8/1/18

Mathematics-IV

Paper-Algebra

Unit-I - Groups (or) Group theory

Defination of group
Properties of groups & finite groups
Sub-groups, Examples of sub-groups & Sub-group tests.
Cyclic groups & properties of cyclic groups.
Permutation groups & Properties of permutation & cheque digit scheme based on D_5.

Unit-II - Isomorphsims

Defination & Examples
Cayleys theorem properties of Isomorphsim & Automorphsim.
Applications of Coset's to permutation groups.
Normal sub-groups & factor groups & applications

Unit-III - Ring theory

Introduction, Examples, Properties of rings
Sub rings
Integral domains
Characteristics of ring & ideals
Prime & maximal ideals

Unit-IV - Ring homorphsim

Defination, Examples, Properties of homorphsim
Field of quotient polynomial rings.

Scanned by CamScanner

Unit-I-Groups

Binary Operations: let S be a non empty set if $f: S \times S \to S$ then f is called binary operation defined on S.

It is denoted as '0' or '*'.

Algebraic structure: A non empty set G equipped with binary operation is called algebraic structure.

Ex: $(Z,0)\ (Z,+)\ (Z,-)\ (N,+)\ (R,-)\ (Q,+)\ (Z,*)$

Properties:

let G be a non empty sub set then

1. **Closure property**: let $a,b \in G \Rightarrow a \circ b \in G$

   Ex: let R be a non empty set of real numbers

   let $a=2, b=3 \Rightarrow a+b = 2+3 = 5 \in R$

   $a \times b = 2 \times 3 = 6 \in R$

2. **Associative property**: let $a,b,c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$

   Ex: let $a=1, b=3, c=4 \in R \Rightarrow a+(b+c) = 1+(3+4) = 8 \in R$
   $(a+b)+c = (1+3)+4 = 8 \in R$ } LHS=RHS

   $\Rightarrow a \cdot (b \cdot c) = 1 \cdot (3 \cdot 4) = 12 \in R$
   $(a \cdot b) \cdot c = (1 \cdot 3) \cdot 4 = 12 \in R$ } LHS=RHS

3. **Identity property**: It is denoted as 'e'. identity element

   let $a \in G \ \exists\, e \in G \Rightarrow a \circ e = e \circ a = a$.

   (R.I) (L.I)

   Ex: $a+e = e+a = a$

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

Note: For the binary operation '+' the identity element $e=0$.

→ For the binary operation '×' the identity element $e=1$.

Scanned by CamScanner

10/1/18

4. Inverse property: let $a \in G \ni b \in G \Rightarrow a \circ b = b \circ a = e$

$+_n \Rightarrow a+b=b+a=e \Rightarrow a+b=0 \Rightarrow b=-a$

Inverse of 'a' is '-a'.

$\times_n \Rightarrow a \cdot b = b \cdot a = e \Rightarrow a \cdot b = 1 \Rightarrow b = 1/a$

Inverse of 'a' is '(1/a)'.

Ex: let $a=2 \in R$

$+_n \Rightarrow a+b=e \Rightarrow 2+b=0 \Rightarrow b=-2$

Inverse of 2 is -2.

$\times_n \Rightarrow a \cdot b = e \Rightarrow a+b=1 \Rightarrow 2 \cdot b = 1 \Rightarrow b = 1/2$

Inverse of 2 is $1/2$.

5. Commutative property: let $a, b \in G \ni a \circ b = b \circ a$

$+_n \Rightarrow a+b=b+a$

$\times_n \Rightarrow a \cdot b = b \cdot a$

Ex: let $a=2$, $b=3$

$+_n \Rightarrow a+b = 2+3 = 5$
$b+a = 3+2 = 5$ } LHS=RHS

$\times_n \Rightarrow a \cdot b = 2 \cdot 3 = 6$
$b \cdot a = 3 \cdot 2 = 6$ } LHS=RHS

Groupoid → closure : let $a, b \in G \Rightarrow a \circ b \in G$

Semigroup → closure : let $a, b \in G \Rightarrow a \circ b \in G$
Associative : let $a, b, c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$

Monoid → closure : let $a, b \in G \Rightarrow a \circ b \in G$
Associative : let $a, b, c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$
Identity : let $a \in G \ni e \in G \Rightarrow a \circ e = e \circ a = a$

Group → closure : let $a, b \in G \Rightarrow a \circ b \in G$
Associative : let $a, b, c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$
Identity : let $a \in G \ni e \in G \Rightarrow a \circ e = e \circ a = a$
Inverse : let $a \in G \ni b \in G \Rightarrow a \circ b = b \circ a = e$

Abelian group (or) commutative group → closure : let $a, b \in G \Rightarrow a \circ b \in G$
Associative : let $a, b, c \in G \Rightarrow a \circ (b \circ c) = (a \circ b) \circ c$
Identity : let $a \in G \ni e \in G \Rightarrow a \circ e = e \circ a = a$
Inverse : let $a \in G \ni b \in G \Rightarrow a \circ b = b \circ a = e$
Commutative : let $a \circ b \in G \Rightarrow a \circ b = b \circ a$

Scanned by CamScanner

$(N,+)$ & $(Q,-)$ are examples of semigroup

18/1/18

Chapter-1 - Defination and Examples of a Group

Semigroup: The algebraic structure (G,O) is said to be a Semigroup if it satisfies closure and associative properties

Group: Let 'G' be a non-empty set and 'O' is a binary operation satisfying closure, associative, identity and inverse properties is called a group.

Abelian group: Let G be a non-empty set and O is a binary operation satisfying closure, associative, identity, inverse and commutative properties is called abelian group.

19/1/18

Examples:

1. $(Z,+)$ $(Q,+)$ $(R,+)$

Sol. $(Z,+)(Q,+)(R,+)$ are all operators with identity zero and inverse of 'a' is '-a'.

2. $(Z,\cdot)$

Sol. $(Z,\cdot)$ is not a group since identity is 1 and inverse of 2 is $\frac{1}{2} \notin Z$.

$\therefore (Z,\cdot)$ is not a group.

Imp 3. The 4th roots of unity forms a group w.r.t $(\cdot)$.

Sol. Composition table:

$\cdot$	1	-1	i	-i
1	(1)	-1	i	-i
-1	-1	(1)	-i	i
i	i	-i	-1	(1)
-i	-i	i	(1)	-1

Here $G = \{1, -1, i, -i\}$; $i^2 = -1$

Scanned by CamScanner

Closure property: All the elements in the composition table belongs to G. ∴ closure property statisfies.

Associative property: let $1, -1, -i \in G$ (4)

$$(1\cdot(-1))\cdot -i = 1\cdot(-1\cdot -i)$$
$$-1\cdot -i = 1\cdot i$$
$$i = i$$

∴ Associative property statisfies

Identity property: From the composition table 1 is the identity.

Inverse property: The inverse of $1, -1, i, -i$ are $+1, -1, -i, i$ respectively.

∴ $(G, \cdot)$ is a Group.

---

4. The set of irrational numbers w.r.t $(\cdot)$.

Sol: The set of irrational numbers w.r.t $(\cdot)$ is not a group ($\because \sqrt{2}\cdot\sqrt{2} = 2 \notin$ irrational no.) so, it is not a closure property.

24/1/18 Addition modulo 'm':-

Let a, b be two +ve integers and m is a fixed +ve integer. The addition modulo m of a, b is the reminder obtained when $a+b \div m$ and is denoted as $a +_m b$.

Ex: $12 +_5 10 = 22 \div 5 = 2$

$33 +_7 6 = 39 \div 7 = 4$

$1 +_4 2 = 3$

Multiplication modulo 'm':-

Let a, b be two +ve integers and m is a fixed +ve integer. The multiplication modulo m of a, b is the reminder obtained then $a\cdot b \div m$ and is denoted as $a \times_m b$.

Scanned by CamScanner

Ex: $7 \times_6 3 = 21 \div 6 = 3$

$2 \times_6 10 = 20 \div 6 = 2$

$2 \times_7 2 = 4$

5. The set $\{0,1,2,3\}$ w.r.t $\times_4$

Sol: Given $G = \{0,1,2,3\}$ and $\times_4$ is a binary operation

Composition table:

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Closure property: All the elements in the composition table belongs to G $\therefore$ closure property statisfies.

Associative property: let 1, 2, 3 elements

$(1 \times_4 2) \times_4 3 = 1 \times_4 (2 \times_4 3)$

$2 \times_4 3 = 1 \times_4 2$

$2 = 2$

Identity property: from the composition table $e=1$ is the identity.

Inverse property: From the composition table the inverse of 0 & 2 doesnot exist.

$\therefore (G, \times_4)$ is not a Group.

Scanned by CamScanner

6. $G=\{0,1,2,3,4,5\}$ w.r.t $+_6$.

Sol: Given $\{0,1,2,3,4,5\}$ and $+_6$ is a binary operation.

Composition table: (6)

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

Closure property: All the elements in the composition table belongs to G ∴ closure property satisfies.

Associative property: let take 3 elements 1,2,3

$$(1+_6 2)+_6 3 = 1+_6 (2+_6 3)$$
$$3+_6 3 = 1+_6 5$$
$$0 = 0$$

Identity property: From the composition table $e=0$ is the identity.

Inverse property: From the table inverse of 0,1,2,3,4,5 are 0,5,4,3,2,1 respectively.

Commutative property: 2 elements:

$$4+_6 5 = 5+_6 4$$
$$3 = 3$$

∴ Abelian property exists.

---

7. $\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2}, +\right)$

Sol: It a group where identity $e=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Scanned by CamScanner

8. The set R^* of non zero real numbers w.r.t ~~oper~~ $\times$

Sol: Is a group where identity $e=1$ and inverse of a is $\frac{1}{a}$

V.Imp 9. Let (Q_+) be the set of all +ve rational numbers and $*$ is the binary operation on Q_+. Defined by $a*b=\frac{ab}{3}$. Verify $(Q_+, *)$ is a group or not.

Sol: Given $G=Q_+$ and $*$ is its binary operation and defined as $a*b=\frac{ab}{3}$.

Closure property: Let 2 elements $a, b \in Q_+$

$a*b=\frac{ab}{3} \in Q_+$

$\therefore$ closure property satisfies.

Associative property: Let 3 elements be $a, b, c \in Q_+$

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

$\left(\frac{ab}{3}\right)*c = a*\left(\frac{bc}{3}\right)$

$\frac{\frac{ab}{3}\cdot c}{3} = \frac{a\cdot\frac{bc}{3}}{3}$

$\frac{abc}{9} = \frac{abc}{9}$

$\therefore$ Associative property satisfies.

Identity property: let $a \in Q_+ \ \exists\ e \in Q_+ \ni a*e=a$

$\frac{ae}{3}=a$

$e=3$

$\therefore$ 3 is the identity.

Inverse property: let $a \in Q_+ \ \exists\ b \in Q_+ \ni a*b=e$

$\frac{ab}{3}=3$

$ab=9$

$b=\frac{9}{a}$

$\therefore \frac{9}{a}$ is the inverse of a.

$\therefore (Q_+, *)$ is a group.

Scanned by CamScanner

10. Let R be the set of real numbers and '0' is the binary operation defined by $a0b = a+b+ab$. Is a group or not.

Sol. Given $G = (R, 0)$ and 0 is the binary operation and defined by $a0b = a+b+ab$. (8)

Closure property: let $a, b \in R$

$$a0b = a+b+ab \in R$$

$\therefore$ closure property satisfies.

Associative property: let $a, b, c \in R$

$$(a0b)0c = a0(b0c)$$
$$(a+b+ab)0c = a0(b+c+bc)$$
$$a+b+ab+c+ac+bc+abc = a+b+c+bc+ab+ac+abc$$

$\therefore$ Associative property satisfies

Identity property: let $a \in R \ \exists \ e \in R \ni a0e = a$

$$a+b+ab = a$$
$$e(1+a) = 0$$
$$e = 0$$

$\therefore$ 0 is the identity.

Inverse property: let $a \in R \ \exists \ b \in R \ni a0b = e$

$$a0b = 0$$
$$a+b+ab = 0$$
$$b+ab = -a$$
$$b(1+a) = -a$$
$$b = \frac{-a}{1+a}$$

$\therefore \frac{-a}{1+a}$ is the inverse of 'a'

$\therefore (R, 0)$ is a group.

27/1/18

Note:

$U(n)$ = the set of all +ve integers $< n$ and are relatively prime to 'n'.

Ex: $U(10) = \{1, 3, 7, 9\}$

$U(12) = \{1, 5, 7, 11\}$

Scanned by CamScanner

11. $U(10)$ is a group w.r.t $(\cdot)$

Sol. $U(10) = \{1, 3, 7, 9\}$

Composition table:

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$10)\,21\,(2$
$\quad\;\; 20$

closure property: All the elements in the composition tab $\in U(10)$.

Associative property: let 1, 3, 7

$$(1 \times_{10} 3) \times_{10} 7 = 1 \times_{10} (3 \times_{10} 7)$$
$$3 \times_{10} 7 = 1 \times_{10} 1$$
$$1 = 1$$

Identity property: From the composition table $e = 1$ is the identity.

Inverse property: From the composition table the inverse 1, 3, 7, 9 are 1, 7, 3, 9 respectively.

$\therefore U(10)$ is a group.

Scanned by CamScanner

29/1/18

Imp

Theorem 1:

Statement: The identity element in a group

Proof: Given $(G, \cdot)$ is a group and let e, e' be abelian identities of G.

Now we prove $e = e'$ (10)

Let $e \in G$, e' is the identity of G.

$\Rightarrow e \cdot e' = e = e' \cdot e$ — ①

Let $e' \in G$, e is the identity of G.

$\Rightarrow e' \cdot e = e = e' \cdot e$ — ②

from ① & ②

$e = e'$

∴ The identity element in a group is unique.

Defination: Cancellation law:

Let $a, b, c \in G$

L.C.L: consider $ab = ac \Rightarrow b = c$

R.C.L: Consider $ba = ca \Rightarrow b = c$

Theorem 2:

Statement: Cancellation laws holds in a group G.

Proof: Given $(G, \cdot)$ be a group with identity e.

Now we prove cancellation laws holds in a group

L.C.L: Let $a, b, c \in G$

Consider $ab = ac$

$a \in G \Rightarrow \bar{a}' \in G$

multiply $\bar{a}'$ to the left

$\Rightarrow \bar{a}'(ab) = \bar{a}'(ac)$

$(\bar{a}'a)b = (\bar{a}'a)c$ [∵ Associative prop]

$eb = ec$ [∵ Inverse prop]

$b = c$ [∵ Identity prop]

Scanned by CamScanner

R.C.L: Let $a, b, c \in G$

Consider $ba = ca$

$a \in G \Rightarrow \bar{a}^{-1} \in G$

multiply $\bar{a}^{-1}$ in the right

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

$b(a\bar{a}^{-1}) = c(a\bar{a}^{-1})$ [$\because$ Associative]

$be = ce$ $\because$ ~~Identity~~ [Inverse]

$b = c$ [$\because$ Identity]

$\therefore$ Cancellation laws holds in a group.

Theorem 3:

Statement: The inverse of an element in a group is unique

Proof: Given $(G, \cdot)$ be a group.

let $a \in G$

let b, c be two inverses of a.

b is the inverse of a.

$\Rightarrow a \cdot b = e = b \cdot a$ — ①

c is the inverse of a.

$\Rightarrow a \cdot c = e = c \cdot a$ — ②

from ① & ②

$\Rightarrow ab = ac$

$b = c$ [L.C.L]

$\therefore$ The inverse of an element in a group is unique.

Theorem 4:

Statement: In a group G $(ab)^{-1} = \bar{b}^{-1}\bar{a}^{-1}$.

Proof: let $(G, \cdot)$ be a group and $a, b \in G$

Consider $(ab)(\bar{b}^{-1}\bar{a}^{-1}) = a(b\bar{b}^{-1})\bar{a}^{-1}$

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

$= a \cdot \bar{a}^{-1}$

$= e$

Similarly consider $(\bar{b}^{-1}\bar{a}^{-1})(ab) = \bar{b}^{-1}(\bar{a}^{-1}a)b$

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

$= \bar{b}^{-1} \cdot b$

$= e$

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

Scanned by CamScanner

30/1/18

Imp D

Problems:

1. S.T $(ab)^n = a^n b^n$ where $a, b \in G$ and G is an abelian group.

Sol. Given G is an abelian group and let $a, b \in G$ we use mathematical induction.

for $n=1 \Rightarrow (ab)^1 = ab$ (12)

$= a^1 b^1$

i.e, it is true for $n=1$

Assume that it is true for $n=k$

for $n=k \Rightarrow (ab)^k = a^k b^k$

Now we prove it is true for $n=k+1$

Consider $(ab)^{k+1} = (ab)^k ab$

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

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

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

$= a^{k+1} b^{k+1}$

$\therefore$ It is true for $n=k+1$

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

---

2. P.T ~~in any~~ in a group G $(ab)^2 = a^2 b^2 \Leftrightarrow ab = ba$

Sol. let G be a group and $a, b \in G$

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

Now we prove $ab = ba$

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

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ba)b$ [$\because$ Associative]

$ab = ba$ [$\because$ By L.C.L & R.C.L]

Conversely $ab = ba$

Now we prove $(ab)^2 = a^2 b^2$

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

$= a(ba)b$

$= a(ab)b$ [$\because ab = ba$]

$= (aa)(bb)$

$= a^2 b^2$

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

Scanned by CamScanner

3. P.T a group G is abelian $\Leftrightarrow (ab)^{-1} = a^{-1}b^{-1}$.

(13)

Sol. Given G is a group and $a, b \in G$

Let G be abelian.

Now we prove $(ab)^{-1} = a^{-1}b^{-1}$.

Consider $(ab)(a^{-1}b^{-1}) = a(ba^{-1})b^{-1}$

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

$= (aa^{-1})(bb^{-1})$

$= e \cdot e$

$= e$.

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

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

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

$= e \cdot e$

$= e$.

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

Conversely suppose $(ab)^{-1} = a^{-1}b^{-1}$

Now we prove G is abelian.

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

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

$\therefore$ G is abelian.

Scanned by CamScanner

31/1/18

2- Sub Groups

Order of a Group: The no. of elements in a group is called order of a group. and is denoted as $O(G)$ or $|G|$.

If the no. of elements are infinite the order of the group is infinite.

Order of an element in a group:

Let $(G, \cdot)$ be a group and $a \in G$, the order of a is the least positive integer 'n' such that $a^n = e$.

Imp **Note:** If order of a, $O(a) = n$ and $a^m = e$ then $n < m$. (14)

Examples:

1. Let G = cube roots of unity
$= \{1, \omega, \omega^2\}$

Here order of group is 3.

$O(1) = 1$

$O(\omega) = 3$ $[\because \omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1 = e]$

$O(\omega^2) = 3$ $[\because \omega^2 = \omega^2, (\omega^2)^2 = \omega, (\omega^2)^3 = 1]$

2. Fourth roots of unity.

Sol. Let G = fourth roots of unity
$= \{1, -1, i, -i\}$

Here order of group is 4.

$O(1) = 1$

$O(-1) = 2$

$O(i) = 4$

$O(-i) = 4$

Scanned by CamScanner

3. Let $G=\{0,1,2,3,4,5\}$ w.r.t $+_6$.

Sol. Here order of $G=6$

Here $e=0$

$O(0)=1$

$O(1)=|+_6|+_6+_6|+_6|+_6|=0$

$O(1)=6$

$O(2)=3$

$O(3)=2$

$O(4)=3$

$O(5)=6$

4. Let $G=\{0,1,2,3,4\}$ w.r.t $+_5$.

Sol. Order of $G=5$

Here $e=0$

$O(0)=1$

$O(1)=5$

$O(2)=5$

$O(3)=5$

$O(4)=5$

5. Let $G=\{1,3,7,9\}$ w.r.t X_{10}

Sol. Order of $G=4$

Here $e=1$

$O(1)=1$

$O(3)=4$ $[\because 3^1=3, 3^2=9, 3^3=27, 3^4=81]$

$O(7)=4$ $[\because 7^1=7, 7^2=49, 7^3=343, 7^4=2401]$

$O(9)=2$ $[\because 9^1=9, 9^2=81]$

6. Find the order of elements in $U(6)$

Sol. Here $U(6)=\{1,5\}$ and X_6 is the binary operation.

Here $e=1$

$O(1)=1$

$O(5)=2$ $[5X_6 5=1]$

Scanned by CamScanner

7. Find the order of element in $U(10)$

Soy. Here $U(10) = \{1,3,7,9\}$ and $\times_{10}$ is the binary operation.

Here $e = 1$

$O(1) = 1$

$O(3) = 4$

$O(7) = 4$

$O(9) = 2$

(16)

Subgroup: Let $(G, \cdot)$ be a group and H be a non empty subset of G is said to be a sub-group of G if H itself is a group with same binary operation.

Note: 1) Binary operation in G & H are same.

2) Identity element in a G & H are same.

3) Inverse of an element in G & H are same.

2/2/18 Imp D

Theorem: Two step sub-group test:

Statement: A non-empty subset H of a group G is a sub-group of G and if and only if

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

ii) $a \in H \Rightarrow \bar{a}^1 \in H$

Proof: Let $(G, \cdot)$ be a group and H is a non-empty subset of G.

First suppose that H is a sub-group of G.

Now we prove (i) & (ii).

By closure property $a, b \in H \Rightarrow ab \in H$

By inverse property $a \in H \Rightarrow \bar{a}^1 \in H$.

Conversly suppose (i) & (ii)

Now we prove H is a sub-group of G.

From (i) closure property is satisfied.

Let $a, b, c \in H \subseteq G$, G satisfies associative property.

$\Rightarrow H$ satisfies associative property.

Let $a \in H$, by (ii) $\bar{a}^1 \in H$

$a \in H, \bar{a}^1 \in H \Rightarrow a\bar{a} \in H = e \in H$

Scanned by CamScanner

∴ Identity is satisfied.
from (ii) inverse property is satisfied.
∴ $(H,\cdot)$ is a sub-group of G.

Theorem: One step sub-group test:

Statement: A non-empty subset H of a group G is a sub-group if and only if

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

Proof: Let $(G,\cdot)$ be a group and H is a non-empty subset of G.

First suppose that H is a sub-group of G.

Now we prove $a,b \in H \Rightarrow ab^{-1} \in H$.

$b \in H \Rightarrow$ by inverse property $b^{-1} \in H$

$a \in H, b^{-1} \in H \Rightarrow$ by closure property $ab^{-1} \in H$.

Conversely suppose $a,b \in H \Rightarrow ab^{-1} \in H$

Now we prove H is a sub-group of G.

Let $a \in H, a \in H \Rightarrow aa^{-1} \in H = e \in H$

∴ Identity property satisfies.

Let $e \in H, a \in H \Rightarrow ea^{-1} \in H = a^{-1} \in H$

∴ Inverse property satisfies.

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

∴ closure property satisfies.

Let $a,b,c \in H \leq G$, G satisfies associative property

∴ $(H,\cdot)$ is a sub-group of G.

Scanned by CamScanner

3/2/18

Imp **Problems:**

1. Let G be an abelian group with identity e. PT $H=\{x\in G / x^2=e\}$ is a sub-group of G.

Sol: Given G is an abelian group and $H=\{x\in G/x^2=e\}$

Since $e^2=e \Rightarrow e\in H$, H is non empty. (1)

Let $a,b\in H \Rightarrow a^2=e,\ b^2=e$

Now we prove $ab^{-1}\in H$

Consider $(ab^{-1})^2 = (a^2)(b^{-1})^2 = e(b^2)^{-1}$

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

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

$\therefore H$ is a sub-group of G.

---

2. Let (H,K) be two sub-groups of G then $H\cap K$ is also a sub-group of G.

D

Sol: Given (H,K) are two sub-groups of G.

Now we prove $H\cap K$ is also a sub-group of G.

Since $e\in H,\ e\in K \Rightarrow e\in H\cap K$.

$\therefore H\cap K$ is non-empty

Let $a,b\in H\cap K \Rightarrow a,b\in H$ and $a,b\in K$

H is a sub-group $i\ a,b\in H \Rightarrow ab^{-1}\in H$ — ①

K is a sub-group of G; $a,b\in K \Rightarrow ab^{-1}\in K$ — ②

from ① & ②

$ab^{-1}\in H\cap K$

$\therefore H\cap K$ is a sub-group of G.

---

3. Let (H,K) be two sub-groups of an abelian group G then $HK=\{hk/h\in H, k\in K\}$ is a sub-group of G.

Sol: Given (H,K) be two sub-groups of G and $HK=\{hk/h\in H, k\in K\}$.

Now we prove HK is a sub-group of G

Since $e\in HK$ where $e\in H,\ e\in K$.

$\therefore HK$ is non empty

Let $a,b\in HK$ where $a=h_1k_1,\ b=h_2k_2$

$h_1,h_2\in H,\ k_1,k_2\in K$

Consider $ab^{-1} = (h_1k_1)(h_2k_2)^{-1}$

$= h_1(k_1h_2^{-1})k_2^{-1}$ ($\because G$ is abelian)

$= h_1(h_2^{-1}k_1)k_2^{-1}$

Scanned by CamScanner

$= (h_1 h_2^{-1})(k_1 k_2^{-1})$

$= \in HK$

$\because h_1, k_1 \in H$ and H is sub-group

$\Rightarrow h_1 h_2^{-1} \in H$, $k_1 k_2^{-1} \in K$

$\therefore HK$ is a sub-group of G.

6/2/18

4. Let G be an abelian group. P.T $H = \{x \in G / |x| \text{ is finite}\}$ or $o(x)$ is a sub-group of G.

Sol: Given G is an abelian group and $H = \{x \in G / |x| \text{ is finite}\}$

Now we prove H is a sub-group of G.

Since $o(e)$ is 1 finite $\Rightarrow e \in H$

$\therefore H$ is non-empty.

Let $a, b \in H$ and $|a| = n$, $|b| = m$

$\Rightarrow a^n = e$, $b^m = e$

Consider $(ab^{-1})^{nm} = a^{nm} \cdot (b^{-1})^{nm}$

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

$= e^m ((b^m)^{-1})^n$

$= e^m e^{-n}$

$= e$

$\therefore |ab^{-1}| = nm$ which is finite

$\therefore ab^{-1} \in H$

$\therefore H$ is a sub-group of G.

D

Imp

Theorem: Finite Sub-group test:

Statement: The necessary and sufficient condition for a non-empty finite sub-set H ~~of G~~ is a sub-group of G if $a, b \in H \Rightarrow ab \in H$.

Proof: Given G is a finite group and H is a non-empty subset of G.

G is finite $\Rightarrow H$ is finite

First suppose that H is a sub-group of G.

Scanned by CamScanner

By closure property $ab \in H$

Conversly suppose $ab \in H$

Now we prove H is a sub group of G.

$ab \in H \Rightarrow$ closure property is satisfied.

let $a, b, c \in H \subseteq G$, G satisfies associative property $\Rightarrow$ H satisfies associative property.

$a \in H$

$a, a \in H \Rightarrow a^2 \in H$

$a^2, a \in H \Rightarrow a^3 \in H$

$\Rightarrow a^n \in H$ - - -

i.e, $\{a, a^2, a^3 - - - a^n - - -\} \in H$ and since H is finite there must be repeatition in the collection of elements.

let $a^r = a^s$ for $r > s$

multiply with $\bar{a}^s$ on both sides

$\Rightarrow a^r \bar{a}^s = a^s \bar{a}^s$

$\Rightarrow a^{r-s} = a^{s-s} = a^0 = 1 = e$

$r > s \Rightarrow r - s > 0 \Rightarrow a^{r-s} \in H \Rightarrow e \in H$

Identity property is satisfied.

$r > s \Rightarrow r - s > 0 \Rightarrow r - s \geq 1 \Rightarrow r - s - 1 \geq 0 \Rightarrow a^{r-s-1} \in H$

Let $a \in H \exists a^{r-s-1} \in H \ni a(a^{r-s-1}) = a^{r-s} = e$.

$\therefore a^{r-s-1}$ is the inverse of a.

$\therefore$ H is a sub-group of G.

7/2/18 **Generated by 'a' :**

Let G be a group and $a \in G$ then generated by a is denoted as $\langle a \rangle = \{a^n / n \in Z\}$.

Ex: 1. In Z_{10} find the generator of 2 w.r.t $+$.

Sol. $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, binary operation is $+_{10}$

$\langle 2 \rangle \Rightarrow 1 \cdot 2 = 2$

$2 \cdot 2 = 4$

$3 \cdot 2 = 6$

$4 \cdot 2 = 8$

$5 \cdot 2 = 0$

$6 \cdot 2 = 2$

$7 \cdot 2 = 4$

$8 \cdot 2 = 6$

$9 \cdot 2 = 8$

$10 \cdot 2 = 0$

Scanned by CamScanner

$\therefore \langle 2 \rangle = \{2, 4, 6, 8, 0\}$

$\langle 6 \rangle \Rightarrow 1 \cdot 6 = 6 \quad 6 \cdot 6 = 6$

$2 \cdot 6 = 2 \quad 7 \cdot 6 = 2$

$3 \cdot 6 = 8 \quad 8 \cdot 6 = 8$

$4 \cdot 6 = 4 \quad 9 \cdot 6 = 4$

$5 \cdot 6 = 0 \quad 10 \cdot 6 = 0$

$\therefore \langle 6 \rangle = \{6, 2, 8, 4, 0\}$

2. In U(10) find the generators of 3.

Sol. $U(10) = \{1, 3, 7, 9\}$, binary operation is $\times_{10}$

$\langle 3 \rangle \Rightarrow 3^1 = 3 \quad 3^6 = 9$

$3^2 = 9 \quad 3^7 = 7$

$3^3 = 7 \quad 3^8 = 1$

$3^4 = 1 \quad 3^9 = 3$

$3^5 = 3 \quad 3^{10} = 9$

$\therefore \langle 3 \rangle = \{3, 9, 7, 1\}$

3. In $Z_{20} \langle 8, 14 \rangle$ w.r.t $+_{20}$.

Sol. $Z_{20} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$; $+_{20}$.

$\langle 8 \rangle \Rightarrow 1 \cdot 8 = 8 \quad 6 \cdot 8 = 8$

$2 \cdot 8 = 16 \quad 7 \cdot 8 = 16$

$3 \cdot 8 = 4 \quad 8 \cdot 8 = 4$

$4 \cdot 8 = 12 \quad 9 \cdot 8 = 12$

$5 \cdot 8 = 0 \quad 10 \cdot 8 = 0$

$\therefore \langle 8 \rangle = \{8, 16, 4, 12, 0\}$

$\langle 14 \rangle \Rightarrow 1 \cdot 14 = 14 \quad 6 \cdot 14 = 4$

$2 \cdot 14 = 8 \quad 7 \cdot 14 = 18$

$3 \cdot 14 = 2 \quad 8 \cdot 14 = 12$

$4 \cdot 14 = 16 \quad 9 \cdot 14 = 6$

$5 \cdot 14 = 10 \quad 10 \cdot 14 = 0$

$\therefore \langle 14 \rangle = \{14, 8, 2, 16, 10, 4, 18, 12, 6, 0\}$

$\therefore Z_{20} \langle 8, 14 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$

Scanned by CamScanner

Problems:

1. P.T $\langle a \rangle$ is a sub-group of G.

Sol: Given $(G, \cdot)$ is a group and $a \in G$.

Clearly $1 = a^0 \in \langle a \rangle$

$\therefore \langle a \rangle$ is non-empty

Let $a^m, a^n \in \langle a \rangle$

Consider $a^m \cdot (a^n)^{-1} = a^m a^{-n}$

$= a^{m-n} \in \langle a \rangle$

$\therefore \langle a \rangle$ is a sub-group of G.

8/2/18

3. Cyclic Groups.

Defination:

Let $(G, \cdot)$ be a group, $a \in G$. G is said to be a cyclic group if every element of G is of the form a^n where $n \in Z$ then G is said to be a cyclic group generated by 'a'.

Examples:

1. The multiplicative group $G = \{1, -1, i, -i\}$ is a cyclic group $\langle i \rangle$ i.e, i^4, i, i^2, i^3.

2. $G = \{1, \omega, \omega^2\}$ under binary operation $(\cdot)$. is a cyclic group $\langle \omega \rangle$ i.e, $\omega^3, \omega, \omega^2$

3. $G = \{0, 1, 2, 3, 4, 5\}$ under operation $+_6$

Here G is a cyclic group $\langle 5 \rangle$ & $\langle 1 \rangle$

$\langle 5 \rangle \Rightarrow 1 \cdot 5 = 5 \quad 6 \cdot 5 = 0$

$2 \cdot 5 = 4$

$3 \cdot 5 = 3$

$4 \cdot 5 = 2$

$5 \cdot 5 = 1$

$\therefore G = \langle 5 \rangle, \langle 1 \rangle$

4. $G = \{0, 1, 2, 3\}$ under X_4. Is cyclic or not.

$\therefore$ G is not a cyclic group

Scanned by CamScanner

5. $U(10)$ is a cyclic group or not.

$U(10) = \{1, 3, 7, 9\}$, binary operation $\times_{10}$.

$\langle 3 \rangle \Rightarrow 3^1 = 3$
$3^2 = 9$
$3^3 = 7$
$3^4 = 1$
$\therefore 3$ is a generator

$\langle 7 \rangle \Rightarrow 7^1 = 7$
$7^2 = 9$
$7^3 = 3$
$7^4 = 1$
$\therefore 7$ is a generator

$\langle 9 \rangle \Rightarrow 9^1 = 9$
$9^2 = 1$
$9^3 = 9$
$\therefore 9$ is not a generator.

$\therefore G$ is a cyclic group generator by 3 & 7.

12/18 **Properties of Cyclic Group:**

Imp **Theorem-1:**

Statement: let G be a group and $a \in G$

i) If a has infinite order then $a^i = a^j \Leftrightarrow i = j$

ii) If a has finite order then $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$ and $a^i = a^j \Leftrightarrow n$ divides $i-j$.

Proof: Given G is a group and $a \in G$.

i) let $O(a)$ is infinite order

Consider $a^i = a^j$

$\Leftrightarrow$ multiply on b.s with a^{-j}.

$\Leftrightarrow a^i \cdot a^{-j} = a^j \cdot a^{-j}$

$\Leftrightarrow a^{i-j} = a^{j-j} = a^0 = 1 = e$

$\Leftrightarrow i - j = 0$ ($\because a$ is of infinite order)

$\Leftrightarrow i = j$

ii) let $O(a)$ is finite and equal to 'n'.

Now we prove $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$

let a^k be an arbitary number.

By division algorithm $\exists$ integers $(q, r) \ni k = nq + r$ where $0 \le r < n$.

Scanned by CamScanner

Consider $a^k = a^{nq+r}$

$= a^{nq} \cdot a^r$

$= (a^n)^q \cdot a^r$

$= e^q \cdot a^r$

$a^k = a^r \in \langle a \rangle$

$\therefore \langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$

Consider $a^i = a^j$

multiply with $\bar{a}^j$'s

$a^i \cdot \bar{a}^j = a^j \cdot \bar{a}^j$

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

$a^{i-j} = e$

By division algorithm $\exists$ integers $(q, r) \in Z$

$i-j = nq+r$ where $0 \le r < n$.

Consider $a^{i-j} = a^{nq+r}$

$= a^{nq} \cdot a^r$

$a^{i-j} = a^r = e$ which is not possible $(\because r < n)$

$\therefore r$ must be 0

$\Rightarrow i-j = nq$

$\Rightarrow n$ divides $i-j$

Conversly suppose n divides $i-j$

$\Rightarrow i-j = nq$

$a^{i-j} = a^{nq}$

$a^i \cdot \bar{a}^j = (a^n)^q = e^q = e$

$a^i \cdot \bar{a}^j = e$

$a^i = a^j$

Satur 10/2/18

Note:

Let G be a group, $a \in G$ and $O(a) = O(\langle a \rangle)$ ~~n if $a^k = e$~~

Corollary:

1. Let G be a group, $a \in G$ and $O(a) = n$ if $a^k = e$ then n/k.

Proof: Given G is a group, $a \in G$, $O(a) = n$ a finite number.

Scanned by CamScanner

We know that "if $O(a)$ is a finite number, $a^i = a^j \Leftrightarrow n/i-j$"

$\Rightarrow$ Given $a^k = e = 1$

$a^k = 1$

$a^k = a^0$

$\therefore n/k-0 \Rightarrow n/k$

---

2. If $a, b \in G$, G is a finite group and $ab = ba$ then $|ab| / |a| \cdot |b|$.

Sol: Given, G is a finite group, $ab \in G$ and $ab = ba$.

Let $|a| = m$, $|b| = n$

$\Rightarrow a^m = e$, $b^n = e$

Consider $(ab)^{mn} = a^{mn} \cdot b^{mn}$

$= (a^m)^n \cdot (b^m)^n$

$= e^n \cdot e^m$

$(ab)^{mn} = e$

We know that "if $a^k = e$ then n/k where n is $O(a)$"

$|ab| / mn$.

$\Rightarrow |ab| / |a| \cdot |b|$

Φ

Scanned by CamScanner

imp **Problems:**

1. If $O(a)=30$ find $\langle a^{26}\rangle$, $\langle a^{17}\rangle$, $\langle a^{18}\rangle$ and $|a^{26}|, |a^{17}|, |a^{18}|$.

Sol: Given, $|a|=30$.

(i) $\langle a^{26}\rangle$

GCD of $(30, 26)=2$

$\therefore \langle a^{26}\rangle = \langle a^2\rangle$

$= \{a^0, a^2, a^4, a^6 \ldots a^{28}\}$

$|a^{26}| = \frac{30}{2} = 15$

(26)

```
26)30(1
   26
   4)26(6
     24
     2)4(2
       4
       0
```

(ii) $\langle a^{17}\rangle$

GCD of $(30, 17)=1$

$\langle a^{17}\rangle = \langle a^1\rangle$

$= \{a^0, a^1, a^2, a^3, \ldots a^{29}\}$

$|a^{17}| = \frac{30}{1} = 30$

```
17)30(1
   17
   13)17(1
      13
      4)13(3
        12
        1)4(4
          4
          0
```

(iii) $\langle a^{18}\rangle$

GCD of $(30, 18)=6$

$\langle a^{18}\rangle = \langle a^6\rangle$

$= \{a^0, a^6, a^{12}, \ldots a^{24}\}$

$|a^{18}| = \frac{30}{6} = 5$

```
18)30(1
   18
   12)18(1
      12
      6)12(2
        12
        0
```

Scanned by CamScanner

2. If $|a|=1000$ find $\langle a^{185}\rangle, \langle a^{400}\rangle, \langle a^{62}\rangle$ and $|a^{185}|, |a^{400}|$, $|a^{62}|$.

Sol: Given $|a|=1000$

(i) $\langle a^{185}\rangle$

GCD of $(1000, 185)$ = GCD of $(2^3 5^3, 2^2 5^2 + 5 \cdot 17)$

$= 2^2 \times 5$ (Take common from both (1000 & 185) $\Rightarrow 2^2$ & 5 are common)

$= 20$

Another method

gcd(1000, 185)

$\Rightarrow$ gcd(1000, 185) = 5

$1000 = 2^3 5^3$

$2^2 5^2 = 100$

$17 \cdot 5 = 85$

$\therefore 185 = 2^2 5^2 + 85$

185)1000(5
925

$\langle a^{185}\rangle = \langle a^{20}\rangle$

$\langle a^{185}\rangle = \{a^0, a^5, a^{10}, \ldots\}$

$= \{a^0, a^{20}, a^{40}, \ldots a^{980}\}$

$|a^{185}| = \frac{1000}{5} = 200$

$|a^{185}| = \frac{1000}{20} = 50.$

(ii) $\langle a^{400}\rangle$

400)1000(2
800
200)400(2
400
0

GCD of $(1000, 400)$ = GCD of $(2^3 5^3, 2^4 5^2)$

$= 2^3 \times 5^2$

$= 200$

gcd(1000, 400) = 200

$\therefore \langle a^{400}\rangle = \{a^0, a^{200}, a^{400}, a^{600}, a^{800}, a^{1000}\}$

$|a^{400}| = \frac{1000}{200} = 5$

$\therefore \langle a^{400}\rangle = \langle a^{200}\rangle$

$= \{a^0, a^{200}, a^{400}, \ldots a^{800}\}$

$|a^{400}| = 5$

$|a^{400}| = \frac{1000}{200} = 5$

(iii) $\langle a^{62}\rangle$

GCD of $(1000, 62)$ = GCD of $(2^3 5^3, 2 \cdot 31)$

$= 2$

gcd$\langle 1000, 62\rangle = 2$

$\Rightarrow \langle a^{62}\rangle = \{a^0, a^2, \ldots a^{998}\}$

$|a^{62}| = \frac{1000}{2} = 500$

62)1000(16
62
380
372
8

$\therefore \langle a^{62}\rangle = \langle a^2\rangle$

$= \{a^0, a^2, a^4 \ldots a^{998}\}$

$|a^{62}| = 1000/2 = 500$

Scanned by CamScanner

12/2/18.

Theorem 2:

Statement: Let G be a group, $a \in G$ and k positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$

Proof: Given G is a group, $a \in G$, $o(a) = n$ and $k \in Z^+$.

Let $d = \gcd(n,k)$ and $k = dr$

Now we prove $\langle a^k \rangle = \langle a^d \rangle$

Consider $a^k = a^{dr} = (a^d)^r \in \langle a^d \rangle$

$\therefore \langle a^k \rangle \subseteq \langle a^d \rangle$ — ①

$d = \gcd(n,k)$

$\Rightarrow \exists\ s,t \in Z \ni d = ns + kt$

$\gcd(m,n) = 1$
$1 = mx + ny$
where $x, y \in Z$.

Consider $a^d = a^{ns+kt}$

$= a^{ns} \cdot a^{kt}$

$= (a^n)^s (a^k)^t$

$= e (a^k)^t$

$= (a^k)^t \in \langle a^k \rangle$

$\therefore \langle a^d \rangle \subseteq \langle a^k \rangle$ — ②

from ① & ②

$\Rightarrow \langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

To prove 2 $|a^d| = n/d$

Consider $(a^d)^{n/d} = a^n = e$

$|a^d| = n/d$ — ③ $\Rightarrow |a^k| = n/d$ $(\because \langle a^k \rangle = \langle a^d \rangle \Rightarrow |a^k| = o(d))$ $|a^k| = \frac{n}{\gcd(n,k)}$

Consider $|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle|$ $(\because \langle a^k \rangle = \langle a^d \rangle)$

$= |\langle a^{\gcd(n,k)} \rangle|$ (from ①)

$= |a^{\gcd(n,k)}|$

$= n / \gcd(n,k)$ (from ③)

$\therefore |a^k| = n/\gcd(n,k)$

Scanned by CamScanner

15/2/18

Theorem 3: Fundamental Theorem on Cyclic Groups:

Statement: Every sub-group of cyclic group is cyclic.

Proof: Let G be a cyclic group $\langle a \rangle$ and H be a sub-group of G.

Now we prove H is a cyclic group

$H \subseteq G$, G is $\langle a \rangle$

$\Rightarrow$ Elements of H can be expressed as a^n for some $n \in Z$.

Let d be the smallest of the integers $\ni a^n \in H$.

Now we prove $H = \langle a^d \rangle$

Let $a^m \in H$ ①

By division algorithm $\exists\ q, r \in Z \ni m = dq + r$; $0 \le r < d$

Consider $a^m = a^{dq+r}$

$= a^{dq} \cdot a^r$

$a^{dq} = (a^d)^q \in H$

by inverse property $a^{-dq} \in H$.

$a^m \in H$, $a^{-dq} \in H$ by closure property $a^m \cdot a^{-dq} \in H \Rightarrow a^{m-dq} \in H$

$\Rightarrow a^r \in H$

[from ① which is not possible $\because r < d$]

$\therefore r = 0$

from ① $m = dq$

$\therefore a^m = (a^d)^q$

$H = \langle a^d \rangle$

$\therefore$ H is a cyclic group

Hence every sub-group of a cyclic group is cyclic.

Theorem-4:

Statement: Every cyclic group is abelian.

Proof: Given G is a cyclic group $\langle a \rangle$

i.e, $G = \{a^n / n \in Z\}$

Now we prove G is abelian group.

Let $a^r, a^s \in G$ where $r, s \in Z$

Consider $a^r \cdot a^s = a^{r+s}$

$= a^{s+r}$ [$\because r, s \in Z$; Z satisfies commutative w.r.t +]

$= a^s \cdot a^r$

Scanned by CamScanner

∴ G is an abelian

Hence every cyclic group is abelian.

Problems:

1. Find the no. of elements of the cyclic sub group of $(Z_{30}, +_{30})$ $\langle 25 \rangle$.

Sol: $|Z_{30}| = 30$, $+_{30}$ is a binary operation

GCD of 25, 30 = 5

$\langle a^{25} \rangle = \langle a^5 \rangle$

$= \{a^0, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$

$|a^{25}| = 30/5 = 6$

(30)

25)30(1
25
5)25(5
25
0

---

2. Find the no. of elements of the cyclic sub-group of $(Z_{42}, +_{42})$ $\langle 30 \rangle$.

Sol: $|z| = 42$, $+_{42}$ is a binary operation.

GCD of 30, 42 = 6

$\langle 30 \rangle = \langle a^6 \rangle$

$= \{a^0, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}\}$

$|a^{30}| = 42/6 = 7$

30)42(1
30
12)30(2
24
6)12
12
0

Scanned by CamScanner

16/2/18

4. Permutations.

Permutation: Let S be a non-empty finite set and a $f: S \to S$ is said to be a permutation if f is one-one and onto (bijection).

Ex: Let $S = \{1,2,3,4,5\}$ the permutation f is denoted as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

(31)

Equal permutations: Two permutations f, g are said to be equal permutations if $f(a) = g(a)\ \forall\ a \in S$

Ex: $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $g = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix}$

$\therefore f = g$

Identity permutation: A permutation f is said to be an identity permutation if $f(a) = a\ \forall\ a \in S$.

Ex: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Inverse of a permutation: If $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ is a permutation then the inverse of f is

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

Product of permutations:

Ex: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$, find

$f \cdot g$, $g \cdot f$.

Sol: $f \cdot g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$

$g \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}$

$\therefore f \cdot g \neq g \cdot f$

Scanned by CamScanner

Orbit of 6: $f^1(6) = 4$

$f^2(6) = 5$

$f^3(6) = 6$

$\therefore$ orbit of $6 = \{4, 5, 6\}$

$\therefore$ The cycles of the permutation f are $(1\,2)(3)(4\,5\,6)$

Ex: Find the orbits of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$ and order of permutation.

Sol: $\sigma^2 = \sigma \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 6 & 7 & 8 \end{pmatrix}$ (34)

$\sigma^3 = \sigma^2 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 3 & 2 & 6 & 8 & 7 \end{pmatrix}$

$\sigma^4 = \sigma^3 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 5 & 3 & 6 & 7 & 8 \end{pmatrix}$

$\sigma^5 = \sigma^4 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix}$

$\sigma^6 = \sigma^5 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 7 & 8 \end{pmatrix}$

$\sigma^7 = \sigma^6 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 6 & 8 & 7 \end{pmatrix}$

$\sigma^8 = \sigma^7 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 3 & 2 & 6 & 7 & 8 \end{pmatrix}$

$\sigma^9 = \sigma^8 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 5 & 3 & 6 & 8 & 7 \end{pmatrix}$

$\sigma^{10} = \sigma^9 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$

$\therefore$ The order of permutation is 10.

$\therefore \sigma^{10} = I$

orbit of 1: $f^1(1) = 2$

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

$f^3(1) = f(3) = 5$

$f^4(1) = f(5) = 4$

$f^5(1) = f(4) = 1$

$\therefore$ orbit of $1 = \{2, 3, 5, 4, 1\}$

Scanned by CamScanner

orbit of 2: $f^1(2)=3$, $f^2(2)=5$, $f^3(2)=4$, $f^4(2)=1$, $f^5(2)=2$

$\therefore$ orbit of $2=\{3,5,4,1,2\}$

orbit of 3: $f^1(3)=5$, $f^2(3)=4$, $f^3(3)=1$, $f^4(3)=2$, $f^5(3)=3$

$\therefore$ orbit of $3=\{5,4,1,2,3\}$

orbit of 4: $f^1(4)=1$, $f^2(4)=2$, $f^3(4)=3$, $f^4(4)=5$, $f^5(4)=4$

$\therefore$ orbit of $4=\{1,2,3,5,4\}$

orbit of 5: $f^1(5)=4$, $f^2(5)=1$, $f^3(5)=2$, $f^4(5)=3$, $f^5(5)=5$

$\therefore$ orbit of $5=\{4,1,2,3,5\}$

orbit of 6: $f^1(6)=6$

$\therefore$ orbit of $6=\{6\}$

orbit of 8: $f^1(8)=7$, $f^2(8)=8$

$\therefore$ orbit of $8=\{7,8\}$

35

orbit of 7: $f^1(7)=8$, $f^2(7)=7$

$\therefore$ orbit of $7=\{8,7\}$

$\therefore$ The cycles of the permutation 'σ' are $(1\,2\,3\,4\,5)(6)(7$

28/2/18 **Transposition:** A cycle of length 2 is called a transpositi

Even and odd permutation:

A permutation is said to be an even (odd) permut if it can be expressed as product of even (odd) numbe of permutation.

Ex: Verify whether the following permutations are even (o

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

Sol: Given $f=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$

The cycles of the permutation f are $(1\,3\,4\,5\,6\,7)($

$\Rightarrow (17)(16)(15)(14)(13)$

$\therefore$ f is odd permutation.

Scanned by CamScanner

2. (1 2 3 4 5) (1 2 3) (4 5)

Sol: (1 5) (1 4) (1 3) (1 2) (1 3) (1 2) (4 5)

$\Rightarrow$ (1 5) (1 4) (1 3) (1 2) (4 5)

$\therefore$ f is odd permutation

Permutation group:

The set of all permutations forms a group called permutation group w.r.t the operations composition of mappings.

Problems:

1. Find the orders of symmetric group S_7.

Sol: Given S_7, the no. of elements in S_7 are 7! (36)

$\Rightarrow 7! = 5 \times 4 \times 3 \times 2 \times 1$

$= 5040$

Consider (7)

(6) (1)

(5) (2)

(5) (1) (1)

(4) (3)

(4) (2) (1)

(4) (1) (1) (1)

(3) (3) (1)

(3) (2) (2)

(3) (2) (1) (1)

(3) (1) (1) (1) (1)

(2) (3) (2)

(2) (3) (1) (1)

(2) (1) (1) (1) (1) (1)

(1) (1) (1) (1) (1) (1) (1)

$\therefore$ The order of S_7 are {7, 6, 10, 5, 12, 4, 3, 2, 1}

Scanned by CamScanner

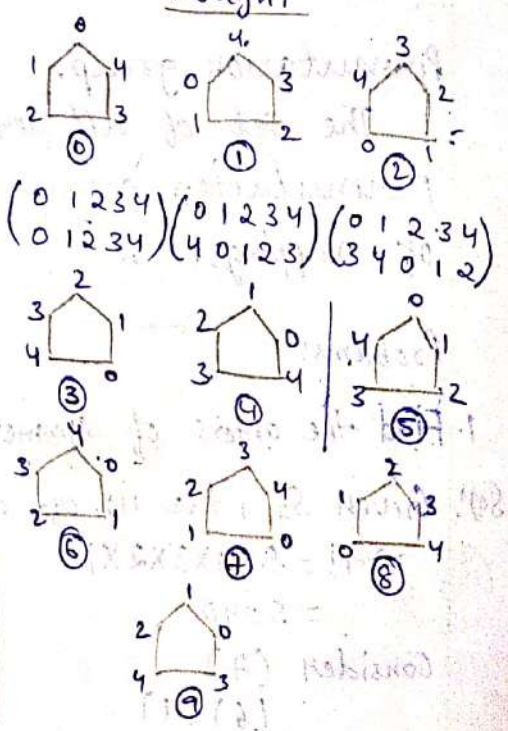
A check digit scheme on D_5:

Composition table:

The number elements in D_5 are $\{0,1,2,3,4,5,6,7,8,9\}$

Here 0,1,2,3,4 are rotations and 5,6,7,8,9 are reflections

Rough:



$\begin{pmatrix}0&1&2&3&4\\0&1&2&3&4\end{pmatrix}$ $\begin{pmatrix}0&1&2&3&4\\4&0&1&2&3\end{pmatrix}$ $\begin{pmatrix}0&1&2&3&4\\3&4&0&1&2\end{pmatrix}$

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

(31)

Scanned by CamScanner

Composition table for permutation:

$\sigma = (0\ 1\ 5\ 8\ 9\ 4\ 2\ 7)(3\ 6)$

Rough:

$$\sigma = \begin{pmatrix} 0 & 1 & 5 & 8 & 9 & 4 & 2 & 7 & 3 & 6 \\ 1 & 5 & 8 & 9 & 4 & 2 & 7 & 0 & 6 & 3 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 0 & 1 & 5 & 8 & 9 & 4 & 2 & 7 & 3 & 6 \\ 5 & 8 & 9 & 4 & 2 & 7 & 0 & 1 & 3 & 6 \end{pmatrix} \cdots \sigma^9$$

Composition table 2;

$*$	0	1	5	8	9	4	2	7	3	6
σ	1	5	8	9	4	2	7	0	6	3
σ^2	5	8	9	4	2	7	0	1	3	6
σ^3	8	9	4	2	7	0	1	5	6	3
σ^4	9	4	2	7	0	1	5	8	3	6
σ^5	4	2	7	0	1	5	8	9	6	3
σ^6	2	7	0	1	5	8	9	4	3	6
σ^7	7	0	1	5	8	9	4	2	6	3
σ^8	0	1	5	8	9	4	2	7	3	6
σ^9	1	5	8	9	4	2	7	0	6	3
σ^{10}	5	8	9	4	2	7	0	1	3	6
σ^{11}	8	9	4	2	7	0	1	5	6	3

38

Problems:

1. Append the check digit to 4 5 7 2 3 :-

Sol: Here $a_1=4$, $a_2=5$, $a_3=7$, $a_4=2$, $a_5=3$.

Consider $\sigma(a_1)\cdot\sigma^2(a_2)\cdot\sigma^3(a_3)\cdot\sigma^4(a_4)\cdot\sigma^5(a_5)\cdot a_6=0$

$\Rightarrow \sigma(4)\cdot\sigma^2(5)\cdot\sigma^3(7)\cdot\sigma^4(2)\cdot\sigma^5(3)\,a_6=0$

$2\cdot 9\cdot 5\cdot 5\cdot 6\cdot a_6=0$

$6\cdot 0\cdot 6\cdot a_6=0$

$6\cdot 6\cdot a_6=0$

$0\cdot a_6=6$. (On two row a_6 value)

Scanned by CamScanner

2. Check digit for 3 6 7 5 1

Sol: Here $a_1=3, a_2=6, a_3=7, a_4=5, a_5=1$

Consider $\sigma(a_1)\cdot\sigma^2(a_2)\cdot\sigma^3(a_3)\cdot\sigma^4(a_4)\cdot\sigma^5(a_5)\cdot a_6=0$

$\Rightarrow \sigma(3)\cdot\sigma^2(6)\cdot\sigma^3(7)\cdot\sigma^4(5)\cdot\sigma^5(1)\cdot a_6=0$

$\Rightarrow 6\cdot 6\cdot 5\cdot 2\cdot 2\cdot a_6=0$

$0\cdot 8\cdot 2\cdot a_6=0$

$8\cdot 2\cdot a_6=0$

$6\cdot a_6=0$ (when we got 6 in 6 row)

2/3/18 Letters Values;

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

Problems:

1. Verify that 7 is appropriate check digit for the number AG8536827U on bank note.

Sol: Here number is A G 8 5 3 6 8 2 7 U (7)

$a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}$

Consider $\sigma(A)\sigma^2(G)\sigma^3(8)\sigma^4(5)\sigma^5(3)\sigma^6(6)\sigma^7(8)\sigma^8(2)\sigma^9(7)\sigma^{10}(U)\cdot a_{11}=0$

$\Rightarrow \sigma(0)\cdot\sigma^2(2)\cdot\sigma^3(8)\cdot\sigma^4(5)\cdot\sigma^6(6)\cdot\sigma^7(8)\cdot\sigma^9(7)\cdot\sigma^{10}(7)\cdot a_{11}=0$

$\Rightarrow 1\cdot 0\cdot 2\cdot 2\cdot 6\cdot 6\cdot 5\cdot 2\cdot 0\cdot 7\cdot a_{11}=0$

$0\cdot 8\cdot 1\cdot a_{11}=0$

$7\cdot a_{11}=0$

$\therefore a_{11}=7$

---

2. Let $f=\begin{pmatrix}1&2&3&4&5\\2&3&5&1&4\end{pmatrix}$. find f^{2012}

Sol: $f^2=f\cdot f=\begin{pmatrix}1&2&3&4&5\\3&5&4&2&1\end{pmatrix}$

$f^3=f^2\cdot f=\begin{pmatrix}1&2&3&4&5\\5&4&1&3&2\end{pmatrix}$

$f^4=f^3\cdot f=\begin{pmatrix}1&2&3&4&5\\4&1&2&5&3\end{pmatrix}$

$f^5=f^4\cdot f=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$

Order of $f=5$

Scanned by CamScanner

$(f)^{2012} = (f^5)^{402} \cdot f^2$

$= I f^2 = f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$

$= f^{2012}$

Now divide 2012 with 5

5)2012(402
20
12
10
2

3. $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 0 & 4 & 3 & 5 \end{pmatrix}$. find σ^{3046}

Soln. $\sigma^2 = \sigma \cdot \sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

order = 2

divide 3046 with 2
= 1523

$\sigma^{3046} = (f^2)^{1523} = \underline{I}$

4. let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ find fgf^{-1}

Soln. $f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

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

40

3/3/18 Properties of permutation: — (1)

Def Every permutation of a finite set can be expressed as a cycle i.e, product of disjoint cycles.

Proof: let f be a permutation on S where S is a finite set $S = \{1, 2, 3, \ldots, n\}$

Now we prove f can be expressed as a cycle (or) product of disjoint cycles.

If f is an identity permutation then

$f = (1)(2)(3)\ldots(n)$

If f is not an identity permutation then we choose

$2 = f(1)$

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

$4 = f^3(1)$

!

!

$1 = f^m(1) = f(m)$

we can express the permutation f as

$f = (1\ 2\ 3\ \ldots\ m)$

Scanned by CamScanner

If $f(i)=i \ \forall \ i>m$ then $f=(1\ 2\ 3 \ldots m)$ is a cycle of length 'm'.

If $f(i)\neq i \ \forall \ i>m$ then we choose $i+1=f(i)$

$i+2=f(i+1)=f^2(i)$

$i+3=f^3(i)$

$\vdots$

$i=f^r(i)=f(r)$

So, f can be expressed as $f=(1\ 2\ 3 \ldots m)(i\ i+1\ i+2 \ldots r)$

Continue the process.

$\therefore$ f can be expressed as a cycle (or) product of disjoint cycles.

---

2. Disjoint cycles commutes

let $\alpha=(a_1\ a_2 \ldots a_m)$

$\beta=(b_1\ b_2 \ldots b_n)$ be two disjoint cycles.

$a_i \neq b_j \ \forall \ i \ \& \ j$

Now we prove $\alpha\beta=\beta\alpha$

i.e, we show $(\alpha\beta)(x)=(\beta\alpha)(x)$

Let $S=\{a_1\ a_2 \ldots a_m, b_1\ b_2 \ldots b_n, c_1\ c_2 \ldots c_k\}$

Case i) let $x=a_i$

Consider $(\alpha\beta)(x)=(\alpha\beta)(a_i)$

$=\alpha(\beta(a_i)) \quad (\because a_i \notin \beta)$

$=\alpha(a_i)=a_{i+1}$

Consider $(\beta\alpha)(x)=(\beta\alpha)(a_i)$

$=\beta(\alpha(a_i))$

$=\beta(a_{i+1})$

$=a_{i+1}$

$\therefore (\alpha\beta)(x)=(\beta\alpha)(x)$

$\therefore \alpha\beta=\beta\alpha$

Case ii) let $x=b_i$

Consider $(\alpha\beta)(b_i)=\alpha(\beta(b_i))$

$=\alpha(b_{i+1})$

$=b_{i+1}$

Scanned by CamScanner

Consider $(\beta\alpha)(b_i) = \beta(\alpha(b_i))$
$= \beta(b_{i+1})$
$= b_{i+1}$

$\therefore \alpha\beta = \beta\alpha$

Case iii) Let $x = c_i$

Consider $(\alpha\beta)(x) = (\alpha\beta)(c_i)$
$= \alpha(\beta(c_i))$
$= \alpha(c_i)$
$= c_i$

Consider $(\beta\alpha)(x) = (\beta\alpha)(c_i)$
$= \beta(\alpha(c_i))$
$= \beta(c_i)$
$= c_i$

$\therefore \alpha\beta = \beta\alpha$

$\therefore$ Every disjoint cycles are commutes.

42.

Signature of a permutations:

The signature of a permutation f is

$$Sig(f) = \begin{cases} 1, & \text{if } f \text{ is an even permutation} \\ 0, & \text{if } f \text{ is an odd permutation} \end{cases}$$

3. The set of even permutations is S_n forms a sub-group of S_n.

Proof: Given S_n is a group and let A_n be the set of all even permutations i.e,

$A_n = \{f \in S_n / sig(f) = 1\}$

Now we prove A_n is a sub-group of S_n.

clearly A_n is non-empty since identity permutation $I \in A_n$

Let $\sigma, z \in A_n$

$sig\sigma = 1, sigz = 1$

Consider $sig(\sigma z^{-1}) = sig\sigma \cdot sig z^{-1}$
$= 1 \cdot 1$
$= 1$

$\therefore \sigma z^{-1} \in A_n$

$\therefore A_n$ is a sub-group of S_n.

Scanned by CamScanner

Alternating group:

Alternating group is a set of all even permutations forms a group is called alternating group.

Note: If $|S_n| = n!$ then $|A_n| = \frac{n!}{2}$

12/3/18

Unit-II

1. Cosets and Lagranges Theorem.

Defination:

Let G be a group and H is a sub-group of G then the $aH = \{ah / h \in H\}$ is called a left coset of h in G generated by a.

$Ha = \{ha / h \in H\}$ is called a right coset of h in G generated by a, where $a \in G$.

Note: 1. If the binary operation is '+' then the left coset is $a+H = \{a+h / h \in H\}$

right coset is $H+a = \{h+a / h \in H\}$.

2. If G is abelian then left coset = right coset.

Properties of Cosets:

1. Statement: Let G be a group and H is a sub-group of G. Then

i) $a \in aH$

ii) $aH = H \Leftrightarrow a \in H$

iii) $aH = bH \Leftrightarrow a \in bH$

iv) $aH = bH$ (or) $aH \cap bH = \phi$ (or) Any two left cosets (right coset) are either disjoint or identical.

Proof: Given G is a group and H is a sub-group of G.

i) Consider $a = a \cdot e$ where $e \in H$

$\Rightarrow a \cdot e \in a \cdot H$

$\Rightarrow a \in aH$

Scanned by CamScanner

ii) First suppose that $aH = H$

Now we prove $a \in H$

$a = a \cdot e \in aH = H$

$a \in H$

Conversly suppose $a \in H$

Now we prove $aH = H$

i.e, we prove $aH \subseteq H$, $H \subseteq aH$

let $ah \in aH / h \in H$

$a \in H, h \in H$ by closure property $ah \in H$.

$aH \subseteq H$ — ①

let $a \in H$, Consider $a = a \cdot e \in aH$

$\Rightarrow a \in aH$

$H \subseteq aH$ — ②

from ① & ②

$aH = H$

---

iii) first suppose that $aH = bH$

Now we prove $a \in bH$

$a = a \cdot e \in aH = bH$

$a \in bH$

Conversly suppose $a \in bH$

Now we prove $aH = bH$

Multiply $a \in bH$ with b^{-1} to the left

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

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

$\Rightarrow b^{-1}aH = H$ ($\because$ from (ii))

$\Rightarrow bb^{-1}aH = bH$ (multiply b)

$\Rightarrow eaH = bH$

$\Rightarrow aH = bH$

---

iv) let aH, bH be two left cosets.

If they are disjoint there is nothing to prove.

Suppose if $aH \cap bH \neq \emptyset$

Now we prove $aH = bH$

Consider $c \in aH \cap bH$

$c \in aH$, $c \in bH$

$c = ah_1$, $c = bh_2$ where $h_1, h_2 \in H$

$ah_1 = bh_2$

multiply with h_1^{-1} to right side

Scanned by CamScanner

$ah_1h^{-1} = bh_2h^{-1}$

$a \cdot e = bh_3$

$a = bh_3$ where $h_3 \in H$

$\therefore a \in bH$

$\therefore aH \subseteq bH$ —①

Similarly consider $b \in aH$

$c \in aH \cap bH$

$c \in aH$, $c \in bH$

$c = ah_1$, $c = bh_2$

$ah_1 = bh_2$

multiply with h_2^{-1} to right side

$ah_1h_2^{-1} = bh_2h_2^{-1}$

$a \cdot h_3 = be$

$b = ah_3$ where $h_3 \in H$

$b \in aH$ —②

from ① & ②

$\therefore aH = bH$

v) $aH = bH \Leftrightarrow a^{-1}b \in H$

First suppose that $aH = bH$

Now we prove $a^{-1}b \in H$

Consider $b = be \in bH = aH$

$b \in aH$

multiply with a^{-1} to left side

$a^{-1}b \in a^{-1}aH$

$a^{-1}b \in eH$

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

Conversly suppose $a^{-1}b \in H$

Now we prove $aH = bH$

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

$a^{-1}bH = H$ (by property (iii))

multiply with a to the left side;

$aa^{-1}bH = aH$

$bH = aH$

Scanned by CamScanner

vi) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

First suppose that $Ha = Hb$

Now we prove $ab^{-1} \in H$

Consider $a = e \cdot a \in Ha = Hb$

$a \in Hb$

multiply with b^{-1} to right side

$ab^{-1} \in Hbb^{-1}$

$ab^{-1} \in He$

$ab^{-1} \in H$

Conversely suppose $ab^{-1} \in H$

Now we prove $Ha = Hb$

Consider $ab^{-1} \in H$

$Hab^{-1} = H$ (from (iii))

multiply with b to right side

$Hab^{-1}b = Hb$

$Hae = Hb$

$Ha = Hb$

---

vii) $|aH| = |bH|$

Define a mapping $f : aH \to bH$ as $f(ah) = bh$

where $h \in H$

Now we prove f is well defined, one-one and onto.

One-one & well defined:

Consider $f(ah_1) = f(ah_2)$

$\Leftrightarrow bh_1 = bh_2$

multiply ab^{-1} to left side

$\Leftrightarrow ab^{-1}bh_1 = ab^{-1}bh_2$

$\Leftrightarrow aeh_1 = aeh_2$

$\Leftrightarrow ah_1 = ah_2$

f is well defined and one-one

Onto

Let $bh \in bH$ $\exists$ an element $ah \in aH \ni f(ah) = bh$

$\therefore f$ is onto

$\therefore f$ is a bijection

$\therefore |aH| = |bH|$

Scanned by CamScanner

viii) aH is a subgroup of G if and only if $a \in H$.

Sol. First suppose that aH is a sub-group of G.

Now we prove $a \in H$

Consider $e \in eH$, $e \in aH$

$\Rightarrow e \in aH \cap eH$

Here $aH \cap eH \neq \phi$

$\therefore aH = H$

$\therefore a \in H$ (from (ii))

Conversely suppose $a \in H$

Now we prove aH is a sub-group of G.

$a \in H$ by property (ii)

$aH = H$, H is a sub-group of G.

$\therefore aH$ is also a sub-group of G.

14/3/18

D Lagranges Theorem:

Statement: The order of a sub-group of a finite group divides order of a group.

Proof: Given G is a finite group and H is a sub-group of G.

Since G is finite, H is also finite.

Let $a_1H, a_2H, \ldots a_kH$ be the left cosets of H in G.

Let $|G| = n$ and $|H| = m$

WKT Every left cosets have same no. of elements

i.e, $|a_1H| = |a_2H| \ldots |a_kH| = |H| = m$ [$\because H = eH$]

The left cosets $a_1H, a_2H \ldots a_kH$ induces a partition of G

$G = a_1H \cup a_2H \cup \ldots \cup a_kH$

$|G| = |a_1H| + |a_2H| \ldots + |a_kH|$

$\Rightarrow n = m + m + m + \ldots + m$ (k-times)

$\Rightarrow n = km$

$\Rightarrow k = \frac{n}{m}$

$\Rightarrow \frac{m}{n}$

$\Rightarrow |H| / |G|$

Scanned by CamScanner

The converse of this theorem is not true

Ex: Let $G=\{1,-1,i,-i\}$

$|G|=4$

Let $|H|=2$

Clearly $|H|/|G| = 2/4$

Let $H=\{1,-i\}$ is not a sub-group (closure property is not satisfied)

15/3/18 Little Fermats Theorem:

48

Statement: For every integer 'a' & prime number 'p'.

$$a^p \equiv a \pmod p$$

Proof: Let $a \in Z$ & P is a prime number

By division algorithm $\exists q, r \in Z \ni a = pq + r$

where $0 \le r < p$ (or) we can write $0 \le r \le p-1$

To prove $a^p \equiv a \pmod p$

we prove $a^{p-1} \equiv 1 \pmod p$ if gcd of $(a,p)=1$

Let $\gcd(a,p)=1$

i.e, a & P are relatively prime

If a leaves remainder r where $0 \le r \le p-1$ on dividing by 'p'.

Then $ka, 1 \le k \le p-1$ also leaves remainder from 1 to p-1

i.e, if $a, 2a, 3a \dots (p-1)a$ are taken gives remainder $1, 2, \dots p-1$

$a \times 2a \times 3a \times \dots \times (p-1)a \equiv 1 \cdot 2 \cdot \dots p-1$

$$(p-1)!\, a^{p-1} \equiv (p-1)!$$

$$a^{p-1} \equiv 1 \pmod p$$

$$\frac{a^p}{a} \equiv 1 \pmod p$$

$$a^p \equiv a \pmod p$$

Hence the theorem.

Scanned by CamScanner

Problems on cosets:

1. Find all the left cosets of $\{1, 11\}$ in U_{30}.

Sol: Here $H = \{1, 11\}$ and $G = U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$

$1H = \{1, 11\}$ $\quad$ $17H = 7H$

$7H = \{7, 17\}$ $\quad$ $19H = \{19, 29\}$

$11H = 1H$ $\quad$ $23H = 13H$

$13H = \{13, 23\}$ $\quad$ $29H = 19H$

$\therefore$ The left cosets are $1H, 7H, 13H, 19H$

---

2. Let $H = \{0, \pm 3, \pm 6, \pm 9 \ldots\}$ find the left cosets of H in Z.

Sol: Here $H = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$ and

$G = Z = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$0 + H = H$

$1 + H = \{\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\}$

$-1 + H = \{\ldots -10, -7, -4, -1, 2, 5, 8 \ldots\}$

$2 + H = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\} = -1 + H$

$-2 + H = \{\ldots -8, -5, -2, 1, 4, 7 \ldots\} = 1 + H$

$3 + H = \{\ldots -6, -3, 0, 3, 6, 9 \ldots\} = H$

$-3 + H = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\} = H$

$4 + H = \{\ldots -5, -2, 1, 4, 7, 10 \ldots\} = 1 + H$

$-4 + H = \{\ldots -7, -4, -1, 2, 5, 8 \ldots\} = -1 + H$

$\therefore$ The left cosets of H in G are $H, 1+H, -1+H$

Scanned by CamScanner

16/3/18

2. Normal Sub-groups

ups is again a

Defination:

Let G be a group, H be a sub-group of G, H is be a normal sub-group of G iff $xhx^{-1} \in H$ where $x \in G, h$ and is denoted as $H \triangleleft G$.

Theorems:

Imp D

1. **Statement:** A sub-group H of a group G is normal if and only if $xHx^{-1} = H$.

Proof: Given, G is a group and H is a sub-group of G.

first suppose that $H \triangleleft G$

Now we prove $xHx^{-1} = H$.

~~Take an element~~

let $xhx^{-1} \in xHx^{-1}$ where $h \in H$

$x \in G, h \in H$ by defination of normal sub-group

$\therefore xhx^{-1} \in H$

$\therefore xHx^{-1} \subseteq H$ — ①

~~let $h \in H$~~

from ① $xHx^{-1} \subseteq H$

put $x = x^{-1}$

$\Rightarrow x^{-1}H(x^{-1})^{-1} \subseteq H$

$\Rightarrow x^{-1}Hx \subseteq H$

multiply the eqn with x to left, x^{-1} to right

$\Rightarrow xx^{-1}Hxx^{-1} \subseteq xHx^{-1}$

$\Rightarrow eHe^{-1} \subseteq xHx^{-1}$

$\Rightarrow H \subseteq xHx^{-1}$ — ②

from ① & ②

$\Rightarrow xHx^{-1} = H$

Conversly suppose $xHx^{-1} = H$

Now we prove $H \triangleleft G$

let $x \in G, h \in H$

Consider $xhx^{-1} \in xHx^{-1} = H$

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

$\therefore H \triangleleft G$

$xHx^{-1} \subseteq H$

$H \subseteq xHx^{-1}$

Scanned by CamScanner

Imp 2. **Statement:** Every sub-group of an abelian group is normal.

Proof: Given G is an abelian group and H is a sub-group of G.

Now we prove $H \trianglelefteq G$.

Let $x \in G, h \in H$

Consider $xhx^{-1} = xx^{-1}h$ ($\because G$ is abelian)

$= e.h$

$= h \in H$

$\therefore H$ is a normal sub-group of G.

5)

17/3/18 **Note:**

1. H is a normal sub-group of $G \Leftrightarrow xH = Hx$
2. $HH = H$

Imp 3. **Statement:** Let G be a group and H is a sub-grap of G then $H \trianglelefteq G \Leftrightarrow$ product of 2 left(rt) cosets is again a left(rt) coset.

Proof: Given G is a group and H is a sub-group of G.

First suppose that $H \trianglelefteq G$

Now we prove $Ha \cdot Hb = Hab$

Consider $Ha \cdot Hb = H(aH)b$

$= H(Ha)b$ ($\because H \trianglelefteq G$)

$= (HH)ab$

$= Hab$

$\therefore$ Product of 2 right cosets is again a right coset.

Conversly suppose $Ha \cdot Hb = Hab$

Now we prove $H \trianglelefteq G$

Let $x \in G, h \in H$

Consider $xhx^{-1} = exhx^{-1} \in HxHx^{-1} = Hxx^{-1} = He = H$

$\therefore xhx^{-1} \in H$

$\therefore H \trianglelefteq G$

Scanned by CamScanner

Imp

4. Statement: The intersection of 2 normal sub-groups is again a normal sub-group:

D

Proof: Let H, K be 2 normal sub-groups of G

Now we prove $H \cap K$ is a normal sub-group of G.

Let $x \in G, h \in H \cap K$

$\Rightarrow h \in H, h \in K$

$x \in G, h \in H, H \triangleleft G$

$\Rightarrow xhx^{-1} \in H \quad -①$

$x \in G, h \in K, K \triangleleft G$

$\Rightarrow xhx^{-1} \in K \quad -②$

from ① & ②

$xhx^{-1} \in H \cap K$

$\therefore H \cap K \triangleleft G$

19/3/18

5. Statement: If G is a group and H is a sub-group of index II in G, then $H \triangleleft G$

Proof: G is a group and H is a sub-group of G with index II

Now we prove $H \triangleleft G$

index $H = 2$

$\Rightarrow$ no. of distinct r.cosets = no. of distinct l.cosets = 2

Let $x \in G$

i.e, l.cosets are H, xH & r.cosets are H, Hx.

Case i) If $x \in H$ then $xH = Hx$

$= H \triangleleft G$

Case ii) If $x \notin H$ then Hx is different from H and xH is different from H and $G = H \cup Hx = xH \cup H$

$\Rightarrow Hx = xH \quad = 2$

$\therefore H \triangleleft G$

Scanned by CamScanner

Note:

1. The inverse of an even permutation is even, inverse of an odd permutation is odd.
2. Product of two odd permutations is even, Product of two even permutations is even.
3. If one permutation is odd and one is even it is odd.
4. Every identity permutation is an even permutation.

6. The Alternating group A_n of all even permutation is a normal sub-group of permutation group S_n of n symbols.

Proof: Given S_n be a permutation group and A_n be the set of all even permutations.

Now we prove $A_n \triangleleft S_n$

Let $f \in S_n$, $g \in A_n$.

$\Rightarrow g$ is an even permutation

Case i) If f is an even permutation

Consider fgf^{-1} = even · even · even

= an even permutation

$\therefore fgf^{-1} \in A_n$

$\therefore A_n \triangleleft S_n$

Case ii) If f is an odd permutation then f^{-1} is also odd

gf^{-1} is an odd permutation

fgf^{-1} is an even permutation

$\therefore fgf^{-1} \in A_n$

$\therefore A_n \triangleleft S_n$

Problems:

1. Find A_3 the normal sub-group of S_3.

Sol: $S_3 = 6$

Let $S_3 = \{f_1 f_2 f_3 f_4 f_5 f_6\}$

Let $S = \{a, b, c\}$

$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ $f_2 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$ $f_3 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$

$= I \rightarrow$ even $= (abc) = (ac)(ab) \rightarrow$ even $= (acb) = (ab)(ac) \rightarrow$ even

Scanned by CamScanner

$f_4 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ $f_5 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$ $f_6 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

$= (bc) \to$ odd $= (ac) \to$ odd $= (ab) \to$ odd

$\therefore A_3 = \left\{ \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \right\}$

---

2. Find A_4 the normal sub-group of S_4

Sol: $S_4 = 4! = 24$

$S_4 = \{a, b, c, d\}$

7. Factor group (or) Quotient:

Statement: $H \triangleleft G$, the set $\frac{G}{H}$ of H in G forms a group w.r.t coset multiplication.

Proof: Given G is a group and $H \triangleleft G$

$$\frac{G}{H} = \{aH / a \in G\}$$

Now we prove $\frac{G}{H}$ is a group w.r.t coset multiplication.

Define $Ha \cdot Hb = Hab$

well-defined:

Consider $Ha = Ha_1$; $Hb = Hb_1$

$ea = a = h_1a_1 / h_1 \in H$; $eb = b = h_2b_1 / h_2 \in H$

$$\begin{aligned} Hab &= H(h_1a_1)(h_2b_1) \\ &= Hh_1(a_1h_2)b_1 \\ &= Hh_1(h_2a_1)b_1 \quad (\because a_1h_2 \in a_1H) \\ &= H(h_1h_2)a_1b_1 \\ &= Ha_1b_1 \quad (\because h_1h_2 \in H) \end{aligned}$$

$\therefore$ The coset multiplication is well-defined

closure property:

let $Ha, Hb \in \frac{G}{H}$

$Ha \cdot Hb = Hab \in \frac{G}{H}$

Associative property:

let $Ha, Hb, Hc \in \frac{G}{H}$

Consider $(Ha \cdot Hb) \cdot Hc = Ha \cdot (Hb \cdot Hc)$

$Hab \cdot Hc = Ha \cdot Hbc$

$Habc = Habc$

Identity property:

let $Ha \in \frac{G}{H}$ $\exists$ $He \in \frac{G}{H}$ $\ni$ $Ha \cdot He = Hae = Ha$

$\therefore$ He is the identity

Inverse property:

let $Ha \in \frac{G}{H}$ $\exists$ $Ha^{-1} \in \frac{G}{H}$ $\ni$ $Ha \cdot Ha^{-1} = Haa^{-1} = He$

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

Scanned by CamScanner

$\therefore \frac{G}{H}$ is a group and is called factor group (or) Quotient group.

(5)

8. Statement: Every quotient of an abelian group is abelian.

Proof: Given G is an abelian group

Now we prove $\frac{G}{H}$ is abelian

Let $Ha, Hb \in \frac{G}{H}$

Consider $Ha \cdot Hb = Hab$

$= Hba$ ($\because ab \in G$ & G is abelian)

$Ha \cdot Hb = Hb \cdot Ha$

$\therefore \frac{G}{H}$ is abelian

Problems:

1. Find $\frac{Z}{4Z}$

Sol: $Z = \{0, \pm 1, \pm 2 ----\}$

$4Z = \{0, \pm 4, \pm 8, \pm 12 ----\}$

First we prove $4Z \lhd Z$

let $x \in Z, h \in 4Z$

Consider $x + h + (-x) = h \in 4Z$

$\therefore 4Z \lhd Z$

$\therefore \frac{Z}{4Z}$ is a Quotient group and the elements are

$0 + 4Z = 4Z$

$1 + 4Z = \{---7, -3, 1, 5, 9---\}$

$2 + 4Z = \{----6, -2, 2, 6, 10---\}$

$3 + 4Z = \{----9, -5, -1, 3, 7, 11, ---\}$

$4 + 4Z = \{---8, -4, 0, 4, 8, 12, ---\} = 4Z$

$\therefore \frac{Z}{4Z} = \{4Z, 1+4Z, 2+4Z, 3+4Z\}$

Scanned by CamScanner

2. Let $G = Z_{18}$ and $H = \langle 6 \rangle$. Find $\frac{Z_{18}}{\langle 6 \rangle}$ where this is a quotient grp

Sol: $Z_{18} = \{0, 1, 2, \ldots 17\}$

$H = \langle 6 \rangle = \{0, 6, 12\}$

$\frac{Z_{18}}{\langle 6 \rangle} =$

$0+H = H$ $\quad$ $5+H = \{5, 11, 17\}$

$1+H = \{1, 7, 13\}$ $\quad$ $6+H = \{6, 12, 0\} = H$

$2+H = \{2, 8, 14\}$ $\quad$ $7+H = \{7, 13, 19\}$

$3+H = \{3, 9, 15\}$

$4+H = \{4, 10, 16\}$

$\therefore \frac{Z_{18}}{\langle 6 \rangle} = \{H, 1+H, 2+H, 3+H, 4+H, 5+H\}$

21/3/18

3. Homomorphism And Isomorphism of Groups.

Homomorphism: Let G, G' be two groups. A mapping $f: G \to G'$ is said to be a homomorphism if $f(a \cdot b) = f(a) \cdot f(b)$ where $a, b \in G$ and $f(a), f(b) \in G'$.

Homomorphism into & Homomorphism onto:

A mapping $f: G \to G'$ is said to be homomorphism onto if f satisfies homomorphism and onto properties.

Homomorphism into means f satisfies only homomorphism but not onto.

Note:

In homomorphism the groups G, G' need not be same binary operation.

Isomorphism: A mapping $f: G \to G'$ is said to be an isomorphism if f satisfies homomorphism, one-one and onto properties.

Scanned by CamScanner

Kernel of f:

Let G, G' be two groups and $f: G \to G'$ is a homomorphism then kernel f is the set of elements in G which are mapped to identity of G'. i.e,

$\ker f = \{x \in G / f(x) = e'\}$

Note:

kernel f is non-empty. ($\because e \in \ker f$)

Theorems:

1. **Statement:** Let ϕ be a homomorphism from a group G into a group G' then kernal f is a sub-group of G.

Proof: Given $\phi: G \to G'$ be a homomorphism

Now we prove $\ker f$ is a sub-group of G

let $a, b \in \ker f$

$\Rightarrow f(a) = e' \;,\; f(b) = e'$

Consider $f(ab^{-1}) = f(a) \cdot f(b^{-1})$ [$\because$ f is homomorphism]

$= e' \cdot [f(b)]^{-1}$

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

$f(ab^{-1}) = e'$

$\therefore ab^{-1} \in \ker f$

$\therefore \ker f$ is a sub-group of G.

---

2. **Statement:** Let ϕ be a homomorphism from a group G into a group G' then $\ker f$ is a normal sub-group of G.

Proof: Given $\phi: G \to G'$ be a homomorphism

Now we prove $\ker f$ is a normal sub-group of G.

First we prove $\ker f$ is a sub-group of G.

let $x \in G$, $h \in \ker f \Rightarrow f(h) = e'$

Now we prove $xhx^{-1} \in \ker f$

Consider $f(xhx^{-1}) = f(x) \cdot f(hx^{-1})$

$= f(x) \cdot f(h) \cdot f(x^{-1})$

$= f(x) \cdot e' \cdot f(x^{-1})$

$= f(x) \cdot f(x^{-1})$

$= f(xx^{-1}) = f(e) = e'$

Scanned by CamScanner

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

$\Rightarrow xhx^{-1} \in \ker f$

$\therefore \ker f$ is a normal sub-group of G.

---

3. Statement: Let ϕ be a homomorphism from a group G into a group G' then $\phi(a) = \phi(b) \Leftrightarrow a \ker \phi = b \ker \phi$.

Proof: Given $\phi: G \to G'$ be a homomorphism

Consider $\phi(a) = \phi(b)$

~~Now we prove~~

multiply the eq^n with $[\phi(a)]^{-1}$

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

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

$\phi(a^{-1} \cdot a) = \phi(a^{-1}b)$ ($\because \phi$ is homomorphism)

$e' = \phi(a^{-1}b)$

$\therefore a^{-1}b \in \ker f$ and $\ker f$ is a sub-group

$\Rightarrow a \ker f = b \ker f$ [$\because a^{-1}b \in H \Leftrightarrow aH = bH$]

22/3/18 Fundamental theorem of Homomorphism: (or)

4. First Isomorphism: Let G, G' be two groups and $f: G \to G'$ be a homomorphism with $\ker f = k$ then $\frac{G}{k}$ is isomorphic to G'. (or) $\frac{G}{k} \cong G'$.

Proof: Given $f: G \to G'$ be a homomorphism with $\ker f = K$

Now we prove $\frac{G}{K} \cong G'$.

Define a mapping $\phi: \frac{G}{k} \to G'$ as $\phi(Ka) = f(a)$.

well defined:

Consider $Ka = kb$

$\Rightarrow ab^{-1} \in K = \ker f$

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

$\Rightarrow f(a) f(b^{-1}) = e'$ ($\because f$ is homomorphism)

multiply with $f(b)$ to right on b's.

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

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

$\Rightarrow f(a) f(e) = f(b)$

Scanned by CamScanner

$\Rightarrow f(a)\cdot e' = f(b)$

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

$\Rightarrow \phi(Ka) = \phi(Kb)$

$\therefore \phi$ is well defined

One-one:

Consider $\phi(Ka) = \phi(Kb)$

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

multiply $f(b^{-1})$ on right

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

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

$\Rightarrow ab^{-1} \in \ker f = K$

$\therefore Ka = Kb$

Homomorphism:

Let $Ka, Kb \in \frac{G}{K}$

Consider $\phi(Ka\cdot Kb) = \phi(Kab)$

$= f(ab)$

$= f(a)f(b)$ [$\because f$ is homomorphism]

$= \phi(Ka)\phi(Kb)$

$\therefore \phi$ is homomorphism.

Onto:

Let $f(a) \in G'$ $\exists$ an element $Ka \in \frac{G}{K} \Rightarrow \phi(Ka) = f(a)$

$\therefore \phi$ is onto

$\therefore \phi$ is an isomorphism

Hence $\frac{G}{K}$ is isomorphic to G'

Scanned by CamScanner

Problems:

1. Let R^* be a group of real no.'s under multiplication and $\phi: R^* \to R^*$ defined by $\phi(x) = |x|$ is a homomorphism, Find ker f.

Sol: Given $\phi: R^* \to R^*$ defined by $\phi(x) = |x|$ and ϕ is a homomorphism.

$\text{Ker } f = \{x \in R^* / \phi(x) = e' = 1\}$

$\Rightarrow \phi(x) = 1$

$\Rightarrow |x| = 1$

$\Rightarrow x = \pm 1$

$\therefore \text{ker } f = \{1, -1\}$

---

2. Let R^* be a group of real no.'s under addition defined by $\phi: R^* \to R^*$ defined by $\phi(x) = x^2$

Sol: Given $\phi: R^* \to R^*$ defined by $\phi(x) = x^2$

Homomorphism:

Let $a, b \in R^*$

Consider $\phi(a+b) = (a+b)^2$

$= a^2 + 2ab + b^2$

Consider $\phi(a) + \phi(b) = a^2 + b^2$

$\therefore \phi(a+b) \neq \phi(a) + \phi(b)$

$\therefore \phi$ is not a homomorphism.

Imp 3. Let $G = U(16)$, $H = \{1, 15\}$, $K = \{1, 9\}$ are H and K isomorphic, Are $\frac{G}{H}$ and $\frac{G}{K}$ isomorphic.

Sol: Given $G = U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $H = \{1, 15\}$, $K = \{1, 9\}$.

Define a mapping $\phi: H \to K$ as $\phi(1) = 1$, $\phi(15) = 9$

clearly ϕ is one-one and onto.

Scanned by CamScanner

Homomorphism:

Consider $\phi(1 \cdot 15) = \phi(15)$

$= 9 = 1 \cdot 9$

$= \phi(1) \cdot \phi(15)$

$\therefore \phi$ is homomorphism

Hence H and K are isomorphic

$\left|\frac{G}{H}\right| = \frac{|G|}{|H|} = \frac{8}{2} = 4$

$1H = H = 15H$

$3H = \{3, 13\} = 13H$

$5H = \{5, 11\} = 11H$

$7H = \{7, 9\} = 9H$

$\therefore \frac{G}{H} = \{1H, 3H, 5H, 7H\}$

$\left|\frac{G}{K}\right| = \frac{|G|}{|K|} = \frac{8}{2} = 4$

$1K = K = \{1, 9\} = 9K$

$3K = \{3, 11\} = 11K$

$5K = \{5, 13\} = 13K$

$7K = \{7, 15\} = 15K$

$\therefore \frac{G}{K} = \{1K, 3K, 5K, 7K\}$

Define a mapping $\phi: \frac{G}{H} \to \frac{G}{K}$ as $\phi(1H) = 1K$

$\phi(3H) = 3K$

$\phi(5H) = 5K$

$\phi(7H) = 7K$

$\therefore$ clearly ϕ is one-one and onto.

Consider $\phi(3H \cdot 5H) = \phi(15H)$

$= \phi(1H)$

$= 1K$

Consider $\phi(3H)\phi(5H) = 3K \cdot 5K$

$= 15K = 7K$

$\therefore \phi$ is not a homomorphism

$\therefore \frac{G}{H}$ is not isomorphic to $\frac{G}{K}$.

Scanned by CamScanner

Isomorphism on Groups.

Monomorphism:

Let G, G' be two groups and $f: G \to G'$ is said to be a monomorphism if f satisfies homomorphism and one-one property.

Endomorphism:

A homomorphism of a group is said to be an endomorphism if the mapping is from G to itself.

Automorphism:

An isomorphism of a group G is said to be an automorphism if the mapping is from group G to itself.

Problem:

1. Let $(G,+)$ be a group then $\phi: G \to G$ defined by $\phi(x) = x^3$ is not an automorphism.

Sol: Given $\phi: G \to G$ defined by $\phi(x) = x^3$

Homomorphism:

Let $x, y \in G$

Consider $\phi(x+y) = (x+y)^3$

Consider $\phi(x) + \phi(y) = x^3 + y^3$

$\therefore \phi(x+y) \neq \phi(x) + \phi(y)$

$\Rightarrow \phi$ is not a homomorphism

$\therefore \phi$ is not an automorphism.

Cayleys Theorem:

Statement: Every finite group is isomorphic to permutation group.

Proof: Given G is a finite group

I Define a mapping $f_a: G \to G$ as $f_a(x) = ax$ where $a, x \in G$.

Scanned by CamScanner

Now we prove f_a is a permutation.

Well defined & one-one:

Consider $f_a(x) = f_a(y)$

$\Leftrightarrow ax = ay$ ($\because$ left cancellation)

$\Leftrightarrow x = y$

Onto:

$\forall a, x \in G \Rightarrow ax \in G \; \exists \; x \in G \ni f_a(x) = ax$

$\therefore f_a$ is a permutation.

II Let $G' = \{f_a / f_a \text{ is permutation}\}$

Now we prove G' is a group w.r.t composition of mappings.

Closure: Let $f_a, f_b \Rightarrow f_a \cdot f_b = f_{ab} \in G'$

Associative: Let $f_a, f_b, f_c \in G'$

Consider $f_a \cdot (f_b \cdot f_c) = (f_a \cdot f_b) \cdot f_c$

$f_a \cdot f_{bc} = f_{ab} \cdot f_c$

$f_{abc} = f_{abc}$

Identity: Let $f_a \in G' \; \exists \; f_e \in G' \ni f_a \cdot f_e = f_{ae} = f_a$

$\therefore f_e$ is the identity.

Inverse: Let $f_a \in G' \; \exists f_{\bar{a}'} \in G' \ni f_a \cdot f_{\bar{a}'} = f_{a\bar{a}'} = f_e$

$\therefore f_{\bar{a}'}$ is the inverse of f_a.

$\therefore G'$ is a group called permutation group.

III Define a mapping $\phi : G \to G'$ as $\phi(a) = f_a$

where $a \in G$, $f_a \in G'$

Now we prove ϕ is isomorphism

Well defined & one-one:

Consider $\phi(a) = \phi(b)$

$\Leftrightarrow f_a(x) = f_b(x)$

$\Leftrightarrow ax = bx$ ($\because$ right cancellation)

$\Leftrightarrow a = b$

Scanned by CamScanner

Homomorphism:

Consider $\phi(ab) = f_{ab}$ (11)

$= f_a \cdot f_b$

$= \phi(a) \cdot \phi(b)$

Onto:

Let $f_a \in G'$ $\exists$ an element $a \in G \ni \phi(a) = f_a$

$\therefore \phi$ is an isomorphism.

Hence G is isomorphic to permutation group G'.

Problems:

1. Find the regular permutation group isomorphic to $\{1, \omega, \omega^2\}$

Sol: Given $G = \{1, \omega, \omega^2\}$ and define a mapping $f_a : G \to G$ as

$f_a(x) = ax$

$\therefore$ The regular permutation group is $\{f_1, f_\omega, f_{\omega^2}\}$

$$f_1 = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix} = I$$

$$f_\omega = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix}$$

$$f_{\omega^2} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix}$$

---

2. Find the regular permutation group isomorphic to $\{1, -1, i, -i\}$

Sol:

Scanned by CamScanner

3. Find the regular permutation group isomorphic to $U(12)$.

Soy.

(12)

D **Properties of homomorphism:**

1. **Statement:** Let G, G' be two groups and $\phi: G \to G'$ be a homomorphism then (i) $\phi(e) = e'$

(ii) $\phi(a^{-1}) = \{\phi(a)\}^{-1}$

(iii) homomorphic image of a group is S.G of G'

(iv) homomorphic image of a group is abelian group if G is abelian.

Proof: Given $\phi: G \to G'$ be a homomorphism.

i) Consider $\phi(e) = \phi(e \cdot e)$

$\Rightarrow \phi(e) = \phi(e) \cdot \phi(e)$

$\Rightarrow e' \phi(e) = \phi(e) \cdot \phi(e)$ (by right cancellation)

$\Rightarrow \phi(e) = e'$

ii) Consider $\phi(a)\phi(a^{-1}) = \phi(a a^{-1})$

$= \phi(e)$

$= e'$

Similarly $\phi(a^{-1})\phi(a) = \phi(a a^{-1})$

$= \phi(e) = e'$

$\therefore \phi(a^{-1}) = \{\phi(a)\}^{-1}$

iii) Given $\phi: G \to G'$ be a homomorphism and the homomorphic image is denoted as $f(G)$

Now we prove $f(G)$ is a S.G of G'

Scanned by CamScanner

Let $\phi(a), \phi(b) \in \phi(G)$

$\Rightarrow \phi(a) = a' \quad , \quad \phi(b) = b'$

Consider $\phi(a)[\phi(b)]^{-1} = \phi(a)\,\phi(b^{-1})$ (13)

$= \phi(ab^{-1}) \in \phi(G)$

$\therefore \phi(G)$ is a S.G of G'.

iv) Let $\phi(a), \phi(b) \in \phi(G)$

Consider $\phi(a) \cdot \phi(b) = \phi(ab)$

$= \phi(ba)$

$= \phi(b) \cdot \phi(a)$

$\therefore \phi(G)$ is abelian.

---

2. Statement: Any infinite cyclic group is isomorphic to $(Z, +)$.

Proof: Given G is an infinite cyclic group.

Define a mapping $f: G \to Z$ as $f(a^n) = n$

Now we prove f is an isomorphism.

well defined & one-one:

Consider $f(a^i) = f(a^j)$

$\Leftrightarrow i = j$

$\Leftrightarrow a^i = a^j$

Homomorphism:

Consider $f(a^i a^j) = f(a^{i+j})$

$\Rightarrow i + j$

$\Rightarrow f(a^i) + f(a^j)$

$\therefore f$ is an homomorphism

onto:

Let $n \in Z$ $\exists$ an element $a^n \in G \ni f(a^n) = n$

$\therefore f$ is an isomorphism.

Scanned by CamScanner

Problem:

1. $\phi: C \to C$ defined by $\phi(a+ib) = a-ib$ be an automorphism of complex no's w.r.t addition. (10)

Sol: Given $\phi: C \to C$ defined by $\phi(a+ib) = a-ib$

Now we prove ϕ is an automorphism.

Homomorphism:

Consider $(a_1+ib_1)+(a_2+ib_2)$

$\Rightarrow \phi(a_1+a_2)+i(b_1+b_2)$

$\Rightarrow (a_1+a_2)-i(b_1+b_2)$

Consider $\phi(a_1+ib_1)+\phi(a_2+ib_2) = \phi(a_1-ib_1)+(a_2+ib_2)$

$= (a_1+a_2)-i(b_1+b_2)$

One-one:

Consider $\phi(a_1+ib_1) = \phi(a_2+ib_2)$

$\Rightarrow a_1 = a_2, b_1 = b_2$

Onto:

Let $a-ib \in C$ $\exists$ an element $a+ib \in C \ni \phi(a+ib) = a-ib$.

$\therefore \phi$ is an automorphism.

---

2. Statement: The set of all automorphisms of a group G forms a group w.r.t composition of mappings.

Proof: Given $A(G) = \{f / f$ is an automorphism$\}$

Now we prove $A(G)$ is a group w.r.t 'o'.

closure: Let $f, g \in A(G)$

$\Rightarrow f, g$ satisfies one-one & onto properties.

$\Rightarrow fog$ also satisfies one-one & onto properties.

Homomorphism: Let $a, b \in G$

Consider $fog(ab) = f(g(ab))$

$= f(g(a)g(b))$ [$\because g$ is homomorphism]

$= f(g(a)) \cdot f(g(b))$ [$\because f$ is homomorphism]

$= fog(a) \cdot fog(b)$

$\therefore fog(ab) \in A(G)$.

Scanned by CamScanner

Associative:
Composition of mappings satisfies associative property.

Identity:
Let $f \in A(G) \exists I: G \to G \in A(G) \ni foI = f$
$\therefore I$ is the identity.

Inverse:
Let $f \in A(G)$
$\Rightarrow f^{-1}$ satisfies one-one & onto properties

Homomorphism:
Let $f^{-1}(a) = a'$; $f^{-1}(b) = b'$
$\Rightarrow \quad a = f(a')$; $b = f(b')$
Consider $f^{-1}(ab) = f^{-1}(f(a') \cdot f(b'))$
$= f^{-1}(f(a'b'))$
$= a'b'$
$= f^{-1}(a) f^{-1}(b)$
$\therefore f^{-1} \in A(G) \ni fof^{-1} = I$
$\therefore A(G)$ is a group.

Problem:

1. Let $a \in G$ defined $f_a: G \to G$ as $f_a(x) = \bar{a}^1 xa \ \forall x \in G$ is an automorphism of G.

Sol. Given $f_a: G \to G$ as $f_a(x) = \bar{a}^1 xa \ \forall x \in G$
Now we prove f_a is an automorphism
Homomorphism:
Let $x, y \in G$
Consider $f_a(xy) = \bar{a}^1 xya$
Consider $f_a(x) \cdot f_a(y) = \bar{a}^1 xa \cdot \bar{a}^1 ya$
$= \bar{a}^1 x(a \cdot \bar{a}^1) ya$
$= \bar{a}^1 xya$
$\therefore f_a(xy) = f_a(x) \cdot f_a(y)$

One-One:
Consider $f_a(x) = f_a(y)$
$\bar{a}^1 xa = \bar{a}^1 ya$ [$\because$ by LCL & RCL]
$x = y$

Scanned by CamScanner

onto:

Let $a \in G, x \in G$.

$\Rightarrow a^{-1}xa \in G \ \exists\ x \in G \ni f_a(x) = a^{-1}xa$.

$\therefore f_a$ is an automorphism.

Inner & Outer automorphism:

Let $a \in G$, define $f_a: G \to G$ as $f_a(x) = a^{-1}xa \ \forall\ x \in G$ is an automorphism called inner automorphism.

If f_a is not inner i.e, $f_a(x) = a^{-1}xa$ then f_a is outer automorphism.

Note: If the group G is abelian then the only inner automorphism is identity mapping.

$f_a(x) = a^{-1}xa$
$= a^{-1}ax$
$= ex = x$
$= I$

Important Questions:

1. Cosets - property (ii) - $a \notin H \Rightarrow aH = H$
2. ~~Product of two~~ Any two left (rt) cosets ~~is again a left (rt) coset~~ are disjoints or
3. $aH = bH \Leftrightarrow a^{-1}b \in H$
4. $|aH| = |bH|$
5. Lagranges
6. $xHx^{-1} = H$
7. H is normal S.G $\Leftrightarrow Ha \cdot Hb = Hab$
8. Every S.G of an abelian group is normal.
9. Factor group
10. Ker f is a N.S.G
11. First isomorphism
12. Cayley's
13. Properties of homomorphism
14. Set of all automorphism
15. Intersection of two N.S.G is a N.S.G.

Scanned by CamScanner

28/3/18

Unit-IV - Ring homomorphism.

Ring: Let R be a non-empty set with two binary operations + and (·) is said to be a ring if

i) $(R,+)$ is an abelian group

ii) $(R,\cdot)$ is a semigroup

iii) R satisfies distributive law i.e, $a\cdot(b+c)=a\cdot b+a\cdot c$ (L.D.L);
$(a+b)\cdot c=a\cdot c+b\cdot c$ (RDL) $\forall a,b,c\in R$.

Commutative ring:

A ring $(R,+,\cdot)$ is said to be a commutative ring if R satisfies commutative property w.r.t $(\cdot)$ i.e,
$a\cdot b=b\cdot a \ \forall a,b\in R$.

Sub ring:

Let $(R,+,\cdot)$ be a ring and S be a non-empty subset of R is said to be a sub ring of R if S itself is a ring.

Note: The condition for sub ring are:

i) $x-y\in S$
ii) $xy\in S$ $\forall x,y\in S$

Ideal:

Let $(R,+,\cdot)$ be a ring and U is a non-empty sub s:t of R. U is said to be an ideal of R if

i) $a-b\in U$
ii) $ar, ra\in U$ $\forall a,b\in U$; $r\in R$

Homomorphism:

Let R, R' be two rings and $f: R\to R'$ is said to be a homomorphism if

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

ii) $f(a\cdot b)=f(a)\cdot f(b)$ where $a,b\in R$, $f(a),f(b)\in R'$

Note: Homomorphism onto means f satisfies Homomorphism and onto.

Scanned by CamScanner

2. Homomorphism into means f satisfies o.

Isomorphism:

Let R, R' be two rings, $f: R \to R'$ is said to be isomorphism if f satisfies homomorphism, one-one &

Endomorphism:

Endomorphism is same as homomorphism where the mapping is $f: R \to R$.

Automorphism:

Automorphism is same as isomorphism mapping from $f: R \to R$.

29/3/18 Note:

1. Let R, R' be two rings and $\phi: R \to R'$ be a homomorphism defined by $\phi(x) = 0', \forall x \in R$ is called zero homomorphism.
2. $\phi: R \to R'$ defined by $\phi(x) = x \ \forall x \in R$ is a homomorphism called identity homomorphism.

Problems:

1. Let Z be ring of integer and $\phi: Z \to 2Z$ defined as $\phi(n) = 2n \ \forall n \in Z$. Is ϕ an isomorphism.

Sol: Given $\phi: Z \to 2Z$ defined as $\phi(n) = 2n \ \forall n \in Z$

Homomorphism:

Let $n_1, n_2 \in Z$

Consider $\phi(n_1 + n_2) = 2(n_1 + n_2)$

$= 2n_1 + 2n_2$

$= \phi(n_1) + \phi(n_2)$

$\therefore \phi(n_1 + n_2) = \phi(n_1) + \phi(n_2)$

Consider $\phi(n_1 n_2) = 2(n_1 n_2)$

$= \phi(n_1)\phi(n_2)$

$= 2n_1 2n_2$

$= 4n_1 n_2$

$\therefore \phi(n_1 n_2) \neq \phi(n_1)\phi(n_2)$

Scanned by CamScanner

$\therefore \phi$ is not a homomorphism.
$\Rightarrow \phi$ is not an isomorphism.

2. Determine the ring homomorphisms of $Z \to Z$.

Sol. Given Z is a ring and $\phi: Z \to Z$ defined as $\phi(x) = ax$ $\forall\ x \in Z, a \in Z$.

ϕ is a homomorphism $\Rightarrow \phi(x+y) = \phi(x) + \phi(y)$

$\phi(xy) = \phi(x) \cdot \phi(y)$

$\Rightarrow a(xy) = ax \cdot ay$

$axy = a^2xy$ $(\because RCL)$

$a = a^2$

$a^2 = a$

$a^2 - a = 0$

$a(a-1) = 0$

$\Rightarrow a = 0, a = 1$

If $a = 0$, then $\phi(x) = 0$ which is a zero homomorphism.

If $a = 1$, then $\phi(x) = x$ which is identity homomorphism.

$\therefore$ The only homomorphism from $Z \to Z$ and zero and identity homomorphism.

Properties:

1. Statement: Let $\phi: R \to R'$ be a homomorphism, zero R, $0' \in R'$ then i) $\phi(0) = 0'$

ii) $\phi(-a) = -\phi(a)$

iii) $\phi(a-b) = \phi(a) - \phi(b)$

iv) $\phi(nr) = n\phi(r)$

v) $\phi(r^n) = [\phi(r)]^n$.

Proof: Given $\phi: R \to R'$ be a homomorphism.

i) Consider $\phi(0) = \phi(0+0)$

$\phi(0) = \phi(0) + \phi(0)$

$0' + \phi(0) = \phi(0) + \phi(0)$ $(\because RCL)$

$\phi(0) = 0'$

Scanned by CamScanner

ii) Consider $\phi(-a)+\phi(a) = \phi(-a+a)$
$= \phi(0)$
$= 0'$
$\therefore \phi(-a)+\phi(a) = 0'$
$\Rightarrow \phi(-a) = -\phi(a)$

iii) Consider $\phi(a-b) = \phi[a+(-b)]$
$= \phi(a)+\phi(-b)$
$= \phi(a)-\phi(b)$

iv) Consider $\phi(nr) = \phi(r+r+---+r)$ n times
$= \phi(r)+\phi(r)+---+\phi(r)$ n times
$= n\phi(r)$

v) Consider $\phi(r^n) = \phi(r.r.----.r)$ n times
$= \phi(r).\phi(r)-----.\phi(r)$ n times.
$= [\phi(r)]^n$

2/4/18

2. Statement: Let $\phi: R \to S$ be a ring homomorphism and A is a subring of R then PT $\phi(A)$ is a subring of S.

Proof: Given $\phi: R \to S$ be a homomorphism and A is a subring of R.

Now we prove $\phi(A)$ is a subring of S.

$\phi(A) = \{\phi(x) / x \in A\}$

Let $\phi(x), \phi(y) \in \phi(A)$ where $x, y \in A$ and A is a subring of $R \Rightarrow x-y \in A, xy \in A$ — ①

Consider $\phi(x)-\phi(y) = \phi(x-y) \in \phi(A)$ [$\because$ from eq^n ①]

Consider $\phi(x).\phi(y) = \phi(xy) \in \phi(A)$ [$\because$ from eq^n ①]

$\therefore \phi(A)$ is a subring of S.

3. Statement: Let $\phi: R \to S$ be a homomorphism and A is an ideal of R then PT $\phi(A)$ is an ideal of S.

Proof: Given $\phi: R \to S$ be a homomorphism and A is an ideal of R.

Now we prove $\phi(A)$ is an ideal of S.

$\phi(A) = \{\phi(a) / a \in A\}$

Let $\phi(a), \phi(b) \in \phi(A)$ where $a, b \in A$ and A is an ideal of $R \Rightarrow a-b \in A$; $ar, ra \in U$

Scanned by CamScanner

Consider $\phi(a)-\phi(b)=\phi(a-b)\in\phi(A)$ ($\because$ from ①)

~~Consider $\phi(a\cdot r)\in\phi(A)\ \phi(r)$ $\because$ from ①~~

~~$\phi(ra)\in\phi(A)$~~

Let $\phi(a)\in\phi(A)$

$r\in R$

$\Rightarrow \phi(r)\in\phi(A)$

$\phi(a)\cdot\phi(r)=\phi(ar)\in\phi(A)$

$\therefore \phi(A)$ is an ideal of S

4. Statement: The homomorphic image of a ring is a ring.

Proof: Let R, R' be two rings and $f: R\to R'$ is a homomorphism

Now we prove $f(R)$ is a ring.

We prove $f(R)$ is a sub ring.

$f(R)=\{f(x)/x\in R\}$

Let $f(x), f(y)\in R$

Consider $f(x)-f(y)=f(x-y)\in f(R)$ | $\because x\in R$, $y\in R\Rightarrow -y\in R$, by closure $x+(-y)\in R\Rightarrow x-y\in R$

Consider $f(x)\cdot f(y)=f(xy)\in f(R)$ | $\because x,y\in R \Rightarrow xy\in R$

$\therefore \phi(R)$ is a subring of R'

$\therefore f(R)$ is a ring $\because$ every sub ring is a ring

3/4/18

Kernel of a homomorphism:

Let R, R' be two rings and $f: R\to R'$ be a homomorphism then $\ker f$ is the set of all elements in R which are mapped to identity of R' i.e,

$\ker f=\{x\in R/f(x)=e'=0'\}$

5. Statement: If $\phi: R\to R'$ be a homomorphism then $\ker\phi$ is an ideal of R.

Proof: Given $\phi: R\to R'$ be a homomorphism.

Now we prove $\ker\phi$ is an ideal of R.

Let $a, b\in\ker\phi$

$\Rightarrow \phi(a)=0', \phi(b)=0'$

Scanned by CamScanner

Consider $\phi(a-b) = \phi(a) - \phi(b)$
$= 0' - 0'$
$= 0'$
$\therefore a-b \in \ker\phi$

Let $a \in \ker\phi$, $r \in R$

Consider $\phi(ar) = \phi(a)\phi(r)$
$= 0'\phi(r) = 0'$

$\therefore ar \in \ker\phi$

Similarly consider $\phi(ra) = \phi(r)\phi(a)$
$= \phi(r)0'$
$= 0'$

$\therefore ra \in \ker\phi$

$\therefore \ker\phi$ is an ideal of R.

---

16 D Statement: If $\phi: R \to R'$ be a homomorphism then ϕ is an into isomorphism if and only if $\ker\phi = \{0\}$.

Proof: Given $\phi: R \to R'$ be a homomorphism

First suppose that ϕ is an into isomorphism i.e, ϕ is homomorphism and one-one.

Now we prove $\ker\phi = \{0\}$

Let $a \in \ker\phi$

$\phi(a) = 0'$

$\phi(a) = \phi(0)$

$a = 0$ ($\because \phi$ is 1-1)

$\therefore \ker\phi = \{0\}$

Conversly suppose $\ker\phi = \{0\}$

Now we prove ϕ is an into isomorphism.

Given ϕ is homomorphism, it is enough if we prove ϕ is one-one.

Consider $\phi(a) = \phi(b)$

$\phi(a) - \phi(b) = 0'$

$\phi(a-b) = 0'$

$a-b \in \ker\phi = 0$

$a-b = 0$

$a = b$

$\therefore \phi$ is one-one

Hence ϕ is an into isomorphism.

Scanned by CamScanner

7. Statement: If U is an ideal of R then the quotient ring $\frac{R}{U}$ is homomorphic image of R.

Proof: Given U is an ideal of R

Define a mapping $\phi: R \to \frac{R}{U}$ as $\phi(a) = a+U$ where $a \in R$, $a+U \in \frac{R}{U}$.

Now we prove ϕ is a homomorphism

Consider $\phi(a+b) = (a+b)+U$

$= (a+U)+(b+U)$

$= \phi(a) + \phi(b)$

Consider $\phi(ab) = (ab)+U$

$= (a+U)\cdot(b+U)$

$= \phi(a)\cdot\phi(b)$.

$\therefore \phi$ is homomorphism

Hence $\frac{R}{U}$ is homomorphic image of R.

8. Fundamental theorem of Homomorphism.

Statement: Let R, R' and $f: R \to R'$ be a homomorphism with $\ker f = U$ then $\frac{R}{U} \cong R'$.

Proof: Given $f: R \to R'$ be a homomorphism and $\ker f = U$

Now we prove $\frac{R}{U} \cong R'$

Define $\phi: \frac{R}{U} \to R'$ as $\phi(a+U) = f(a)$

where $a+U \in \frac{R}{U}$, $a \in R$, $f(a) \in R'$

well-defined and one-one:

Consider $\phi(a+U) = \phi(b+U)$

$\Leftrightarrow f(a) = f(b)$

$\Leftrightarrow f(a)-f(b) = 0'$

$\Leftrightarrow f(a-b) = 0'$

$\Leftrightarrow a-b \in \ker f = U$

$\Leftrightarrow a+U = b+U$

$\therefore \phi$ is well-defined & 1-1.

Scanned by CamScanner

Homomorphism:

Consider $\phi((a+U)+(b+U)) = \phi((a+b)+U)$

$= f(a+b)$

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

$= \phi(a+U)+\phi(b+U)$

Consider $\phi((a+U)\cdot(b+U)) = \phi((ab)+U)$

$= f(ab)$

$= f(a)\cdot f(b)$

$= \phi(a+U)\cdot\phi(b+U)$

$\therefore \phi$ is homomorphism

Onto:

Let $\phi(a) \in R'$ $\exists$ an element $(a+U) \in \frac{R}{U}$ $\ni$ $\phi(a+U) = f(a)$.

$\therefore \phi$ is onto.

$\therefore \frac{R}{U} \cong R'$

10/4/18

2. Ring of polynomials. (15)

Polynomial ring: Let R be a ring, a polynomial $f(x)$ with co-efficients in R is $a_0+a_1x+a_2x^2+---+a_nx^n+----$ $= \sum_{i=1}^{\infty} a_ix^i$ where $a_i \in R$ $\forall i = 1,2,---$ is a polynomial ring and is denoted as $R[x]$.

Note:

1. The zero polynomial in $R[x]$ is $0[x] = (0,0,----0)$
2. The constant polynomial is $(a_0,0,---0)$ where $a_0 \in R$.

Model-I (Sum & product of polynomials):

1. Find the sum & product of $f(x) = 5+4x+2x^2+2x^3$ and $g(x) = 1+4x+5x^2+3x^3$ over Z_6 and find degree$[f(x)+g(x)]$ & $\deg[f(x)\cdot g(x)]$.

Sol: Given $f(x) = 5+4x+2x^2+2x^3$

$g(x) = 1+4x+5x^2+3x^3$

$f(x)+g(x) = 0+2x+1x^2+5x^3$

$= 2x+x^2+5x^3$

$f(x)\cdot g(x) = 5+20x+25x^2+15x^3+4x+16x^2+20x^3+12x^4+2x^2+8x^3+$

$10x^4+6x^5+2x^3+8x^4+10x^5+6x^6$

Scanned by CamScanner

$= 0x^6 + 4x^5 + 0x^4 + 3x^3 + 1x^2 + 0x + 5$

$= 4x^5 + 3x^3 + x^2 + 5$

$\deg[f(x)+g(x)] = \max(3,3) = 3$ (16)

$\deg[f(x)\cdot g(x)] = \deg[f(x)+g(x)] = 3+3 = 6$

Here $\deg[f(x)\cdot g(x)] < \deg[f(x)+g(x)]$

---

2. $f(x) = 2+3x+4x^2+2x^3$ and $g(x) = 4+2x+3x^4$ find $f(x)+g(x)$ & $f(x)\cdot g(x)$ Z5.

Soln: Given $f(x) = 2+3x+4x^2+2x^3$

$g(x) = 4+2x+3x^4$

$f(x)+g(x) = 1+0x+4x^2+2x^3+3x^4$

$= 1+4x^2+2x^3+3x^4$

$f(x)\cdot g(x) = 8+4x+6x^4+12x+6x^2+9x^5+16x^2+8x^3+12x^6+8x^4$

$+4x^6+6x^7$

$= 1x^7+2x^6+4x^5+4x^3+2x^2+1x+3$

$\deg[f(x)+g(x)] = \max(3,4) = 4$

$\deg[f(x)\cdot g(x)] = \deg[f(x)]+\deg[g(x)] = 4+3 = 7$

Model-II

1. If $f(x) = x^6+3x^5+4x^2-3x+2$ & $g(x) = x^2+2x-3$ are polynomials in $Z_7[x]$. Find $q(x)$ & $r(x)$.

Soln: Given $f(x) = x^6+3x^5+4x^2-3x+2$ & $g(x) = x^2+2x-3$

$x^2+2x-3 \;)\; x^6+3x^5+4x^2-3x+2 \;(\; x^4+x^3+x^2+x-2$

$x^6 \pm 2x^5 \mp 3x^4$

$x^5+3x^4+4x^2$

$x^5 \pm 2x^4 \mp 3x^3$

$x^4+3x^3+4x^2-3x$

$x^4 \pm 2x^3 \mp 3x^2$

x^3+0x^2-3x+2

$x^3 \pm 2x^2 \mp 3x$

$-2x^2+2$

$\mp 2x^2 \mp 4x \pm 6$

$4x-4$

$\therefore q(x) = x^4+x^3+x^2+x-2$

$r(x) = 4x-4$

Scanned by CamScanner

2. If ~~$f(x)=x^4+5x^2+4x+50$~~ $f(x)=x^4-3x^3+2x^2+4x-1$ and $g(x)=x^2-2x+3$ in Z_5. find $q(x)$ & $r(x)$

Sol: Given $f(x)=x^4-3x^3+2x^2+4x-1$ & $g(x)=x^2-2x+3$ (17)

$$
\begin{array}{r|l}
x^2-2x+3 \;)\; x^4-3x^3+2x^2+4x-1 & (x^2-x-3 \\
\cline{2-2}
\underline{x^4 \mp 2x^3 \pm 3x^2} & \\
-x^3-x^2+4x-1 & \\
\underline{\mp x^3 \pm 2x^2 \mp 3x} & \\
-3x^2+2x-1 & \\
\underline{-3x^2+6x-4} & \\
4x+3 &
\end{array}
$$

$\therefore q(x)=x^2-x-3$

$r(x)=x+3$

3. If $f(x)=x^4+5x^3-3x^2$ and $g(x)=5x^2-x+2$ in Z_{11}

Sol: Given $f(x)=x^4+5x^3-3x^2$ & $g(x)=5x^2-x+2$.

Scanned by CamScanner

1. Division algorithm theorem:

Statement: let F be a field, given two polynomials $f(x), g(x) \neq 0(x)$ in $F[x]$ then $\exists$ unique polynomials $q(x), r(x)$ in $F[x] \ni f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ (or) $\deg[r(x)] < \deg[g(x)]$.

Proof: Given $f(x), g(x)$ be two non-zero polynomials in $F[x]$

Consider the set $S = \{f(x) - h(x)g(x) / h(x) \in F[x]\}$

clearly the set $S \neq \phi$ $(\because f(x) - 0(x)g(x) = f(x) \in F[x])$

Casei) If $0(x) \in S$

then $0(x) = f(x) - q(x)g(x)$ where $q(x) \in F[x]$

$\Rightarrow f(x) = q(x)g(x) + 0(x)$

which is in the form of $f(x) = q(x)g(x) + r(x)$; $r(x) = 0$

Hence the theorem is proved

Caseii) If $0(x) \notin S$

Let $r(x) \in S$ be the polynomial of least degree.

By defination of S, $r(x) = f(x) - q(x)g(x)$

$\Rightarrow f(x) = q(x)g(x) + r(x)$

Now we prove $\deg[r(x)] < \deg[g(x)]$

Let us suppose $\deg[r(x)] \geq \deg[g(x)]$

Let $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ i.e, $\deg[g(x)] = n$

Let $r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_mx^m$ i.e, $\deg[r(x)] = m$

Consider $c_m a_n^{-1} x^{m-n} g(x)$

$\Rightarrow c_m a_n^{-1} x^{m-n} [a_0 + a_1x + a_2x^2 + \cdots + a_nx^n]$

$\Rightarrow c_m a_n^{-1} x^{m-n} a_0 + c_m a_n^{-1} x^{m-n+1} a_1 + c_m a_n^{-1} x^{m-n+2} a_2 + \cdots + c_m a_n^{-1} x^{m-1} a_{n-1} + c_m x^m$

$\Rightarrow c_m a_n^{-1} x^{m-n} a_0 + c_m a_n^{-1} x^{m-n+1} a_1 + \cdots + c_m a_n^{-1} x^{m-1} a_{n-1} + (r(x) - (c_0 + c_1x + \cdots + c_mx^m))$

$\Rightarrow r(x) - c_m a_n^{-1} x^{m-n} g(x) = c_0 + c_1x + \cdots c_{m-1}x^{m-1} - c_m a_n^{-1} x^{m-n} a_0 + \cdots + c_m a_n^{-1} x^{m-1} a_{n-1}$

$\Rightarrow r(x) - c_m a_n^{-1} x^{m-n} g(x) = \alpha(x)$; $\deg[\alpha(x)] = m-1$

$\Rightarrow r(x) - c_m a_n^{-1} x^{m-n} g(x) = \alpha(x)$

i.e, $\alpha(x) \in S$ and $\deg[\alpha(x)] = m-1 < m = \deg[r(x)]$

Scanned by CamScanner

which is a contradiction.
$\therefore \deg[r(x)] < \deg[g(x)]$
Hence the theorem is proved.

2. **Factor theorem:**

Statement: An element $\alpha \in F$, where F is a field, is a zero of $f(x) \in F[x] \Leftrightarrow (x-\alpha)$ is a factor of $f(x)$ in $F[x]$

Proof: Given F is a field, $\alpha \in F$

First suppose that $f(\alpha)=0$

Now we prove $(x-\alpha)$ is a factor of $f(x)$

let $g(x)=(x-\alpha)$ i.e, $\deg[g(x)]=1$

By division algorithm $\exists\ q(x), r(x) \in F[x] \ni f(x)=g(x)q(x)+r(x)$ —①

where either $r(x)=0$ (or) $\deg[r(x)] < \deg[g(x)]=1$

$\Rightarrow r(x)$ is a constant polynomial

using evaluation homomorphism i.e, $\phi_\alpha : F[x] \to F$ as

$\phi_\alpha[f(x)] = \phi_\alpha[g(x)q(x)+r(x)]$

$f(\alpha) = \phi_\alpha[(x-\alpha)q(x)+r(x)]$

$f(\alpha) = r(\alpha) = r$

$\Rightarrow 0 = r$

Sub in eq^n ①

$\therefore f(x) = q(x) \cdot g(x)$

$\Rightarrow f(x) = q(x)(x-\alpha)$

$\therefore (x-\alpha)$ is a factor of $f(x)$.

Conversly suppose $(x-\alpha)$ is a factor of $f(x)$

Now we prove $f(\alpha)=0$.

By division algorithm $\exists\ q(x) \in F[x] \ni f(x) = (x-\alpha)q(x)$

by using evaluation homomorphism i.e, $\phi_\alpha : F[x] \to F$

$\phi_\alpha[f(x)] = \phi_\alpha[(x-\alpha)q(x)]$

$f(\alpha) = 0$

Hence the theorem is proved.

Scanned by CamScanner

16/4/18

Unit-III - Ring theory.

1. Rings & Sub rings.

Ring: Let R be a non-empty set and $(+,\cdot)$ are two binary operations. The algebraic structure $(R,+,\cdot)$ is said to be a ring if ①

1. $(R,+)$ is abelian group.
2. $(R,\cdot)$ is a semigroup.
3. R satisfies distributive laws $a(b+c)=(a\cdot b)+(a\cdot c)$ (LDL)
   $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ (RDL)

Ring with unity:

Let $(R,+,\cdot)$ be a ring, $\exists\, 1\in R \ni a\cdot 1=1\cdot a=a\ \forall a\in R$

Commutative ring:

A ring satisfying commutative property w.r.t $(\cdot)$ is a commutative ring.

Boolean ring:

Let $(R,+,\cdot)$ be a ring and $a\in R$ if $a^2=a\ \forall a\in R$ then R is said to be a boolean ring.

Properties of ring:

Statement: In a ring $(R,+,\cdot)$ then

i) $0a=a0=0$
ii) $a(-b)=(-a)b=-(ab)$
iii) $(-a)(-b)=ab$
iv) $a(b-c)=ab-ac$

Proof: Given $(R,+,\cdot)$ be a ring then

i) Consider $0\cdot a=(0+0)a$

$0\cdot a=0a+0a$

$0+0a=0a+0a$

$0a=0$ — ①

Similarly $a0=a(0+0)$

$a0=a0+a0$

$0+a0=a0+a0$

$a0=0$ — ②

$\therefore 0a=a0=0$

Scanned by CamScanner

ii) Consider $a(-b)+ab = a.(-b+b)$
$= a0$
$= 0$
$a(-b)+ab = 0$
$a(-b) = -(ab)$ — (1)
$\therefore a(-b) = (-a)b = -(ab)$

Similarly $(-a)b+ab = (-a+a)b$
$= 0b$
$= 0$
$(-a)b+ab = 0$
$(-a)b = -(ab)$ — (2)

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

iv) Consider $a(b-c) = a(b+(-c))$
$= ab+a(-c)$
$= ab-ac$

(2)

Imp

D

Properties of boolean ring:

Statement: If R is a boolean ring then
i) $a+a=0 \ \forall \ a \in R$
ii) $a+b=0 \Rightarrow a=b$
* iii) R satisfies commutative property

Proof: Given R is a boolean ring
i) Let $a \in R \Rightarrow a^2 = a$
$a+a \in R \Rightarrow (a+a)^2 = a+a$
$(a+a)(a+a) = a+a$
$a^2+a^2+a^2+a^2 = a+a$
$(a+a)+(a+a) = (a+a)+0$
$a+a = 0$

ii) Consider $a+b = 0$
$a+b = a+a$ ($\because$ from (i))
$a = b$

iii) Let $a, b \in R$
$\Rightarrow a^2 = a, \ b^2 = b$
$a+b \in R$
$\Rightarrow (a+b)^2 = a+b$
$(a+b)(a+b) = a+b$ ($\because$ from (ii))
$a^2+ab+ba+b^2 = a+b$

Scanned by CamScanner

16. $a+ab+ba+b=a+b$

$ab+ba=0$ (from ii)

$ab=ba$

Problems. (3)

1. Find the units of Z_8

Sol: $Z_8=\{0,1,2,3,4,5,6,7\}$

Composition table:

X_8	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1				
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1		
6	0	6	4	2	3			
7	0	7	6	5	4	3	2	1

$\therefore$ The units of Z_8 are $\{1,3,4,7\}$

17/4/18

2. If R is a commutative ring then P.T $(a+b)^2=a^2+2ab+b^2$

Sol: Given R is a commutative ring i.e, $ab=ba$

Consider $(a+b)^2=(a+b)(a+b)$

$=a^2+ab+ba+b^2$

$=a^2+ab+ab+b^2$

$=a^2+2ab+b^2$

Sub ring: Let $(R,+,\cdot)$ be a ring and S is a non-empty subset of R $(S\subseteq R)$. S is said to be a sub-ring if S itself is a ring

Scanned by CamScanner

Subring test: let R be a ring and $S \subseteq R$ is a subring $\Leftrightarrow$

$\left.\begin{array}{l} i)\ a-b \in S \\ ii)\ ab \in S \end{array}\right\} \forall a, b \in S$

Proof: Given $(R, +, \cdot)$ is a ring

First suppose that S is a subring of R

Now we prove i) $a-b \in S$ (4)

ii) $ab \in S$

Let $a, b \in S$

$b \in S \Rightarrow$ by inverse property w.r.t $+$, $-b \in S$

$a \in S, -b \in S \Rightarrow$ by closure property w.r.t $+$,

$a+(-b) \in S$

$a-b \in S$

$a, b \in S \Rightarrow$ by closure property w.r.t $(\cdot)$, $ab \in S$

Conversely suppose i) $a-b \in S$

ii) $ab \in S$

Now we prove S is a sub-ring.

$(S, +)$ is an abelian group:

Let $a, a \in S \Rightarrow a-a \in S$

$\Rightarrow 0 \in S$ (Identity)

Let $0 \in S, a \in S \Rightarrow 0-a \in S$

$\Rightarrow -a \in S$ (Inverse)

Let $a \in S, -b \in S \Rightarrow a-(-b) \in S$

$\Rightarrow a+b \in S$ (Closure)

Let $a, b, c \in S \subseteq R$, R satisfies associative & commutative prop

$\Rightarrow S$ satisfies associative & commutative

$\therefore (S, +)$ is an abelian group

$(S, \cdot)$ is a semigroup:

from (ii) closure property is satisfied

Let $a, b, c \in S \subseteq R$, R satisfies associative property

$\Rightarrow S$ satisfies associative property.

$\therefore (S, \cdot)$ is a semigroup

Distributive law:

Let $a, b, c \in S \subseteq R$, R satisfies distributive law.

$\Rightarrow S$ satisfies distributive law

$\therefore (S, +, \cdot)$ is a ring $\Rightarrow$ Hence S is a sub-ring of R.

Scanned by CamScanner

Theorem:

Statement: The intersection of two sub-rings is again a sub-ring.

Proof: Let S_1, S_2 be two sub-rings of R.

Now we prove $S_1 \cap S_2$ is a sub-ring of R.

Let $a, b \in S_1 \cap S_2$ (5)

$\Rightarrow a, b \in S_1$ & $a, b \in S_2$

$\Rightarrow a, b \in S_1$, $a, b \in S_2$

S_1 is subring, S_2 is subring

$\Rightarrow ab \in S_1 - (1)$ $ab \in S_2 - (2)$

from (1) & (2)

$a - b \in S_1 \cap S_2$

$a, b \in S_1 \cap S_2$

$\therefore S_1 \cap S_2$ is a sub-ring

Problems on Sub-ring:

1. ST $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ is a sub-ring of 2×2 matrices whose elements are integers.

Sol: Given $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a, b, c, d \in Z \right\}$

$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} / a, b, c \in Z \right\}$

Now we prove S is a sub-ring of R.

Let $A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$

$$A - B = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in S$$

$$AB = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix} \in S$$

$\therefore S$ is a sub-ring

Scanned by CamScanner

2. Let R be a ring, $a \in R$. PT $S = \{x \in R / ax = 0\}$ is a sub-ring of R.

Sol: Given R is a ring and $S = \{x \in R / ax = 0\}$

Now we prove S is a sub-ring

Let $x, y \in S \Rightarrow ax = 0, ay = 0$

consider $a(x-y) = ax - ay$

$= 0 - 0$

$= 0$ (6)

$\Rightarrow x - y \in S$

consider $a(xy) = ax \cdot y$

$= 0 \cdot y$

$= 0$

$\Rightarrow xy \in S$

$\therefore S$ is a sub-ring

---

3. If R is a ring, $C(R) = \{x \in R / ax = xa\}$ is a sub ring of R.

Sol:

Scanned by CamScanner

2. Integral domain and Fields

Ring with zero divisors and without zero divisors:

Let $(R,+,\cdot)$ be a ring and $a,b \in R$

Consider $ab=0$

if either $a=0$ (or) $b=0$ then R is said to be ring without zero divisor. (or) no-zero divisor.

if $a\neq 0$ and $b\neq 0$ then R is said to be ring with zero divisor.

Ex: In $(Z_{12},+,\cdot)$ Find the zero divisors.

Sol: $Z_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$

The zero divisors of Z_{12} are 2,3,4,6,8,9

$(2\times 6=0, 3\times 4=0, 4\times 6=0, 8\times 3=0, 9\times 4=0)$.

Cancellation laws:

Let $(R,+,\cdot)$ be a ring and $a,b,c \in R$

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

$ba=ca \Rightarrow b=c$ (RCL)

Theorem:

Statement: A ring R has no zero divisors if and only if cancellation laws holds in R.

Proof: Given $(R,+,\cdot)$ is a ring and

First suppose that R has no zero divisors

Now we prove cancellation laws holds in R

Let $a,b,c \in R$ and $a\neq 0$

L.C.L: Let $ab=ac$

$ab-ac=0$

$a(b-c)=0$

$b-c=0$

$b=c$

R.C.L: Let $ba=ca$

$ba-ca=0$

$(b-c)a=0$

$b-c=0$

$b=c$

Scanned by CamScanner

Conversely suppose cancellation laws holds in R.
Now we prove R has no zero divisors.
Let $a, b \in R$ and $a \neq 0$
Consider $ab = 0$
$ab = a0$ (LCL)
$b = 0$

$\therefore$ R has no zero divisors

(8)

Types of Rings:

1. Integral domain: Let $(R, +, \cdot)$ be a ring is said to be an integral domain if R satisfies
i) commutative
ii) unity
iii) R has no zero divisors.
i.e, commutative $\Rightarrow ab = ba$
unity $\Rightarrow 1 \in R$
No zero divisors $\Rightarrow ab = 0$ either $a = 0$ (or) $b = 0$.

Ex: Ring of Integers is an integral domain

2. Division ring (or) skew field: Let $(R, +, \cdot)$ be a ring is said to be a division ring if R satisfies
i) Unity
ii) Every non zero element has multiplicative inverse

Ex: A ring of integers is not a division ring ($\because$ inverse property is not satisfied). The set of real no. is a division ring.

3. Field: Let $(R, +, \cdot)$ be a ring is said to be a field if R satisfies
i) Commutative
ii) Unity
iii) Every non zero has multiplicative inverse

Ex: Set of real no's.

Scanned by CamScanner

Theorems:

1. Statement: A field has no zero divisors.

Proof: Given $(R,+,\cdot)$ be a field

Now we prove R has no zero divisors.

Let $a,b \in R$ & $a \neq 0$ (9)

Consider $ab=0$

$a \neq 0 \Rightarrow \bar{a}^{-1} \in R$

$\bar{a}^{-1}ab = \bar{a}^{-1}0$ (∵ multiply with $\bar{a}^{-1}$)

$(\bar{a}^{-1}a)b = 0$

$e \cdot b = 0$

$b = 0$

∴ R has no zero divisors

Imp D

2. Statement: Every field is an integral domain.

Proof: Given $(R,+,\cdot)$ be a field

Now we prove R is an integral domain

It is enough if we prove R has no zero divisors

Same as theorem 1.

V. Imp D

3. Statement: Every finite integral domain is a field.

Proof: Given R is a finite integral domain

Let $0, 1, a_1, a_2, \ldots, a_n$ be the $n+2$ distinct elements of R.

Now we prove R is a field

It is enough if we prove every non zero elements has multiplicative inverse.

Let $a \neq 0 \in R$

Consider the $n+1$ products

$a1, aa_1, aa_2, \ldots, aa_n$ we proved that $n+1$ product are distinct

Suppose $aa_i = aa_j$

$a_i = a_j$ ⊗ (∵ LCL)

Scanned by CamScanner

which is a contradiction

∴ The n+1 products are distinct and belongs to R.

Hence by counting the n+1 products $a1, aa_1, aa_2 \cdots aa_n$ are the n+1 elements of $1, a_1, a_2 \cdots a_n$ of some order.

∴ $\exists a_i \in R \ni aa_i = 1$

$\Rightarrow a_i$ is the inverse of a

∴ R is a field

Hence every finite integral domain is a field.

(10)

16/4/18

Idempotent element: In a ring $(R,+,\cdot)$ if $a^2=a$ for $a \in R$ then a is called idempotent element of R.

Problems:

1. If a is an idempotent element of an integral domain then $a=1$.

Sol: Given $(R,+,\cdot)$ is an integral domain and $a \in R$ is an idempotent element $\Rightarrow a \neq 0 \in R$

$$a^2 = a$$
$$a^2 - a = 0$$
$$a(a-1) = 0$$

R has no zero divisors either $a=0$ (or) $a-1=0$

$$a - 1 = 0$$
$$a = 1$$

Characteristic of a ring R:

The characteristic of a ring R is the least +ve integer P ∋ $Pa=0 \ \forall a \in R$.

Here P is the characteristic of R

Ex: Let $R=\{0,1,2,3,4,5,6\} \in$ the ring $(Z_7, +_7, \times_7)$. Find characteristic of R.

Sol: $Z_7 = \{0,1,2,3,4,5,6\}$

$7(1) = 7 = 0$

$1+1+1+1+1+1+1$ (7 times) $= 0$

$2+2+2+\cdots\cdots$ (7 times) $= 0$

$3+3+3+\cdots\cdots = 0$

$4+4+4+\cdots\cdots = 0$

$5+5+5+\cdots\cdots = 0$

$6+6+6+\cdots\cdots = 0$

Scanned by CamScanner

$\therefore (7)a = 0 \ \forall a \in \mathbb{Z}_7$

$\therefore$ characteristic of $R = 7$

Imp Theorem:

1. Statement: The characteristic of integral domain is either '0' (or) prime.

Proof: Given $(R, +, \cdot)$ is an integral domain

If the characteristic of R is 0 there is nothing to prove.

If the characteristic of $R \neq 0$ we prove it as a prime no.

Suppose if possible the characteristic of R is p which is not a prime no.

i.e, $p = m \cdot n$ where $1 < m, n < p$.

let $a \neq 0 \in R$

$\Rightarrow a \cdot a = a^2 \in R$

$\Rightarrow p \cdot a^2 = 0$ ($\because$ characteristic of $R = p$)

$\Rightarrow mn\, a^2 = 0$

$\Rightarrow (ma)(na) = 0$

$\Rightarrow$ either $ma = 0$ (or) $na = 0$.

i) If $ma = 0$ for any $x \in R$

$(ma)x = 0x = 0$

$m(ax) = 0$ ⊗

which is a contradiction ($ax \in R$ and char $R = p$ & $m < p$)

$\therefore p$ is a prime no.

ii) Similarly if $na = 0$ for any $y \in R$

$(na)y = 0y = 0$

$n(ay) = 0$ ⊗

which is a contradiction

$\therefore p$ is a prime no.

$\therefore$ Hence characteristic of integral domain is prime.

Scanned by CamScanner

2. Statement: The characteristic of a field is either 0 (or) prime.

Proof: First we prove every field is an integral domain (theorem 2) and we prove characteristic of integral domain is either 0 (or) prime (above theorem).

Problems:

1. If R is a ring, $a^2=a$ $\forall a \in R$ then PT characteristic of $R=2$ (or) The characteristic of a boolean ring is 2.

Sol: Given $(R,+,\cdot)$ is a ring and ~~char~~ $a^2=a$ $\forall a \in R$

$a+a \in R \Rightarrow (a+a)^2=a+a$.

$(a+a)(a+a)=a+a$

$a^2+a^2+a^2+a^2=a+a$ (12)

$(a+a)+(a+a)=(a+a)+0$

$a+a=0$

$2a=0$ $\forall a \in R$

$\therefore$ characteristic of $R=2$

2. Find the characteristic of $Z_3 \times Z_4$.

Sol: $Z_3=\{0,1,2\}$; $Z_4=\{0,1,2,3\}$

$Z_3 \times Z_4=\{(0\,0)\,(0\,1)\,(0\,2)\,(0\,3)\,(1\,0)\,(1\,1)\,(1\,2)\,(1\,3)\,(2\,0)\,(2\,1)\,(2\,2)\,(2\,3)\}$

containing 12 pair of elements with zero element (00) and unity (11).

Consider $1(1\,1)=(1\,1)\neq(0\,0)$

$2(1\,1)=(2\,2)\neq(0\,0)$

$3(1\,1)=(3\,3)=(0\,3)\neq(0\,0)$

$4(1\,1)=(4\,4)=(1\,0)\neq(0\,0)$

$5(1\,1)=(5\,5)=(2\,1)\neq(0\,0)$

$6(1\,1)=(6\,6)=(0\,2)\neq(0\,0)$

$7(1\,1)=(7\,7)=(4\,3)=(1\,3)\neq(0,0)$

$8(1\,1)=(8\,8)=(2\,0)\neq(0,0)$

$9(1\,1)=(9\,9)=(0\,1)\neq(0,0)$

$10(1\,1)=(10\,10)=(1\,2)\neq(0,0)$

$11(1\,1)=(11\,11)=(1\,3)\neq(0,0)$

$12(1\,1)=(12\,12)=(0\,0)$ $\therefore$ char of $Z_3 \times Z_4=12$

Scanned by CamScanner

3. If characteristic of R is 2 and a, b commutes then PT $(a+b)^2 = a^2+b^2 = (a-b)^2$

Soln: Given, charc of $R=2$ i.e, $2a=0 \ \forall a \in R$ and $ab=ba$

Consider $(a+b)^2 = (a+b)(a+b)$.

$= a^2+ab+ba+b^2$ (13)

$= a^2+ab+ab+b^2$

$= a^2+2ab+b^2$

$a, b \in R \Rightarrow ab \in R$ and charc of $R=2$

$= a^2+0(b)+b^2$

$= a^2+b^2$ — ①

Consider $(a-b)^2 = (a-b)(a-b)$

$= a^2-ab-ba+b^2$

$= a^2-ab-ab+b^2$

$= a^2-2ab+b^2$

$= a^2-0(b)+b^2 \quad (\because 2a=0)$

$= a^2+b^2$ — ②

from ① & ②

$\therefore (a+b)^2 = a^2+b^2 = (a-b)^2$

4. If R is a commutative ring with unity and charc of $R=3$ then PT $(a+b)^3 = a^3+b^3$

Scanned by CamScanner

5. PT the set $Z[i]=\{a+ib / a,b\in Z, i^2=-1\}$ Goassian integers. Is an integral domain but not a field.

Sol: Given $Z[i]=\{a+ib / a,b\in Z\ i^2=-1\}$

First we prove $Z[i]$ is a ring (14)

w.r.t (+):

closure: let $(a_1+ib_1),(a_2+ib_2)\in Z[i]$

$(a_1+ib_1)+(a_2+ib_2)=(a_1+a_2)+i(b_1+b_2)\in Z[i]$

Associative: let $(a_1+ib_1),(a_2+ib_2),(a_3+ib_3)\in Z[i]$

$[(a_1+ib_1)+(a_2+ib_2)]+a_3+ib_3=a_1+b_1+[(a_2+ib_2)+(a_3+ib_3)]$

$(a_1+a_2+a_3)+i(b_1+b_2+b_3)=(a_1+a_2+a_3)+i(b_1+b_2+b_3)$

Identity: let $a+ib\in Z[i]\ \exists\ 0+i0\in Z[i]\ni(a+ib)\in(0+i0)=a+ib$

Inverse: let $a+ib\in Z[i]\exists -a-ib\in Z[i]\ni(a+ib)+(-a-ib)=0+i0$

Commutative: let $(a_1+ib_1)+(a_2+ib_2)\in Z[i]$

$(a_1+ib_1)+(a_2+ib_2)=(a_2+ib_2)+(a_1+ib_1)$

$(a_1+a_2)+i(b_1+b_2)=(a_2+a_1)+i(b_2+b_1)$

$\therefore (Z[i],+)$ is an abelian group.

w.r.t (·):

closure: Let $(a_1+ib_1),(a_2+ib_2)\in Z[i]$

$(a_1+ib_1)(a_2+ib_2)=(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)\in Z[i]$

Associative: let $(a_1+ib_1),(a_2+ib_2),(a_3+ib_3)\in Z[i]$

$[(a_1+ib_1)(a_2+ib_2)]a_3+ib_3=a_1+ib_1[(a_2+ib_2)(a_2+ib_3)]$

$[(a_1a_2-b_1b_2)a_3-(a_1b_2+a_2b_1)b_3]+i[(a_1a_2-b_1b_2)b_3+(a_1b_2+a_2b_1)a_3]$

RHS $\Rightarrow (a_1+ib_1)$

Commutative: let $(a_1+ib_1)(a_2+ib_2)=(a_2+ib_2)(a_1+ib_1)$

$(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)$

Unity: clearly $1+0i\in Z[i]$ is the unity

Nozero divisor: Consider $(a_1+ib_1)(a_2+ib_2)=(0+i0)$

$(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)=0+i0$

$a_1a_2-b_1b_2=0=a_1b_2+a_2b_1$

Scanned by CamScanner

It is possible only if either $a_1+ib_1=0$ (or) $a_2+ib_2=0$.
$\therefore Z[i]$ is an integral domain.

Inverse: Let $2+3i \in Z[i]$

Consider $(2+3i)(a+ib)=(0+i0)$

$(2a-3b)+i(2b+3a)=0+i0$

$2a-3b=0$	$2b+3a=0$
$2a=3b$	$2b+3(\frac{3}{2}b)=0$
$a=\frac{3}{2}b \notin Z$	$2b+\frac{9b}{2}=0$
	$\frac{4b+9b}{2}=0$

(15)

$\therefore$ Inverse property is not satisfied

$\therefore Z[i]$ is not a field.

6. PT $Q\sqrt{2}=\{a+b\sqrt{2}/a,b\in Q\}$ is a field

20/4/18

3. Ideal's and Factor Ring.

Ideal: Let $(R,+,\cdot)$ be a ring and U is a non-empty subset of R is said to be an ideal of R if

i) $a-b \in U$

ii) $ar, ra \in U$ $\forall$ $a,b \in U$ & $r \in R$

(16)

Note:

1. U is an ideal $\Rightarrow$ U is both left & right ideal.
2. If R is a commutative ring then left ideal = right ideal.
3. Singleton $\{0\}$ is an ideal of R is always a null ideal.

Theorems:

1. **Statement:** If U is an ideal of R ring with unity, $1 \in U$ then PT $U=R$.

Proof: Given R is a ring with unity, $1 \in U$ and U is an ideal of R.

Now we prove $U=R$

U is an ideal of $R \Rightarrow U \subseteq R$ — ①

Let $x \in R$; $1 \in U$ and U is an ideal of R.

$\Rightarrow x1 \in U \Rightarrow x \in U$

$\therefore R \subseteq U$ — ②

from ① & ②

$\therefore U=R$

Imp

2. **Statement:** The only ideals of a field F, $\{0\}$ and F itself.

Proof: Given $(F,+,\cdot)$ is a field

Let U be an ideal of F and $U \neq \{0\}$

Now we prove $U=F$

U is an ideal of $F \Rightarrow U \subseteq F$ — ①

Let $a \in U \subseteq F$

$\Rightarrow a \in F$, F is a field

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

$\Rightarrow a \in U$, $a^{-1} \in F$ and U is an ideal of F

Scanned by CamScanner

$\Rightarrow a \cdot a^{-1} \in U$

$\Rightarrow 1 \in U$

Let $x \in F, 1 \in U$ and U is an ideal of F

$\Rightarrow x \cdot 1 \in U$

$\Rightarrow x \in U$

$\Rightarrow F \subseteq U$ — ②

from ① & ②

$\therefore U = F$

∴ The only ideals of F are {0} and F itself.

(17)

---

3. Statement: The intersection of two ideals is again an ideal.

Proof: Let U_1, U_2 be two ideals of R.

Now we prove $U_1 \cap U_2$ is an ideal of R.

Let $a, b \in U_1 \cap U_2$

$\Rightarrow a, b \in U_1$ & $a, b \in U_2$

$\Rightarrow a, b \in U_1$ and U_1 is an ideal of R

$\Rightarrow a-b \in U_1$ and $ar, ra \in U_1$ — ①

$a, b \in U_2$ and U_2 is an ideal of R

$\Rightarrow a-b \in U_2$ and $ar, ra \in U_2$ — ②

from ① & ②

$a-b \in U_1 \cap U_2$ and $ar, ra \in U_1 \cap U_2$

$\therefore U_1 \cap U_2$ is an ideal of R.

VImp #4. Statement: If U_1, U_2 be two ideals of R then $U_1 \cup U_2$ is an ideal of R if and only if one is contained in other. (or) $(U_1 \subseteq U_2$ (or) $U_2 \subseteq U_1)$.

Proof: Given U_1, U_2 are two ideals of R.

First suppose that either $U_1 \subseteq U_2$ (or) $U_2 \subseteq U_1$

Now we prove $U_1 \cup U_2$ is an ideal.

If $U_1 \subseteq U_2$ then $U_1 \cup U_2 = U_2$, U_2 is an ideal

$\Rightarrow U_1 \cup U_2$ is an ideal.

Scanned by CamScanner

If $U_2 \subseteq U_1$ then $U_1 \cup U_2 = U_1$, U_1 is an ideal
$\Rightarrow$ $U_1 \cup U_2$ is an ideal

conversely suppose $U_1 \cup U_2$ is an ideal of R

Now we prove either $U_1 \subseteq U_2$ (or) $U_2 \subseteq U_1$.

Suppose if possible $U_1 \not\subseteq U_2$ and $U_2 \not\subseteq U_1$

$U_1 \not\subseteq U_2 \Rightarrow \exists a \in U_1 \ni a \notin U_2$

$U_2 \not\subseteq U_1 \Rightarrow \exists b \in U_2 \ni b \notin U_1$ (18)

$a, b \in U_1 \cup U_2$ and $U_1 \cup U_2$ is an ideal

$\Rightarrow a-b \in U_1 \cup U_2$

$\Rightarrow$ either $a-b \in U_1$

$a \in U_1, a-b \in U_1$	$a-b \in U_2$
$a-(a-b) \in U_1$	$a-b \in U_2, b \in U_2$
$b \in U_1$ ⊗	$a-b+b \in U_2$
	$a \in U_2$ ⊗

which is a contradiction

$\therefore$ Either $U_1 \subseteq U_2$ (or) $U_2 \subseteq U_1$

Problems:

1. If R is a commutative ring then $Ra = \{ra / r \in R\}$ is an ideal of R.

Soln: Given $Ra = \{ra / r \in R\}$

Now we prove ra is an ideal.

i) Let $r_1 a, r_2 a \in R$

where $r_1, r_2 \in R$

consider $r_1 a - r_2 a = (r_1 - r_2)a \in Ra$

ii) Let $r_1 a \in Ra$, $r \in R$

consider $r \cdot r_1 a = (r r_1)a \in Ra$

R is a commutative ring $\Rightarrow$ left ideal = right ideal

$\therefore$ Ra is an ideal

→ If U_1 & U_2 are 2 Ideals then PT $U_1 + U_2$ is an Ideal of R

2. PT $\{U\} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ where $a, b \in Z$ is a sub-ring but not an ideal.

3. $U = \{x \in R \mid ax \in 0\}$

21/4/18

Quotient ring (or) Factor ring:

Statement: Let $(R, +, \cdot)$ be a ring and U is an ideal of R then $R/U = \{x+U / x \in R\}$ forms a ring called Quotient ring (or) Factor ring.

Imp D Factor ring theorem:

Statement: If U is an ideal of R then $\frac{R}{U} = \{x+U / x \in R\}$ is a ring w.r.t $(+, \cdot)$ cosets.

Proof: Given R is a ring and U is an ideal of R.

Now we prove $(\frac{R}{U}, +, \cdot)$ is a ring.

Since $(R, +)$ is abelian group

$\Rightarrow (\frac{R}{U}, +)$ is also abelian group.

We prove the coset $(\cdot)$ is well defined.

Consider $a+U = a_1+U$ | $b+U = b_1+U$

$a+0 = a_1+u_1$ | $b+0 = b_1+u_2$ where $u_1, u_2 \in U$

$a = a_1+u_1$ | $b = b_1+u_2$

Scanned by CamScanner

$ab = (a_1+u_1)(b_1+u_2)$

$= a_1b_1 + a_1u_2 + b_1u_1 + u_1u_2$

$ab - a_1b_1 = a_1u_2 + b_1u_1 + u_1u_2 \in U$ ($\because U$ is an ideal)

$ab - a_1b_1 \in U$

$ab + U = a_1b_1 + U$

$\therefore$ coset $(\cdot)$ is well-defined. (20)

Closure: Let $a+U, b+U \in R/U$

$(a+U)(b+U) = ab+U \in R/U$

Associative: Let $a+U, b+U, c+U \in R/U$

$[(a+U)(b+U)](c+U) = a+U[(b+U)(c+U)]$

$abc+U = abc+U$

$\therefore R/U$ is a semigroup

Distributive: Consider $(a+U)\cdot[(b+U)+(c+U)]$

$\Rightarrow (a+U)\cdot[(b+c)+U]$

$\Rightarrow a(b+c)+U$

$\Rightarrow ab+ac+U$

$\Rightarrow (ab+U)+(ac+U)$

Similarly $[(a+U)(b+U)]\cdot(c+U) = (ac+U)+(bc+U)$

$\therefore (\frac{R}{U}, +, \cdot)$ is a ring

Prime ideal:

Let R be a commutative ring with unity and U is an ideal of R. U is said to be a prime ideal if $ab \in U$ $\Rightarrow$ either $a \in U$ (or) $b \in U$ where $a, b \in U$.

Maximal ideal:

Let R be a ring, an ideal M of R is said to be a maximal ideal if $\exists$ an ideal U of R with $M \subseteq U \subseteq R$ then either $U = M$ (or) $U = R$.

Scanned by CamScanner

Prime ideal theorem:

Statement: An ideal U of a commutative ring R is a prime ideal if and only if $\frac{R}{U}$ is an integral domain.

Proof: Given R is a commutative ring and U is an ideal of R.

First suppose that U is prime ideal.

i.e, $ab \in U \Rightarrow$ either $a \in U$ (or) $b \in U$.

Now we prove $\frac{R}{U}$ is an integral domain.

Consider let $a+U, b+U \in \frac{R}{U}$.

Consider $(a+U)(b+U) = 0+U$

$$ab+U = 0+U$$

$$ab-0 \in U$$

$ab \in U$ and ~~ab~~ is an prime ideal

$a \in U$	$b \in U$
$a+U=U$	$b+U=U$

$\therefore \frac{R}{U}$ has no zero divisors.

$\therefore \frac{R}{U}$ is an integral domain.

Conversly suppose $\frac{R}{U}$ is an integral domain.

Now we prove U is prime ideal.

let $a, b \in U$

Consider $ab \in U$

$\Rightarrow ab+U = U$

$\Rightarrow (a+U)(b+U) = 0+U$ and $\frac{R}{U}$ is an integral domain

$\Rightarrow$ either $a+U=0+U$ (or) $b+U=0+U$ (or) has no zero divisors

$a \in U$ (or) $b \in U$

$\therefore U$ is a prime ideal.

Scanned by CamScanner

23/11/18 Theorem:

Statement: An ideal U of a commutative ring R with unity is maximal $\Leftrightarrow \frac{R}{U}$ is a field.

Proof: Given R is a commutative ring and U is a ideal of R

first suppose that U is a maximal ideal of R

Now we prove $\frac{R}{U}$ is a field.

R is commutative with unity (22)

$\Rightarrow \frac{R}{U}$ is commutative with unity.

It is enough if we prove every non zero element of $\frac{R}{U}$ has multiplicative inverse.

Let $x+U$ be a non zero element of $\frac{R}{U}$

$\Rightarrow x+U \neq 0+U$

$x \notin U$

$\langle x \rangle$ is an ideal of R, U is an ideal of R

$\Rightarrow \langle x \rangle + U$ is also an ideal of R.

$U \subseteq \langle x \rangle + U \subseteq R$ and U is a maximal

$\Rightarrow \langle x \rangle + U = R$

$\Rightarrow x\alpha + a = 1$ where $\alpha \in R, a \in U, 1 \in R$

Consider $1+U = (x\alpha+a)+U$

$= (x\alpha+U)+(a+U)$

$= (x\alpha+U)+U \quad (\because a \in U \Rightarrow a+U=U)$

$= x\alpha+U$

$= (x+U)(\alpha+U)$

$\therefore$ for $(x+U) \in \frac{R}{U}$ $\exists (\alpha+U) \in \frac{R}{U} \ni (x+U)(\alpha+U) = 1+U$

$\therefore \frac{R}{U}$ is a field

Conversely suppose $\frac{R}{U}$ is a field.

Now we prove U is a maximal ideal of R.

Let U' be an ideal of R with $U \subseteq U' \subseteq R$ and $U' \neq U$

It is enough if we prove $U' = R$

Clearly $U' \subseteq R$

We prove $R \subseteq U'$

$U' \neq U$

$\Rightarrow \exists x \in U' \ni x \notin U$

Scanned by CamScanner

$\Rightarrow x+U \neq U$ i.e, $x+U$ is a non zero element of $\frac{R}{U}$ and $\frac{R}{U}$ is a field.

$\Rightarrow \alpha+U$ be the inverse of $x+U$. where $\alpha \in R$

$\Rightarrow (x+U)(\alpha+U) = 1+U$

$\Rightarrow x\alpha+U = 1+U$

$\Rightarrow 1-x\alpha \in U \subseteq U'$

$\Rightarrow 1-x\alpha \in U'$

$\Rightarrow x \in U'$, $\alpha \in R$ and U' is an ideal of R

$\Rightarrow x\alpha \in U'$

$\Rightarrow (1-x\alpha)+x\alpha \in U'$

$\Rightarrow 1 \in U'$

$\Rightarrow R \subseteq U'$

Hence $U'=R$

$\therefore U$ is a maximal ideal

Scanned by CamScanner

31/5/18

Model (1) Find the sum and product.

Model (2) Problems on division algorithm.

Model (3) Is $2\mathbb{Z}$ isomorphic to $3\mathbb{Z}$, find all ring hom from $\mathbb{Z}$ to $\mathbb{Z}$

Model (4) Problems on divisible by 9.

Model (5) If R is a ring of charac 2 & $\phi: R \to R$ by $\phi(x) = x^2$ P.T ϕ is homo.

Model (6) Find the factors, P.t ring homo carries idempotent to idempotent

Model (3):

1. Define $\phi: 2\mathbb{Z} \to 3\mathbb{Z}$ as $\phi(2x) = 3x \quad \forall x \in \mathbb{Z}$

Sol: Homo:

Consider $\phi(2x+2y) = \phi(2(x+y))$
$= 3(x+y)$
$= 3x+3y$
$= \phi(2x) + \phi(2y)$

Consider $\phi(2x \cdot 2y) = \phi(2(2xy))$
$= 3(2xy)$
$= 6xy$

$\phi(2x) \cdot \phi(2y) = 3x \cdot 3y$
$= 9xy$

$\therefore \phi(2x \cdot 2y) \neq \phi(2x) \cdot \phi(2y)$

$\therefore 2\mathbb{Z}$ is not isomorphic to $3\mathbb{Z}$.

2. Find all the ring homo from $\mathbb{Z}$ to $\mathbb{Z}$

Sol: Define $\phi: \mathbb{Z} \to \mathbb{Z}$ as $\phi(x) = ax$, where $a, x \in \mathbb{Z}$

Given ϕ is a homo

ie, $\phi(x+y) = \phi(x) + \phi(y) = ax + ay = a(xy)$

$\phi(xy) = \phi(x) \cdot \phi(y) = ax \cdot ay$

$\Rightarrow a(xy) = axay$

$a(xy) = a^2xy$

$a^2 - a = 0$

$a(a-1) = 0$

$\therefore$ For $a=0$, $\phi(x)=0$ is a zero homomorphism and for $a=1$.

Scanned by CamScanner

3. Find the ring homo from Z_6 to Z_6

Sol: Define $\phi : Z_6 \to Z_6$ which is a homo and

$Z_6 \{0,1,2,3,4,5\}$ as $\phi(x) = ax$

let $a \in Z_6$ and $|a| = 1, 2, 3, 6$ (divisors of 6).

$\therefore$ The elements are $0, 1, 2, 3, 4, 5$.

Consider $a^2 = a$

$0^2 = 0$

$1^2 = 1$

$2^2 = 4 \neq 2$

$3^2 = 9 = 3$

$4^2 = 16 = 4$

$5^2 = 25 \neq 1 \neq 5$

$\therefore$ The ring homomorphism $Z_6 \to Z_6$ are

$\phi(x) = 0$, $\phi(x) = x$, $\phi(x) = 3x$, $\phi(x) = 4x$.

Model ⑥:

1. Find homo carries idempotent to idempotent.

Sol: Let $\phi : Z \to Z$ be a ring homo

let a be an idempotent element in Z.

Now we prove $[f(a)]^2 = f(a)$

Consider $[f(a)]^2 = f(a) \cdot f(a)$

$= f(a^2)$

$= f(a)$

$\therefore$ Ring homo carries idempotent to idempotent.

Model ⑤:

Sol: Given R is a commutative & characteristic of $R = 2$

i.e, $2a = 0 \ \forall \ a \in R$

$\phi : R \to R$

$\phi(x+y) = \phi(x+y)^2$

$= (x+y)(x+y)$

$= x^2 + y^2 + xy + xy$

$= x^2 + 2xy + y^2$

$= x^2 + y^2$ ($\because x, y \in R \Rightarrow xy \in R \Rightarrow 2xy = 0$)

$= \phi(x) + \phi(y)$

Scanned by CamScanner

Consider $\phi(xy) = (xy)^2$
$= x^2y^2$
$= \phi(x) \cdot \phi(y)$

$\therefore \phi$ is a homo.

Model ④:

Sol: Divisible by 99:

1) 9,897,654,527,609,805 is divisible by 99:

Sol: Let $n = 9,897,654,527,609,805$ which is a two decimal representation with

$n = a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$ where $a_0 = 05, a_1 = 98, a_2 = 60, a_3 = 27, a_4 = 45, a_5 = 65, a_6 = 97, a_7 = 98$.

$n = a_7 100^7 + a_6 100^6 + a_5 100^5 + a_4 100^4 + a_3 100^3 + a_2 100^2 + a_1 100^1 + a_0$

Let the function $\alpha : \mathbb{Z} \to \mathbb{Z}_{99}$ be a natural homo with $\alpha(x) = x \pmod{99}$ and $\alpha(100) = 1$

n is divisible by 99 $\Leftrightarrow \alpha(n) = 0$

Consider $\alpha(n) = \alpha(a_7 100^7 + a_6 100^6 + a_5 100^5 + a_4 100^4 + a_3 100^3 + a_2 100^2 + a_1 100 + a_0)$

$= \alpha(a_7)\alpha(100)^7 + \alpha(a_6)\alpha(100)^6 + \cdots + \alpha(a_1)\alpha(100) + \alpha(a_0)$

$= \alpha(a_7 + a_6 + a_5 + a_4 + a_3 + a_2 + a_1 + a_0)$

$= \alpha(495)$

$= \alpha(4) + \alpha(95)\alpha(100)$

$= \alpha(99) = 0$.

$\alpha(n) = 0$

$\therefore 9,897,654,527,609,805$ is divisible by 99.

Unit-III

Model ① Find the units of Z_6 (or) Z_7

Model ② Problems on sub-ring conditions

Model ③ Ring of Guassian integer is an integral domain.

Model ④ The characteristic of boolean ring is 2. Find the characteristic of $Z_3 \times Z_4$.

Model ⑤ Problems on ideal & maximal ideal.

Scanned by CamScanner

Model ⑤:

1. Find the maximal ideal of Z_8.

Sol: $Z_8 = \{0,1,2,3,4,5,6,7\}$ is a commutative ring with unity

$\langle 1 \rangle = \{0,1,2,3,4,5,6,7\} = Z_8$

$\langle 2 \rangle = \{0,2,4,6\}$

$\langle 4 \rangle = \{0,4\}$

$\langle 8 \rangle = \{0\}$

Clearly $\langle 4 \rangle \subseteq \langle 2 \rangle \subseteq \langle 1 \rangle = Z_8$

$\langle 2 \rangle$ is a maximal ideal

Unit-II

Model ① Problems on Cayleys theorem

Model ② Problems on Homo & iso

Model ③ Find the cosets of $H = \{1, 15\}$ in $G = U(32)$.

Model ④ Problems on factor group.

Unit-I

Model ① Problems on composition table & definations of problems

Model ② Permutations problems.

Model ③ Problems on cyclic groups.

---

1. Find the no. of generators of Z_{12}

Sol: $Z_{12} = \{0, 1, 2, ---11\}$

The prime factors of Z_{12} are 2, 3

$\therefore$ The no. of generators $= n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

$= 12 \times \frac{1}{2} \times \frac{2}{3}$

$= 4$

Scanned by CamScanner

If R is a ring with unity then prove that R has no zero divisors iff concellation laws holds in R

Proof:- G.T R is a ring with unity

case(i) If R has no zero divisors then we have to prove concellation laws holds in R

let $ab = ac \; \forall \; a \neq 0, b, c \in R$

$\Rightarrow ab - ac = 0$

$\Rightarrow a(b-c) = 0$

$\Rightarrow b - c = 0$ (∵ R has no zero divisors)

$\Rightarrow b = c$

∴ R satisfies left concellation law

let $ba = ca \; \forall \; a \neq 0; b, c \in R$

$ba = ca = 0$

$(b-c)a = 0$

$b - c = 0$ (∵ R has no zero divisor)

$b = c$

R satisfies R.C.L

case(ii) If concellation laws holds in R the we have to show the R has no zero divisors

let $ab = 0 \; \forall \; a \neq 0 \; b \in R$

$\Rightarrow ab = a \cdot 0$

By using L.C.L we get $b = 0$

let $ab = 0 \; \forall \; b \neq 0, a \in R$

$ab = 0 \cdot b$

By using R.C.L $a = 0$

for $ab = 0 \Rightarrow a = 0$ (or) $b = 0$

∴ R has no zero divisors

Theorem:- If R is a commutative ring with unity P is an ideal of R then prove that P is a prime ideal of R iff R/P is an integral domain

Scanned by CamScanner

Proof: G.T R is commutative ring with unity and P is an ideal of R

$\Rightarrow$ R/P is commutative ring with unity

Case(i) If P is prime ideal of R then we have to prove R/P is an integral domain

For this it is sufficient to prove R/P has no zero divisors

Let $(P+a)(P+b) = P \;\forall\; P+a, P+b \in \frac{R}{P}$

$P+ab = P$

$ab \in P$ ($\because H+a = H \Leftrightarrow a \in H$)

$a \in P$ (or) $b \in P$ ($\because$ P is prime ideal)

$P+a = P$ (or) $P+b = P$

$\therefore$ R/P has no zero divisors

$\therefore$ R/P is an integral domain

Case(ii) If R/P is an integral domain then we have to prove P is prime ideal of R

Let $ab \in P$ for $a, b \in R$

$P+ab = P$

$(P+a)(P+b) = P$ ($\because$ R/P has no zero d)

$P+a = P$ (or) $P+b = R$

$a \in P$ (or) $b \in P$

$\therefore$ P is prime ideal of R

Theo: If R is a commutative ring with a unity and M is ideal of R then prove that M is a maximal ideal of R iff R/M is a field

Proof:- G.T R is a commutative ring with unity and M is an ideal of P

$\Rightarrow$ R/M is commutative ring with unity

Zero element in R/M is $M = M+0$ and $M+1$ is unity in R/M

Scanned by CamScanner

Case (i) If M is maximal ideal of R then we have to prove R/M is field

For this it is sufficient to prove every non zero element of R/M has multiplicative inverse ie

$\forall M+a \neq m \in \frac{R}{M} \Rightarrow M+b \in \frac{R}{m} \Rightarrow (M+b)(M+a) = M+1$

Let $M+a \neq M \in R/m$

$a \notin m$ $\because M+a = M \Leftrightarrow a \in M$ so that $M+a \neq M$

$\Leftrightarrow a \notin M$)

Let us define $Ra = \{ra / r \in R\}$

W.K.T Ra is an ideal of R

$M+Ra$ is an ideal of R

$\Rightarrow M+Ra \subseteq R \rightarrow (1)$

Let $x \in M$

But $x = x+0 \cdot a \in M+Ra$

$\Rightarrow x \in M+Ra$

$\Rightarrow M \subseteq M+Ra \rightarrow (2)$

But $a = 0+1 \cdot a \in M+Ra$

$a \in M+Ra$

But $a \notin M$

$\Rightarrow M+Ra \neq M$

from (1) & (2)

$M \subset M+Ra \subseteq R$

$\therefore M$ is maximal ideal $\Rightarrow M+Ra = R$

W.K.T $1 \in R$ be unity

$1 \in M+Ra$

$1 = M+ba$ where $b \in R$

$M+1 = M+M+ba = M+ba$ $(M+M=M)$

$M+1 = (M+b)(M+a)$

$M+b$ is a multiple inverse of $M+a \neq m+a \neq m \in \frac{R}{M}$

$\therefore \frac{R}{M}$ is field

Case(iv) If R/M is a field then we have to prove M is a maximal ideal of R

Let U is an ideal of $R \to M \subseteq U \subseteq R$

consider $U \neq M$ then we have to prove $U = R$

Q.T R/M is field

$\to (M+b)(M+a) = M+1$

$M+ba = M+1$

$ba - 1 \in M$

$ba - 1 = m \in M$

$ba - m = 1 \in M$

$1 \in U \quad (\because m \subset U)$

Q.T U is an Ideal of ring R with unit and $1 \in U$

$\therefore$ U is an ideal of R

$U \subseteq R \to (1)$

let $x \in R$ But $x = 1.x \in U$

$x \in U$

$R \subseteq U \to (2)$

From (1) & (2) $U = R$

M is a maximal ideal of R

Scanned by CamScanner