$|SL(n, Z_p)| = ??$, p prime.

$GL(2, Z_p)$. $A \in GL(2, Z_p)$.

$A = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, r_i row vectors.

r_1 has (p^2-1) choices as $r_1 \neq (0\ 0)$

$r_1 \ (a \ b)$ — a: p, b: p

For each choice of r_1, r_2 has (p^2-p) choices as r_1, r_2 are L.I. (linearly independent).

$r_2 \ (c \ d)$ — p^2

Ex:- If $r_1 = (1\ 2)$, then r_2 can't be $(1,2), (2,4), \ldots (p-1, 2(p-1)), (p, 2p) = (0,0)$

$\begin{vmatrix} 1 & 2 \\ 2 & 4 \end{vmatrix} = 0$

$(1,1), (1,2), \ldots, (p-1, 2(p-1)), (0,0)$

(p^2-p) choices.

$A = \begin{pmatrix} 2 & 5 \\ c & d \end{pmatrix}$ $\begin{pmatrix} 2 & 5 \end{pmatrix}$

$(cd) = (2\ 5), (4, 10) = (4, 3), (6, 1), (1, 8), (3, 4), (5, 2), (0, 0)$

$f^2 = 49$ Z_7 $F^2 - 7 =$ $\begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$

3. $(2\ 5) = (6\ 15) = (6\ 1)$

4. $(2\ 5) = (8\ 20) = (1\ 6)$

5 $(2\ 5) = (10\ 25) = (3\ 4)$

$\begin{vmatrix} 2 & 5 \\ 4 & 6 \end{vmatrix} = 12 - 20 = -8 = 6 \neq 0$

$$|GL(2, Z_p)| = (p^2-1)(p^2-p)$$

$$|GL(n, \mathbb{Z}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

If $A \in GL(2, \mathbb{Z}_p)$, $\det A$ may be $1, 2, \ldots, p-1$.

If $A \in SL(2, \mathbb{Z}_p)$, $\det A = 1$.

$\therefore |GL(2, \mathbb{Z}_p)| = (p-1)$ times $|SL(2, \mathbb{Z}_p)|$

$$|GL(n, \mathbb{Z}_p)| = (p-1)\,|SL(n, \mathbb{Z}_p)|$$

$$\therefore |SL(n, \mathbb{Z}_p)| = \frac{|GL(n, \mathbb{Z}_p)|}{(p-1)}$$

$$= \prod_{k=0}^{n-1} (p^n - p^k) \Big/ (p-1) \quad \checkmark$$

$$|SL(2, \mathbb{Z}_p)| = \frac{|GL(2, \mathbb{Z}_p)|}{(p-1)}$$

$$= \frac{(p^2-1)(p^2-p)}{p-1} \quad \checkmark$$

$$= (p-1)\,p\,(p+1).$$

Ex :— $GL(2, \mathbb{Z}_3)$

$\begin{pmatrix} 1 & 2 \\ 1 & a \end{pmatrix} \in GL(2, \mathbb{Z}_3)$

$a = 0, 1, a \neq 2$

$a = 0$, $\begin{vmatrix} 1 & 2 \\ 1 & 0 \end{vmatrix} = -2 = 1 \in SL(2, \mathbb{Z}_3)$

$a = 1$, $\begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = -1 = 2$

$\# GL(2, \mathbb{Z}_5)$, $\begin{pmatrix} 1 & 2 \\ 1 & a \end{pmatrix}$,

$a = 0, 1, 3, 4$

$a = 0$, $\left|\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}\right| = -2 = 3$

$a = 1$, $\left|\begin{matrix} 1 & 2 \\ 1 & 1 \end{matrix}\right| = -1 = 4$

$a = 3$, $\left|\begin{matrix} 1 & 2 \\ 1 & 3 \end{matrix}\right| = 1 \in SL(2, \mathbb{Z}_5)$

$a = 4$, $\left|\begin{matrix} 1 & 2 \\ 1 & 4 \end{matrix}\right| = 2$

Subgroup

Def:- Let $(G, *)$ be a group and $H \subseteq G$. $*$ is a induced operation on H. Then if $(H, *)$ forms a group itself, then $(H, *)$ is called a subgroup of $(G, *)$.

H is a subgp of G, is denoted by $H \leq G$.

Ex:- For $(G, *)$, G itself a subgroup of G. G is improper subgroup of G.

All other subgroups are proper.

$\{e\}$ is a subgroup of G, $\{e\}$ is the trivial subgroup of G. All other subgroups are non-trivial.

$\{e\} < H < G$, then H is a

non trivial proper subgroup of G.

Ex:— 1) $(\mathbb{R}, +)$ group.

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ proper subgroups of $(\mathbb{R}, +)$.

$\{0\}$ is the only trivial subgroup of $\mathbb{R}$.

2) $(\mathbb{R}^+, \cdot)$ be a group.

$(\mathbb{Q}^+, \cdot)$ proper subgroup of $(\mathbb{R}^+, \cdot)$

$(\mathbb{Z}^+, \cdot)$ is not a subgroup.

3) $(\mathbb{Z}, +)$ be a group.

$(n\mathbb{Z}, +)$, $n > 1$ proper subgroup.

$\langle n \rangle = n\mathbb{Z} = \{\ldots -2n, -n, 0, n, 2n, 3n, \ldots\} = \{m.n : m \in \mathbb{Z}\}$

$\langle 5 \rangle = 5\mathbb{Z} = \{\ldots -5, 0, 5, 10 \ldots\} = \{m.5 : m \in \mathbb{Z}\}$

$(\mathbb{Z}_n, +) \not\leq (\mathbb{Z}, +)$

$+$ mod n ; $+$ usual

4) K-4 group $\{e, a, b, c\}$

$\{e\}, \{e, a\}, \{e, b\}, \{e, c\} = \langle c \rangle$

proper subgroups.

$A = \{e, a, b\}$ is not a subgroup.

as $a.b = c \notin A$.

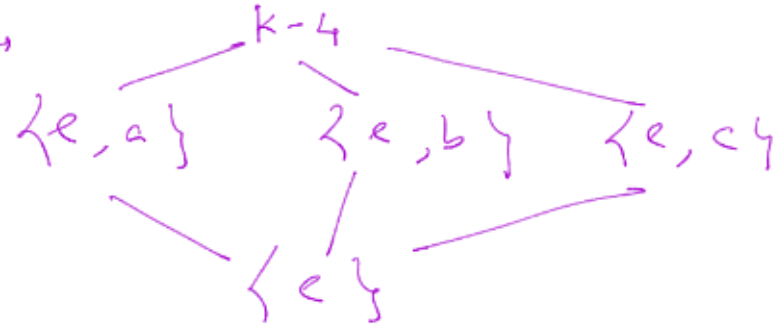
5) $G = \{1, -1, i, -i\} \leq \mathbb{C}^*$

$\{1\}$, $\{1, -1\} \rightarrow \langle -1 \rangle$ proper subgroups.

Any subgroup including i is G itself. $G = \{ i^n : n \in \mathbb{Z} \} = \langle i \rangle$

Subgroup lattice :— $= \langle -i \rangle$

$K-4$ →



$G = \{1, -1, i, i\} = \langle i \rangle$

$\{1, -1\}$

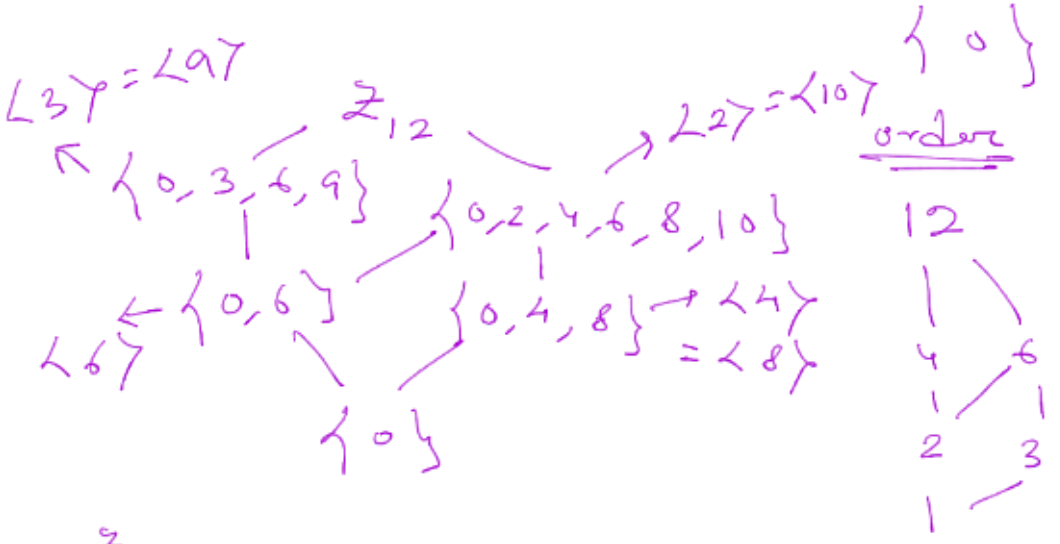
$\{1\}$

$\cong$ (isomorphic)

$Z_4 = \{0, 1, 2, 3\}$

$\{0, 2\}$

$\{0\}$



Z_{12}, $|a| = 4$

$a = 3$ subgroup of order 4

$= \{3, 6, 9, 0\} = \langle 3 \rangle$

$a = 9$ $= \{9, 6, 3, 0\} = \langle 9 \rangle$

$(G, \cdot)$ be any group.

Let $a \neq e \in G$.

$a, a^2, a^3, \ldots \in G$.

$H = \{ e, a, a^2, a^3, \ldots \}$ subgroup of G.

$H = \{ a^n : n \in \mathbb{Z} \}$ is the smallest subgroup containing 'a'.

$\Rightarrow$ $H = \{ a^n : n \in \mathbb{Z} \}$, $a \in G$.

$a \in H$, H is non-empty.

Let $a^m, a^n \in H$

$a^m \cdot a^n = a^{m+n} \in H$, $\because m+n \in \mathbb{Z}$.

Associative prop. holds in H.

[Heredity].

$n = 0$, $a^0 = e \in H$.

$a^p \in H$, $a^{-p} \in H \Rightarrow a^p \cdot a^{-p} = a^0 = e$.

H is a subgroup of G.

Let $a \in K$ and $K < H$.

Then for some $q \in \mathbb{Z}$, $a^q \notin K$.,

contradicts the closure prop.

$\therefore$ H is the smallest subgp of G containing 'a'.

$H = \{ a^n : n \in \mathbb{Z} \} = \langle a \rangle$.

H is generated by 'a'.

$(G, +)$, $H = \{ n.a : n \in \mathbb{Z} \}$

$a^n = e$

$H = \{ a^n : n \in \mathbb{Z} \}$ is called cyclic subgroup of G generated by 'a'. and is denoted by $\langle a \rangle$.

Ex :— $(\mathbb{R}, +)$

$\langle 1 \rangle = \{ \ldots, -2, -1, 0, 1, 2, 3, \ldots \}$

$= \mathbb{Z}$

$\langle 2 \rangle = 2\mathbb{Z}$

$\langle n \rangle = \{ m.n : m \in \mathbb{Z} \}$

$= n\mathbb{Z}$.

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

$\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$

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

$\langle 9 \rangle = \{9, 1\} < U(10)$

D.

$$\langle R_{90} \rangle^4 = \{ R_{90}, R_{180}, R_{270}, R_0 \}$$

$$= \langle R_{270} \rangle = \langle R_{90}^{-1} \rangle$$

$$\langle R_{180} \rangle = \{ R_0, R_{180} \}$$

$$\{H^{-1}\} = \langle H \rangle = \{ R_0, H \} \quad \Big| \quad \langle D \rangle = \{ R_0, D \}$$

$$\langle V \rangle = \{ R_0, V \} \quad \Big| \quad \langle D' \rangle = \{ R_0, D' \}$$