Group Theory

Lecture 4

Take 3 exams on Moodle each of 30 marks and take best 2 out of 3. (=60%).

One subjective test = 20%

One assignment = 20%.

1st Moodle Test = 3rd Feb

2nd Moodle Test = 21st Feb

3rd Moodle Test = 14th March

Subjective test = 7th April

Question: How can you construct subgroups from a given gp?

Consider $\mathbb{Z}$. $\exists\, a$. . let H be a subg containing a.

$a, 2a, 3a, - - - - \in H$.

$-a, -2a, -3a, - - - \in H$.

$0 \in H$.

H is a subgp which is of the form $a\mathbb{Z} = \{an \mid n \in \mathbb{Z}\} \subseteq \mathbb{Z}$ subgp.

$a\mathbb{Z}$ is the smallest subgp containing a.

Q. How does a subgp of $\mathbb{Z}$ look like?

Prop^n. Any subgp of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ where $m \in \mathbb{Z}$.

pf: Let K be any subgp of $\mathbb{Z}$.

WTS $K = m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

Let m be the least +ve int $\in K$.

Let $b \in K$. Then by division algorithm $b = mq + r$ where $0 \le r < m$

$r = b - mq \in K$.

then $r = 0$. Thus $K = m\mathbb{Z}$.

Example. $S_3 \ni (123)$.

$$\langle (123) \rangle = \{ (123), (132), (1) \}$$

Let G be a group, $x \in G$.

Consider $H = \{ x^n \mid n \in \mathbb{Z} \}$. Then H is the smallest subgp containing x.

A gp G is called a cyclic gp if G can be generated by a single elt i.e $\exists$ some $x \in G$ s.t $G = \{x^n \mid n \in \mathbb{Z}\}$.

Example - (1) $\mathbb{Z}$ is a cyclic gp which is gen by 1.

(2) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ is a cyclic gp gen by $\bar{1}$.

(3) $\mathbb{Z}/6\mathbb{Z}$. is genb by $\bar{1}$ as well as $\bar{5}$ also.

$\bar{5}$

$\bar{5} + \bar{5} = \bar{4}$

$\bar{5} + \bar{5} + \bar{5} = \bar{3}$

$\bar{5} + \bar{5} + \bar{5} + \bar{5} = \bar{2}$

$\bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \bar{1}$

$\bar{5} + \ldots + \bar{5} = \bar{0}$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{0}\} \subseteq \mathbb{Z}/6\mathbb{Z}$.

Propn. Let $H = \langle x \rangle$. Then

(1) If $|H| = \infty$ then $x^n \neq 1$ for any $n \neq 0$.

(2) If $|H| = n$ then $x^n = 1$.

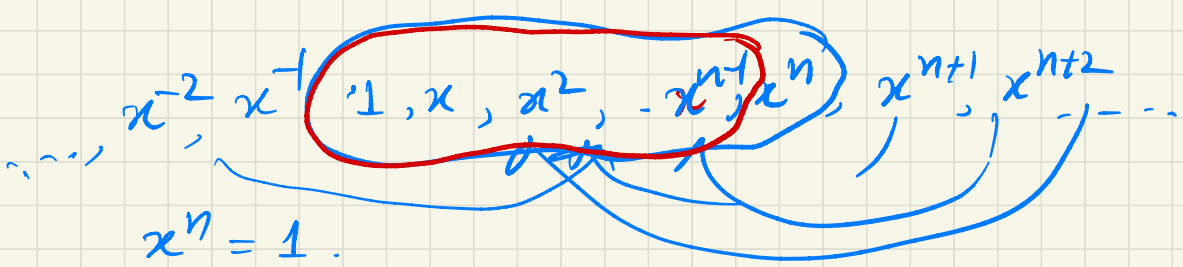
and $H = \{1, x, x^2, \ldots, x^{n-1}\}$.

Pf: (1) Suppose $x^n = 1$ for some $n \neq 0$.

assume $n > 0$.

Let $m \geq n$. Then $m = nq + r$ with $0 \leq r < n$

Then $x^m = x^{nq+r} = x^{nq} \cdot x^r = x^r$.



$x^n = 1$.

$x^{-1} = x^{n-1}$ $\quad x^{-2} = x^{n-2}$ ---.

Thus $H = \{1, x, \ldots, x^{n-1}\}$. But $|H| = \infty$.

$\therefore x^n \neq 1$ for any $n \neq 0$.

(2) Let $|H| = n$ WTS $|x| = n$.

$\Rightarrow H = \{1, \ldots, x^{n-1}\}$.

Since $|H| = n$, not all the powers of H are distinct $\exists\ a > b$ s.t

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

If m is the smallest $\oplus$ve int s.t $x^m = 1$. Then $H = \{1, \ldots, x^{m-1}\}$

But $|H| = n$. Hence $m = n$. [by (1)].

Example. $\mathbb{Z}/6\mathbb{Z} = \langle \bar{1} \rangle$.

$|\bar{2}| = 3$. $|\bar{3}| = 2$

$\langle \bar{2} \rangle$ is a cyclic subgp of $\mathbb{Z}/6\mathbb{Z}$.

Order 2 subgp. $\langle \bar{3} \rangle$,

Order 3 subgp $\langle \bar{2} \rangle$.

Prop. Let $H = \langle x \rangle$ be a cyclic gp.

(1) Every subgp K of H is either

(1) or $\langle x^d \rangle$ where d is the smallest $+$ve power of x in K.

(2) If $|H| = n$ then for every divisor d of n $\exists$ a unique subgp H of order d. This subgp is the cyclic gp $\langle x^{n/d} \rangle$.

Pf: Let $K \neq \langle 1 \rangle \leq H$.

Consider $P = \{ n \geq 1 \mid x^n \in K \}$.

By well ordering principal P has a smallest $+$ve int d.

WTS $K = \langle x^d \rangle$.

Note that $\langle x^d \rangle \subseteq K$.

WTS $K \subseteq \langle x^d \rangle$.

Let $x^b \in K$. Then by division algorithm we have $b = qd + r$ where $0 \leq r < d$

$$x^r = x^{b-qd} = x^b \cdot x^{-qd} \in K.$$

Since $r < d \Rightarrow r = 0$.

$\therefore x^b = x^{qd} \in \langle x^d \rangle$.

$\therefore K = \langle x^d \rangle$.

(2) Since $|H| = n$ $\therefore |x| = n$.

Let $n = d \cdot d'$ Consider $\langle x^{d'} \rangle = K$.

WTS $|x^{d'}| = d$.

Let $|x^{d'}| = m$.

$\Rightarrow \quad x^{d'm} = 1$.

Since $|x| = n$, $\Rightarrow n \mid d'm$

$\Rightarrow dd' \mid d'm$

$\Rightarrow d \mid m$.

$\therefore \quad d = m$ i.e. $|x^{d'}| = d$.

Let H' be another subgp of order d.

$\because H'$ is cyclic $\quad H' = \langle x^l \rangle$

$x^{ld} = 1$.

Now $n \mid ld \Rightarrow dd' \mid ld \Rightarrow d' \mid l$

$\Rightarrow l = d'l'$.

$\therefore x^l = (x^{d'})^{l'} \in \langle x^{d'} \rangle \Rightarrow H' \subseteq K$

$\|$ $\quad$ $\|$

K. $\quad$ $H' = K$.

Propn. Let G be a gp and let $x \in G$

If $|x| = n$ then $|x^a| = \dfrac{n}{\gcd(a,n)}$

where $a \in \mathbb{Z}$.

Pf: Let $\gcd(a,n) = d$ and $n = dd'$

and $a = db'$

with $\gcd(b', d') = 1$

Let $y = x^a$ WTS $|y| = d'$.

$$y^{d'} = (x^a)^{d'} = x^{ad'} = x^{db'd'} = x^{nb'} = 1.$$

Let $|y| = k \Rightarrow k \mid d'$. Then $y^k = 1$

$\Rightarrow x^{ak} = 1 \Rightarrow n \mid ak$

$\Rightarrow dd' \mid db'k$

$\Rightarrow d' \mid b'k \Rightarrow d' \mid k.$

$\therefore d' = k$

Cor. Let $H = \langle x \rangle$ and $|H| = n$.
Then $H = \langle x^a \rangle$ iff $\gcd(a, n) = 1$.
In partical the number of gens of H is $\varphi(n)$ [where φ is the Euler's φ fn. which counts the no. of elts which is co-prime to n and $< n$.].

Example. $\mathbb{Z}/5\mathbb{Z}$ is gen by each of $\bar{1}, \bar{2}, \bar{3}, \bar{4}$.

Example. (1) $A = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq GL_n(\mathbb{R})$.
A is a cyclic gp gen by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
Thm $|A| = \infty$. $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq Id$ for any n.

(2) $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \subseteq SL_n(\mathbb{R})$.

$|\langle A \rangle| = ?$ (Calculate).

(3) In the gp $(\mathbb{Z}/12\mathbb{Z}, +)$ find how many subgps of $\mathbb{Z}/12\mathbb{Z}$ are there. Explicitly describe them and find the order of each subgp. (Ex).

How to compare two groups ?

$f : V_1 \longrightarrow V_2$.

$f(x+y) = f(x) + f(y)$

$f(cx) = c\, f(x)$.

For vector spaces we use linear transformation.

Group homomorphism :

Let G & G' be two groups.
A map $f : G \longrightarrow G'$ is called a group homomorphism if

$$f(g \cdot h) = f(g) \cdot f(h) \quad \forall g, h \in G.$$

Examples of group homomorphism :

(1) $f : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$

$$f(A) = \det A.$$

$$f(A \cdot B) = \det(AB) = \det A \cdot \det B$$
$$= f(A) \cdot f(B)$$

$\therefore$ f is a gp homo.

(2) $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$

$$f(x) = e^x.$$

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

$\therefore$ f is a group homo.

(3) $\phi : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$ where G is a gp written multiplicatively.

$$\phi(n) = a^n \quad \text{for a fixed } a \in G.$$

$$\phi(n+m) = a^{n+m} = a^n \cdot a^m = \phi(n)\cdot\phi(m)$$

ϕ is a gp homo.

(4) Let H be a any subgp of a gp G.

Then $i : H \longrightarrow G$ defined by

$$i(x) = x \text{ is a gp homo.}$$

(5). Let G_1, G_2 be two groups.

Define their product.

$$G_1 \times G_2 = \{(a,b) \mid a \in G_1, b \in G_2\}.$$

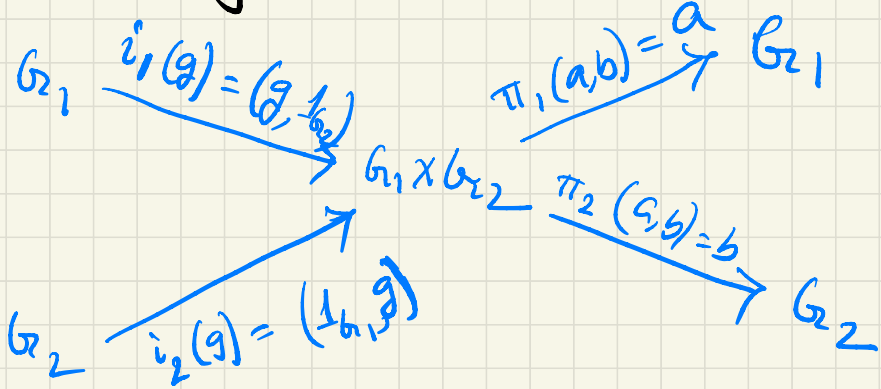
Define a binary operation on $G_1 \times G_2$ as

$$(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$$

$(a,b) \in G_1 \times G_2$, $(c,d) \in G_1 \times G_2$, $(a\cdot c, b\cdot d) \in G_1 \times G_2$.

Identity elt of $G_1 \times G_2$ is $(1_{G_1}, 1_{G_2})$.

inverse of (a,b) is (a^{-1}, b^{-1}).



All these maps i_1, i_2, π_1 & π_2 are group homomorphisms.