Algebra

① G is a group $\Rightarrow (G, *)$ where $*$ is a bin-op.

(a) $a, b \in G \Rightarrow a * b \in G$ — Closed

(b) $a(b*c) = (a*b)*c$ — Associative

(c) $a * e = e * a = a$ — Identity (+) Unique ✓

(d) $a * b = b * a = e$ — Inverse (+) Unique ✓

② Some trivial proofs

(a) $ax = b$ has unique-soln in x in G.

Given G is group, $a \in G \Rightarrow a^{-1} \in G$.

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

Put $x = a^{-1}b$ in original $\Rightarrow a.(a^{-1}b) = b \Rightarrow (e.b = b)$

Hence $x = a^{-1}b$ is a solution.

- Uniqueness $\equiv$ $ax_1 = b$, $ax_2 = b \Rightarrow ax_1 = ax_2$.

$\Rightarrow a^{-1}(ax_1) = a^{-1}(ax_2)$

$\Rightarrow x_1 = x_2$

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

Given $a \in G$, $a^{-1} \in G$, $b \in G$, $b^{-1} \in G$. ; $ab \in G$, So $(ab)^{-1}$ exists

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

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

(c) Left identity ($ea = a$) is also right identity in G.

$a \in G$, e be left id then 'a' has left inverse $\Rightarrow a^{-1}a = e$

Now, $a^{-1}(ae) = (a^{-1}a)e = ee = e = a^{-1}(a)$

$a^{-1}(ae) = a^{-1}(a) \Rightarrow$ Cancellation $\Rightarrow ae = a \Rightarrow$ Hence Proved

:) Show $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ α is $\mathbb{R}$, forms group under matrix multiplication.

(i) Closure $\equiv A_\alpha \cdot A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix}$

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

(ii) Matrix mult is associative.

(iii). $0 \in \mathbb{R} \Rightarrow A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in A_\alpha$

$A_0 A_\alpha = A_\alpha A_0 = A_\alpha$ A_0 is identity.

(iv). $\alpha \in \mathbb{R} \Rightarrow -\alpha \in \mathbb{R}$.

$A_{-\alpha} A_\alpha = A_0$ ($A_{-\alpha}$ is inverse)

So, A_α forms a group.

:) $a * b = |a| \cdot b$ on R_0, where $R_0 = \mathbb{R} - \{0\}$

Is it a group? Examine.

$a * b = a \Rightarrow |a| b = a \Rightarrow b = a/|a|$ $\begin{cases} -1 \text{ if } a<0 \\ 1 \text{ if } a>0 \end{cases}$ Not unique

So, not a group.

NOTE: STICK TO ONLY LEFT OR RIGHT Identity, Inverse in proving Group. Also, Check inverse by putting it back in equation.

3) Composition Table

- Closure ≡ All entries in table $\in G$
- If any row coincides with top row ⇒ Identity element
- Every row and column contains identity ⇒ Inverse property
- Abelian ≡ If no change on interchange rows, columns

8 Show $f_1(z)=z$, $f_2=\frac{1}{z}$, $f_3=1-z$, $f_4=\frac{z}{z-1}$, $f_5=\frac{1}{1-z}$, $f_6=\frac{z-1}{z}$. on set of $\mathbb{C}-\{0,1\}$ form a finite non-abelian group of order 6 w.r.t composition of functions

$f_1 f_2=\frac{1}{z}$, $f_1 f_3=1-z$, $f_1 f_4=\frac{z}{z-1}$, $f_1 f_5=\frac{1}{z-1}$, $f_1 f_6=\frac{z-1}{z}$

$f_1=\frac{1}{z}$; $f_2 f_2=z$; $f_2 f_3=\frac{1}{1-z}$; $f_2 f_4=\frac{z-1}{z}$; $f_2 f_5=1-z$; $f_2 f_6=\frac{z}{z-1}$

ly for f_3, f_4, f_5, f_6.

Construct Composition table.

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

(i) All entries $f_1, f_2, f_3, f_4, f_5, f_6$

(ii) $h(gf)=(hg)f$ As comp of f's is associative

(iii) f_1 is identity

(iv) Inverse for each element

(v) Non commuting $f_2 f_3 \neq f_3 f_2$

6 elems. So $o(G)=6$.

4) Some Groups

- Roots of Unity (x^m) ≡ Order n, Abelian Groups
- Quaternion Group ≡ Non-abelian order 8 $\{\pm 1, \pm i, \pm j, \pm k\}$
  - $i^2=j^2=k^2=-1$; $ij=-ji=k$ and so on

$+_m$ modulo m $\quad a +_m b = r \quad (0 \le r < m)$

$a \equiv b \mod m$ if $a-b$ is divisible by m (Congruence)

- $x \equiv y \pmod 5$
  - Modulo 5 partitions the set of integers into 5 equivalence classes $[(5k+0) \cup (5k+1) \cup (5k+2) \cup (5k+3) \cup (5k+4)]$
    - Set of residue classes mod m (5)

Prove $G = \{0,1,2,3,4\}$ is an abelian group of order 5 w.r.t. $+_5$

- Construct composition table

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(i) Closed
(ii) Assoc - obvious
(iii) Id = 0
(iv) Inverse ⇒ 0 in each row and column
(v) Abelian ⇔ interchange rows, columns.

$$U_n = \{ x \in Z \mid 1 \le x < n \mid (x, n) = 1 \}$$

(6) X_p module p (p need not be prime, U_p)

$3 X_7 3 = 2$; $-32 X_4 5 = 0$ $\quad \therefore 0 \notin U_p$ $\quad$ ($1 \le i < p$)

. p is prime ≡ if $p \neq 0$ and $p \neq \pm 1$ and only $p, \pm 1$ divide

. U_p is a group of order $p-1$.

(X) └ Closure ⇒ $a, b \in U_p \Rightarrow TS: = ab \neq 0$;

$\Downarrow$

$a, b \neq 0 \Rightarrow ab \bmod p = 0$ iff

$p \mid a$ or $p \mid b$ ⇒ but $a \in (1 \dots p-1)$ So $p \nmid a$, likely $p \nmid b$.

Hence $ab \neq 0$.

└ Inverse ⇒ $k \in U_p$

$\gcd(k, p) = 1 \Rightarrow kx + py = 1 \Rightarrow kx = 1 - py \Rightarrow$

$kx = 1 \bmod p \Rightarrow x$ is inverse of k.

(*) └ Closure (U_n) : $a X_n b = c$ $\quad TS: (c \neq 0) = 1$

$c \neq 0$ or else $n \mid ab$, not as $\underbrace{(a,n) = 1}_{①} = \underbrace{(b,n)}_{②}$

So, $c \neq 0$ ✓

Assume, If c, n are not co-prime ⇒ ∃ p prime s.t $p \mid c$, $p \mid n$

Also $ab = nq + c$; $\quad p \mid ab$

└ $p \mid a$ or $p \mid b$

Then $p \mid a$ and n ⇒ $(a,n) \neq 1$ Contradicts ①

$p \mid b$ and n ⇒ $(b,n) \neq 1$ Contradicts ②

So, $(c,n) = 1 \Rightarrow c \in U_n$

$ax + py = 1 \quad ax = 1 - py \longrightarrow ax \equiv 1 \bmod p$

So x is inverse of a

① Show / Proofs / Thms

NOTE: Thms of n, look for induction

(1) If $n>0$, integer $a.a^n = a^n.a$

$n=1 \Rightarrow a.a = a.a \Rightarrow a^2 = a^2$.

$n=k \Rightarrow a.a^k = a^k.a$.

$n=k+1 \Rightarrow a.a^{k+1} = a^{k+1}.a$ (TS)

$\Rightarrow (a.a^k)a = (a^{k+1}).a \leftarrow$ Hence Proved

(2) $\boxed{(ab)^n = a^n b^n}$ only when G is abelian

* Proof by induction.

(3) $a^2 = e \Rightarrow G$ is abelian.

$+a.$

$a(ba)b = e \Rightarrow a^2(ba)b^2 = ab \Rightarrow \boxed{ba = ab}$

* $(ab)^2 = e \Rightarrow (ab)(ab) = e \Rightarrow (ab)^{-1} = ab \Rightarrow b^{-1}a^{-1} = ab$

$a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$. Illy $b^{-1} = b$ $\boxed{ba = ab}$ Hence Proved

(4) $(ab)^m = a^m b^m$ for 3 consecutive integers. Show abelian.

Assume for m, $m+1$, $m+2$

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

$\Rightarrow b^m a = ab^m$ — (1)

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

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

$b.b^m a = b^{m+1}a \Rightarrow ab^{m+1} = bab^m \Rightarrow ab = ba$ Proved

* $ab = b^2abaa^2 = b(ba)^2 a$

$= bea = ba$..

③ Order of an element.

$(G, .)$, $a \in G$.

$o(a)$ is least +ve integer n such that $a^n = e$. (0 for + groups)

(1) Order $(a^r) \leq$ Order (a).

$a^n = e$. $(o(a) = n)$ $\equiv$ n is least +ve integer

Let $o(a^r) = m$. $\Rightarrow (a^r)^m = e$. m is least +ve integer

$a^n = e \Rightarrow (a^n)^r = e \Rightarrow (a^r)^n = e. \Rightarrow o(a^r) \leq n$

$\Rightarrow \boxed{m \leq n}$ Hence Proved

(2) **Order of a and $b^{-1}ab$ is same.** $o(a) = o(a^{-1})$

(3) $o(a) = n$, p is prime to $n \Rightarrow o(a^p) = n$

$o(a) = n \Rightarrow \boxed{a^n = e}$. $o(a^p) = m \Longrightarrow \boxed{(a^p)^m = e.}$

$(a^p)^n = (a^n)^p = e^p = e \Rightarrow o(a^p) \leq n. \Rightarrow m \leq n.$

$\gcd(n, p) = 1 \Rightarrow nx + py$

$a = a^{nx+py} \Rightarrow a = a^{py} \Rightarrow a^m = ((a^p)^m)^y \Rightarrow a^m = e \Rightarrow n \leq m$

So $\boxed{n = m}$ Ans

Prove for any integer n, $(bab^{-1})^n = ba^nb^{-1}$

↳ Must Show for $\boxed{n < 0}$

(7) $a^5 = e$ $aba^{-1} = b^2$ find $o(b)$.

$(aba^{-1})^2 = (aba^{-1})(aba^{-1}) = ab^2a^{-1} = aaba^{-1}a^{-1} = \underline{a^2ba^{-2}}$

IIly $(aba^{-1})^n = (ab^na^{-1})$

$(aba^{-1})^4 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b^2a^{-2}$

$= a^3ba^{-3}$.

$(aba^{-1})^8 = a^4ba^{-4}$.

$(aba^{-1})^{16} = a^5ba^{-5} = b$.

$\Downarrow$

$(b^2)^{16} = b^{32}$

$\Rightarrow b = b^{32} \Rightarrow \boxed{b^{31} = e}$ Ans

if $b = e$

So $o(b) \mid 31 \Rightarrow 31$ is prime. So $o(b) = 1$ or 31

as $b \neq e$

(8) $x^2ax = a^{-1}$ is solvable iff a is cube of some elm in G.

$x^2ax = a^{-1}$ is solvable $\Rightarrow$ $c^2ac = a^{-1} \Rightarrow c.(ca).(ca) = e$

$\Rightarrow (ca)(ca)c = e \Rightarrow (ca)(ca)(ca) = a \Rightarrow (ca)^3 = a$ $\forall c \in G$.

$\Leftarrow a = b^3 \Rightarrow$ Let $x = b^{-2} \Rightarrow b^{-4}b^3b^{-2} = b^{-3} = (b^3)^{-1} = a^{-1}$

So $x = b^{-2}$ is a solution

NOTE: All groups of order ≤ 4 are commutative

Revise

If $a \in G$ $o(a) = n$, then for any $k \in \mathbb{Z}^+$

- $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$
- $|a^k| = n/\gcd(n,k)$. [Shows previous $\Rightarrow |a^d| = n/d$]

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

$a^k = a^{dy} = (a^d)^y \Rightarrow a^k \in \langle a^{\gcd(n,k)} \rangle \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$

$a^d = a^{nx+ky} = e.a^{ky} = (a^k)^y \Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle$

Hence Proved.

TS: $|a^d| = \frac{n}{d}$ (Instead of a^k Use $\langle a^d \rangle$)

- $(a^d)^{n/d} = a^n = e \Rightarrow |a^d| \leq \frac{n}{d}$

If $|a^d| = s$ then let $1 \leq s < n/d$.

$(a^d)^s = a^{ds} = e \Rightarrow sd < n \rightarrow \leftarrow$ as $o(a) = n$.

So, $|a^d| = \frac{n}{d}$.

$|a^k| = |\langle a^k \rangle| = |\langle a^{n/d} \rangle| = |a^d| = n/d$ Hence Proved

Revise

Show that a group of order 4 must be abelian

Suppose not abelian $\Rightarrow \exists\, x, y \neq e \in G$ such that $xy \neq yx$.

- $xy \neq e$ and $yx \neq e$ as xy don't commute
- $xy \neq x$, $yx \neq x$ $(y \neq e)$ - $xy \neq y$, $yx \neq y$ $(x \neq e)$

So we have 5 elements e, x, y, xy, yx order = 4 So, abelian

* $G \neq \{\phi\}$, closed and associative with:

Rest
- $\exists\, e \in G$ such that $a \cdot e = a$, $\forall a \in G$
- $a \in G$, there exists $y(a) \in G$ such that $a \cdot y(a) = e$

Prove G is group.

- TS $e \cdot a = a$ $\quad y(a) \in G \Rightarrow \exists\, y(y(a)) \in G$ s.t $y(a) \cdot y(y(a)) = \varepsilon$

~~$a \cdot e = a \Rightarrow a \cdot e \cdot y(a) = a \cdot y(a) \Rightarrow ((a \cdot e) \cdot y(a)) \cdot a = e \cdot a$~~

$\Rightarrow$ ~~$(a \cdot y(a)) \cdot a = e \cdot a \Rightarrow$~~

$y(a) \cdot a = (y(a) \cdot a) \cdot \varepsilon = (y(a) \cdot a) \cdot (y(a) \cdot y(y(a)))$;

$= (y(a) \cdot \varepsilon) \cdot y(y(a)) = e$

So, $\boxed{y(a) \cdot a = e}$

$e \cdot a = (a \cdot y(a)) \cdot a = a \cdot e = a.$

} So G is a group

→ Permutation Groups (S_n ≡ perms on n symbols) ← Symmetric group

[For examples of finite non abelian]

Multiplication of permutations
└ Not commutative, Associative ✓

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

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

$fg \neq gf$

3] Show S_3 is finite non-abelian group
(Lengthy ≡ Composition Table)

Orbit ⇒ of permutation f.
Orbit of element a under $f = \{a, f(a), f^2(a) \ldots f^{n-1}(a)\}$
All the values a can attain on repeated application of f
Orbit of a = Cycle (one of many) of f.

→ Cyclic notation. ≡ $(1\ 4\ 3\ 5\ 2)$, $(1\ 5\ 4\ 2)$ (above)
fg gf

- Transposition = Cycle of length 2.
  └ ($f = f^{-1}$)
- Product of disjoint cycles is commutative
  $f = (2\ 3\ 6)$ $g = (1\ 4\ 6)$
  └ Not disjt.
  $fg = (1\ 4\ 2\ 3\ 6) \neq gf = (1\ 4\ 6\ 2\ 3)$

fg → First operate g, then f

- Inverse ≡ $f = (2\,3\,4\,1)$; $f^{-1} = (1\,4\,3\,2)$

- Every permutation can be expressed as a product of disjoint cycles.

  [Also as product of transpositions]

$\Rightarrow$. $(2\ 4\ 3) = (23)(24)$

$(1\ 2\ 3\ 4) = (14)(13)(12)$

* Even and Odd permutations

└ Product of even and odd transpositions.

(1) Id is an even permutation.

$I = (12)(21)$

$= (12)(21)(13)(31)$ ..So, every time 2 transpositions added together.

(2) Product of two odd is even permutation

$f = r$, $g = s$ transpositions

$fg = r+s$ transpositions = even

(3) f is odd $\Rightarrow f^{-1}$ is odd

$f f^{-1} = I$ ← even

odd

So, f^{-1} must be odd.

(4) ~~$n \geq 1$~~,
$n \geq 1$, Show order $A_n = \frac{n!}{2}$.

Alternating group $\equiv$ Gp of even perms of order n

For each odd perm $\Rightarrow \alpha$

we can have $(12)\alpha$ as even.

$(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$ (by LCL)

Thus there are atleast as many even as odd perms

$\therefore$ atleast as many odd as even.

$o(S_n) = n! \Rightarrow$ Equal odd & even $\Rightarrow$ # of even $= \frac{n!}{2}$.

$\boxed{o(A_n) = \frac{n!}{2}}$

NOTE: Set of ~~ed~~ even perms is a group
(Not set of odd as product of odd is even)

(3) List all perms of S_4.

Ans (1), 12, 13, 14, 23, 24, 34 — 7
123, 124, 132, 134, 142, 143, 234, 243. — 8
1234, 1243, 1324, 1342, 1423, 1432. — 6
(12)(34), (23)(14), (31)(24). — 3
24

(5) Order of n-cycle is n.

$f = (1,2,3,\ldots n) \Rightarrow ff = (\ldots)$ each f shifts by 1.

So, $f^n = (1)$ Ans

(6) Order of product of disjt cycles $\equiv$ LCM of lengths

*Cayley's Theorem (Revise) (Revise 2).

Every group is isomorphic to a permutation group.

3 Steps

→ G be given group

$A(G)$ be group of all permutations of set G.

For any $a \in G$, define $f_a : G \to G$ s.t

$$f_a(x) = ax.$$

① f_a → well-defined : $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$ ✓

1-1 : $f_a(x) = f_a(y) \Rightarrow x = y$ ✓

onto : for $y \in G$, $f(a^{-1}y) = y$ ✓

So f_a is a permutation on G. ⟶ $f_a \in A(G)$.

K be set of all such permutations.

② TS: K is subgroup of $A(G)$

- $K \neq \phi$ as $f_e \in K$.
- $f_a, f_b \in K$. (Let)

Then $f_b \circ f_{b^{-1}}(x) = b(b^{-1}x) = f_e(x) \Rightarrow f_{b^{-1}} = (f_b)^{-1}$

$f_a \circ f_b(x) = f_{ab}(x)$

So, K is a subgroup of $A(G)$.

$\phi : G \to K$. s.t $\phi(a) = f_a$.

③ TS: ϕ is isomorphism → 1-1 : $a = b \Leftrightarrow ax = bx \Leftrightarrow f_a(x) = f_b(x)$

$\Leftrightarrow f_a = f_b \Leftrightarrow \phi(a) = \phi(b)$

$\phi(ab) = f_{ab} = f_a \circ f_b$

$= \phi(a)\phi(b)$

→ ϕ is onto - trivial.

- G is finite group of order n, then G is isomorphic to a subgroup of S_n.

Subgroup $\Leftrightarrow$ $ab^{-1} \in H$.

) G group, H is finite subset of G. H is s.g $\Leftrightarrow$ $ab \in H$.

$\Leftarrow$ • Identity $\equiv$ $a \in H$.

$a^2, \ldots a^n \ldots \in H$. ∞ elements, but H is finite

So, we must have $a^r = a^s$ $r > s$, r, s integers

$a^s \in H$; $a^s \in G \Rightarrow a^{-s} \in G$.

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

As $r > s$, $a^{r-s} \equiv$ integral +ve power of a

Hence $a^{r-s} \in H$ $\because a^{r-s} = e \Rightarrow e \in H$.

• Inverse $\Rightarrow$ $r > s \Rightarrow r - s \geq 1 \Rightarrow r - s - 1 \geq 0$

$a^{r-s-1} \in H$. Now, $a \cdot a^{r-s-1} = a^{r-s} = e$.

So, inverse of a is a^{r-s-1} R

) $HK = KH \Rightarrow HK$ is subgroup of G. (*)

TS: $(HK)(HK)^{-1} = HK$

$(HK)(K^{-1}H^{-1}) = HKK^{-1}H^{-1} = (HK)H^{-1} = KHH^{-1} = KH = HK$.

So, HK is subgroup of G

HK is S.g :- TS: $HK \subseteq KH$

$x \in HK$,
$x^{-1} \in HK$.
$x^{-1} = h^* k$
$x = k^* h^{-1}$
$x \in KH$.

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

$a \in H_1$ $a \notin H_2$
$b \in H_2$ $b \notin H_1$

$ab \in H_1 \cup H_2 \Rightarrow ab \in H_1$ or $ab \in H_2$.
If $ab \in H_1 \Rightarrow a^{-1}(ab) \in H_1 \Rightarrow b \in H_1$ $(\leftrightarrow\leftarrow)$

(3) Normalizer of 'a' in G. (N(a)) $\{x : ax = xa\}$

└ Set of all elements of G which commute with a

TS: N(a) is a subgroup of G.

$ea = ae \Rightarrow e \in N(a) \Rightarrow N(a)$ is non-empty

Let $x, y \in N(a)$ then $ax = xa$, $ya = ay$

TS: $y^{-1}a = ay^{-1}$

~~$ya = yay$~~ $(ya)^{-1} = (ay)^{-1}$

$a^{-1}y^{-1} = y^{-1}a^{-1} \Rightarrow a \cdot a^{-1}y^{-1} = ay^{-1}a^{-1}$

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

TS: $xy^{-1} \in N(a)$. / ALTER: Only $xya = axy$

$y^{-1}a = ay^{-1} \Rightarrow xy^{-1}a = xay^{-1}$

$\Rightarrow (xy^{-1})a = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$

So, $xy^{-1} \in N(a) \Rightarrow N(a)$ is subgroup of G

• Self conjugate element $\equiv$ a is self conjugate if $\boxed{a = x^{-1}ax}$

(4) Centre of Group G $\equiv$ Set of all self-conjugate elements

$(Z(G) = z \mid zx = xz \ \forall x \in G)$

Z(G) is Subgroup of G.

$a, b \in Z \Rightarrow ax = xa$, ~~$bx = xb$~~

Show $b^{-1} \in Z \Rightarrow$ $x^{-1}b^{-1} \xleftarrow{(-1)} b^{-1}x^{-1} \xrightarrow{\downarrow} b^{-1}x = xb^{-1}$

Show $ab^{-1} \in Z \Rightarrow (ab^{-1})x = axb^{-1} = x(ab^{-1})$ ← Easy

Instead b^{-1}, ab only

Same as before

Examples of Groups

1) Non-abelian with Abelian subgroups

↓ S_3 ↓ A_3

Quaternion

2) Non-abelian with non-abelian subgroups

↓ S_4 ↓ A_4.

3×3 Matrices → Upper Δr

3) Abelian, not Cyclic.

$\left(\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}-1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&0\\0&-1\end{bmatrix} \begin{bmatrix}-1&0\\0&-1\end{bmatrix}, \otimes\right)$

4) Non-Abelian with every subgroup as normal.

- Quaternion $\{\pm 1, \pm i, \pm j, \pm k\} \equiv S.g[\pm 1 | \pm 1, \pm i \,|\, \ldots]$

5) Cyclic subgroup which is not normal

$G = S_3$ $H = \{I, (1,2)\}$

Cosets

. Left Coset of H (a s.g.) in G generated by 'a' = $\{aH = ah \mid h \in H\}$
Illy right coset.

aH & Ha are subsets of G.

(1) $a \in H$ then $aH = Ha = H$.

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

. $aH = bH \Rightarrow ah_1 = bh_2 \Rightarrow a^{-1}a h_1 = a^{-1} b h_2 \Rightarrow h_1 = a^{-1}b h_2$.

$\Rightarrow h_1 h_2^{-1} = a^{-1}b$

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

→ Short cut)

. $a^{-1}b \in H \Rightarrow a^{-1}bH = H \Rightarrow a(a^{-1})bH = aH$.

$\Rightarrow \boxed{bH = aH}$ Bow

(3) $a \in bH \Leftrightarrow aH = bH$; $a \in Hb \Leftrightarrow Ha = Hb$

~~$a = bh_k \Rightarrow ab^{-1} = h_k \Rightarrow ab^{-1} \in H$.~~

$aa^{-1} = bh$

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

$\Rightarrow aH = bH$

$aH = bH \Rightarrow a \in aH \Rightarrow a \in bH$.

(4) $\boxed{aH = bH \text{ or } (aH \cap bH) = \phi}$.

Let $aH \cap bH = \{c\}$ $\Rightarrow$ $c \in bH \Rightarrow cH = bH$ } $aH = bH$
$c \in aH \Rightarrow cH = aH$

or $aH \cap bH = \phi$

(5) H is a subgroup of G. Then there is 1-1 correspondence between any two left cosets of H in G.

- Let aH, bH be two left cosets.

Define $f: aH \to bH$ such $f(ah) = bh$

- 1-1 $\Rightarrow f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2 \Rightarrow h_1 = h_2$
- onto $\Rightarrow bh \in bH \Rightarrow \exists\ h$ s.t $bh \in bH$
  $\Rightarrow \exists\ h$ s.t $ah \in aH$.
  For that $ah \in aH$, $f(ah) = bh$ (onto)

So, there is 1-1 correspondence.

- Cor. $\Rightarrow |aH| = |bH|$

* $a \equiv b \pmod H$ if $(b^{-1}a \in H)$

equivalence relation

- Index of H in $G \equiv (G:H)$ or $i_G(H)$
  - # of distinct left (right) cosets of H in G.
  - $\frac{\#\text{ elems in } G}{\#\text{ elems in } H}$ $\left(\frac{o(G)}{o(H)}\right)$

agrange's Theorem :

Order of subgroup of a finite group divides the order of the group.

Case I : $H = G \Rightarrow o(H) \mid o(G)$

Case II : $H \neq G \Rightarrow o(G) = n$, $o(H) = m$.

Consider right cosets of H in G.

$Ha, Hb, \ldots Hn$ (As G is finite, only finite cosets)

W.k.t $o(Ha) = o(Hb) = \ldots o(H) = m$.

Let distinct right cosets be k.

↳ induce a partition of G. [as $Ha = Hb$ or $Ha \cap Hb = \phi$]

$o(G) = o(Ha) + o(Hb) + \ldots o(Hk)$

$n = km \Rightarrow \boxed{k = n/m} \Rightarrow o(H)$ divides $o(G)$.

NOTE :

ONLY FINITE GROUPS.

CONVERSE NOT TRUE. ($m \mid n$ but no s.g of $o = m$ possible)

[$A_4 \rightarrow$ no s.g of order 6]

G is finite. $o(a) \mid o(G)$. [Show $\langle a \rangle$ is s.g $\Rightarrow$ ⊕ Lagrange's]

- $a^{o(G)} = e$. [TRIVIAL]
- G of prime order has no proper subgroup.

ise

A finite group can't be expressed as union of 2 proper subgroups.

Let $G = H \cup K$ $\quad e \in H, K \Rightarrow$ So, one of H, K must have $\geq \frac{1}{2}$ of G's elements

$\frac{n}{2} < o(H) < n \Rightarrow$ So $o(H) \nmid o(G) \rightarrow H$ is not s.g

Not possible

(3) H, K be two finite subgroups.

$HK = \{hk \mid h \in H, k \in K\}$. Then $\boxed{|HK| = |H||K| / |H \cap K|}$

- HK has $|H||K|$ products.

Several are repeated as:

$hk = h'k'$ where $h' \neq h$, $k' \neq k$.

$\forall\, t$ in $|H \cap K|$ we have $\Rightarrow$

$hk = htt^{-1}k = (ht)(t^{-1}k) = h'k'$

So, each hk is represented multiply as described.

↳ by $|H \cap K|$ products

So, $\boxed{|HK| = \dfrac{|H||K|}{|H \cap K|}}$ ← VVI

CYCLIC GROUPS

Describe all elements in cyclic group of $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} = A$

$A^2 = \begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$, ... $A^5 = \begin{bmatrix}1 & 5\\ 0 & 1\end{bmatrix}$

$A^{-1} = \begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}$, $A^{-2} = \begin{bmatrix}1 & -2\\ 0 & 1\end{bmatrix}$, ... $A^n = \begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}$ $n \in \mathbb{Z}$

↑ Both +ve, -ve powers need to be looked at.

Show $(Z_m, +)$ is cyclic, where m is prime.

$Z_m = \{0, 1, \dots m-1\}$

$1 = 1$; $1+1 = 2$, $1+1+1 = 3$ ... $1+1+\dots(m-1) = m-1$, $m(1) = m = 0$

So 1 generates $Z_m \Rightarrow$ Hence, cyclic

Properties of Cyclic Groups

- Abelian ✓
- a is generator $\Rightarrow a^{-1}$ is generator [TRIVIAL]
- # of generators of infinite cyclic group is 2.

Let $G = \langle a \rangle$ $\quad G = a^n \mid n \in I$

As G is $\infty \Rightarrow (a^n = e \Leftrightarrow n = 0)$ [Else Show not ∞]

Let b be other gen $\Rightarrow$ $b = a^k$; $a = b^l$

$b^l = (a^k)^l \Rightarrow a = a^{kl} \Rightarrow kl - 1 = 0 \Rightarrow kl = 1 \begin{cases} k=1, l=1 \\ k=-1, l=-1 \end{cases}$

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

- Group of order p (prime) is cyclic
- $G = \langle a \rangle$, if a^m is generator of G iff $(m, n) = 1$.
- $G = \langle a \rangle$, then all subgroups of G are those generated by a^m, where m/n. [All s.gs of G are cyclic $\equiv$ least $k = \langle a^k \rangle$ division rule

(Other cases s.g not obtained)

(1) Every group of order < 6 is abelian

└ G order ≤ 4 is abelian + order 5 is prime-abelian

(2) Generators of cyclic of order 8

└ $(m, 8) = 1 \Rightarrow a^1, a^3, a^5, a^7$

(3) Show U_9 is cyclic

($U_n \equiv$ Ints relatively prime to n under (X_n) ;)

$U_9 = \{1, 2, 4, 5, 7, 8\}$

$2, 2^2, 2^3, 2^4, 2^5, 2^6$

$2 \quad 4 \quad 8 \quad 7 \quad 5 \quad 1 \Rightarrow \boxed{U_9 = \langle 2 \rangle}$

$o(U_9) = 6 \Rightarrow$ +ve ints < 6 and prime to $6 \Rightarrow 1, 5.$

So, gens $\equiv 2^1, 2^5 \Rightarrow \boxed{2, 5}$

(4) $U_{17} \equiv \{1, 2, \ldots 16\}$ $\quad o(U_{17}) = 16$

So, ints < 16 and prime to $16 \Rightarrow 1, 3, 5, 7, 9, 11, 13, 15.$

Now, find any one gen of $U_{17} \equiv \langle 3 \rangle$ (Check!)

So, all gens are $\Rightarrow 3^1, 3^3, 3^5, \ldots$ so on.

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

Euler-phi Function.

- $\phi(n)$ = # of +ve ints $< n$ and co-prime to n

  $(\phi(1)=1)$ $(\phi(p)=p-1)$

(*) · No. of generators of finite cyclical group of order 'n' is $\phi(n)$

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots$$

($p_1, p_2, \ldots$ are prime factors of n)

• G is finite group, $H \neq G$ is a subgroup of G such that $o(G) \nmid (i(H))!$, then H must contain a non-trivial normal subgroup of G.

$\rightarrow |G| = 99$, $|H| = 11$, then $i(H) = 9$.

$99 \nmid 9!$ So, H contains a non-trivial normal subgroup of G.

As $|H| = 11 \Rightarrow$ H must be normal

no subgroup possible

Normal Subgroups

- H is normal s.g of a group G if $\forall x \in G$ and $\forall h \in H$ (given to a s.g) $\boxed{xhx^{-1} \in H.}$

- Simple group ⇒ A group with no proper normal s.g.
  - A gp of prime order

1) Subgroup H is normal iff $\boxed{xHx^{-1} = H}$ $\forall x \in G$

TS: H is normal ⇒ $H \subseteq xHx^{-1}$.

$xHx^{-1} \subseteq H$ ⇒ Replace x by $x^{-1} \in G$ ⇒ $x^{-1}Hx \subseteq H$.

$xx^{-1}Hxx^{-1} \subseteq xHx^{-1}$ ⇒ $H \subseteq xHx^{-1}$ = Dem

2) S.g H is normal iff each left coset of H in G is a right coset of H in G.

⇐ Every left is .... in G. ⇒ $xH = Hy$ for some $x, y \in G$.

$xH = Hy$ ⇒ $xe \in xH$, $xe \in Hy$. ⇒ $x \in Hy$ ⇒ $Hx = Hy$ ⇒ $xH = Hx$.

⇒ $xHx^{-1} = H$. Norma

Conclusion: $\boxed{H \text{ is normal} \Leftrightarrow xH = Hx}$

⇐ $\boxed{x^{-1}hx \in H \Leftrightarrow xHx^{-1} = H \Leftrightarrow xH = Hx \Leftrightarrow (Ha)(Hb) = Hab.}$

) H is s.g, N is normal s.g ⇒ HN is a subgroup

* H is s.g of index 2, then H is normal s.g of G.

Revise

⇒ Index 2 ⇒ 2 distinct right cosets

H, Hx. Corresponding left cosets ≡ H, xH

- $x \in H$ or $x \notin H \Rightarrow x \in Hx$ (≡ xH) $\Rightarrow H \neq Hx$, $H \neq xH$.

$x \in H$ ⇓

$Hx = H = xH$

$\Rightarrow Hx = xH$.

$G = H \cup Hx = H \cup xH$.

$Hx = xH$

(*) M, N are normal s.g of G, $M \cap N = \{e\}$.

Then every element of M commutes with every elem of N.

Let $n \in N$, $n^{-1} \in N$, $m \in M$, $m^{-1} \in M$.

$m(n^{-1})m^{-1} \in N$ (Normal)

$n[m(n^{-1})m^{-1}] \in N$ (Closure)

$[n(m)n^{-1}]m^{-1} \in M$ (Normal + Closure)

So, $nmn^{-1}m^{-1} = \varepsilon \Rightarrow \boxed{nm = mn}$

Quotient Group $[G/N = \{Nx \mid x \in G\}$, N is normal $Nx = xN]$

* Set of all cosets of normal s.g H in G w.r.t coset multiplication is a group

⇒ Coset multiplication : $\boxed{(Ha)(Hb) = Hab.}$

↳ TS well defined ≡ $Ha = Ha_1$, $Hb = Hb_1$ in G/H. ⇒ $a = a_1 h_1$, $b = b_1 h_2$

→ $a = ea = h_1 a_1$ $\quad eb = b = h_2 b_1$ for some $h_1, h_2 \in H$.
(Ha) (Ha_1) (Hb) (Hb_1)

$Hab = H(h_1 a_1)(h_2 b_1) = H h_1 (a_1 h_2) b_1 = H h_1 (h_3 a_1) b_1$
$= H a_1 b_1$

So, $Hab = Ha_1 b_1 \Rightarrow$ Well defined coset (✓)n.

• Identity = $He = H$. • Inverse ≡ Ha^{-1}

Q Show $H = \{1, -1\}$ is normal s.g of $\{\pm 1, \pm i\}$.
Write composition table for quotient group G/H.

↳ $1H = -1H = H$. $\quad iH = \{i, -i\} = -iH$.

	H	iH
H	H	iH
iH	iH	$-1H = H$ ∈ H

(D) Quotient Gp of Cyclic G is cyclic

$G = \langle a \rangle$, N is sg $\Rightarrow$ N is normal $\Rightarrow$ G/N is subgroup

$G/N = \{Nx \mid x \in G\}$

$Na \in G/N \Rightarrow \langle Na \rangle \subseteq G/N$.

$Nx \in G/N \Rightarrow x \in G \Rightarrow x \in \langle a \rangle$

$x = a^k$ for some $k \in \mathbb{Z}$

$Nx = Na^k = (Na.Na...Na) = (Na)^k$.

So, $Nx \subseteq G/N \Rightarrow N(x) \in \langle Na \rangle \Rightarrow G/N \subseteq \langle Na \rangle$

So, $\boxed{G/N = \langle Na \rangle}$

2003

(Q) H s.g of G, s.t $x^2 \in H \ \forall x \in G$. Prove H normal.

$g \in G \Rightarrow g^{-1} \in G \qquad g^{-2} \in H. \qquad h \in H$

$hg \in G \Rightarrow (hg)^2 \in H. \ / (gh)^2 \in H.$

Let, $(gh)^2 h^{-1} g^{-2} \in H. \Rightarrow ghghh^{-1}g^{-2} \Rightarrow \underline{ghg^{-1} \in H}$

Proved

2001

(8) N be normal. G/N is abelian $\Leftrightarrow xyx^{-1}y^{-1} \in N$ $\forall x, y \in G$

G/N is abelian $\Leftrightarrow XY = YX \quad X, Y \in G/N$

$\Leftrightarrow NxNy = NyNx$

$\Leftrightarrow Nxy = Nyx$

$\Leftrightarrow xy(yx)^{-1} \in N$

$\Leftrightarrow xyx^{-1}y^{-1} \in N$ Bonus

Coset property
$ab^{-1} \in H \Leftrightarrow Ha = Hb$

Conjugate elements

$a \sim b$ if $\exists\, x \in G$ s.t $a = x^{-1}bx$

Conjugate class of $a \equiv C[a]$ or $[a] \equiv [x \in G \mid x \sim a]$

↳ equivalence class of a

(9) Find all conjugate classes of S_3 ← Similar

$S_3 = \{I, 12, 13, 23, 123, 132\}$

$[I] = I$ — (1)

$[12] = \theta\,[12]\,\theta^{-1} = [\theta(1)\ \theta(2)]$ IMPORTANT

$= 12, 13, 23$ — (2)

$[123] = 123, 132$ — (3)

use diff

$\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix} = (2,3)$

$\theta(2) = 3$

$\theta(1) = 1$

$\downarrow$

$[1\ 3]$ -

Illy others

Also $\bigcup_i [a_i] = G$ Union = Group

(All different styles of cycles give different Conjugate classes)

an element

② Normalizer of a Group $(N(a))$

Set of all elements which commute with 'a'.

$$N(a) = \{x \in G \mid xa = ax\}$$

$$\text{Thm} \equiv o(C[a]) = \frac{o(G)}{o(N(a))}$$

• Class equation of Group.

If G is finite group $\equiv o(G) = \sum_{a \in G} i_G(N(a)) = \sum_{a \in G} \frac{o(G)}{o(N(a))}$

③ Centre of Group $Z = \{z \in G \mid zx = xz \ \forall x \in G\}$

└ Normal subgroup of G.

└ Any z has only itself in its conjugate class $\equiv (xzx^{-1} = xx^{-1}z = z)$

• Class Equation (2nd form)

$$o(G) = o(Z) + \sum_{(a \notin Z)} \frac{o(G)}{o(N(a))}$$

IMP

Left Thm Pg 90

8 $o(G) = p^n$, where p is prime, then $Z \neq \{e\}$ i.e $o(Z) > 1$.

Class equation of finite group ≡

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

$\forall a$, $N(a)$ is subgroup of $G \Rightarrow o(N(a))$ divides $o(G)$ [Lagrange]

So, $o(N(a)) = p^k$ $(1 \leq k < n)$ if $a \notin Z$.

$$\frac{o(G)}{o(N(a))} = p^{n-k} \quad (n-k \geq 1)$$

$\Rightarrow p$ divides $\frac{o(G)}{o(N(a))}$, p divides $o(G)$

$\Rightarrow$ p divides $o(G) - \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \Rightarrow p$ divides $o(Z)$

As $p \geq 2$, so $o(Z) \geq 2 \Rightarrow o(Z) > 1$ Proved

9 $o(G) = p^2$ then G is abelian.

From previous, $o(Z) > 1$

Z is subgroup of $G \Rightarrow o(Z) \mid o(G) \Rightarrow o(Z) = p^2$ or p

Case I: $o(G) = p^2 = o(Z) \Rightarrow Z = G$.

$\therefore \forall x \in G \Rightarrow x \in Z \Rightarrow xy = yx \quad \forall y \in G \Rightarrow G$ is abelian.

Case II: $o(Z) = p$, $G \neq Z \Rightarrow Z \subset G$ proper subgroup

$\exists (a \notin Z)$, $a \in G$

Consider $N(a)$, $\varepsilon \in N(a)$, $\varepsilon \in Z$

w.k.t $N(a)$ is a subgroup.

$x \in Z \Rightarrow x \in N(a) \Rightarrow Z \subsetneq N(a)$ ⊕ $a \notin Z$. $\Rightarrow o(Z) < o(N(a))$

$o(N(a)) > p$.

By Lagrange $o(N(a)) \mid o(G) \Rightarrow o(N(a)) = p^2 \Rightarrow N(a) = G$.

$\Rightarrow a \in Z \rightarrow \leftarrow$

So $o(Z) = p$ — Not possible

Homomorphisms, Isomorphisms

Def^n: $(G,\cdot)$, $(G',*)$ be two groups $\quad \forall a,b \in G$.

Then $f: G \to G'$ is homo if $f(a.b) = f(a) * f(b)$

↳ **A homomorphic mapping** or homomorphism

Def^n: If $f: G \to G'$ is homomorphism and **onto**, then G' is said to be a **homomorphic image** of G.

$G \simeq G'$ — Homomorphism exists + Onto

Def^n: **Isomorphism** from $G \to G'$

If $f: G \to G'$ is homo and 1-1, then f is called isomorphism from $G \to G'$

Def^n: G' is called **isomorphic image** of G / G' is iso to G / $G \cong G'$

If $f: G \to G'$ is **homo** + **1-1** + **onto**

Examples

$(\mathbb{Z}, +) \to [(2^n / n \in \mathbb{Z}), \times]$

$(\mathbb{R}^+, \times) \to (\mathbb{R}, +) \Rightarrow f(x) = \log_{10} x.$

Onto $\equiv y \in \mathbb{R} \in G'$
Consider $10^y \in \mathbb{R}^+ \in G$
$f(10^y) = y.$
So $\forall y, \exists 10^y$ in G

1) Properties

- $f(e) = e'$
- $f(a^{-1}) = [f(a)]^{-1}$
- f: homo $G \to G'$ then $(f(G), \cdot)$ is a subgroup of G'
- f: from Abelian maps to abelian
- [Converse: S_3 non-abelian, A_3 is normal s.g of S_3 (Counter Example) S_3/A_3 is a homomorphic image of S_3. $\circ \left(S_3/A_3\right) = 2$ and S_3/A_3 is abelian while S_3 is not ∴]
- G be group, $f: G \to G'$ homo + onto $\Rightarrow$ G' is a group [LENGTHY BUT BASIC PROOF]

2) Kernel of f: $G \to G'$ (└ homo)

Set K of $g \in G$ s.t $\boxed{f(g) = e'}$

$\boxed{\text{Ker } f = \{x \in G \mid f(x) = e'\} = K}$

- Ker f is a normal subgroup of G.
- $\boxed{f \text{ homo, onto is isomorphism} \Leftrightarrow K = \{e\}}$

└ For f to be isomorphism $\Rightarrow$ f must be 1-1

So, equivalently $\boxed{f \text{ is 1-1} \Leftrightarrow K = \{e\}}$

$\Rightarrow$ Let f is 1-1, $f(a) = e' \Rightarrow f(a) = f(e) \Rightarrow a = e \Rightarrow K = \{e\}$. ($a \in \ker f$)

$\Leftarrow$ Let $\ker f = \{e\}$, $a, b \in G$ s.t. $f(a) = f(b) \Rightarrow f(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in \ker f \Rightarrow ab^{-1} = e \Rightarrow a = b$ ∴ f is 1-1

Thm Given f homo : $G \xrightarrow{\text{onto}} G'$, $\ker f = K$ s.t $f(a) = a'$.
Then set of elements of G having image a' in G' is coset Ka of K in G.

⇒ Let e, e' be identity in G, G'

$f^{-1}(a') = \{x \in G \mid f(x) = a'\} = T$

TS: $\boxed{f^{-1}(a') = Ka}$

- $y \in Ka \Rightarrow y = ka \Rightarrow f(y) = f(a) = a' \Rightarrow y = f^{-1}(a')$.

$\therefore Ka \subseteq f^{-1}(a')$

- $z \in f^{-1}(a')$ then $f(z) = a'$ — Transform to make RHS = e'

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

- $f(z \cdot a^{-1}) = f(z)[f(a)]^{-1} = a'(a')^{-1} = e'$

$\therefore$ So, $f(z \cdot a^{-1}) = e' \Rightarrow za^{-1} \in K \Rightarrow za^{-1}a \in Ka \Rightarrow z \in Ka$.

$f^{-1}(a') \subseteq Ka$

$\Rightarrow f^{-1}(a') = Ka$ Proved

Q $f: G \to G$ be homo, $f(x) = x^2$. Prove G is abelian

$a, b \in G \Rightarrow ab \in G$. $f(ab) = (ab)^2$

f is homo $\Rightarrow f(ab) = f(a)f(b) = a^2b^2$.

$abab = a^2b^2 \Rightarrow ba = ab$ Hence abelian

Thm

① G, N be normal sg of G.

$f: G \to G/N$ defined by $f(x) = Nx$ for $x \in G$.

Then f is a homo, onto $G \to G/N$ and $\ker f = N$.

[BASIC PROOF]

② Fundamental Theorem on homomorphism of Groups:

* If $f: G \to G'$ is homo, onto with $\ker f = K$.
Prove $G/K \cong G'$.

Pf: $\Rightarrow$ Ker $f \equiv K = \{x \in G \mid f(x) = e' \in$ identity in $G'\}$

K is a normal sg of G. So G/K quotient is defined.

$G/K = \{Ka \mid a \in G\}$

TS: $G/K \cong G'$

Consider $\phi: G/K \to G'$ Such that

$\phi(Ka) = f(a) \quad \forall a \in G$.

① Show ϕ is well defined $[Ka = Kb \Rightarrow \phi(Ka) = \phi(Kb)]$

For $a, b \in G$, $Ka, Kb \in G/K$.

we have $Ka = Kb \Rightarrow ab^{-1} \in K$.

$f(ab^{-1}) = e' \Rightarrow f(a) f(b)^{-1} = e'$

$\Rightarrow f(a) = f(b) \Rightarrow \phi(Ka) = \phi(Kb)$

} Add more steps

② ϕ is 1-1.

$\phi(Ka) = \phi(Kb) \Rightarrow f(a) = f(b) \Rightarrow f(ab^{-1}) = \varepsilon \Rightarrow ab^{-1} \in K$

$Ka = Kb$

§102 - Ex

(2) ϕ is onto.

Let $x \in G' \Rightarrow$ As f is onto, $\exists\ a \in G$ s.t $f(a) = x$.

$\therefore Ka \in G/K$ and $\phi(Ka) = f(a) = x$.

$\therefore \phi(Ka) = x\ \forall x \Rightarrow \phi$ is onto.

(4) ϕ is homomorphism. ← Rem. to show

$\phi[(Ka)(Kb)] = \phi[Kab] = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$

---

(3) $f: G \to G'$

If order of a is finite, then $\boxed{o(f(a)) \mid o(a)}$

(4) If f is isomorphism then $o(f(a)) = o(a)$

$o(f(a)) = m$

$o(a) = n \Rightarrow a^n = e \Rightarrow (f(a))^n = e' \Rightarrow m \le n.$

$o(f(a)) = m \Rightarrow f(a) \dots f(a) = e' \Rightarrow f(a^m) = e' \Rightarrow a^m = e \Rightarrow n \le m$ (As 1-1)

($K = \{e\}$).

$\therefore n = m.$

(5) Show $[\{0,1,2,3\}, +_4]$ and $[\{1,-1,i,-i\}]$ are isomorphic

Define f: $0 \to 1$, $1 \to i/-i$, $2 \to -1$, $3 \to -i/i$ } onto, 1-1.

TIP:
Map id to id
Map same order elements

TS f homomorphism.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

} Now see mapping (check! values)

NOTE: Creating an isomorphic mapping $G \to G'$

- Should be Homo + 1-1 + onto
- Must preserve Identity, inverses, orders

(5) Second Theorem on Isomorphism — Recheck on 10

H and N are s.g of G and N is normal s.g of G,

then $\frac{HN}{N} \cong \frac{H}{H \cap N}$.

$\Rightarrow$ H is s.g, N is normal s.g $\Rightarrow$ HN is subgroup of G; $H \cap N$ is normal s.g of G; $N \subseteq HN$.

So, quotient groups $\frac{HN}{N}$, $\frac{H}{H \cap N}$ are defined.

Define $\phi : H \to HN/N$ s.t.

$\phi(x) = N(x) \quad \forall x \in H$. $\left[\because N \subseteq HN, x \in H \Rightarrow x \in HN \Rightarrow Nx \in HN/N\right]$

1) Show ϕ is well-defined

$x_1, x_2 \in H$.

$x_1 = x_2 \Rightarrow Nx_1 = Nx_2 \Rightarrow \phi(x_1) = \phi(x_2)$.

2) ϕ is homomorphism.

$x_1, x_2 \in H$, $Nx_1, Nx_2 \in \frac{HN}{N}$ s.t $\phi(x_1) = Nx_1, \phi(x_2) = Nx_2$

$\phi(x_1 x_2) = N(x_1 x_2) = Nx_1 Nx_2 = \phi(x_1)\phi(x_2)$.

3) ϕ is onto.

$x \in \frac{HN}{N} \Rightarrow x = Ng$ for some $g \in HN \Rightarrow g = hn$

~~Consider $\phi(g) = Ng = x$.~~

N is normal in G $\Rightarrow HN = NH \Rightarrow g = hn = n'h'$

$\phi(h') = Nh' = (Nn')h' = N(n'h') = N(hn) = Ng$

ϕ : onto

ϕ is homo, onto $H \to \frac{HN}{N}$.

By 1st Theorem $\Rightarrow \frac{H}{\ker\phi} \cong \frac{HN}{N}$.

IS: $\ker\phi = H \cap N$.

$x \in \ker\phi \Leftrightarrow \phi(x) = N$ and $x \in H$.

$\Leftrightarrow Nx = N$ and $x \in H$

$\Leftrightarrow x \in N$ and $x \in H \Leftrightarrow x \in H \cap N$.

$\boxed{\ker\phi = H \cap N}$ Hence Proved

Only Show

1. Well-def
2. Homo
3. Onto

$\Rightarrow$ Use 1st Iso

* No isomorphism $\langle \mathbb{Q}, + \rangle$ to $\langle \mathbb{Q}^+, \cdot \rangle$.

$2 \in \mathbb{Q}^+$

$\forall f : \quad f(\alpha) = 2.$

$f\left(\frac{\alpha}{2} + \frac{\alpha}{2}\right) = 2 \Rightarrow \left(f\left(\frac{\alpha}{2}\right)\right)^2 = 2. \Rightarrow f\left(\frac{\alpha}{2}\right) = \sqrt{2}$

No such rational exists

* $\langle R, + \rangle$ cannot be isomorphic to $R^* \equiv R - \{0\}$ in ...

Order of $1, -1$ in R^* is 2.

But R has no element of order 2, except 0.

* G is additive of reals, N is integers. H is all $\mathbb{C}$ with mod 1 under multiplication

Show isomorphism.

$f : G \to H$ s.t $f(\alpha) = e^{i2\pi\alpha}$.

* Number of homomorphisms from Z_{15} to Z_{10}

Z_{15} is cyclic. We need to determine $\phi(1)$.

$\phi : Z_{15} \to Z_{10}$

Let $\phi(1) = x$. Then $\left.\begin{matrix} o(x) \mid 15 \\ o(x) \mid 10 \end{matrix}\right\} x = 1, 5.$

If $o(x) = 5$.

In Z_n, number of elements of order $k = \phi(k)$ if $k \mid n$.

So, in Z_{10} # of elements of order 5 $= \underline{4}$

$\phi(5) = 1, 2, 3, 4$

* A_4 has no subgroup of order 6

If possible let there be H

But 9 elements of order 3

So x s.t $o(x) = 3$ and $x \notin H$.

H, Hx, Hx^2 be cosets

order $6 \Rightarrow i = 2$ [12/6] $\to$ max 2 cosets

$H \neq Hx$ as $x \notin H$.

$Hx = Hx^2 \Rightarrow x \in H \to\leftarrow$

$H = Hx^2 \Rightarrow H = Hx^{-1} \Rightarrow H = Hx \to\leftarrow$

* Closure for U_n.

$a, b \in G$, Let $a \textcircled{x} b = c$.

$c \neq 0$ or $n \mid ab$ but not as $(a,n) = (b,n) = 1$

and $c \in [1, n)$

If $(c, n) = d$ then $d \mid c$ and $d \mid n$. where d is a prime

$ab = nq + c. \rightarrow d \mid ab. \Rightarrow d \mid a$ or $d \mid b$.

$d \mid a, d \mid n$

$\Rightarrow (a,n) \neq 1$

* For a finite field with characteristic p, # of elements is p^n.

Let $o(F) = n$.

and p, q be primes dividing n.

We have a, b s.t $o(a) = p$ $o(b) = q$

→ Order of an element divides its characteristic

$\Rightarrow q \mid p \Rightarrow p$ is not prime →←

9 Show a cyclic group of order 6 is isomorphic to product of cyclic groups of order 2 and 3. Can you generalize this?