrow$ a = b.

We now show that e is left identity

Consider, (ea)a' = e(aa') = e, e = e

Also aa' = e

$\therefore$ e is also left identify of G.

Again (a'a)a' = a'(aa') = a'e = a'

and ea' = a'

$\Rightarrow$ (a'a)a' = ea'

$\Rightarrow$ a'a = e by right cancellation law

$\Rightarrow$ a' is also left inverse of a

so, G is a group.

Problem 5 : If in a semi-group S. $x^2y = y = yx^2$ $\forall$x, y. Then show that S is abelian.

Solution : $x^2y = y \Rightarrow x^2y^2 = y^2$

$yx^2 = y \quad \forall x, y \in S$

$\Rightarrow xy^2 = x \quad \forall x, y \in S$

$\Rightarrow x^2y^2 = x^2$

So $x^2 = y^2 \quad \forall x, y \in S$

Now $x^2y = y \Rightarrow y^2y = y \Rightarrow y^3 = y \quad \forall y \in S$

Also $yx^2y = y^2$ (i)

Now $xy^2 = x \Rightarrow xy^2x = x^2$ (ii)

By (i) and (ii), $xy^2x = yx^2y$

Since $y = y^3 \quad \forall y \in S$, we get

$xy = (xy)^3 = xy\,xy\,xy$

$= xy\,xy\,x^3y = x(yx)^2x(xy)$

$= (yx)x^2(yx)\,(xy)$

$= yx^3\,yx^2y = yxy\,x^2y$

$= (yx)xy^2x$

$= y(y^2x)$ (as $y = yx^2$)

$= y^3x$

$= yx$ (as $y^3 = y$)

Thus $xy = yx \ \forall\ x, y \in S$

Hence S is abelian.

Problem 6 : Show that if G is a group then $a \in G$ is an idempotent if and onlyif $a = e$, the identity of G.

Solution : Given G is a group.

Let $a \in G$ is an idempotent element

$\Rightarrow \quad a^2 = a$

$\Rightarrow \quad aa = ae$

$\Rightarrow \quad a = e.$ [Using left cancellation law]

Conversely let $a = e$, the identity of G

$\therefore \quad aa = ae$

$= ee = e = a$ $[\because a = e]$

$\Rightarrow \quad a^2 = a$

$\Rightarrow$ a is an idempotent element.

1.1.7 Summary : In this lesson, we have studied that how a group is formed? The concept is made elaborative using simple examples. Moreover, elementary properties of groups and various results concerning it have been discussed alongwith their proofs.

1.1.8 Key Concepts : Group, Order, Semi-group, Monoid, Identity element, Inverse element, Abelian group, Quarternion group

1.1.9 Long Questions :

1. Let G be the set {± e, ± a, ± b, ± c} where

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, c = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Show that G forms a group under matrix multiplication.

2. Show that a group G is abelian iff $(ab)^2 = a^2b^2$.

3. Prove that a group in which every element is its own inverse is abelian.

4. Show that a monoid is a group if and only if cancellation laws hold in it.

5. Show that a finite semi-group G with identity is a group iff G contains only one idempotent.

1.1.10 Short Questions :

1. Check whether the following systems form a group or not

(a) G = set of rational numbers under composition * defined by

$$a * b = \frac{ab}{2},\ a, b \in G$$

(b) Set of all 2 × 2 matrices over integers under matrix multiplication.

(c) Set of all matrices of the form $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \theta \in R$, under matrix multiplication.

(d) Q = set of all rational numbers under * where a * b = a + b – ab.

(e) G = {(a,b) | a, b ∈ Z} under * defined by
(a, b) * (c, d) = (ac + bd, ad +bc).

2. Define Semi-group and monoid with suitable example of each.

3. Define order of a group.

1.1.11 Suggested Readings :

I. N. Herstein : Topics in Algebra

2. P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul : Basic Abstract Algebra, Cambridge University Press, Second Edition

B.A. PART–III **MATHEMATICS : PAPER I**
(SEMESTER - V) **ABSTRACT ALGEBRA**

LESSON NO. 1.2 **AUTHOR : DR. CHANCHAL**

Last updated on May, 2023

GROUPS – II

1.2.1 Objectives :

For this lesson, our main objectives are :

- To study about subgroups and its properties
- To understand the concept of centre of a group
- To get knowledge of cosets

1.2.2 Introduction to Subgroups

We have seen that R, the set of real numbers, forms a group under addition, and Z, the set of integers, also forms a group under addition. Also Z is a subset of R. Now, we define a subgroup as :-

Definition

A non empty subset H of a group G is said to be a subgroup of G, if H forms a group under the binary composition of G.

Obviously, if H is a subgroup of G and K is a subgroup of H, then K is subgroup of G. If G is a group with identity element e then the subsets {e} and G are the trivial subgroups of G. All other subgroups will be called non-trivial (or proper subgroups).

Thus it is easy to see that the even integers form a subgroup of (z, +), which is : subgroup of (Q, +) which is a subgroup of (R, +).

Again the subset {1, –1) will be a subgroup of G = {1, –1, i, –i) under multiplication. Notice that Z_5 = {0, 1, 2, 3, 4} mod 5 is not a subgroup of Z under addition as addition modulo 5 is not the composition of Z. Similarly, Z_5 is not subgroup of Z_6 etc.

We sometimes use the notation $H \leq G$ to signify that H is a subgroup of G and $H < G$ to mean that H is a proper subgroup of G.

1.2.3. Properties of Subgroups

I. The identity element of a subgroup is same as the identity elements of the group.

Proof. Let H be a subgroup of a group G.

Let e and e' be the identity elements of G and H respectively

Let $a \in H$ be any element

$\therefore$ a e' = a [$\because$ e' is the identity of H]

Also $\because$ $a \in H$ and $H \subseteq G \Rightarrow a \in G$

$\therefore$ a e = a [$\because$ e is the identity of G]

$\therefore$ we have a e = a e'

$\Rightarrow$ e = e' [by left cancellation law]

Hence the identity of a group and that of a subgroup is the same.

II. The inverse of any element of a subgroup is the same as the inverse of the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ be any element.

Since $H \subseteq G$ $\therefore a \in G$.

Let b be the inverse of a in H and c be the inverse of a in G.

$\therefore$ b a = e and c a = e

$\Rightarrow$ ba = c a

$\Rightarrow$ b = c [by right cancellation law]

Hence the inverse of any element of a subgroup is same as the inverse of the same element regarded as an element of the group.

III. The order of any element in a subgroup is the same as the order the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ such that o(a) = n

$\Rightarrow a^n = e$ and $a^m \neq e$ for every m < n.

Also $a \in H$ $\Rightarrow a \in G$ and so $a^n = e \in G \Rightarrow o(a) = n$ in G.

Hence order of any element in a subgroup is same as the order of element regarded as the element of the group.

IV. Subgroup of an abelian group is abelian.

Proof. Let H be a subgroup of an abelian group G

$\therefore H \subseteq G$.

Let a, b $\in$ H be any two elements

$\therefore$ a, b $\in$ G $\Rightarrow$ a b = b a [$\because$ G is abelian]

$\therefore$ $\forall$a, b $\in$ H we have a b = b a

Hence H is an abelien subgroup of G.

The converse of above result is false

i.e., A subgroup may be abelian even if G is not abelian.

For example : (i) The sets {1, –1} and {1, –1, i, – i} are abelian subgroups of the non-abelian group of Quaternions Q_8 under multiplication.

Theroem 1 : A non empty subset H of a group G is a subgroup of G iff

(i) a, b $\in$ H $\Rightarrow$ ab $\in$ H

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

Proof: Let H be a subgroup of G then by definition it follows that (i) and (ii) hold.

Conversely, let the given conditions hold in H.

Closure holds in H by (i).

Again a, b, c $\in$ H $\Rightarrow$ a, b, c $\in$ G $\Rightarrow$ a(bc) = (ab)c

Hence associativity holds in H.

Also for any a $\in$ H, a^{-1} $\in$ H and so by (i)

aa–1 $\in$ H $\Rightarrow$ e $\in$ H

thus H has identity.

Inverse of each element of H is in H by (ii).

Hence H satisfies all conditions in the definition of a group and thus it forms a group and therefore a subgroup of G.

Theorem 2 : A non void subset H of a group G is a subgroup of G iff a, b $\in$ H $\Rightarrow$ ab^{-1} $\in$ H .

Proof : If H is a subgroup of G then, a, b $\in$ H $\Rightarrow$ ab^{-1} $\in$ H (follows easily by using definition).

Conversely, let the given condition hold in H.

That associativity holds in H follows as in previous theorem.

Let a $\in$H be any element (H $\neq$ φ)

then a, a $\in$ H $\Rightarrow$ aa^{-1} $\in$ H $\Rightarrow$ e $\in$ H.

So H has identity.

Again, for any a $\in$ H, as e $\in$ H

ea^{-1} $\in$ H $\Rightarrow$ a^{-1} $\in$ H

i.e., H has inverse of each element.

Finally, for any a, b $\in$ H ,

a, b^{-1} $\in$ H

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

i.e., H is closed under multiplication.

Hence, H from a group and therefore a subgroup of G.

Remark : If the binary composition of the group is dehated by '+', the above condition can be stated as : $a, b \in H \Rightarrow a - b \in H$. Note that, the identity e is always in H.

Problem 1 : Show that the sets H = {0, 3} and K = {0, 2, 4} are subgroups of the group G = {0, 1, 2, 3 , 4, 5} under the operation addition modulo 6.

Sol. Clearly, H and K are non-empty subsets of G. The composition table for H and K are given below:

Composition table for H

$+_6$	0	3
0	0	3
3	3	0

Composition table for K

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

From the composition table, it is easy to see that H and K form groups and hence are subgroups of G.

1.2.4 Centre of a Group

Theorem 3 : Centre of a group G is a subgroup of G.

Proof : Let Z(G) be the centre of the group G.

Then $Z(G) \neq \varphi$ as $e \in Z(G)$

Again, $x, y \in Z(G) \Rightarrow xg = gx$

$yg = gy$ for all $g \in G$

$\Rightarrow g^{-1} x^{-1} = x^{-1} g^{-1}$

$g^{-1} y^{-1} = y^{-1} g^{-1}$ for all $g \in G$

Now $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1}$

$= (xy)y^{-1} (g^{-1}g)$

$= xg(y^{-1} g^{-1})g = xg (g^{-1} y^{-1})g$

$= x(gg^{-1}) y^{-1} g$

$= (xy^{-1})g$ for all $g \in G$

$\Rightarrow xy^{-1} \in Z(G)$

Hence Z(G) is a subgroup.

Remark : obviously, G is abelian iff Z(G) = G.

Definition : Let G be a group, $a \in G$ be any element. The subset $N(A) = \{x \in G / xa = ax\}$ is called normalizer or centralizer of a in G.

Problem 2 : Find centre of S_3.

Solution : We have $S_3 = \{I, (1), (13), (23), (123), (132)\}$

Centre of S_3, $Z(S_3) = \{\sigma \in S_3 \mid \sigma\,\theta = \theta\sigma \text{ for all } \theta \in S_3\}$

Since $(12)(13) = (132)$

$(13)(12) = (123)$

We find (12), (13) do not commute.

$\Rightarrow$ (12) & (13) do not belong to $Z(S_3)$

Again, $(23)(132) = (12)$

$(13)(12) = (123)$

$\Rightarrow$ (23), (132) do not belong to $Z(S_3)$

Also, $(123)(12) = (13)$

$(132)(23) = (13)$

Shows $(123) \notin Z(S_3)$

Hence $Z(S_3)$ contains only l.

Problem 3 : Let G be the group of all 2 × 2 non singular matrices over the reals. Find centre of G.

Solution : If $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any element of the centre Z(G) of G then it should commute with all members of G, In particular we should have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\Rightarrow b = c, a = d$

Also $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ gives

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$\Rightarrow a + b = a, b = c = 0$

Hence any member $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of Z(G) turns out to be of the type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

In other words, members of the centre Z(G) are the 2 × 2 scalar matrices of G.

Problem 4 : Show that $N(x–1\ ax) = x^{-1} N(a)x$ for all $a, x \in G$.

Solution: Let $y \in N(x^{-1}\ ax)$

then $(x^{-1}\ ax)y = y(x^{-1}\ ax)$

$\Rightarrow y^{-1}\ x^{-1}\ axy = x^{-1}\ ax$

$\Rightarrow xy^{-1}\ x^{-1}\ a = axy^{-1}\ x^{-1}$

$\Rightarrow xy^{-1}\ x^{-1} \in N(a)$

$\Rightarrow xy^{-1}\ x^{-1} = b \in N(a)$

$y^{-1} = x^{-1}\ bx$

$\Rightarrow y = x^{-1}\ b^{-1}\ x,\ b^{-1} \in N(a)$ as $b \in N\ (a)$

$\Rightarrow y \in x^{-1}\ N(a)\ x$

$\therefore$ $N(x^{-1}\ ax) \subseteq x^{-1}\ N(a)\ x$

Let $z \in x^{-1}\ N(a)x \Rightarrow z = x^{-1}\ cx,\ c \in N(a)$

$\therefore$ $z(x^{-1}\ ax) = (x^{-1}\ cx)\ (x^{-1}\ ax)$

$= x^{-1} cax$

$= x^{-1} acx$ as $c \in N(a)$

$= (x^{-1} ax)(x^{-1} cx)$

$= (x^{-1} ax)z$

$\Rightarrow z \in N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x \subseteq N(x^{-1} ax)$

$\Rightarrow x^{-1} N(a)x = N(x^{-1} ax)$ for all $a, x \in G$.

It would be an easy exercise to show that intersection of two subgroups will be a subgroup.

In fact, one can prove that if $\{H_i \mid i \in I\}$ be any set of subgroups of group G then

$\bigcap_{i \in I} H_i$ will be a subgroup of G.

Problem 5 : Show that union of two subgroups may not be a subgroup.

Solution : Let $H_2 = \{2n \mid n \in Z\}$

$H_3 = \{3n \mid n \in Z\}$

where (Z, +) is the group of integers. H_2 and H_3 will be subgroups of Z and

$2n - 2m = 2(n - m) \in H_2$

Now, $H_2 \cup H_3$ is not a subgroup as $2, 3 \in H_2 \cup H_3$

But $2 - 3 = -1 \notin H_2 \cup H_3$

Can union of two subgroups be a subgroup ? For this, we prove the following theorems.

Therorem 4 : Union of two subgroups is a subgroup iff one of them is contained in the other.

Proof : Let H, K be two subgroups of a group G and suppose $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

Conversely, let H, K be two subgroups of G s.t., $H \cup K$ is also a subgroup of G. We show one of them must be contained in the other. Suppose it is not true, i.e.,

$H \not\subseteq K, K \not\subseteq H$

Then $\exists\, x \in H$ s.t., $x \notin K$

$\exists\, x \in H$ s.t., $y \notin H$

Also then $x, y \in H \cup K$ and since $H \cup K$ is a subgroup, $xy \in H \cup K$

$\Rightarrow xy \in H$ or $xy \in K$

Ir $xy \in H$, then as $x \in H$, $x^{-1}(xy) \in H \Rightarrow y \in H$, which is not true.

Again, if $xy \in K$, then as $y \in K$, $(xy)y^{-1} \in K \Rightarrow x \in K$ which is not true.

i.e., either way we land up with a contradiction.

Hence our supposition that $H \not\subseteq K$ and $K \not\subseteq H$ is wrong.

Thus one of the two is contained in the other.

1.2.5. Cosets

Definition : Let H be a subgroup of a group G. For a, b $\in$ G, we say a is congruent to be mod H if $ab^{-1} \in H$.

In notational form, we write $a \equiv b \bmod H$.

It is easy to prove that this relation is an equivalence relation. Corresponding to this equivalence relation, we get equivalence classes. For any a $\in$ G, the equivalence class of 'a' will be given by

$cl(a) = \{x \in G \mid x \equiv a \bmod H\}$.

Definition (Coset) : Let H be a subgroup of G and let a $\in$ G be any element. Then $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

We show in the following theorem that any right coset of H in G is an equivalence class.

Theorem 5 : $Ha = \{x \in G \mid x \equiv a \bmod H\} = cl(a)$ for any a $\in$ G.

Proof : Let $x \in Ha$

Then $x = ha$ for some $h \in H$

$\Rightarrow xa^{-1} \in h$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow x \equiv a \bmod H$

$\Rightarrow x \in cl(a)$

thus $Ha \subseteq cl(a)$.

A gain let $x \in cl(a)$ be any element.

Then $x \equiv a \bmod H$

$\Rightarrow xa^{-1} \in H$

$\Rightarrow xa^{-1} = h$ for some $h \in H$

$\Rightarrow x = ha \in Ha$

thus $cl(a) \subseteq Ha$

and hence $Ha = cl(a)$

Since right cosets are equivalence classes, therefore we are free to use the results that we know about equivalence classes. We can, therefore state that any two right cosets are either equal or have no element in common and also that union of all the right cosets of H is G will be equal to G.

Remark : Note that a coset is not essentialy a subgroup. If G be the Quaternion group, then $H = \{1, -1\}$ is a subgroup of G. Take a = i, then $Ha = \{i, -i\}$ which is not a subgroup of G (it doesn't contain identity).

Lemma : There is always a 1 – 1 onto mapping between any two night cosets of H in G.

Proof : Let Ha, Hb be any two right cosets of H in G.

Define a mapping $f : Ha \to Hb$, s.t.,

$f(ha) = hb$

Then $h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$

$\Rightarrow f(h_1a) = f(h_2a)$

i.e., f is well defined.

$f(h_1a) = f(h_2a) \Rightarrow h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$

Showing f is 1 – 1.

That f is onto, is easily seen, as for any $hb \in Hb$, ha would be its pre image.

The immediate utility of this lemma is seen, if the group G happens to be finite, because in that case the lemma asserts that any two right cosets of H in G have the same number of elements. Since H = He is also a right coset of H in G, this lead us to state that all right cosets of H in G have the same number of elements as are in H(G, being, of course, finite). We are now ready to prove the following result.

Theorem 6 (Lagrange's) : If G is a finite group and H is a subgroup of G, then o(H) divides o(G).

Proof : Let o(G) = n.

Since corresponding to each element in G, we can define a right coset of H in G, the number of distinct right cosets of H in G is less than or equal to n.

Using the properties of equivalence classes we know

$$G = Ho_1 \cup Ha_2 \cup \ldots\ldots \cup Ha_1$$

where t = no. of distinct right cosets of H in G.

$$\Rightarrow o(G) = o(Ha_1) + o(Ha_2) + \ldots. + o(Ha_1)$$

(reminding ourselves that two right cosets are either equal or have no element in common

$$\Rightarrow o(G) = o(H) + o(Ha) \underset{\text{t times}}{+\ldots\ldots\ldots} + o(H) \text{ using the above lemma}$$

$\Rightarrow o(G) = t.\ o(H)$

or that $o(H) \mid o(G)$

Converse of Lagrange's theorem does not hold.

Remarks : (i) If G is a group of prime order, it will have only two subgroups G and {e}.

(ii) A subset $H \neq G$ with more than half the elements of G cannot be a subgroup of G.

We have been talking about right cosets of H in G all this time. Are there left cosets also?

The answer should be an obvious yes. After all we can similarly talk of

$aH = \{ah \mid h \in H\}$, for any $a \in G$, whch would be called a left coset. One can by defining similarly an equivalence relation ($a \equiv b \bmod H \Leftrightarrow a^{-1} b \in H$) prove all similar results for left cosets.

Theorem 7 : Let H be a subgroup of G then

(i) $Ha = H \Leftrightarrow a \in H$; $aH = H \Leftrightarrow a \in H$

(ii) $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $aH = bH \Leftrightarrow a^{-1} b \in H$

(iii) Ha (or aH) is a subgroup of G iff $a \in H$.

Proof : (i) Let Ha = H

Since $e \in H$, $ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H$.

Let $a \in H$, we show Ha = H.

Let $x \in Ha \Rightarrow x = ha$ for some $h \in H$

Now $h \in H$, $a \in H \Rightarrow ha \in H \Rightarrow x \in H \Rightarrow Ha \subseteq H$

Again, let $y \in H$, since $a \in H$

$ya^{-1} \in H$

$\Rightarrow ya^{-1} = h$ for some $h \in H$

$\Rightarrow y = ha \in Ha$

$\Rightarrow H \subseteq Ha$

Hence Ha = H.

(ii) $Ha = Hb$

$\Leftrightarrow (Ha)b^{-1} = (Hb)b^{-1}$

$\Leftrightarrow Hab^{-1} = He$

$\Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ (using (i))

(iii) If $a \in H$ then Ha = H which is a subgroup. Conversely, if Ha is a subgroup of G then $e \in Ha$ and thus the right cosets Ha and He have one lement e in common and hence $Ha = He = H \Rightarrow a \in H$ by (i)

Corresponding results for lelt cosets can be proved similarly.

Definition : Let G be a group and H, a subgroup of G. Then index of H in G is the number of distinct right (left) cosets of H in G. Is is denoted by $i_G(H)$ or [G:H].

The proof of Lagrange's theorem suggests that if G is a finite group then $i_G(H) = \dfrac{O(G)}{O(H)}$.

Problem 6 : Give an example to show that an infinite group G can have a subgroup $H \neq G$ with finite index.

Solution : Let < Z, + > be the group of integers under addition.

Let $H = \{2n \mid n \in Z\}$ then H is a subgroup of Z. We show H has only three right cosets in Z namely H, H + 1 ; H + 2.

If $a \in Z$ be any element ($\neq$ 0, 1, 2) then we can write (bi division algorithm).

$a = 3n + r, \quad 0 \leq r < 3$

which gives

$H + a + H + (3n + r) = (H + 3n) + r = H + r$

where $0 \leq r < 3$

Hence H has only 3 right cosets in Z and thus has index 3.

Notice, $H - 1 = (H + 3) - 1 = H + (3 - 1) = H + 2$ etc.

Problem 7 : Show that there exists a one-one onto map between the set of all left cosets of H in G and the set all right cosets of H in G where H is a subgroup of a group

G.

Solution : Let $\mathfrak{I}$ = set of all left cosets of H in G.

$\mathfrak{R}$ = set of all right cosets of H in G.

Define a mapping $\theta : \mathfrak{I} \to \mathfrak{R}$, s.t.,

$\theta(aH) = Ha^{-1}$ $a \in G$

θ is well defined as $aH = bH$

$\Rightarrow a^{-1} b \in H$

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

$\Rightarrow \theta(aH) = \theta(bH)$

Taking the steps backwards, we find θ is 1 – 1. Again, for any $Ha \in \mathfrak{R}$, $a^{-1} H$ is the required pre-image under $\theta$is onto.

If G is finite, then the above result reduces to saying that number of left cosets of H in G is same as the number of right cosets of H in G.

Problem 8 : Let H be a subgroup of a group G and $N(H) = \{a \in G \mid aHa^{-1} = H\}$. Prove that N(H) is a subgroup of G which contains H.

Solution : $N(H) \neq \phi$ subset of G as

$eHe^{-1} = H \Rightarrow e \in N(H)$

Let now $a, b \in N(H)$ be any two elements, then

$aHa^{-1} = H$

$bHb^{-1} = H$

then $bHb^{-1} = H \Rightarrow b^{-1} (bHb^{-1})\, b = b^{-1} Hb$

$\Rightarrow (b^{-1} b)\, Hb^{-1} b = b^{-1} Hb$

$\Rightarrow H = b^{-1} Hb$

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

$\Rightarrow aHa^{-1} = ab^{-1} Hba^{-1}$

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

$\Rightarrow ab^{-1} \in N(H)$ i.e., N(H) is a subgroup of G.

Since $h \in H \Rightarrow hHh^{-1} = H$ ($Ha = H \Leftrightarrow a \in H$ etc).

We find $h \in N(H)$ showing that $H \subseteq N(H)$.

Problem 9 : Suppose that H is a subgroup of a group G such that whenever $Ha \neq Hb$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.

Solution : It is given that if $Ha \neq Hb$ then $aH \neq bH$

thus if $aH = bH$ then $Ha = Hb$

Let now $g \in G$, $h \in H$ be any elements, then

$(g^{-1} h)\, (g^{-1})^{-1} \in H$ ($Ha = Hb \Rightarrow ab^{-1} \in H$)

$\therefore$ By (1) $H(g^{-1} h)\, Hg^{-1}$

$\Rightarrow (g^{-1} h)(g^{-1})^{-1} \in H$ ($Ha = Hb \Rightarrow ab^{-1} \in H$)

$\Rightarrow g^{-1}hg \in H$ for all $h \in H$

$\Rightarrow g^{-1}He \subseteq H$.

Definition : Let H and K be two subgroups of a group G. We define $HK = \{hk : h \in H, k \in K\}$, then HK will be a non empty subset of G.

Theorem 8 : HK is a subgroup of G iff HK = KH.

Proof : Let HK be a subgroup of G. We show HK = KH

Let $x \in HK$ be any element

Then $x^{-1} \in HK$ (as HK is a subgroup)

$\Rightarrow x^{-1} = hk$ for some $h \in H$, $k \in K$

$\Rightarrow x = (hk)^{-1} = k^{-1}h^{-1} \in KH$

thus $HK \subseteq KH$

Again let $y \in KH$ be any element

then $y = kh$ for some $k \in K$, $h \in H$

$\Rightarrow y^{-1} = h^{-1}k^{-1} \in HK$

$\Rightarrow y \in HK$ (as HK is a subgroup)

$\Rightarrow KH \subseteq HK$

Hence $HK = KH$.

Let $a, b \in HK$ be any two elements, we show $ab^{-1} \in HK$

$a, b \in HK \Rightarrow a = h_1k_1$ for some $h_1, h_2 \in H$

$b = h_2k_2$ $k_1, k_2 \in K$

Then $ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)\left(k_2^{-1}h_2^{-1}\right)$

$$= h_1\left(k_2k_2^{-1}\right)h_2^{-1}$$

Now $\left(k_1k_2^{-1}\right)h_2^{-1} \in KH = HK$

thus $\left(k_1k_2^{-1}\right)h_2^{-1} = hk$ for some $h \in H$, $k \in K$

then $ab^{-1} = h_1(hk) = (h_1h)k \in HK$

Hence HK is a subgroup.

Remarks : (i) HK = KH does not mean that each element of H commutes with every element of K. It only means that for each $h \in H$, $k \in K$, $hk = k_1h_1$ for some $k_1 \in K$ and $h_1 \in H$.

(ii) If G has binary composition +, we define

$H + K = \{h + k \mid h \in H, k \in K\}$.

Theorem 9: If H and K are finite subgroups of a group G then

$$o(HK) = \frac{o(H).o(K)}{o(H \cap K)}$$

Proof : Let D = H $\cap$ K then D is a subgroup of K and as in the proof of Lagrange's theorem, $\exists$ a decomposition of K into disjoint right cosets of D in K and

$$K = DK_1 \cup Dk_2 \cup \ldots\ldots \cup Dk_1$$

and also $t = \frac{o(K)}{o(D)}$

Again, $HK = H\left(\bigcup_{i=1}^{1} Dk_i\right)$ and since $D \subseteq H$, HD = H

Thus $HK = \bigcup_{i=1}^{1} Hk_i = Hk_1 \cup Hk_2 \cup \ldots\ldots \cup Hk_i$

Now no two of $Hk_1, Hk_2, \ldots\ldots\ldots, Hk_t$ can be equal as if $Hk_i = Hk_j$ for some i, j

then $k_ik_j^{-1} \in H \Rightarrow k_ik_j^{-1} \in H \cap K \Rightarrow k_ik_j^{-1} \in D \Rightarrow Dk_i = Dk_j$

which is not true.

Hence $o(HK) = o(Hk_1) + (Hk_2) + \ldots + o(Hk_t)$

$$= o(H) + o(H) + \ldots\ldots + o(H)$$

$$= t \,.\, o(H)$$

$$= \frac{o(H).o(K)}{o(H \cap K)}$$

Which proves the result.

1.2.6. Summary

In this lesson, we have studied the concept od subgroups and its various properties. We made the concept more understandable using simple examples. Further, we have discussed about centre of a group and cosets. Some results and theorems including Lagrange's theorem have been stated and proved accordingly.

1.2.7. Key concept

Subgroup, Centre of a group, Coset, Left coset, Right coset, Equivalence class, Lagrange's theorem, Product of subgroups, Normalizer, Centralizer, Index

1.2.8. Long Questions

1. Show that intersection of two subgroups of a group G is a subgroup of G.
2. If H is a subgroup of G, show that

$g^{-1} Hg = \{g^{-1} hg \mid h \in H\}$ is a subgroup of G.

3. Let G be the Quaternion group. Find centre of G. Find also the normalizer of i in G.

4. Show that normalizer of an element a in a group G is a subgroups of G.

5. Show that H = {0, 2, 4} is a subgroup of Z_6 = {0, 1, 2, 3, 4, 5} addition modulo 6.

6. If H and K are subgroups whose orders are relatively prime then show that $H \cap K = \{e\}$.

7. Show that for a group G, $Z(G) = \bigcap_{a \in G} N(a)$.

8. Show that the centralizer C(H) of a subgroup H of a group G is a subgroup of G.

1.2.9. Short Questions

1. Define subgroup of a group G. Give an example.
2. Define centralizer of an element'a' in group 'G'.
3. Prove that centre of a group G is a subgroup of G.
4. Define coset and give suitable example.
5. Define index of a subgroup H in group G.

1.2.10 Suggested Readings :

1. I.N. Herstein : Topics in Algebra

2. P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul : Basic Abstract Algebra, Cambridge University Press, Second Edition

LESSON NO. 1.3 **AUTHOR : DR. CHANCHAL**

Last updated on May, 2023

GROUPS – III

1.3.1 Objectives

In continuation with the previous lesson, in this lesson, we are going to study

- Cyclic groups and its generators
- Converse of Lagrange's theorem
- Euler's theorem and Fermat's theorem
- Normal subgroups and its properties

1.3.2 Cyclic Groups

Firstly , we define the order of an element:-

Definition (Order of an element) : Let G be a group and $a \in G$ be any element. We say a is of order (or period) n if n is the least +ve integer s.t., $a^n = e$. If binary composition of G is denoted by +, it is read as $na = 0$, where 0 is identity of G.

If it is not possible to find such n, we say a has infinite order. Order of a is be denoted by o(a) or $|a|$. It is obvious that $o(a) = 1$ iff $a = e$.

Cyclic Group : A group G is called a cyclic group if $\exists$ an element $a \in G$, such that every element of G can be expressed as a power of a. In that case a is called generator of G. We express this fact by writing $G = <a>$ or $G = (a)$.

Thus G is called cyclic if $\exists$ an element $a \in G$ s.t., $G = \{a^n \mid n \in Z\}$. Again, if binary composition of G is denoted by +, the words 'power of a' would mean multiple of a.

Note : The number of generators may be more than one. Moreover, if a is generator so is a^{-1}. A simple example of a cyclic group is the group of integers under addition, 1 being its generator.

Again the group G = {1, –1, i, –i} under multiplication is cyclic as we can express its members as i, i^2, i^3, i^4. Thus i (or – i) is a generator of this group.

Example 1 : Consider, Z_8 = {0, 1, 2, ...7} addition modulo 8.

Then we can check that 1, 3, 5, 7 will be generators of Z_8

Here, $3^1 = 3$, $3^2 = 3 \oplus 3 = 6$, $3^3 = 3 \oplus 3 \oplus 3 = 1$

$3^4 = 3 \oplus 3 \oplus 3 \oplus 3 = 4$ and so on

i.e., <3> = {3, 6, 1, 4, 7, 2, 5, 0}

or 3 is a generator of Z_8 Observe that 1, 7 and 3, 5 are each others inverses.

Theorem 1 : Order of a cyclic group is equal to the order of its generator.

Proof : Let G = <a> i.e., G is a cyclic group generated by a.

Case (i) : o(a) is finite, say n, then n is the least +ve integer s.t., $a^n = e$.

Consider the elements $a^0 = e$, a, a^2,......a^{n-1}

These are all elements of G and are n is number.

Suppose any two of the above elements are equal

say $a^i = a^j$ with i > j

then $a^i. a^{-j} = e \Rightarrow a^{i-j} = e$

But $0 < i - j \leq n - 1 < n$, thus $\exists$ a + ve integer i – j, s.t., $a^{i-j} = e$ and i – j < n, which is a contradiction to the fact that o(a) = n.

Thus no two of the above n elements can be equal, i.e., G contains at least n elements. We show it does not contain any other element. Let $x \in G$ be any elemnt. Since G is cyclic, generated by a, x will be some power of a.

Let $x = a^m$

By division algorithm, we can write

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

Now $a^m = an^{q+r} = (a^n)^q. a^r - e^q, a^r = a^r$

$\Rightarrow x = a^r$ (where $0 \leq r < n$

i.e., x is one of $a^0 = e$, a, a^2, ...a^{n-1}

or G contains precisely n elements

$\Rightarrow$ o(g) = n = o(a)

Case (ii): o(a) is infinite.

In this case no two powers of a can be equal as if $a^n = a^m$ (n > m) then $a^{n-m} = e$, i.e., it is possible to find a +ve integer n – m s.t., $a^{n-m} = e$ meaning thereby that a has finite order.

Hence no two powers of a can be equal. In other words words G would contain infinite number of elements.

Problem 1 : If $a \in G$ be of finite order n and also $n^m = e$ then show that n/m.

Solution : Let o(a) = n, then by definition n is the least +ve integer s.t., $a^n = e$.

Suppose $a^m = e$ for some m

By division algorithm, $m = nq + r$, where $0 \leq r < n$

$a^m = qnq + r$

$\Rightarrow e = a^{nq}. a^r = (a^n)^q. a^r = e^q. a^r = a^r$

where $0 \leq r < n$

Since n is such least +ve integer, we must have r = 0

i.e., $m = nq$ or that n/m.

Problem 2 : If G is a finite abelian group then show that o(ab) is a divisor of l.c.m. of o(a). o(b).

Solution : Let o(a) = n, o(b) = m, c(ab) = k.

Let l = 1 c.m. (m, n)

then $m \mid l, n \mid l, \Rightarrow l = mr_1, l = nr_2$

Now $(ab)^1 = a^l b^l$ (G is abelian)

$= a^{nr_2} b^{mr_1} e.e = e$

$\Rightarrow o(ab) \mid l$

$\Rightarrow k \mid l.$

Problem 3 : If in group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$ then show that o(b) = 31.

Solution : We have $b^2 = aba^{-1}$

$\Rightarrow b^4 = (aba^{-1})(aba^{-1})$

$= ab(a^{-1}a)^{nr} b^2 ab^{mrl} = ab^2a^{-1}$

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

$\Rightarrow b^4 = a^2ba^{-2}$

$\Rightarrow b^8 = (a^2b^{-2})(a^2ba^{-2}) = a^2b^2a^{-2}$

$= a^2(aba^{-1})a^{-2} = a^3ba^{-3}$

$\Rightarrow b^{16} = a^4ba^{-4}$ (as above)

$\Rightarrow b^{32} = a^5ba^{-5} = b$ as $a^5 = e$

$\Rightarrow b^{31} = e \Rightarrow 31$ is a multiple of o(b)

Since 31 is a prime number, it is the least +ve integer such that $b^{31} = e$

$\Rightarrow o(b) = 31$

We are, of course, taking $b \neq e$.

Problem 4 : Let G be a finite group with more than one element. Show that G has no element of prime order.

Solution : Let $e \neq a \in G$

Consider $a, a^2, \ldots\ldots a^1, \ldots\ldots$

Since G is finiter, for some integers i and j, $a^i = a^i$, $i > j$.

So, $a^{i-i} = e$

$\Rightarrow a^n = e$, $n = i - j > 0$

Since $a \neq e$, $n > 1$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_r^{\alpha_r}$, where p_i's are distinct primes

$$\text{So, } \left(a^{p_1^{\alpha_1} p_2^{\alpha_2} ......p_r^{\alpha_r - 1}} \right) = e$$

$$\Rightarrow \left(a^{p_1^{\alpha_1} p_2^{\alpha_2} ......p_r^{\alpha_r - 1}} \right) = 1 \text{ or } p_r$$

$$\text{If } O\left(a^{p_1^{\alpha_1} p_2^{\alpha_2} ......p_r^{\alpha_r - 1}} \right) = p_r \text{, then the result follows}$$

Let $a^{p_1^{\alpha_1} p_2^{\alpha_2} ......p_r^{\alpha_r - 1}} = e$, then (proceeding as above, we get an element of prime order as $a \neq e$.)

Problem 5 : Suppose that G is a finite group with the property that every non identity element has prime order. If Z(G) is non trivial, prove that every non identity element of G has the same order.

Solution : Let $e \neq a \in Z(G)$. Let $o(a)$ = prime p.

Let $b \in G$ such that $o(b)$ = prime q.

since $a \in Z(G)$, $ab = ba$

So, $(ab)^{pq} = a^{pq}\, b^{pq} = e$

$\Rightarrow o(ab)$ divises pq

$\Rightarrow o(ab) = 1$, p or q

If $o(ab) = 1$, then $a = b^{-1}$

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

$\Rightarrow p = q$.

If $o(ab) = p$, then $(ab)^p = e$

$\Rightarrow a^p b^p = e$

$\Rightarrow b^p = e$

$\Rightarrow q = o(b) \mid p \Rightarrow q = p$.

Similarly, if $o(ab) = q$, then $p = q$.

Therefore, every non identity element of G has the same order.

Theorem 2 : A subgroup of a cyclic group is cyclic.

Proof : Let G = <a> and let H be a subgroup of G. If H = {e}, there is nothing to prove. Let H ≠ {e}. Members of H will be powers of a. Let m be the least +ve integer s.t., $a^m \in$ H. We claim H = $<a^m>$.

Let $x \in H$ be any element. Then $x = a^4$ for some k. By division algorithm, k = mq + r where $0 \leq r < m$

$$\Rightarrow r = k - mq$$

$$\Rightarrow a^r = a^k.\ a^{-mq} = x.(a^m)^{-q} \in H$$

But m is the least +ve integer s.t., $a^m \in H$, meaning thereby that r= 0

Thus $k = mq$

or that $x = a^k = (a^m)^q \Rightarrow$ H is cyclic, gererated by a^m.

Theorem 3 : A cyclic group is abelian.

Proof : Let G = <a>. If x, y ∈G be any elements then $x = a^n$, $y = a^m$ for some integers m, n.

Now $xy = a^n, a^m = a^{n+m} = a^{m+n} = a^m . a^n = y.x$

Hence G is abelian.

Theorem 4 : If G is a finite group, then order of any element of G divides order of G.

Proof : Let $a \in G$ be any element,

Let $H = \{a^n |\ n \text{ an integer}\}$

Then H is a cyclic subgroup of G, generated by a, as

$$x, y \in H \Rightarrow x = a^n, y = a^m$$

$$\therefore \quad xy^{-1} = a^n.\ a^{-m} = a^{n-m} \in H$$

By Lagrange's theorem o(H)|o(G). But o(H) = o(a)

$$\therefore \quad o(a)|o(G).$$

Cor.: If G is a finite group then for any $a \in G$, then $a^{o(G)} = e$

Proof : $o(a)|o(G) \Rightarrow o(G) = o(a)k$ for some k

Now $a^{o(G)} = a^{o(a)k} = (a^{o(a)})^k = e^k = e$

Thus any element of a finite group, has finite order (which is less than or equal to the order of the group).

Problem 6 : Show that a group of even order has an element of order 2 and that the number of elements of order 2 is odd.

Solution : Let o(G) = even

Let $H = \{x \in G | x^2 = e\}$, $K = \{x \in G |\ x^2 \neq e\}$,

Then $G = H \cup K$

Now, $x \in E \Rightarrow x^{-1} \neq x$ also is in K.

⇒ number of elements is K is even and thus number of elements in H will also be even.

Since, $e \in H(a^2 = e)$, $\exists$ some $x \in H$, s.t., $x \neq e$.

Now, $x \neq e$, $x \in H \Rightarrow o(x) = 2$

$\Rightarrow$ G has an element of order 2.

Every element of order 2 is in H, and as $e \in H$, o(H) = even, the number of elements of order 2 is odd.

Theorem 5 : Converse of Lagrange's theorem holds in finite cyclic groups.

Proof : Let G = <a> be a finite cyclic group of order n,

Then $o(G) = o(a) = n$

Suppose $m|n$, We show $\exists$ a subgroup of G having order m.

Since $m|n$, $\exists$ k s.t., $n = mk$

Let H be the cyclic group generated by a^k

then H is a subgroup of G and $o(H) = o(a^k)$

We show $o(a^k) = m$

Now $(a^k)^m = a^{km} = a^n = e$, as $o(a) = n$

Suppose now, that $(a^k)^t = e$

Then $a^{kt} = e$

$\Rightarrow o(a)|kt \Rightarrow n|kt$

$\Rightarrow km|kt \Rightarrow m|t$

thus $o(a^k) = m$

which proves the result.

Problem 7 : Let G be a cyclic group of order n and suppose d divides n. Show that $x^d = e$ has exactly d solutions.

Solution : Let G = <a>, then o(g) = o(a) = n. Since $d|n$, there exists a unique subgroup H of G with order d. Let H = <b>

Then o(H) = o(b) = d.

$$H = \{b, b^2, \ldots\ldots b^{d-1}, b^d = e\}$$

If $b^i \in H$ be any element, then

$$(b^i)^d = (b^d)^i = e$$

Thus, every element of H is solution of $x^d = e$, which gives d distinct solutions in G.

Let now $c \in G$ be any solution of $x^d = e$ then $c^d = e$

and, therefore, $o(c)|d$. If o(c) = m, then $m|d = o(H)$ and thus there exists a subgroup K of H s.t., o(K) = m. Since K is unique of order m, and <c> is also of order m, K = <c> or that $<c> \subseteq H$ as $K \subseteq H$ and so $c \in H$ and thus any solution of $x^d = e$ is in H.

Hence there exist exactly d solutions.

Theorem 6 : A group G of prime order must be cyclic and every element of G other than identity can be taken as its generator.

Proof : Let o(G) = p, a prime

Take any $a \in G$, $a \neq e$

and let $H = \{a^n | n \text{ an integer}\}$ then H is a cyclic subgroup of G.

$\therefore \quad o(H) | o(G) \Rightarrow o(H) = 1$ or p

But $\quad o(H) \neq 1$ as $a \in H$, $a \neq e$,

Thus $o(H) = p \Rightarrow H = G$, i.e., G is a cyclic group generated by a. Since a was taken as any element (other than e), any element of G can act as its generator.

Cor.: A group of prime order is abelian.

Theorem 7 : A group G of prime order cannot have any non trivial subgroups.

Proof : If H is any subgroup of G then as $o(H) | o(G) = p$, a prime

we find $\quad o(H) = 1$ or p

i.e., $\quad H = \{e\}$ or $H = G$.

Theorem 8 : A group of finite composite order has at least one non-trivial subgroup.

Proof : Let $o(G) = n = rs \quad$ where $1 < r, s < n$

Since $n > 1$, $\exists\, e \neq a \in G$. Consider a^r.

Cose (i) : $\quad a^r = e$

then $\quad o(a) \leq r$, let $o(a) = k$

then $\quad 1 < k \leq r < n \quad (k > 1$, as $\neq e)$

Let $\quad H = \{a, a^2, a^3, ...a^k = e\}$

then H is a non empty. finite subset of G and it is closed under multiplication, thus H is a subgroup of G. Since $o(H) = k < n$, we have proved the result.

Case (ii) : $\quad a^r \neq e$, then since $(a^r)^s = a^{rs} = a^n = a^{o(G)} = e$

$o(a^r) \leq s$, Let $o(a^r) = t$ then $1 < t \leq s < n$.

If we take $K = \{a^r, 2^r, ...a^{tr} = e\}$ then K is a non empty finite subset of G, closed under multiplication and is therefore a subgroup of G. Its order being less than n, it is the required subgroup.

Theorem 9 : An infinite cyclic group has precisely two generators.

Proof : Let G = <a> be an infinite cyclic group.

As metioned earlier, if a is a generator of G then so would be a^{-1}.

Let now b be any generator of G,

then as $b \in G$, a generates G, we get $b = a^n$ for some integer n

again as $a \in G$, be generates G, we get $a = b^m$ for some integer m

$\Rightarrow a = b^m = (a^n)^m = a^{nm}$

$\Rightarrow a^{nm-1} = e \Rightarrow o(a)$ is finite and $\leq nm - 1$

Since of o(G) = o(a) is infinite, the above can hold only it

$nm - 1 = 0 \Rightarrow nm = 1$

$\Rightarrow m = \frac{1}{n}$ or $n = \pm 1$ as m, n are integers.

i.e., $b = a$ or a^{-1}

In other words, a and a^{-1} are precisely the generators of G.

1.3.3. No. of Generators of a finite cyclic group.

Euler's φ function (or Euler's totient function). as :

For this purpose, we firstly define. For any integer n, we define φ (1) = 1 and for n > 1, φ(n) to be the number of +ve integers less than n and relatively prime to n. As an example φ(6) = 2, φ(10) = 4 etc.

Note 1, 5 are less than 6 and relatively prime to 6 and 1, 3, 7, 9 (four in number) are less than 10 and relatively prime to 10 etc. Obviously, φ(p) = p – 1, if p is a prime.

Note : (i) If $p_1, p_2, \ldots..p_n$ are distinct prime factors of n (>1), then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots.\left(1 - \frac{1}{p_k}\right)$$

(ii) If, m n are co-prime then

$\varphi(mn) = \varphi(m)\,\varphi(n)$, $(m, n \geq 1)$

We are now ready to prove

Theorem 10 : Number of generators of a finite cyclic group of order n is φ(n).

Proof : Let G= <a> be a cyclic group of order n

then o(a) o(G) = n

We claim a^m is generator of G iff (m, n) = 1, i.e., m, n are relatively prime.

[For instance, if n = 8, then φ(8) = 4 will be number of generators as we will show a, a^3, a^5, a^7 will generate G and no other element ca generate G. So here m can have values 1, 3, 5, 7].

Let now a^m be a generator of G for some m

since $a \in G$, $a = (a^m)^i$ for some i

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

$\Rightarrow n \mid mi - 1$

$\Rightarrow mi - 1 = nj$ for some integer j

i.e., $mi - nj = 1$

$\Rightarrow (m, n) = 1$

Conversely, let (m, n)= 1

Then ∃ integers x and y s.t.,

$mx + ny = 1$

$\Rightarrow a^{mx + ny} = a$

$\Rightarrow a^{mx}. a^{ny} = a$

$\Rightarrow a^{mx} (a^{n})^{y} = a$

$\Rightarrow a^{mx} = a$ as $o(a) = n$

$\Rightarrow a = (a^{m})^{x}$

Since every element of G is a power of a and a itself is a power of a^m, we find a^m generates G, which proves our result.

Remark : We thus realize that if a is a generator of a finite cyclic group G of order n, then other generators of G are of the type a^m where m and n are coprime.

In fact an integer k will be a generator of Z_n if and only if k and n are coprime, and thus generators of Z_n would indeed be the elements of U_n.

1.3.3.1 Euler's Theorem

Theorem 11 : Let a, n(n ≥ 1) be any integers such that g.c.d. (a, n) = 1. Then $a^{\varphi(n)} \equiv 1 \pmod n$.

Proof : Let $U_n = \{x | x$ is an integer, $(x, n) = 1,\ 1 \le x < n\}$

Then U_n is a group under multiplication modulo n.

By definition of Euler's φ–function,

$o(U_n) = \varphi(n)$.

If n = 1, then $\varphi(n) = \varphi(1) = 1$ and $a^{\varphi(n)} = a^1 \equiv 1 \pmod 1$ (as 1 divides a – 1)

Let $n > 1$

Now by Euclid's algorithm

$a = nq + r$, for some integers q, r where $o \le r < n$.

If r = 0. then $a = nq \Rightarrow n | a \Rightarrow (a, n) = n > 1$, a contradiction

$\therefore \quad 1 \le r < n$

Also $(r, n) = d \Rightarrow d | r, d | n \Rightarrow d | a\text{-}nq, d | nq$

$\Rightarrow d | a, d | n$

$\Rightarrow d | (a, n)= 1$

$\Rightarrow d = 1$

$(r, n) = 1$ and $1 \le r < n$

$\Rightarrow r \in U_n$

Also $a = nq + r \Rightarrow a \equiv r(\bmod n)$

It follows from Lagrange's theorem that,

$r \otimes r \otimes ..... \otimes r =$ identity of $U_n = 1$ $[a^{o(G)} = e]$

where ⊗ is composition multiplication modulo n is U_n a φ(n) is order of group U_n.

$\therefore \quad r^{\varphi(n)} - nq_1 =1$, for some integer q_1

$\Rightarrow r^{\varphi(n)} \equiv 1 \pmod n$

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

so $a \equiv r \pmod{n} \Rightarrow a^{\varphi(n)} \equiv r^{\varphi(n)} \pmod{n}$.

1.3.3.2 Fermat's Theorem

Theorem 12 (Fermat's) : For any integer a and prime p,

$$a^{P} \equiv a \left(\text{mod } p\right).$$

Proof : If (a, p) = 1, then by Euler's theorem

$$a^{\varphi(p)} \equiv 1 \left(\text{mod } p\right)$$

$$\Rightarrow a^{p-1} \equiv 1 \left(\text{mod } p\right) \text{ as } \varphi\left(p\right) = p - 1$$

$$\Rightarrow a^{p} \equiv a \left(\text{mod } p\right)$$

If (a, p) = p, then $p \mid a \Rightarrow p \mid a^{p}$

$$\therefore \quad p \mid a^{p} - a$$

$$\Rightarrow a^{p} \equiv a \left(\text{mod } p\right).$$

(Note (a, p) = 1 or p as 1 and p are only divisors of p).

Problem 8 : Prove that 3, 5, and 7 are the only three consecutive odd integers that are prime.

Solution : Suppose p and p + 2 are consecutive primes, p > 3. We show that 12 divides their sum.

$p > 3 \Rightarrow$ g.c.d (p, 3) = 1

$\Rightarrow p^2 \equiv 1 \pmod{3}$ by Fermat's theorem

$\Rightarrow 3 \mid p^2 - 1$

$\Rightarrow 3 \mid (p - 1)(p + 1)$

If $3 \mid p - 1$, then $p - 1 = 3k \Rightarrow p = 3k + 1 \Rightarrow p + 2 = 3k + 3$ = multiple of 3.

But p + 2 is a prime > 3

So, we get a contradiction

Therefore, $3 \mid p + 1 \Rightarrow p + 1$ = multiple of 3

Since p is odd, p + 1 is also a multiple of 2

So, p + 1 is a multiple of 6.

Therefore, p + (p + 2) = 2p + 2 = 2(p + 1) = multiple of 12.

$\Rightarrow 12 \mid p + (p + 2)$

Problem 9 : Let G be a group.

Show that $o(a^n) = \dfrac{o(a)}{\left(o\left(a\right), n\right)}$ for all $a \in G$

where n is an integer and (0(a), n) = g.c.d (o(a), n).

Solution : Let o(a) = m

Let $d = (m, n) \Rightarrow \frac{m}{d}, \frac{n}{d}$ are integers

$\therefore \quad (a^n)^{m/d} = (a^m)^{n/d} = e^{n/d} = e$

Let $(a^n)^r = e \Rightarrow a^{nr} = e$

$\Rightarrow o(a) \mid nr$

$\Rightarrow m \mid nr$

$$\Rightarrow \frac{m}{d} \Big| \frac{n}{d} r$$

$$\Rightarrow \frac{m}{d} \Big| r \text{ as } \left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

$$\Rightarrow r \geq \frac{m}{d}$$

$$\therefore \quad o\left(a^n\right) = \frac{m}{d} = \frac{o(a)}{\left(o(a), n\right)}.$$

1.3.4. Normal Subgroup :

Definition : A subgroup H of a group G is called a normal subgroup of G if Ha = aH for all a ∈ G

Clearly G and {e} are normal subgroups of G known as the trivial normal subgroups. A group G ≠ {e} is called a simple group if the only normal subgroups of G are {e} and G. Any group of prime order is simple.

It is easy to see that if H is a normal subgroup of G and K is a subgroup of G s.t., $H \subseteq K \subseteq G$ then H is normal in K. Again, if G is abelian, all its subgroups will be normal.

We use the notation $H \trianglelefteq G$ to convey that H is normal in G.

For Example : H = {1, –1} is a normal subgroup of the Quaternion group G. Indeed Ha = {a, –a} = aH for any a ∈ G.

Theorem 13 : A subgroup H of a group G is normal in G iff $g^{-1} Hg = H$ for all g ∈ G.

Proof : Let H be normal in G

then Hg = gH for all g ∈ G

$\Rightarrow g^{-1} Hg = g^{-1} (gH) = (g^{-1} g) H = H.$

Conversely, let $g^{-1}Hg = H$ for all g ∈ G

Then $g(g^{-1} Hg) = gH$

$\Rightarrow (gg^{-1})Hg = gH$

$\Rightarrow Hg = gH.$

Hence H is normal.

Theorem 14 : A subgroup H of a group G is normal in G iff $g^{-1} hg \in H$ for all $h \in H$, $g \in G$.

Proof : Let H be normal in G, then

$Ha = aH$ for all $a \in G$

Let $h \in H$, $g \in G$ be any elements, then

$hg \in Hg = gh$

$\Rightarrow hg = gh_1$ for some $h_1 \in H$

$\Rightarrow g^{-1}hg = h_1 \in H$

which proves the result,

Conversely, let $a \in G$ be any element,

Then $a^{-1}ha \in H$ for all $h \in H$

$\Rightarrow a(a^{-1} ha) \in aH$ for all $h \in H$

$\Rightarrow g^{-1} hg = h_1 \in H$

$\Rightarrow Ha \subseteq aH$

Taking $b = a^{-1}$, we note, as $b \in G$

$b^{-1} hb \in H \qquad h \in H$

$\Rightarrow aha^{-1} \in H$ for all $h \in H$

$\Rightarrow (aha^{-1})a \in Ha$ for all $h \in H$

$\Rightarrow ah \in Ha$ for all $h \in H$

$\Rightarrow aH \subseteq Ha.$

Hence $Ha = aH$, showing H is normal.

Theorem 15 : A subgroup H of a group G is normal subgroup of G iff product of two right cosets of H in G is again a right coset of H in G.

Proof : Let H be a normal subgroup of G.

Let Ha and Hb be any two right coses of H in G.

then $(Ha)(Hb) = H(aH)b$

$= H(Ha)b$

$= HHab$

$= HaB \qquad ab \in G$

Conversely, we are given that product of any two right cosets of H in G is again a right seet.

To shwo H is normal, let $g \in G$ be any element.

Then Hg and Hg^{-1} are two right cosets of H in G. Thus $HgHg^{-1}$ is also a right coset of H $\in$ G.

We claim $HgHg^{-1} = He$

$egeg^{-1} \in HgHg^{-1}$

$\Rightarrow e \in HgHg^{-1}$

Also $e \in H$

Thus H and $HgHg^{-1}$ are two right cosets having one element common. Recalling the properties of equivalence classes, we know that any two right cosets are either equal or have no element in common. Thus, (as e is common element)

$$H = HgHg^{-1}$$

Now $hgh_1g^{-1} \in HgHg^{-1}$ for all $h, h_1 \in H, g \in G$

$\Rightarrow hgh_1g^{-1} \in H$ for all $h, h_1 \in H, g \in G$

$\Rightarrow h^{-1}(hgh_1g^{-1}) \in h^{-1} H$

$\Rightarrow gh_1g^{-1} \in H$ for all $h_1 \in H, g \in G$

$\Rightarrow$ H is normal in G.

Hence the result.

Remark : Let H be a subgroup of a group G. Define

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

then $g^{-1}Hg$ forms a subgroup of G.

Again, if we define a mapping $f : H \rightarrow g^{-1}Hg$, by

$$f(h) = g^{-1}hg$$

then f will be a 1 – 1 onto mapping.

In case G is finite, this would mean that both H and $g^{-1}Hg$ (for any $g \in G$) will have same number of elements.

Using this result we have thus proved that if H be a subgroup of a finite group G s.t., there is no other subgroup of G having the same number of elements as H has, then H is normal in G. After all, H and $g^{-1}Hg$ (for any $g \in G$) have same number of elements which mean that they are equal and $H = g^{-1}Hg$ means H is normal.

Problem 10 : Prove that a non empty subset H of a group G is normal subgroup of G $\Leftrightarrow$ for all $x, y \in H, g \in G, (gx)(gy)^{-1} \in H$.

Solution : Let H be normal subgroup of G.

Let $x, y \in H, g \in G$ be any elements,

then $(gx)(gy)^{-1} = (gx)(y^{-1} g^{-1}) = g(xy^{-1})g^{-1} \in H$

as $xy^{-1} \in H, g \in G$, H is normal in G.

Conversely, we show H isnormal subgroup of G.

Let $x, y \in H$ be any elements,

then $xy^{-1} = exy^{-1} e = (ex)(ey)^{-1} \in H$ as $e \in G$

i.e., H is a subgroup of G.

Again, let $h \in H, g \in G$ be any elements

Then as $(gh)(ge)^{-1} \in H$

we get $(gh)(eg^{-1}) \in H$

$\Rightarrow ghg^{-1} \in H$

$\Rightarrow$ H is normal.

Problem 11 : Show that the normaliser N(a) of a in a group G may not be a normal subgroup of G.

Solution : Let G = S_3 and a = (23), then Na(a) = N((23)) = $(\sigma \in S_3 | \sigma(23) = (23)\sigma\}$ = {I, (23)}

Since, N(a)(12) = {(2), (132)}

and (12)N(a) = {(12), (123)}

we find N(a)(12) $\neq$ (12)N(a) or that N(a) is not normal.

Problem 12 : If N is a normal subgroup of order 2, of a group G then show that N $\subseteq$ Z(G), then centre of G.

Solution : Let N = {a, e}.

Since e $\in$ Z(G) (centre being a subgroup contains e) all that we want to show is that a $\in$ Z(G)

i.e., ag = ga for all g $\in$ G

or $g^{-1}ag = a$ for all g $\in$ G

Let g $\in$ G be any element then as a $\in$ N and N is normal, g^{-1} ag $\in$ N = {a, e}

$\Rightarrow g^{-1}ag = a$ or g^{-1} ag = e

since $g^{-1}ag = e \Rightarrow ag = ge \Rightarrow ag = eg \Rightarrow a = e$, which is not true

we get g^{-1} ag = a $\Rightarrow$ a $\in$ Z(G)

or N $\subseteq$ Z(G).

Problem 13 : Show that a subgroup of index 2 in a group G is a normal subgroup of G.

Solution : Let H be a subgroup of G, with index 2 then number of distinct right (left) cosets of H is G is 2 and also then G is union of these two right (left) cosets.

Let g $\in$ G be arbitary.

Case (i) : g $\in$ H, then Hg = gH (=H)

Hence H is normal.

Case (ii) : g $\notin$ H then gH $\neq$ H, Hg $\neq$ H

Thus Hg and H = He are the two distinct right cosets of H in G and

$$G = Hg \cup H$$

Similarly, $G = gH \cup H$

$\Rightarrow Hg \cup H = gH \cup H$

$\Rightarrow Hg = gH$ (as $Hg \cap H = gH \cap H = \varphi$)

$\Rightarrow$ H is normal in G.

Remarks : Converse is not true. Indeed H = {1, –1} has index 4 in the Quaternion group and is normal.

Problem 14 : Let H be a subset of a group G. Let $N(H) = \{x \in G \mid Hx = xH\}$ be the normalizer of H is G.

We have already shown that N(H) is a subgroup of G. Show

(i) If H is a subgroup of G then N(H) is the largest subgroup of G in which H is normal.

(ii) If H is a subgroup of G then H is normal in G iff N(H) = G.

(iii) Show by an example, the converse of (ii) fails if H is only a subset of G.

(iv) If H is a subgroup of G and K is a subgroup of N(H) then H is normal subgroup of HK.

Solution : (i) We show H is normal in N(H).

Since Hh = hH for all $h \in H$, we find

$$h \in N(H) \text{ for all } h \in H$$

Thus $H \leq N(H)$.

Again by definition of N(H), Hx = xH for all $x \in N(H)$

$\Rightarrow$ H is normal in N(H)

To show that N(H) is the largest subgroup of G in which H is normal, suppose K is any subgroup of G such that H is normal in K.

Then $k^{-1} Hk = H$ for all $k \in K$

$\Rightarrow Hk = kH$ for all $k \in K$

$\Rightarrow k \in N(H)$ for all $k \in K$

$\Rightarrow K \subseteq N(H)$.

(ii) Let H be a normal subgroup of G

then $N(H) \subseteq G$ (by definition)

Let $x \in G$ be any element,

then xH = Hx as H normal in G.

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

Hence G = N(H)

Conversely, let G = N(H), H is a subgroup of G (given)

Let $h \in H$, $g \in G$ be any elements

Then $g \in N(H)$ as N(H) = G

$\Rightarrow gH = Hg$

$\Rightarrow$ H is normal in G.

(iii) Consider $G = <a> = \{e, a, a^2, a^3\}$

then G being cyclic is abelian group.

Take $H = \{a\}$

thenf H is a subset and not a subgroup of G ($e \neq H$)

Also N(H) = G as G is abelian.

(iv) Let K be a subgroup of N(H)

then $k \in K \Rightarrow k \in N(H) \in Hk = kH$

i.e., $Hk = kH$ for all $k \in K$

$\Rightarrow HK = KH$

$\Rightarrow$ HK is subgroup of N(H)

Note, $h \in H \Rightarrow Hh = hH$ (=H)

$\Rightarrow H \subseteq N(H)$ Also $K \subseteq N(H)$

Again $H \subseteq HK \subseteq N(H)$

Hence H is a subgroup of HK

$\Rightarrow$ H is normal subgroup of HK

$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$.

Problem 15 : Let H be normal in G such that o(H) and $\frac{o(G)}{o(H)}$ are co-prime. Show that H is unique subgroup of G of given order.

Solution : Let o(H) = $m, \frac{o(G)}{o(H)} = n$, Suppose K is a subgroup of G of order m.

Then $o(HK) = \frac{m.m}{d}$, where d = o(H $\cap$ K)

Since H is normal, $HK \leq G$

Thus $o(HK) \mid o(G)$

$$\Rightarrow m.\frac{m}{d} \mid m.n \Rightarrow \frac{m}{d} \mid n$$

$$\Rightarrow d\frac{m}{d} \mid dn \Rightarrow m \mid dn$$

$\Rightarrow m \mid d$ as (m, n) = 1

But $d \mid m$ as $H \cap K \leq H$

Thus d = m and hence

$o(H \cap K) = o(H) = o(K)$

$\Rightarrow H = K$.

1.3.5. Summary

In this lesson, we have studied order of an element and generators following the concept of cyclic groups. We have also studied about number of generators of finite and infinite cyclic groups. Several important theorems such as Euler's theorem and Fermat's theorem have been discussed with proofs. We have also discussed about normal subgroups. Various articles and theorems have been discussed with proofs during the study in this lesson.

1.3.6. Key Concepts

Order, Generator, Cyclic group, Finite cyclic group, Infinite cyclic group, Euler's function, Euler's theorem, Fermat's theorem, Normal subgroup

1.3.7. Long Questions

1. If order of a group G is pq, where p, q are primes, then show that every proper subgroup of G is cyclic.

2. Let G be a finite group whose order is not divisible by 3. Suppose $(ab)^3 = a^3b^3$ for all a, b $\in$ G, then show that G is abelian.

3. Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$ then show that N is a normal subgroup of G.

4. Show that every subgroup of a cyclic group is normal.

5. Show that intersection of two normal subgroups is a normal subgroup.

6. Every subgroup of an obelian group is normal. Prove that converse is not true. (Consider Quaternion group).

7. Show that C(H) is a normal subgroup of N(H), where $H \leq G$.

1.3.8. Short Questions

1. Find order of each element in the group G = {±1, ±1} under multiplication.

2. Show that a finite cyclic group with three or more elements has even number of generators.

3. Prove that centre of a group is a normal subgroup.

1.3.9. Suggested Readings

1. I.N. Herstein : Topics in Algebra

2. P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul : Basic Abstract Algebra, Cambridge University Press, Second Edition

B.A. PART–III **MATHEMATICS : PAPER I**
(SEMESTER - V) **ABSTRACT ALGEBRA**

LESSON NO. 1.4 **AUTHOR : DR. CHANCHAL**

Last updated on May, 2023

GROUPS – IV

1.4.1. Objectives

Using the concept of normal subgroups from previous lesson, in this lesson, we are going to extend the idea to quotient groups. The students would be able to get the knowledge of homomorphisms, isomorphisms and various important theorems based upon these.

1.4.2. Quotient Groups

Let G be a group of N a normal subgroup of G. Let us collect all the right cosets of N in G and form a set to be denoted by $\frac{G}{N}$ or G/N. Since N is normal in G, product of any two right cosets of N will again be a right coset of N in G, i.e., we have a well defined binary composition $\frac{G}{N}$ (Prove it). We now show that this set $\frac{G}{N}$ forms a group under this product as its binary composition.

For $\quad Na, Nb \in \frac{G}{N}, NaNb = Nab \in \frac{G}{N}$

If Na, Nb, Nc $\in \frac{G}{N}$ be any members, then

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

Again Ne $\in \frac{G}{N}$ will act as identity of $\frac{G}{N}$ and for any $Na \in \frac{G}{N}$, Na^{-1} will be the inverse of

Na. Thus $\frac{G}{N}$ forms a group, called the Quotient group or the factor group of G by N.

It is easy to see that if G is abelian then so would be any of its quotient groups as NaNb = Nab = Nba = NbNa.
Converse of this result may not hold.

Remarks : (i) In $\frac{G}{N}$, as N is normal, it does not matter whether we use the word right cosets or left cosets, as Na = aN for all a.

Theorem 1 : If G is a finite group and N is a normal subgroup of G then

$$o\left(\frac{G}{N}\right)=\frac{o(G)}{o(N)}$$

Proof : Since G is finite, using Lagrange's theorem

$$\frac{o(G)}{o(N)} = \text{number of distinct right cosets of N in G}$$

$$= o\left(\frac{G}{N}\right)$$

Theorem 2 : Every quotient group of a cyclic group is cyclic.

Proof : Let G = <a> be a cyclic group.
Then G is abelian, so every subgroup of G is normal. Let H be any subgroup of G. We show $\frac{G}{N}$ is cyclic. In fact we claim $\frac{G}{N}$ is generated by Ha.

Let Hx $\in \frac{G}{N}$ be any element.

Then x $\in$ G = <a>, i.e., x will be some power of a

Let $x = a^m$

Then $Hx = Ha^m = Ha\ a \ldots\ldots a$ (m times)

$= Ha\ Ha \ldots\ldots Ha$ (m times)

$= (Ha)^n$

i.e., any element Hx of $\frac{G}{N}$ is a power of Ha $\Rightarrow$ Ha generates $\frac{G}{N}$ or that $\frac{G}{N}$ is cyclic.

Remarks : (i) The above result is proved for $m > 0$. In case $m \leq 0$, the proof follows similarly. Notice $a^m = a^{-n} = (a^{-1})^n$ where $n > 0$ and remember that $Ha^{-1} = (Ha)^{-1}$ and so $(Ha^{-1})^n = (Ha)^{-n} = (Ha)^m$,

(ii) If $G = <a>$ is cyclic and $H \leq G$, then $o(G/H)$ is the least +ve integer m, s.t., $a^m \in H$.

Also, $G/H = <Ha>$. So $o(G/H) = o(Ha) = m$

(iii) The converse of above result is not true.

1.4.3. Examples of Quotient Groups

Example 1 : Let G be the set of 2 × 2 matrices over reals of the type $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Then it is easy to see that G will form a group under matrix multiplication $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity, $\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$ will be inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ Also G is not abelian.

Let N be the subset containing members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a subgroup of G (Prove). Also it is normal as the product of the type

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - \frac{b}{d} \\ 0 & 1 \end{bmatrix} \in N$$

So, we get the quotient group $\frac{G}{N}$. We show $\frac{G}{N}$ is abelian.

Let Nx, Ny $\in \frac{G}{N}$ be any elements, then x, y $\in$ G.

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian iff NxNy = NyNx

$\Leftrightarrow$ Nxy = Nyx

$\Leftrightarrow xy\,(yx)^{-1} \in N$

$\Leftrightarrow xyx^{-1}\,y^{-1} \in N$

We can easily check that the product

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} \frac{1}{c} & -\frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix} \text{ is a matrix of the type } \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

Thus we can have an abelian quotient group.

Example 2 : Let < Z, + > be the group of integers and let N = {3n | n $\in$ Z}, then N is a normal subgroup of Z.

$\frac{Z}{N}$ will consist of members of the type N + a, a $\in$ Z

We show $\frac{Z}{N}$ contains only three elements. Let a $\in$ Z be any element, where a $\neq$ 0, 1, 2, then we can write, by division algorithm,

$a = 3q + r$ where $0 \leq r \leq 2$

$\Rightarrow N + a = N + (3q + r) = (N + 3q) + r = N + r$ as $3q \in N$

but r can take values 0, 1, 2

Hence N + a will be one of N, N + 1, N + 2

or that $\frac{Z}{N}$ contains only these three members.

Remarks : (i) This example shows that in case of cosets, Ha = Hb may not necessarily mean a = b. For instance, N + 4 = N + 1, but 4 $\neq$ 1 in above example.

[N + 4 = (N + 3) + 1 = N + 1]

(ii) It also serves as an example of an infinite group which has a subgroup N having finite index in G.

Problem 1 : If G is group such that $\frac{G}{Z(G)}$ is cyclic, where Z(G) is centre of G then show that G is abelian.

Solution : Let us write Z(G) = N. Then $\frac{G}{N}$ is cyclic. Suppose it is generated by Ng.

Let a, b $\in$ G be any two elements,

then $Na, Nb \in \frac{G}{N}$

$\Rightarrow Na = (Ng)^n, Nb = (Ng)^m$ for some n, m

$\Rightarrow Na = Ng. Ng \ldots\ldots Ng = Ng^n$

$Nb = Ng^m$

$\Rightarrow ag^{-n} \in N, bg^{-m} \in N$

$\Rightarrow ag^{-n} = x, bg^{-m} = y$ for some $x, y \in N$

$\Rightarrow a = xg^n, b = yg^m$

$\Rightarrow ab = (xg^n)(yg^m) = x(g^ny)\, g^m$

$= x(yg^n)g^m$ as $y \in N = Zn\ (G)$

$= xyg^n\, g^m$

$= xyg^{n+m}$

Similarly, $ba = (yg^m)(xg^n) = y(g^mx)\, g^n = y(xg^m)\, g^n$

$= (yx)g^{m+n}$

$\Rightarrow ab = ba$ as $xy = yx$ as $x, y \in Z(G)$

Showing that G is abelian.

Remarks : (i) We are talking about $\frac{G}{Z(G)}$ assuming, therefore, that Z(G) is a normal subgroup of G, a result which can be proved easily.

(ii) One can, moving on same lines as in the above solution prove that if G/H is cyclic, where H is a subgroup of Z(g), then G is abelian.

(iii) If G is a non abelian group then G/Z(G) is not cyclic.

(iv) If $\frac{G}{H}$ is cyclic for some normal subgroup H of G then G may not be abelian. Take G = Quaternion group and H = {±1, ±i}, then o(G/H) = $\frac{8}{4} = 2$, a prime. So G/H is cyclic, but G is not abelian.

Problem 2 : Let G be a non-abelian group of order pq where p, q are primes then o(Z(G)) = 1.

Solution : Since G is non-abelian, by Problem 1, $\frac{G}{Z(G)}$ is not cyclic.

Now, $o(Z(G)) \mid o(G) = pq$

$\Rightarrow o(Z(G)) = 1, p, q \text{ or } pq$

$o(Z(G)) = pq \Rightarrow Z(G) = G$

$\Rightarrow$ G is abelian which is not so.

$o(Z(G)) = p \Rightarrow o(G/Z(G)) = \frac{pq}{p} = q$, a prime, meaning G/Z(G)) is cyclic which is also not true.

Similarly, o(Z(G)) = q cannot hold and we are left with the only possiblility that o(Z(G)) = 1.

1.4.4. Homomorphisms – Isomorphisms

Definition : Let < G, * > and < G', o > be two groups.

A mapping f : G → G' is called a homomorphism if

$f(a * b) = f(a) \circ f(b)$ a, b ∈ G

We shall use the same symbol (.)for both binary composition.

With that as notation, we find a map f : G → G' is a homomrphism if

$f(ab) = f(a) f(b)$

If, in addition, f happens to be one -one, onto, we say f is an isomorphism and in that case, we write $G \cong G'$.

An onto homomorphism is called epimorphism.

A one-one homomorphism is called monomorphism.

A homomorphism from a group G to itself is called an endomorphism of G.

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

If f : G → G' is onto homomorphism, then G' is called homomorphic image of G.

Example 1 : Let <Z, + > and < E, + > be the groups of integers and even integers.

Define a map f : Z → E, s.t.,

$f(x) = 2x$ for all $x \in Z$

then f is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

Also f is 1 – 1 (can be proved by taking the steps backwards.)

Now, f is a homomorphism as

$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$

Also f is onto as any even integer 2x would have x as its pre-image.

Hence f is an isomorphism.

In fact this example shows that a subset can be isomorphic to its superset.

Example 2 : Let f be a mapping from <Z, + > the group of integers to the group G = {1, –1} under multiplication defined as

$f : Z \to G$, s.t.,

$f(x) = 1$ if x is even

$= -1$ if x is odd

then f is clearly well defined. We check, if it is a homomorphism.

Let $x, y \in Z$ be any elements.

Case (i) : x, y are both even, then x + y is even and as

$$f(x + y) = 1, f(x) = 1, f(y) = 1$$

we notice $f(x + y) 1 = 1.1 = f(x). f(y)$

Case (ii) : x, y are both odd, then x + y is even and

$$f(x + y) + 1 = (-1)(-1) = f(x) f(y)$$

Case (iii) : x is odd, y is even, then x + y is odd and

$$f(x + y) = -1 = (-1)(1) = f(x) f(y)$$

thus in all case $f(x + y) = f(x) f(y)$

Showing thereby that f is a homomorphism. Is it an isomorphism? Obviously, f is onto. But f is not 1 – 1 as $f(x) = f(y)$ does not necessarily mean $x = y$. Indeed $f(2) = f(4)$ but $2 \neq 4$.

Example 3 : Let R^+ be the group of positive real numbers under multiplication and R be the group of all real numbers under addition. Then the map

$$\theta : R^+ \to R \text{ s.t., } \theta(x) = \log x$$

is an isomorphism,

θ is clearly well defined.

Now, $\theta(x) = \theta(y)$

$\Rightarrow \log x = \log y$

$\Rightarrow e^{\log x} = e^{\log y}$

$\Rightarrow x = y$

$\Rightarrow$ θ is, one-one.

Since $\theta(xy) = \log xy = \log x + \log y = \theta(x) + \theta(y)$

θ is homomorphism.

Finally, if $y \in R$ be any member, then

Since $e^y \in R^+$ and $\theta(e^y) = y$, therefore θ is onto and hence on isomorphism (The map $f : R \to R^+$, s.t., $f(a) = e^a$ can also be considered).

Example 4 : Let G be a group and N, a normal subgroup of G. Define a map

$$f : G \to \frac{G}{N} \text{ s.t.,}$$

$$f(x) = Nx,\ x \in G$$

then f is clearly well defined. Again

$$f(xy) = Nxy = NxNy = f(x)\,f(y)$$

shows f is a homomorphism.

It is sometimes called the natural (or canonical) homomorphism. Also, f is onto.

Remark : The relation of isomorphism in group is an equivalence relation. Thus whenever a group G is isomorphic to another group G', G' will be isomorphic to G. So we can say that G and G' are isomorphic and denote it by $G \cong G'$.

Theorem 1 : If $f : G \to G'$ is a homomorphism then

(i) $f(e) = e'$

(ii) $f(x^{-1}) = (f(x))^{-1}$

(iii) $f(x^n) = [f(x)]^n$, n an integer.

where e, e' are identity elements of G and G' respectively.

Proof : (i) We have

$$e.\ e = e$$
$$\Rightarrow f(e.\ e) = f(e)$$
$$\Rightarrow f(e).\ f(e) = f(e)$$
$$\Rightarrow f(e).\ f(e) = f(e).\ e'$$
$$\Rightarrow f(e) = e' \text{ (Left cancellation law)}$$

(ii) Again $xx^{-1} = e = x^{-1}x$

$$\Rightarrow f(xx^{-1}) = f(e) = f(x^{-1}x)$$
$$\Rightarrow f(x)\,f(x^{-1}) = e' = f(x^{-1})\,f(x)$$
$$\Rightarrow (f(x))^{-1} = f(x^{-1})$$

(iii) Let n be a +ve integer.

$$f(x^n) = \underset{(n\,\text{times})}{f(x.x.........x)}$$
$$= f(x).\ f(x)\ ......f(x)\ (n \text{ times})$$
$$= (f(x))^n$$

If n = 0, we have the result by (i). Incase n is –ve integer, result follows by using (ii).

Problem 1 : Show that <Q, +> cannot be isomorphic to <Q*, >, where $Q^* = Q - \{0\}$ and Q = rationals.

Solution : Suppose f is an isomophism from Q to Q*. Then as $2 \in Q^*$. Then as $2 \in Q^*$, f is onto, $\exists\, \alpha \in <Q, +>$, s.t., $f(\alpha) = 2$

$$\Rightarrow f\left(\frac{\alpha}{2}+\frac{\alpha}{2}\right)=2$$

$$\text{or } \Rightarrow f\left(\frac{\alpha}{2}\right)f\left(\frac{\alpha}{2}\right)=2$$

$$\Rightarrow x^2 = 2 \text{ where } x=f\left(\frac{\alpha}{2}\right)\in Q^*$$

But that is a contradiction as there is no rational no. x.s.t., $x^2 = 2$. Hence the result follows.

Problem 2 : Find all the homomorphisms from $\frac{Z}{4Z}$ to $\frac{Z}{6Z}$.

Solution : Let $f:\frac{Z}{4Z}\rightarrow\frac{Z}{6Z}$ be a homomorphism.

Then $f(4Z + n) = n\, f(4Z + 1)$
So, f is completely known if $f(4Z + 1)$ is known.
Now order of $(4Z + 1)$ is 4 and so $o(f(4Z + 1))$ divides 4
Also $o(f(4Z + 1))$ divides 6 and thus $o(f(4Z + 1)) = 1$ or 2

If $o(f(4Z + 1)) = 1$, then $f(4Z + 1) = 6Z =$ zero of $\frac{Z}{6Z}$

Hence $f(4Z + n) =$ zero
If $o(f(4Z + 1)) = 2$, then $f(4Z + 1) = 6Z + 3$
$\Rightarrow f(4Z + n) = 6Z + 3n$
Also $f(4Z + n + 4Z + m) = f(4Z + n + m)$
$= 6Z + 3(n + m)$
$= (6Z\ \ 3n) + (2Z + 3m)$
$= f(4Z + n) + f(4Z + m)$

Thus there are two choices for f and it can be defined as

$$f:\frac{Z}{4Z}\rightarrow\frac{Z}{6Z}\text{s.t.,}$$

$$f(4Z + n) = 6Z + 3n$$

Notice $4Z + n = 4Z + m$
$\Rightarrow n - m \in 4Z$

$$\Rightarrow 3(n - m) \in 12Z \subseteq 6Z$$
$$\Rightarrow 3(n - m) \in 6Z$$
$$\Rightarrow 6Z + 3n \in 6Z + 3m$$

i.e., f is well defined.

So there are two homomorphisms from $\frac{Z}{4Z} \to \frac{Z}{6Z}$. In fact, in general, there are homomorphisms from $\frac{Z}{mZ} \to \frac{Z}{nZ}$ where d = g.c.d (m, n)

1.4.5. Kernel of Homomorphism

Definition : Let $f : G \to G'$ be a homomorphism. The Kernel of f, (denoted by Ker f) is defined by

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

where e' is identity of G'.

Theorem 2 : If $f : G \to G'$ be a homomorphism, then Ker f is a normal subgroup of G.

Proof : Since $f(e) = e'$, $e \in$ Ker f, thus Ker f $\neq \varphi$.

Again, $x, y \in$ Ker f $\Rightarrow f(x) = e', f(y) = e^1$

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

$\Rightarrow xy^{-1} \in$ Ker f

Hence it is a subgroup of G.

Again, for any $g \in G$, $x \in$ Ker f

$$f(g^{-1}xg) = f(g^{-1})f(x)\, f(g)$$
$$= (f(g))^{-1}\, f(x)\, f(g) = (f(g))^{-1}\, e'\, f(g)$$
$$= (f(g))^{-1}\, f(g) = e'$$
$$\Rightarrow g^{-1}\, xg \in \text{Ker } f$$

Hence, it is a normal subgroup of G.

Theorem 3 : A homomorphism $f : G \to G'$ is one-one iff Ker f = {e}.

Proof : Let $f : G \to G'$ be one-one.

Let $x \in$ Ker f be any element

then $f(x) = e'$ and as $f(e) = e'$

$f(x) = f(e) \Rightarrow x = e$ as f is 1 – 1

Hence Ker f = {e}.

Conversely, let Ker f contain only the identity element.

Let $f(x) = f(y)$

Then $f(x)\, (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \text{Ker } f = \{e\}$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$ or that f is one-one.

Problem 3 : Let $f : G \to G'$ be a homomorphism. Let $a \in G$ be such that $o(a) = n$ and $o(f(a)) = m$. Show that $o(f(a)) \mid o(a)$ and f is 1 – 1 iff $m = n$.

Solution : Since $o(a) = n$

we find $a^n = e \Rightarrow f(a^n) = f(e)$

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

$\Rightarrow (f(a))^n = e'$

$\Rightarrow o(f(a)) \mid n = o(a)$

Again, let f be 1 –1

since $o(f(a)) = m$

we find $(f(a))^m = e'$

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

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

$\Rightarrow f(a^m) = e' = f(e)$

$\Rightarrow a^m = e$ (f is 1 – 1)

i.e., $o(a) \mid m$ or $n \mid m$, but already $m \mid n$

Hence $m = n$.

Conversely, let $o(a) = o(f(a))$.

Then $f(x) = f(y)$

$\Rightarrow f(x)\ (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow o(f(x^{-1})) = 1$

$\Rightarrow o(xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y$

$\Rightarrow$ f is 1–1.

Remark: Under an isomorphism, order of any element is preserved.

Problem 4 : Show that the group <R, +> of real numbers cannot be isomorphic to the group R* of non zero real numbers under multiplicaiton

Solution : $-1 \in R^*$ and order of -1 is 2 as $(-1)^2 = 1$. But R has no element of order 2. As if $x \in R$ is of order 2 then $2x = x + x = 0$. But this does not hold in <R, +> for any x except $x = 0$.

By above remark, under an isomorphism order of an element is preserved. Thus there cannot be any isomorphism between R and R*.

Problem 5 : Let G be a group and $f : G \to G$ s.t. $f(x) = x^{-1}$ be a homomorphism. Show that G is abelian.

Solution : Let x, y $\in$ G be any elements.

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

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

$= yx$, hence G is abelian.

1.4.5.1 First Theorem of Isomorphisms

Theorem 4 (Fundamental theorem of group homomorphism) : If $f : G \to G'$ be an onto homomorphism with K = Ker f, then $\frac{G}{K} \cong G'$.

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G.

Proof : Define a map $\varphi : \frac{G}{K} \to G'$ s.t.,

$$\varphi(Ka) = f(a),\ a \in G$$

We show φ is an isomorphism.

The φ is well defined follows by

$Ka = Kb$

$\Rightarrow ab^{-1} \in K = \text{Ker } f$

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

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

$\Rightarrow \varphi(Ka) = \varphi(Kb)$

By retracing the steps backwards, we can prove that φ is 1 –1.

Again as $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)\, f(b)$

$= \varphi(Ka)\, \varphi(Kb)$

Therefore, φ is a homomorphism.

To check that φ is onto, let $g' \in G'$ be any element. Since $f : G \to G'$ is onto, $\exists\, g \in G$, s.t.,

$f(g) = g'$

Now $\varphi(Kg) = f(g) = g'$

Which shows that Kg is the required pre-image of g' under φ.

Hence φ is an isomorphism.

Remark : The above theorem is also called **first theorem of isomorphism.** It can also be stated as:

If $f : G \to G'$ is a homomorphism with K = Ker f, then $\frac{G}{\text{Ker} f} \cong f(G)$.

1.4.5.2 Second Theorem of Isomorphism

Theorem 5 : Let H and K be two subgroup of a group G. where H is normal in G then

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

Proof : It is easy to see that $H \cap K$ will be a normal subgroup of K as $H \subseteq HK \subseteq G$, H will be normal in HK.

Define $f : K \to \frac{HK}{H}$ s.t., $f(k) = Hk$

As $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

So, f is well defined.

Again $f(k_1k_2) = Hk_1k_2 = Hk_1\,Hk_2 = f(k_1)f(k_2)$

Which shows f is a homomorphism.

Now obviously f is onto and thus using Fundamental theorem, we have

$$\frac{HK}{H} \cong \frac{K}{\operatorname{Ker} f}$$

Since $k \in \operatorname{Ker} f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow K \in H$

$\Leftrightarrow k \in H \cap K$ ($k \in K$ as $\operatorname{Ker} f \subseteq K$)

We find $\operatorname{Ker} f = H \cap K$

Hence Proved.

1.4.5.3 Third Theorem of Isomorphism

Lemma : If H and K are two normal subgroups of a group G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$, and conversely.

Proof : $\frac{K}{H}$ is non empty subset of $\frac{G}{H}$ (by definition)

For any $Hk_1, Hk_2 \in \frac{K}{H}$

$$(Hk^1)(Hk_2)^{-1} = \left(Hk_1\right)\left(Hk_2^{-1}\right) = Hk_1k_2^{-1} \in \frac{K}{H}$$

i.e., $\frac{K}{H}$ is a subgroup.

Again, for any $Hk \in \frac{K}{H}$ and $Hg \in \frac{G}{H}$, we have

$$(Hg)^{-1}(Hk)(Hg) = Hg^{-1}HkHg$$

$$= Hg^{-1}kg \in \frac{K}{H}$$

as $g \in G$, $k \in K$, K is normal in G gives $g^{-1}kg \in K$.

The converse part is left as an exercise for the reader.

Theorem 6 : (Third theorem of isomorphism) : If H and K are two normal subgroups of G such that $H \subseteq K$ then

$$\frac{G}{K} \cong \frac{G/H}{K/H}$$

Proof : The above lemma ensures that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk of $\frac{G/H}{K/H}$.

Define a map $f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$$f(Ha) = Ka, \; a \in G$$

f is well defind as

$$Ha = Hb$$

$$\Rightarrow ab^{-1} \in H \subseteq K$$

$$\Rightarrow Ka = Kb$$

$$\Rightarrow f(Ha) - f(Hb)$$

f is a homomorphism as

$$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)\,f(Hb).$$

Obviously, f is onto.

Using Fundamental theorem of group homomorphism, we can say

$$\frac{G}{K} \cong \frac{G/H}{\operatorname{Ker} f}$$

We claim Ker $f = \frac{K}{H}$

A member of Ker f will be some member of $\frac{G}{H}$.

Now $\quad Ha \in \operatorname{Ker} f \Leftrightarrow f(Ha) = K$ (identity of G/K)

$$\Leftrightarrow Ka = K$$

$$\Leftrightarrow a \in K$$

$$\Leftrightarrow Ha \in \frac{K}{H}$$

Hence we find $\quad \frac{G}{K} \cong \frac{G/H}{K/H}$

Which proves our result, it is also called Freshman's theorem.

Remark : Since $\frac{K}{H}$ = Ker f, we notice that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{K}$.

Problem 6 : Let G be the group of all non zero complex numbers under multiplication and let G' be the group of all real 2 × 2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where not both a and b are zero, under matrix multiplication, show that G ≅ G'.

Solution : Define a map

$$\varphi : G \to G', \text{ s.t.,}$$

$$\varphi\,(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

φ is clearly well-defined,
Also

$$\varphi[(a + ib)\ \varphi(c + id)] = \varphi[(ac - bd) + i(ad + bc)] = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}$$

and

$\varphi(a + ib)\ \varphi(c + id) \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix}$

shows that φ is a homomorphism.

Also for $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, the required pre-image is (a + ib).

Thus φ is onto

Also, $\varphi(a + ib) = \varphi(c + id)$

$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$\Rightarrow a = c,\ b = d \Rightarrow a + ib = c + id$$

Hence φ is an isomorphism.

Problem 7 : Suppose G is a group of order p^2, where p is a prime. Let $\varphi : G \to H$ be an onto homomorphism, where H is a group. Then show that either φ is an isomorphism or φ maps each element x of G onto the identity e of H and H = {e} or else, for each $y \in H$, ∃ exactly p elements x of g such that $\varphi(x) = y$.

Solution : $\varphi : G \to H$ is an onto homomorphism

$o(G) = p^2$.

Since Ker φ is a subgroup of G, by Lagrange's theorem $o(\text{Ker } \varphi) \mid o(G) = p^2$

$\Rightarrow o(\text{Ker } \varphi) = 1$, p or p^2

Case (i) : $o(\text{Ker } \varphi) = 1 \Rightarrow \text{Ker } \varphi = \{e\}$

$\Rightarrow \varphi$ is 1 – 1.

Hence φ is an isomorphism.

Case (ii) : $o(\text{Ker } \varphi) = p^2$

$\Rightarrow \text{Ker } \varphi = G$

$\Rightarrow$ for all $x \in G$, $x \in \text{Ker } \varphi \Rightarrow \varphi(x) = e$ for all $x \in G$

Since φ is onto, each element of H has pre-image, but all members of G are mapped to e.

∴ H = {e}

Case (iii) : $o(\text{Ker } \varphi) = p$

Let $y \in H$ be any element then as φ is onto, $\exists\ x \in G$, s.t., $\varphi(x) = y$

Let $\text{Ker } \varphi = \{a_1 = e, a_2, a_3, \ldots\ldots a_p\}$

We claim $xa_1, xa_2, \ldots\ldots., xa_p$ are distinct.

Suppose $xa_i = xa_j$. then $a_i = a_j$

Which is not true.

Thus $xa_1, xa_2, \ldots\ldots\ldots\ldots, xa_p$ are distinct members of G.

Now $\varphi(xa_i)\ \ \varphi(x)\varphi(a_i)$ i = 1, 2, ..., p,

$= ye = y$ for all i ($a_i \in \text{Ker } \varphi$)

thus y has p pre-images $x = xa_1, ax_2, \ldots\ldots\ldots\ldots, xa_p$

To show that y does not have more than p pre-images, let x' be any other pre-image of y under φ

Then
$$\begin{aligned}&\varphi(x') = y = \varphi(x)\\ &\Rightarrow (\varphi(x))^{-1}\, \varphi(x') = e\\ &\Rightarrow \varphi(x^{-1}\, x') = e\\ &\Rightarrow x^{-1}x' \in \text{Ker } \varphi\\ &\Rightarrow x^{-1}\, x' = a_i \text{ for some } i\\ &\Rightarrow x' = xa_i \text{ for some } i\end{aligned}$$

i.e., it is one of the p pre-images, we have considered.

Hnece y has exactly p pre-images.

1.4.6 Summary : In this lesson, we have studied about quotient groups with the help of suitable examples. We have also gone through the concept of homomorphisms and isomorphisms. Many important theorems and results based upon homomorphisms and isomorphisms, have been studied alongwith their proofs.

1.4.7 Key Concepts : Quotient group, Homomorphism, Isomorphism, Epimorphism, Monomorphism, Endomorphism, Automorphism, Homomorphic image, Kernel, Fundamental theorem of group homomorphism, First theorem of isomorphism, Second theorem of isomorphism, Third theorem of isomorphism.

1.4.8 Long Questions :

1. For a fixed element a in a group G, define

$f_a : G \to G$, s.t., $f_a(x) = a^{-1}\, xa,\ x \in G$

Show that f_a is an isomorphism.

2. Let f, g be homomorphisms from $G \to G'$. Show that

$H = \{x \in G \mid f(x) = g(x)\}$ is a subgroup of G.

3. Show that $2Z \equiv 3Z$ by considering the mapping $2x \to 3x$. Generalise.

4. Let N be a normal subgroup of G then show that $\frac{G}{N}$ is abelian iff $xyx^{-1}\, y^{-1} \in N$, for all $x, y \in G$.

5. Show that a subgroup H of a group G is normal in G iff the set $\frac{G}{H}$ of all its right cosets is closed under multiplication.

6. If H and K are two normal subgroups of G such that (G/H) and (G/K) are abelian then show that $\frac{G}{H \cap K}$ is abelian.

7. Show that $\frac{Q}{Z}$ is an infinite group and is not cyclic.

8. Let N be a normal subgroup of a group G. Show that $o(Na)\,|\,o(a)$ for any $a \in G$.

1.4.9 Short Questions :

1. Show that the relation of isomorphism in groups is an equivalence relation.

2. Show that homomorphi image of

(a) an abelian group is abelian

(b) a cyclic group is cyclic.

(c) a finite group is finite.

1.4.10 Suggested Readings :

1. I.N. Herstein : Topics in Algebra

2. P. B. Bhattacharya, S. K. Jain, S. R. Nagpaul : Basic Abstract Algebra, Cambridge University Press, Second Edition

Mandatory Student Feedback Form

https://forms.gle/KS5CLhvpwrpgjwN98

Note: Students, kindly click this google form link, and fill this feedback form once.