Lec 2

Def If G is a grp $H \subseteq G$ is a subgrp p.t.
1) H is closed under $\cdot$
2) $H \ni e$
3) H closed under inv

e.g. If $m \in \mathbb{Z}$ then $m\mathbb{Z}$ is a subgrp of $(\mathbb{Z}, +)$

Prop Every subgrp of $\mathbb{Z}$ is of the form $m\mathbb{Z}$

Pf Let H subgrp of $\mathbb{Z}$. If $H = \{0\}$ then $H = m\mathbb{Z}$ for $m = 0$

If $H \neq \{0\}$. Note $\exists$ pos int in H. By assumption $\exists\ 0 \neq a \in H$. If $a > 0$ done else note $-a > 0$ & $-a \in H$

Thus let m be smallest pos int in H (well def by above)

Show $m\mathbb{Z} \subseteq H$. We know $m \in H$. As H closed under $+$ so $\square$

Show $H \subseteq m\mathbb{Z}$. Suppose $a \in H$ positive. Write $a = mq + r$ by div with remainder where $q, r \in \mathbb{Z}_{\geq 0}$, $0 \leq r < m$.

as $a \in H$, $mq \in H \Rightarrow r \in H$. but $r < m$ and by char of m $\Rightarrow r = 0$. Thus $a = mq \Rightarrow a \in m\mathbb{Z}$ $\square$

If a negative apply same to $-a$.

Given $a, b \in \mathbb{Z}$. Write $a\mathbb{Z} + b\mathbb{Z} = \{ar + bs \mid r, s \in \mathbb{Z}\}$ a subgrp by above $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.

Prop
1) $d = ar + bs$
2) d divides a & b
3) Anything that divides a, b divides d

} $d = \gcd(a, b)$

Pf
1) follows from $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
2) $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \Rightarrow a \in d\mathbb{Z} \Rightarrow d \mid a$
similarly $d \mid b$
3) let $e \mid a$, $e \mid b \Rightarrow a\mathbb{Z} \subset e\mathbb{Z}$ and $b\mathbb{Z} \subset e\mathbb{Z}$
as $e\mathbb{Z}$ grp $\Rightarrow a\mathbb{Z} + b\mathbb{Z} \subset e\mathbb{Z} \Rightarrow d\mathbb{Z} \subseteq e\mathbb{Z}$
$\Rightarrow e \mid d$

$\square$

Rmk $a\mathbb{Z} \cap b\mathbb{Z} = d\mathbb{Z}$ where $d = \text{lcm}(a,b)$

$m\mathbb{Z}$ is the smallest subgrp of $\mathbb{Z}$ containing m → generated.

Say G is any grp $x \in G$.

notation: $n \in \mathbb{Z}$ $\quad x^n = \begin{cases} x \cdot \dots \cdot x & n>0 \\ 0 & n=0 \\ (x^{-1}) \cdots (x^{-1}) & n<0 \end{cases}$

Claim $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgrp of G

1) $x^n \cdot x^m = x^{n+m} \in H$
2) $x^0 = e \in H$
3) $x^n \Rightarrow x^{-n} \in H$

→ H is the subgrp of G generated by x.

a) it is cyclic since it is gen by 1 elt

e.g $G = \mathbb{C}^*$ (complex nums w/ mult rule)

Let $x = e^{\frac{2\pi i}{3}}$ $\quad x^2 = e^{\frac{4\pi i}{3}}$ $\quad x^3 = 1$

Then $H = \{x^n \mid n \in \mathbb{Z}\} = \{e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}, 1\}$

Let $G = S_n$ symmetric grp.

Notation: i) Let $\sigma \in S_n$ be identity $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

2) (1) is cycle

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

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

Let $G = S_6$ and $\sigma = (2\ 3\ 5)$

$\Rightarrow \sigma^2 = (2\ 5\ 3)$ $\quad \sigma^3 = (1)$

Let $G = S_6$ $\quad$ Let $\sigma = (1\ 2\ 3\ 4)$

$\sigma^2 = (1\ 3)(2\ 4)$! → not a cycle!

$\sigma^3 = (1\ 4\ 3\ 2)$

Lemma Let G grp $\quad x \in G$. $\quad H = \{n \in \mathbb{Z} \mid x^n = e\}$ is a subgrp of $(\mathbb{Z}, +)$

Pf pf $n, m \in H$ $\quad x^{n+m} = x^n x^m = e \cdot e = e$

$\Rightarrow \therefore n+m \in H$!

2) $x^0 = e \Rightarrow 0 \in H$

3) $n \in H \Rightarrow x^n = e \Rightarrow x^{-n} = e \Rightarrow -n \in H$

D

Rmk by above $H = m\mathbb{Z}$ for $m \in \mathbb{Z}_{\geq 0}$

1) if $m = 0 \Rightarrow H = \{0\} \Rightarrow$ all power of x dist. inf → $x^n = x^0 \Rightarrow a \to e \in H$

2) $m > 0$. Smallest pos m so $x^m = e$ → order