Lecture 7 (Introduction to Group Theory) Jan 25, 2022

Discussion.

Subgroups of $(\mathbb{Z}, +)$

$n\mathbb{Z}$ for some integer n

for example $2\mathbb{Z}$

$3\mathbb{Z}$ etc.

Assume H_1 and H_2 are two subgroups of $\mathbb{Z}$.

Then $H_1 = a\mathbb{Z}$ for some $a \in \mathbb{Z}$,

$H_2 = b\mathbb{Z}$ for some $b \in \mathbb{Z}$.

Further assume that $a \neq 0$ and $b \neq 0$ to avoid trivial subgroup into discussion.

How to define $H_1 + H_2$?

Set theoretically, $\{ n \in \mathbb{Z}$ such that $n = ar + bs$ for some $r, s \in \mathbb{Z} \}$

$\underset{\overset{\shortparallel}{a\mathbb{Z}}}{H_1}$, $\underset{\overset{\shortparallel}{b\mathbb{Z}}}{H_2}$

If $H_1 + H_2$ is a subgroup of $\mathbb{Z}$, then

$H_1 + H_2 = d\mathbb{Z}$ for some $d \in \mathbb{Z}$. Here $d = ?$

$\gcd(a,b)$ $\quad$ $\overset{\shortparallel}{\gcd(a,b)}$

$$\begin{array}{ccccc} a\mathbb{Z} & & b\mathbb{Z} & & \\ \parallel & & \parallel & & \\ H_1 & + & H_2 & = & d\mathbb{Z} \end{array}$$, then we say

" d generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$ ".

$(\mathbb{Z}, +) \supseteq H = d\mathbb{Z}$ for some d

Proposition. Let $a, b \in \mathbb{Z}$ with $a \neq 0 \neq b$. Let d be a positive integer which generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$. Then

(i) d can be written in the form $ar + bs$ for some $r, s \in \mathbb{Z}$.

(ii) $d \mid a$ and $d \mid b$.

(iii) If $e \in \mathbb{Z}$ is such that $e \mid a$ and $e \mid b$, then $e \mid d$.

Proof.

(i) $d \in a\mathbb{Z} + b\mathbb{Z}$, and hence $d = ar + bs$ for some $r, s \in \mathbb{Z}$

(ii) $$\underbrace{d\mathbb{Z}}_{\text{Multiple of } d} = a\mathbb{Z} + b\mathbb{Z}$$

every member here should be multiple of d

$\Rightarrow d \mid a$ and $d \mid b$

(iii) $e \mid a \Rightarrow a \in e\mathbb{Z}$

$e \mid b \Rightarrow b \in e\mathbb{Z}$

$\Rightarrow ar + bs \in e\mathbb{Z}$

$\Rightarrow d \in e\mathbb{Z}$

$\Rightarrow e \mid d$.

Note. A pair of integers a, b is said to be relatively prime [i.e. $\gcd(a,b) = 1$]

$\Longleftrightarrow \exists$ integers r, s such that $ra + sb = 1$.

$$ra + sb = 1$$

$$\mathbb{Z}a + \mathbb{Z}b = 1 \cdot \mathbb{Z} = \mathbb{Z}$$

Notation. $\mathbb{Z}a$ and $a\mathbb{Z}$ are same, we may use both.

$$H_1 \qquad H_2 \rightsquigarrow H_1 \cap H_2$$

$H_1 = a\mathbb{Z}$, $H_2 = b\mathbb{Z}$

Assume $a \neq 0$, $b \neq 0$

$H_1 \cap H_2 =$ set theoretically $\{ n \in \mathbb{Z}$ such that $n \in H_1$ and $n \in H_2 \}$

Want: Subgroup structure in $\mathbb{Z}$.

Claim. $(a\mathbb{Z} \cap b\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$; $m = \text{lcm}(a, b)$. [Exercise].

Remark, $a\mathbb{Z} \cap b\mathbb{Z}$ being a subgroup, must be of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

Set. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Then

(i) m is divisible by both a and b.

(ii) If an integer n is divisible by a and b, then it must be divisible by m.

Exercise. $\gcd(a,b)\cdot \operatorname{lcm}(a,b) = ab \quad ; \quad a,b \in \mathbb{Z}^+$

CYCLIC GROUPS

Examples.

$x^3 = 1$

1. $U_3 = \{1, \omega, \omega^2\}$ cube roots of unity

$(U_3, \cdot)$ multiplication is a group

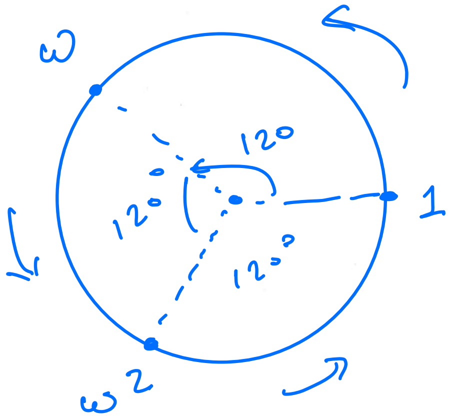
$\cdot : U_3 \times U_3 \longrightarrow U_3$

$(\alpha, \beta) \longmapsto \alpha\beta$

$\cdot : U_3 \times U_3 \longrightarrow U_3$

$(a, b) \longmapsto ab$

Write $1, \omega, \omega^2$ on circle



$$\left\{\begin{array}{l}
(1, \omega) \longmapsto \omega \\
(1, \omega^2) \longmapsto \omega^2 \\
(\omega, \omega^2) \longmapsto \omega^3 = 1 \\
(\omega, 1) \longmapsto \omega \\
(\omega^2, 1) \longmapsto \omega^2 \\
(\omega^2, \omega) \longmapsto \omega^3 = 1
\end{array}\right.$$

$\omega, \omega^2, \underset{\substack{\parallel \\ 1}}{\omega^3}, \omega, \omega^2, \underset{\substack{\parallel \\ 1}}{\omega^3}$

$\{1, \omega, \omega^2\}$

In general,

$$U_n = \{ x \mid x^n = 1 \} \quad n^{th} \text{ roots of unity}$$

$$(U_n, \cdot) = \langle \omega \rangle$$

2. Group generated by a single element.

We are looking for a class of subgroups generated by an arbitrary element x of a group G.

We will be using multiplicative notation here.

Definition. The cyclic subgroup H generated by x is the set of all elements that are powers of x:

x^0 = identity elt

$$H = \{ \ldots, x^{-2}, x^{-1}, \underset{\substack{\| \\ 1 \ (\text{or } e)}}{x^0}, x, x^2, x^3, \ldots \}$$

Notation.

$H = \langle x \rangle$ subgroup generated by x.

Note. 1. We may also write $H = \langle x^{-1} \rangle = \langle x \rangle$

2. It is also possible that x^n, x^m may represent the same element in H.

Example.

(1) $H = (\mathbb{R} - \{0\}, \cdot)$ Group

$-1 \in \mathbb{R} - \{0\}$

$K = \langle -1 \rangle$

$= \{ \ldots, -1, 1, -1, 1, \ldots \} = \{-1, 1\}$

$\ldots, (-1)^0, (-1)(-1), (-1)(-1)(-1), \ldots$

$\{ \ldots, x^{-1}, e, x, x^2, x^3, \ldots \}$

$L = \langle 1 \rangle = \{ \ldots, 1, 1, 1, \ldots \} = \{1\}$

(2) $G = U_3$, with $\cdot$ $(U_3, \cdot)$

$U_3 = \{1, \omega, \omega^2\}$

$H = \langle \omega \rangle$ $\{ \ldots, 1, \omega^{-2}, \omega^{-1}, 1, \omega, \omega^2, 1, \omega^3, \omega^4, \ldots \}$

$\overset{?}{=}$ $\overset{?}{=}$ YES

$K = \langle \omega^2 \rangle$ $\{ \ldots, (\omega^2)^0, \omega^2, (\omega^2)^2, (\omega^2)^3, \ldots \}$, $(\omega^2)^2 = \omega$

$L = \langle 1 \rangle$ $\{ \ldots, 1, 1, 1, \ldots \}$

Proposition. Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by an element $x \in G$.

identity element in G

Set $S = \{ k \in \mathbb{Z}$ such that $x^k = 1 \}$.

Then

(i) The set S is a subgroup of the additive group $(\mathbb{Z}, +)$.

(ii) $x^r = x^s \iff x^{r-s} = 1 \iff r - s \in S$.

(iii) Suppose that S is not the trivial subgroup. Then $\boxed{S = n\mathbb{Z}}$ for some $n \in \mathbb{Z}$. The powers $1, x, x^2, \dots, x^{n-1}$ are the distinct element of the subgroup $\langle x \rangle$, and

$$\operatorname{ord}(\langle x \rangle) = n.$$

smallest

Proof.

(i) To show that S is a subgroup of $(\mathbb{Z}, +)$.

Let $m, n \in S$.

$x^0 = 1$ $\Rightarrow 0 \in S$	$x^m = 1$ and $x^n = 1$ $\Rightarrow x^m \cdot x^n = x^{m+n} = 1$ $\Rightarrow m+n \in S$	$x^{-n} \cdot x^n = x^0 = 1$ $\Rightarrow -n \in S$ if $n \in S$.

(ii) Easy.

(iii) Given $S \neq \{0\} \Rightarrow S = n\mathbb{Z}$ for some n.

$S = n\mathbb{Z}$ [Choose n to be smallest positive integer]

Claim. $\{1, x, x^2, \dots, x^{n-1}\}$ distinct elements.

Let x^k be any element. Then

$k = q \cdot n + r$; where $0 \leq r < n$

$$\Rightarrow x^k = x^{q \cdot n + r} = x^{q \cdot n} \cdot x^r = \boxed{(x^n)^q} \cdot x^r = x^r$$

$= ?$

$S = \{ k \in \mathbb{Z} \text{ s.t. } x^k = 1 \}$

$\quad \parallel$

$n\mathbb{Z} \qquad (x^n)^q = 1$

This implies, $x^k \in \{1, x, \dots, x^{n-1}\}$ since $r < n$

This completes the proof. $\square$

$x^n = e = 1$

$x^{n+1} = x$

Let $x \in G$ some group element.

$H = \{1, x, x^2, \dots, x^{n-1}\}$ [Distinct powers]

$\parallel$

$\langle x \rangle$ and $x^n = 1$.

Such a group H is called a Cyclic group of order n

Example.

$U_n = \{ z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z} \}$

Roots of unity in $\mathbb{C}$.

Recall.

$\text{Order}(G)$ is the number of elements in G.
$\text{Order}(G) = |G|$

$x \in G$, $|x| = n$ if n is the smallest positive integer with $x^n = 1$.

↑

Cyclic subgroup $\langle x \rangle$ generated by x has order n.

Example. $G = (GL_2(\mathbb{R}), \cdot)$

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

Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$.

$|A| = \infty$

$\text{order}(A) =$ smallest +ve integer s.t. $A^n =$ identity ell. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

∞

Let $B = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \in GL_2(\mathbb{R})$

$\langle B \rangle =$

$B^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$|B| = 6$ (verify this)

$B^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\langle A \rangle = \{ \quad \ldots, A^{-1}, I, A, A^2, A^3, \ldots \}$$

$$\langle B \rangle = \underline{\{ B^{-5}, B^{-4}, B^{-3}, B^{-2}, B^{-1}, I, B, B^2, B^3, B^4, B^5 \}}$$

$$= \{ I, B, B^2, B^3, B^4, B^5 \}$$

$$B^6 = Id.$$

$$| \langle B \rangle | = 6$$

$x \in G \cup A$

$H = \langle x \rangle$

$\langle A \rangle$ cyclic group generated by subset.

Discussion. Cyclic subgroup is generated by an arbitrary single element from the group.

To generalize this, one may ~~ak~~ ask

" The subgroup of a group G generated by a $\mathcal{U}$ <u>subset</u>, say $\mathcal{U} \subseteq G$ ".

Finite set — Infinite set

$$= \{ \alpha_1, \alpha_2, \ldots, \alpha_m \}$$

Such a subgroup

- should contain $\mathcal{U}$,
- consists of all elements of G that can be expressed as a product of a string of elements of $\mathcal{U}$ and their inverses.

Definition.

A subset $\mathcal{U}$ of G is said to generate the group G if every element of G is such a product of a string of elements of $\mathcal{U}$ and of their inverses.

Exercise. $G = (GL_2(\mathbb{R}), \cdot)$

$\cup$

Can you describe $\mathcal{U}$?

$\|$ Elementary metrices

$\{ -, -, -, - \}$ s.t.

$$\langle \mathcal{U} \rangle = G$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = I_2 + 1 \cdot e_{12}$$

$$\left\{ \begin{array}{l} E_{ij}(\lambda) \\ E_i(\lambda) \\ P_{ij} \end{array} \right.$$

"Symmetric" Group

Set S_n := set of all bijections from

$\{1, \dots n\} \longrightarrow \{1, 2, \dots, n\}$

$(S_n, \circ)$ composition as binary operation

GROUP.

$\circ : S_n \times S_n \longrightarrow S_n$

$(f, g) \longmapsto \circ(f, g) := f \circ g$

Examples.

$\{1,2\} \to \{1,2\}$

S_2 $\{1, 2\}$

$i : 1 \longrightarrow 1$
$\quad 2 \longrightarrow 2$

$\tau : 1 \longrightarrow 2$
$\quad 2 \longrightarrow 1$

Note that $\tau^2 = i$

S_3 : Group of permutations of $\{1, 2, 3\}$.

1, 2, 3

123
132
213
231
312
321

3!