Lec 3

G is a grp. $x \in G$ The cyclic subgrp $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$

Def | The order of G is $\# G$ e.g. S_n has ord $n!$

Def | The order of $x \in G$ in G is the order of $\langle x \rangle \leq G$

Alt: smallest +ive int so $x^n = 1$ or inf if one.

Def | Given $x_1, \dots, x_n \in G$. we have $\langle x_1, \dots, x_n \rangle$ subgrp of G gen by $x_1, \dots, x_n$. Smallest subgrp gen by $x_1, \dots, x_n$.

1) All fin words from x_1 to x_n & x_1^{-1} to x_n^{-1}
2) Intersection of all subgps containing $x_1 \dots x_n$

Def We say G is finitely gen. If $\exists\, x_1, \dots, x_n \in G$ so $\langle x_1, \dots, x_n \rangle = G$

Def | G is cyclic if $\exists\, x \in G$ so $\langle x \rangle = G$

e.g. $GL_2(\mathbb{Z})$ is fin generated.

non eg. $(\mathbb{Q}, +)$ is not fin gen. Only finitely many prime denom.
$\hookrightarrow$ if G fin gen subgrp of $\mathbb{Q}$ $\exists\, N \neq 0 \in \mathbb{Z}$ so $Nx \in G$ $\forall x \in G$

non eg. $(\mathbb{Q}^*, \cdot)$ not fin gen.

Isomorphism

$G = S_4$, $x = (1\ 2\ 3)$ $y = (2\ 3\ 4)$

$\langle x \rangle = \{1, x, x^2\}$, $\langle y \rangle = \{1, y, y^2\}$ $\longrightarrow$ these subgrp have similar structure

Def | An isomorphism between G & H grps. Is a bijective corr $G \leftrightarrow H$ That is compatible with grp law

i.e. $g_1 \leftrightarrow h_1$, $g_2 \leftrightarrow h_2 \Rightarrow g_1 g_2 \leftrightarrow h_1 h_2$

Equiv: a bijective fnc $\varphi: G \to H$ so $\forall g_1, g_2 \in G$
$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ $\quad (G \cong H)$

e.g 1) $G = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{R} \right\} \cong (\mathbb{R}, +)$ $\quad \varphi: x \longmapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$
$\leq GL_2(\mathbb{R})$

$\varphi(x)\varphi(y) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$

2) $G = (\mathbb{R}_{>0}, *) = \mathbb{R}^{x} \cong (\mathbb{R}, +)$ $\quad \varphi: (\mathbb{R}, +) \longrightarrow G$
$x \longmapsto e^x$

3) let $x \in G$ have ∞ order $\cong (\mathbb{Z}, +)$
$n \longmapsto x^n$

4) $x \in G$, $y \in H$ so $ord(x) = ord(y) \implies \langle x \rangle \cong \langle y \rangle \cong \mathbb{Z}/_{\text{ord}}$

Rmk | 1) $id_G : G \to G$ is an iso. $\implies G \cong G$

2) ~~If~~ $\varphi : G \to H$ is iso. So is $\varphi^{-1} : H \to G$

so $G \cong H \implies H \cong G$

3) If $\varphi : G \to H$, $\psi : H \to K$ iso $\implies \psi \circ \varphi : G \to K$ iso

So $G \cong H$, $H \cong K \implies G \cong K$

So, equiv reln!

Consider eg2 $G = (\mathbb{R}_{>0}, *) = \mathbb{R}^* \cong (\mathbb{R}, +)$

$$\mathbb{R} \xrightarrow{\varphi} G \qquad \mathbb{R} \xrightarrow{\psi} G \qquad \text{both iso.}$$
$$x \mapsto e^x \qquad x \mapsto e^{2x}$$

$$\mathbb{R} \xrightarrow{\psi} G \xrightarrow{\varphi^{-1}} \mathbb{R} \quad \text{so} \quad \varphi^{-1} \circ \psi = 2x$$

Def | An automorphism is an isomorphism from grp to itself

e.g $\alpha : \mathbb{R} \to \mathbb{R}$, $x \to 2x$ $(\mathbb{R}, +)$ is an auto

from above $\to \psi = \varphi \circ \alpha$

Gen obs | if $\varphi : G \to H$ and $\psi : H \to G$ Then $\alpha = \varphi^{-1} \circ \psi$ is an automorphism of G. Also $\varphi \circ \alpha = \psi$.

Isomorphisms vary by an automorphism α

Let G grp. $g, h \in G$. $ghg^{-1} \to$ conjugate of h by g.

$\gamma_g : G \to G$, $h \mapsto ghg^{-1}$ is the conjugation by g map.

This is always an automorphism!

1) $\gamma_g \circ \gamma_{g^{-1}} = \gamma_{g^{-1}} \circ \gamma_g = id_G \implies$ bijectivity

2) $\gamma_g(h)\gamma_g(h') = ghg^{-1}gh'g^{-1} = ghh'g^{-1} = \gamma_g(hh')$

$\implies$ homomorphism

e.g. $G = S_n$ $\sigma \in S_n$ $\sigma (m_1 \dots m_r) \sigma^{-1}$ ← r cycle

$= (\sigma(m_1) \dots \sigma(m_r))$! cool!