Groups Theory

Properties

(i) Closure law

$\forall a, b \in G$, $a * b \in G$ — $*$ = Binary Operation

(ii) Associative law

$\forall a, b, c \in G$ $\quad a * (b * c) = (a * b) * c$

(iii) Identity law

$\forall a \in G$, $a * e = e * a = a$ $\quad$ let $e \in G$ be the identity element

(iv) Inverse law

$\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

(v) Commutative law

$\forall a, b \in G$, $a * b = b * a$

Algebraic System: A set 'A' with one or more binary (closed) operations defined on it

Ex: $(N, +)$ (Natural no), $(Z, +, -)$ (Integers)

If properties (i) & (ii) is satisfied ⟶ Semigroup

(i) (ii) (iii) ⟶ Monoid

(i) (ii) (iii) (v) ⟶ Abelian monoid

(i) (ii) (iii) (iv) ⟶ Group

(i) (ii) (iii) (iv) (v) ⟶ Abelian Group

Ex: Show that, the set of all integers is a group with respect to addition.

Sol: $(Z, +)$ is

let $a, b, c \in Z$

(i) $a + b \in Z$ for all $a, b \in Z$

(ii) $a + (b + c) = (a + b) + c$ for all $a, b, c \in Z$

(iii) $0 \in Z$ $\quad a + 0 = 0 + a = a$ $\quad \therefore 0$ is identity element

(iv) $-a \in Z$ such that $a + (-a) = 0$

$a + e = e + a = a$

let $a = 3$

$3 + e = 3$

$e = 3 - 3$

$e = 0$

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

Say $a = 3$ $\quad 3 + a^{-1} = 0$

$3^{-1} = -3$

papergrid
Date: / /

Group Theory

$N = \{1, 2, 3, 4 \ldots \infty\}$
$Z = \{$ Set of all int $-\infty, \infty\}$
$Q = \{$ Set of all rational no $\}$
$R = \{$ Set of all real no $\}$
$C = \{$ Set of all complex no $\}$

$Q^* =$ Q without zero
$Z_n^+ =$ additive modulus

AS ↓ Semigroup ↓ Monoid ↓ Group ↓ Abelian

Algebric Structure : A non empty set S is algebric structure wrt to binary operation $*$ closure operation
if $(a * b) \in S \quad \forall (a, b) \in S$

Semigroup : An algebraic structure $(S, *)$ is semigroup if it follows associative property.
$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$

Monoid : $(S, *)$ if there exists an element 'e' $\in S$ such that
$(a * e) = (e * a) = a \quad \forall a \in S$ ↓ identity element

Group : Monoid $(S, *)$ with identity element 'e' is called group if to each element $a \in S$, there exist an element $b \in S$ such that $(a * b) = (b * a) = e$ then b is inverse of a
$a^{-1} = b$ & $b^{-1} = a$

Abelian / Commutative Group : $(a * b) = (b * a) \quad \forall a, b \in G$ $(G, *)$

Theorem

① ST in group G, Identity element is unique

Soln : Suppose there are two identities e_1 & e_2 in G

~~$e_1 \notin G$~~ ~~$e_2 \notin G$~~

If e_1 is identity element & $e_2 \in G$
$e_1 * e_2 = e_2 * e_1 = e_2 \longrightarrow (1)$

If e_2 is identity element & $e_1 \in G$
$e_2 * e_1 = e_1 * e_2 = e_1 \longrightarrow (2)$

From (1) (2)
$e_1 = e_2$.

papergrid

Date: / /

② ST in group G, the inverse of each element is unique

Sol^n: Suppose $a^{-1} = b$ & $a^{-1} = c$, $a, b, c \in G$

$a * b = b * a = e \longrightarrow (1)$

$a * c = c * a = e \longrightarrow (2)$

$(b * a) * c = b * (a * c)$ => Associative property

$e * c = b * e$

$c = b$

∴ Inverse of 'a' is unique

③ ~~ST in G, the if a,~~ If $a, b, c \in G$ & $ab = ac$ then $b = c$

(Left cancellation property)

Sol^n: Suppose $ab = ac$

since $a \in G$, we know $a^{-1} \in G$

Then $a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$ by associativity on both side

$eb = ec$ bcoz $a^{-1}a = e$

$b = c$ bcoz e is identity.

④ If $a, b, c \in G$ & ~~$ac = bc$~~ $ba = ca$, then ~~$a = b$~~ $b = c$ (Right cancellation)

Sol^n: Suppose $ba = ca$

Since $a \in G$, we have $a^{-1} \in G$

Then $(ba)a^{-1} = (ca)a^{-1}$

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

$be = ce$ by $a^{-1}a = e$

$b = c$ by identity

Subgroup

A non empty subset H of group G is called subgroup of G if

(i) H is stable (closed) for composition defined in G

(ii) H itself is a group for composition induced by that of G

$(G, +) \longrightarrow (H, +)$.

Every group G has $\{e\}$ or G as subgroup. Then it is trivial and improper subgroups. All others are nontrivial or proper.

$(\mathbb{C}-\{0\}, \cdot)$ $\quad H = \left\{1, \frac{1+\sqrt{3}i}{2}, \frac{1+\sqrt{3}i}{2}\right\}$ (sub)

Theorem

① If H is a non-empty subset of group G then H is subgroup of G if & only if

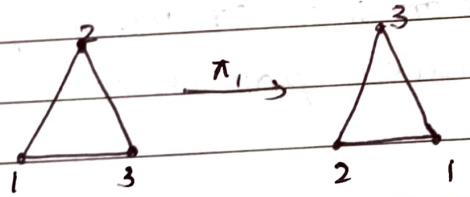
(i) for all $a, b \in H$, $ab \in H$

Sol: ~~Assuming~~ $(G, \cdot)$ ~~is group~~.

let H be subgroup of G then $(H, \cdot)$

let $a, b \in H$, $a \in H$

$a^{-1} \in H$



$\pi_1 : \{1,2,3\} \to \{1,2,3\}$

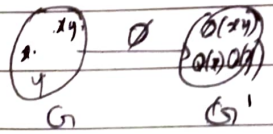
$\pi_1(1) = 3 \quad \pi_1(2) = 1 \quad \pi_1(3) = 2$

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

Homomorphism

$\phi : G \to G'$ is a group homomorphism iff $\phi(xy) = \phi(x)\,\phi(y)$

$\forall x, y \in G$



ϕ

Pi

$\phi(xy) = \phi(x) * \phi(y)$

Identity mapped to Identity

$e \in G \quad e' \in G'$

$\phi(e) = e'$

$\phi(e) = \phi(ee) = \phi(e)\,\phi(e)$

$e'\,\phi(e) = \phi(e)\,\phi(e)$

In homomorphism, identity of G will always be mapped to identity of G'

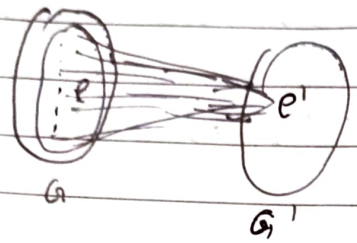
papergrid

Date: / /

Kernel $\ker \phi = \{x \in G : \phi(x) = e'\}$ — normal subroot

$\ker \phi \triangle G$ $\quad \frac{G}{\ker \phi}$ → Factor group

trivial homomorphism



Isomorphism = $G \cong G'$

In $\phi : G \longrightarrow G'$ it needs to be homomorphism, 1-1, onto

Cyclic groups $< \ >$

Group that can be generated by single element of that group.
An element 'g' generates the group if every element of the group can be obtained by repeatedly applying the group operation or its inverse to g.

Homomorphism with 1-1 function is called monomorphism
Homomorphism with onto is called epimorphism

papergrid
Date: / /

Coding Theory

$r = c + e$

r = recieved ~~bit~~ word c = coding word e = error word

→ When we know the position of errors $p^k (1-p)^{n-k}$

→ When we know the no. of errors $({}^nC_k)(p^k)(1-p)^{n-k}$

① c = 1010110 e = 0101101

1010110

(XOR) 0000101

r = 1111011 k = 4 errors

Compare c & r → To get k

$p^k (1-p)^{n-k}$ p = 0.05

$(0.05)^4 (1-0.05)^3$

= 7.289 $\times 10^{-6}$

= 0.000007289

② c = 1010110 p = 0.02 r = 1011111

c = 1010110

r = 1011111

e = 0001001 k = 2 errors

$= (0.02)^2 (1-0.02)^{7-2}$

= 0.000 36

To get e, check the changes in c & r, whichever is changed will be marked 1.

③ p = 0.05 e = 011011101 k = 1

n = 9 $\binom{9}{1}(0.05)^1(1-0.05)^8$

0.2985

111 011 100

111 011 110

papergrid
Date: / /

16/8 •• Encode

Decode

$D(x) = D(x_1 x_2 \ldots x_m x_{m+1} \ldots x_{2m} x_{2m+1} \ldots x_{3m})$

$= S_1 S_2 \ldots S_m$

$S_i = \begin{cases} 1 & \text{if } x_i x_{i+m} x_{i+2m} \text{ has majority of 1's} \\ 0 & \text{has majority of 0's} \end{cases}$

① $E(00)\ E(01) = 00000\ 11111 = 5$

$E(00)\ E(10) = 5$ min = 5

$E(00)\ E(11) = 10$ ED = 4

$E(01)\ E(10) = 10$ EC = 2

$E(01)\ E(11) = 5$

$E(10)\ E(11) = 5$

②

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

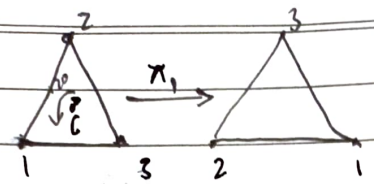
Decode

$$H = \begin{bmatrix} 1+0+1+1+0+0 \\ 1\ 1\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 0\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{matrix} 1+0+1+1+0 \\ 1+1+0+1+0 \\ 0+1+0+0+1 \end{matrix}$$

papergrid
Date: / /

Ex: 15.32

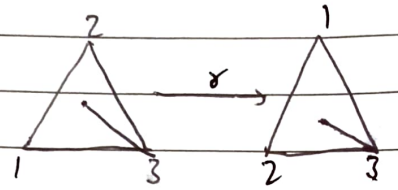


$1 \xrightarrow{\pi_1} 3$

$\pi_1 : \{1, 2, 3\} \longrightarrow \{3, 1, 2\}$

$\pi_1(1) = 3$

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



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

π, γ $\quad 1 \xrightarrow{\pi_1} 3 \xrightarrow{\gamma_1} 3$

$2 \xrightarrow{\pi_1} 1 \xrightarrow{\gamma_1} 2$

S_3 : Symmetric group 3 symbols

Excercise 16.1

① a) $\{-1, 1\}$ under multiplication

$1 \cdot 1 = -1$

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

$1 \cdot \boxed{1} = -1$ $\quad -1 \cdot \boxed{\frac{1}{-1}} = 1$ ✓

b) $\{-1, 1\}$ under addition ✗ $\quad -1 + 1 = 0$ ✗

c) $\{-1, 0, 1\}$ under addition ✓

d) $10n_1 + 10n_2 =$ ✓ $\quad 10n + \boxed{0} = 10n$ $\quad 10n \boxed{-10n} = 0$ ✓

e) $g(1) \cdot (g(2) \cdot g(3))$ ✗

$g(1) \cdot (g(g(2)))$ $\quad g(g(1)) \cdot g(2)$

$g(1) \cdot 2$ $\quad 1 \cdot g(2)$

$1 \cdot 2$ $\quad = \quad 1 \cdot 2$

papergrid
Date: / /

③ let $a=0 \quad b=2 \quad c=4$

Asso $\Rightarrow (0-2)-4 = 0-(2-4)$

$(-2)-4 = -(-2)$

$-6 \neq -4$

⑭ $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ $\quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$

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

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

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

④ ~~$-2, \frac{2}{3}$~~

~~$-2 + \frac{2}{3} + \frac{-2}{3} \quad \frac{2}{3} = 2 - \frac{4}{3}$~~

~~for $x \circ y = x+y-xy = x$~~

~~$x-y-xy+x(-y-xy)$~~

~~$x-y-xy-xy-x^2y$~~

~~x~~

for every x, closure ✓

for $x \circ (y \circ z) = x \circ (y+z+yz)$ ✓

$= x+y+z+yz+xy+xz+xyz$

$(x \circ y) \circ z = (x+y+xy) \circ z$

$= x+y+xy+z+xz+yz+xyz$

$x \circ e = x$

$x+e+xe = x$

$e+xe = 0$

✓ $e(1+x) = 0$

$\boxed{e=0}$

$x \circ a = 0$

$x+a+xa = 0$

$a+xa = -x$

✓ $a(1+x) = -x$

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

$x \circ y = x+y+xy$

$y \circ x = y+x+yx$

✓

paperg
Date: / /

(8) Done in example

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

~~lets~~ $a = g^{-1}$ $(a^{-1})^{-1} = b = g^{-1}$ ~~lets~~ take $a = g^{-1}$ $(a^{-1})^{-1} = g^{-1}$

~~$a \neq e$~~

$a * g^{-1} = e$

$b * g^{-1} = e$

$a * g^{-1} = b * g^{-1}$

lets take $a \in G$

$a * a^{-1} = e$ Since $a^{-1} \in G$, $a^{-1} * (a^{-1})^{-1} = e$

$a * e = a$

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

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

$a * e = a$

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

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

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

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

~~$a, b \in G$~~

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

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

$\therefore a e a^{-1} = e$

$aa^{-1} = e$

$e = e$

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

lets take

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

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

$\therefore a e a^{-1} = e$

$aa^{-1} = e$

$e = e$

$\therefore$ It means that our assumption is right ie, $(ab)(b^{-1}a^{-1}) = e$

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

papergrid
Date: / /

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

Since it is abelian $b^{-1}a^{-1} = a^{-1}b^{-1}$

∴ By prev question $(ab)^{-1} = b^{-1}a^{-1}$

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

Generating subgroups = divisors of modolo element

a) $(Z_{12}, +)$

elements = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} = 12

12 % 1 = 0
12 % 2 = 0
12 % 3 = 0
12 % 4 = 0
12 % 5 = 2 X

{0}, {0,6} {0,3,6,9} {0,4,8} {0,2,4,6,8,10}
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}

b) $(Z_{11}^*, \cdot)$

{1,2,3,4,5,6,7,8,9,10}. {1,2,4,6,8,10} {

Theorem

① Let $(G, \circ)$, $(H, *)$ be groups with respective identities e_G, e_H. If $f: G \to H$ is a homomorphism then

a) $f(e_G) = e_H$

→ Bcoz f is homomorphism

$f(a \circ b) = f(a) * f(b)$

$e_G \circ a = a \circ e_G = a$

$f(e_G \circ e_G) = f(e_G) * f(e_G)$

$g \in G$

$g \circ e_G = g$

$f(g \circ e_G) = f(g)$ ← Homomorphism

$f(g) * f(e_G) = f(g)$ —— ①

$h \in H$ e_H is identity of H $h * e_H = h$ —— ②

Since g is some arbitary element of G then $f(g)$ will map some arbitary element of H.

Since ① ② are resembling to each other if $f(e_G) = H$ then the equation will be satisfied.

b) $f(S)$ is a subgroup of H for each subgroup S of G

→ Let S be subgroup of G

so $S \neq \emptyset$ (not empty) ∴ $f(S)$ must map to some elements

$x, y \in f(S)$

$x = f(a)$ $y = f(b)$ for some $a, b \in S$

Since S is subgroup of G

$a \circ b^{-1} \in S$

$f(a \circ b^{-1})$ Bcoz f is homomorphism

$f(a) * f(b^{-1})$

$f(a) * [f(b)]^{-1}$

$x * y^{-1} \in f(S)$

Since $f(S)$ is closed under operation $*$ and has inverses $f(S)$ is subgroup of H.

papergrid
Date: / /

$f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

→ $a \in G$

$a \circ a^{-1} = e_G$

$f(a \circ a^{-1}) = f(e_G)$

$f(a) \circ f(a^{-1}) = f(e_G)$

$f(a) \circ f(a^{-1}) = e_H$ By theorem a)

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

$f(a^n) = [f(a)]^n$ for all $a \in G$ & $n \in Z$

→

for $n \geq 0$,

$a^n = a \circ a \circ a \circ \ldots \circ a$ (n times)

$f(a^n)$

$= f(a \circ a \circ a \circ a \ldots \circ a)$

$= f(a) * f(a) * \ldots * f(a)$

$= [f(a)]^n$

for $n < 0$,

paperg
Date: /

To find cyclic element, ~~first~~ for each element try to find out its ~~power~~ mod ~~no~~ of Power and if it gives

(In multiplication identity elements will also be cyclic element also

For addition

Ex $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

~~0 is cyclic element~~

Check 0: ~~0+0=0~~ $0.0 = 0$

Check 1: $1 = 1$
$2.1 = 2$
$3.1 = 3$
$4.1 = 4$
$5.1 = 5$
$6.1 = 0$

Check 2: $2 = 2$
$2.2 = 4$
$2.3 = 0$

Check 3: $3 = 3$
$2.3 = 6$

✓ Check 5: $5 = 5$
$2.5 = 4$
$3.5 = 3$
$4.5 = 2$
$5.5 = 1$
$6.5 = 0$

Check 4: $4 = 4$
$2.4 = 2$
$3.4 = 0$

1 and 5 are cyclic element

For multiplication

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Check 2: $2^1 = 2$
$2^2 = 4$
$2^3 = 8 = 1$

✓ Check 3: $3^1 = 3$
$3^2 = 9 = 2$
$3^3 = 6$
$3^4 = 4$
$3^5 = 5$
$3^6 = 1$

Check 4: $4^1 = 4$
$4^2 = 2$
$4^3 =$

papergrid
Date: / /

Order If G is group & a is element in G, order of a or O(a) is the smallest positive integer such that $a^n = e$, where e is identity element of group

- $\langle a \rangle = \{e\}$ then $O(a) = 1$
- $\langle a \rangle \neq e$ ∴ which means its finite

$$\langle a \rangle = \{a^m \mid m \in Z\} \qquad a^s = a^t \quad 1 \leq s \leq t$$

$$a^{t-s} = e$$

$O(a)$ is $t-s$

- $\langle a \rangle$ $(1$ to $n-1) \neq a^n = e$

Theorem

① If $a \in G$ with $O(a) = n$. If $k \in Z$ and $a^k = e$ then $n \mid k$

Soln: By Division Algo

$$k = qn + r \qquad 0 \leq r < n,$$

W.k.t $a^k = e$

$$a^{qn+r} = e$$

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

$$(a^n)^q \cdot a^r = e \qquad (a^n = a^k = e)$$

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

$$a^r = e$$

∴ We basically need smallest positive integer than n such that $a^r = e$ So r is 0

∴ $k = qn$

which ↳ $n \mid k$

② Let G be cyclic group

papergrid
Date: / /

Excersise.

2) a) $A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ $A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ $A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

b) $\{A, A^2, A^3, A^4\}$ under matrix multiplication

2) a) $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ $A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

b) Closure ✓
Associativity ✓ $A(A^2, A^3) = (A, A^2)A^3$
Identity ✓ I or A^4
Inverse ✓
Commutativity ✓ $A \cdot A^2 = A^2 \cdot A$ ✓

c) $A \longrightarrow i$ $A^2 \longrightarrow -1$ $A^3 \longrightarrow -i$ $A^4 \longrightarrow 1$

$A \cdot A = i \cdot i = A^2 = -1$

$A \cdot A^2 = A^3 = i \cdot -1 = -i$

$A \cdot A^3 = A^4 = i \cdot -i = 1$

So, 1 to 1 onto ∴ It is Isomorphism

4) $f: G \longrightarrow H$ is homomorphism onto

Since f is onto, every elements in H is mapped

$a, b \in G$ $x, y \in H$

$f(a) = x$ $f(b) = y$

$xy = f(a) f(b)$

$= f(ab)$ Base of homomorphism

$= f(ba)$ G is abelian

$f(b)f(a)$

yx

$xy = yx$

Since $x, y \in H$ & $xy = yx$

H is abelian

papergrid
Date: / /

Theorem

(1) Let G be cyclic group

a) If |G| is infinite, then G is isomorphic to (Z, +)

→ G is generated by a

so $G = \langle a \rangle = \{ a^k \mid k \in Z \}$

$f : G \to Z$ s.t. $\Longrightarrow$ so $f(a^k) = k$

proving one to one

assuming $f(a^k) = f(a^t)$ which means $k = t$

this means that element $a^k = a^t$ must be same or else it would contradict to the one to one. So there is no two elements mapping to same element

proving onto

lets take any $m \in Z$. $\bigcirc \longrightarrow m$

$f(a^m) = m$

This says that for every integer $m \in Z$, there is some mapping done

proving homo

$a^m, a^n \in G$

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

$= m+n$

w.k.t $f(a^m) + f(a^n) = m+n$ by homomorphism

So $f(a^m . a^n) = f(a^m) + f(a^n)$

∴ It is homomorphism, onto & one to one

∴ It is isomorphism

b) If $|G| = n$, where $n \geq 1$, then G is isomorphic to $(Z_n, +)$

→ G is cyclic group so $G = \langle a \rangle$

and $a^n = e$ $|G| = n$

$f : G \to Z_n$ by $f(a^k) = [k]$ — represents the equivalence class of k mod n in Z_n.

$f(a^k . a^m) = f(a^{k+m})$

$= [k+m]$

$= [k] + [m]$

$= f(a^k) + f(a^m)$

papergrid
Date: / /

f is one to one and onto bcoz each distinct power a^r maps to unique element in Z_n bcoz $n \geq 1$ Which means that every element of Z_n has preimage in G

$\therefore$ G is isomorphic to Z_n

(2) Every subgroup of a cyclic group is cyclic.

Let G be cyclic group generated by 'a'

i.e. $G = \langle a \rangle$

H be subgroup of G

Let k be least +ve int such that $a^k \in H$ & $b \in H$

Since $b \in H \therefore b \in G$

$b = a^m$ for some integer m

We claim that $k | m$

By division algo, $m = qk + r$, $0 \leq r < k$

$a^r = a^{m - qk}$

$a^m \cdot a^{-qk}$

$b \cdot (a^k)^{-q} \in H$ $\quad a^k \in H$, $b \in H$

$a^r \in H$, $0 < r < k$

But k is some least +ve int which will divide $k | m$

$m = qk$ for some int q

$b = a^m \cdot a^{rq}$

But b is arbitary element $b \in G$ and $b \in H$

Every element of H can be expressed as $H = \langle a^r \rangle$

H is cyclic

G is cyclic group

Let H be non-trivial subgroup of G

$S = \{ n : n \in \mathbb{Z} \text{ & } g^n \in H \}$

Let d be least +ve int such that $g^d \in H$ and d is smallest exponent

$H = \langle g^d \rangle$

By division algo, $m = dq + r$ $\quad 0 \leq r < d$

$g^m = g^{dq + r}$

papergrid

Date: / /

$g^m = g^{dq} \cdot g^r$

$= (g^d)^q \cdot g^r$

Since $g^m \in H$ $(g^d)^q$ and $g^r \in H$

d is smallest positive int $g^d \in H$, r must be 0

$g^m = (g^d)^q$

$m = dq$

$g^d \in H$ $H = \langle g^d \rangle$

∴ H is cyclic

③ Lagrange's Theorem

If G is finite group of order n with H a subgroup of order m, then m divides n.

→ Let G be group $|G| = n$

Let H be subgroup of G $|H| = m$ $\{a_1, a_2 \ldots a_m\}$

left coset of H = $gH = \{gh \mid h \in H\}$ for some $g \in G$

Since $g \notin H$ $gH \neq H$

so $gH \cap H \neq \emptyset$

If $G = aH \cup H$, then $|G| = |aH| + |H|$

=

This will work for every other elements g outside the H

$G = a_1H \cup a_2U \ldots Ua_kH$ k is the member of left cosets of H

$|G| = k|H|$

$n = km$

∴ m divides n

No. of coset formula

$$\frac{\text{No. of elements}}{\text{No. of subgroup}}$$

No. of subgroup can be identified by seeing the original group where it gives back the same group

Lemma

① If H is subgroup of finite group G, then for all $a, b \in G$

a) $|aH| = |H|$

→ Consider left coset $aH = \{ah \mid h \in H\}$

Assuming size of aH is at most the size of H $\quad |aH| \leq |H|$

$h_i, h_j \in H \quad h_i, h_j$ are distinct elements of H

ah_i, ah_j are distinct elements of aH

$\therefore |aH| = |H|$

b) either $aH = bH$ or $aH \cap bH = \emptyset$

$aH \cap bH \neq \emptyset$

$aH \cap bH$, so $x = ah_1 = bh_2$ for some h_1, h_2 in H

$a = bh_2 h_1^{-1}$

so $y = bh_2 = ah_1$

$b = ah_1 h_2^{-1}$

$bH \subseteq aH$ and $aH \subseteq bH$ $\therefore aH = bH$

papergrid
Date: / /

Exercise

(a) Let p be a prime

a) If G has order 2p, p.t every subgroup of G is cyclic

→ $|G| = 2p$ where p is prime

Possible orders of G are divisors of 2p

i.e, 1, 2, p, 2p

But 1 & 2p are trivial subgroups and G itself.

If there is subgroup H of order p since p is prime

it is cyclic (all groups of prime order are cyclic)

If there is subgroup H of order 2 it must also be cyclic

bcz there's only one such subgroups generated by any element of order 2.

∴ All proper subgroups of G is cyclic

b) If G has order p^2, p.t G has subgroup of order p

→ $|G| = p^2$

If G is cyclic, $G = \langle g \rangle$ then subgroup generated by g^p has order p

If G is not cyclic, G is isomorphic to either Z_{p^2} or $Z_p \times Z_p$ both of which have subgroups of order p.

∴ G has subgroup of order p

Note

Finding the order will be x which is smallest +ve $kx \equiv 0$ (after modulus)

Ex: Elements of order 10 $a^k = \frac{40}{\gcd(40,k)} = \frac{40}{\gcd(40,10)} = \frac{40}{4}$

$10 = \frac{40 \cdot 4}{\gcd(40,k)}$

$\gcd(40,k) = 4$

papergrid
Date: / /

Exercice

③ $G = (Z_6, +)$ $H = (Z_3, +)$ $K = (Z_2, +)$

$H \times K$ $(\overset{H}{a}, \overset{K}{b})$

$H = \{0, 1, 2\}$ $K = \{0, 1\}$

$(0,0)$ $(0,1)$ $(1,0)$ $(1,1)$ $(2,0)$ $(2,1)$

$G = \{0, 1, 2, 3, 4, 5\}$

$f(0) = (0,0)$

$f(1) = (0,1)$ ....

⑤ $f: \underset{\oplus}{Z \times Z} \longrightarrow \underset{+}{G}$ $(a,b) \oplus (c,d) = (a+c, b+d)$

$f(1,3) = g_1$ $f(3,7) = g_2$

$f(4,6) = ?$ g_1 g_2

~~$f(4,6) = f(a(1,3)) \oplus f(b(3,7))$~~

$f(4,6) = a(1,3) \oplus b(3,7)$

$f(4,6) = f(a(1,3)) + f(b(3,7))$

$f(4,6) = a f(1,3) + b f(3,7)$

$(4,6) = (1a, 3a) \oplus (3b, 7b)$

$(4,6) = 1a+3b,\ 3a+7b$

$4 = 1a+3b$ $6 = 3a+7b$

$4 - a = 3b$ ~~$\frac{6 = a + 7b}{3}$~~

$18 = 9a + 21b$

$18 - 9a = 21b$ ~~$18 - 9a = 21b$~~

~~$4 = a - 3b$~~

$4 = 1a+3b$ $6 = 3a+7b$

$4 - 3b = a$ $\longrightarrow$ $6 = 12 - 9b + 7b$

$6 - 12 = -2b$

$4 - 9 = a$ $-6 = -2b$

$\boxed{a = -5}$ $\longleftarrow$ $\boxed{b = 3}$

$f(4,6) = a f(1,3) + b f(3,7)$

$= -5 g_1 + 3 g_2$

$(a,b) = a(1,3) \oplus b(3,7)$

$(a,b) = a + 3b,\ 3a + 7b$

$a + 3b = 4$

$3a + 7b = 6$

$ab = 12$

$7b = 6$

$2b = 6$

$b = 3$

$a = -5$

10 2/3

papergrid

Date: / /

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

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

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

(9)

(1) $(Z_p^*, \cdot)$ $\{1, \ldots, p-1\}$

Z_5

$5^1 \equiv 5$

$5^2 = 25 = 5$

$(Z_5^*, \cdot) = \{1, 2, 3, 4\}$ 2, 3 is cyclic element

$\times 1$: $2^1 = 2$ $3^1 = 3$ $4^1 = 4$

$2^2 = 4$ $3^2 = 9 = 4$ $4^2 = 1$ $\langle 2 \rangle$ $\langle 3 \rangle$

$2^3 = 8 = 3$ $3^3 = 2$

$2^4 = 1$ $3^4 = 1$

16.3

(3) $S_4 = 4! = 24$ order = 2 No. of subgroup = 2

coset $= \frac{24}{2} = 12$

(5) $|G| = 660$ $|K| = 66$ $K \subseteq H \subseteq G$

$66 < H < 660$

$|G| = 660 = (2 \times 2 \times 3 \times 5 \times 11)$

$|K| = 66 = (2 \times 3 \times 11)$

$2 \times 2 \times 3 \times 5 \times 11$

$2 \times 3 \times 11$

2 or 5

$|H| = \frac{|G|}{|K|} \times (|G| \cap |K|)$

$= 2\,(2 \times 3 \times 11)$ or $5(2 \times 3 \times 11)$

$= 132$ or 330