MA-222

Note Title 31-08-2021

Lec-14

Subgp of $(G, *)$

$(H, *)$

$H \leq G$

$H \leq G$

or $H \leq G$

or $H < G$

$(GL_n(\mathbb{R}), \cdot) \subseteq (M_n(\mathbb{R}), +)$

$GL_n(\mathbb{R})$ = set of $n \times n$ invertible real matrices

But $GL_n(\mathbb{R}) \not\subseteq M_n(\mathbb{R})$.

$\mathbb{Z}_m \not\subseteq \mathbb{Z}_n$ $\quad m \neq n$

$\mathbb{Z}_3 \not\subseteq \mathbb{Z}_4$

$\{0,1,2\} \not\subseteq \{0,1,2,3\}$

Thm: A nonempty subset H of gp G is a subgp iff

{ i) $a * b \in H \quad \forall a, b \in H$
ii) for every $a \in H$, $a^{-1} \in H$. }

Pf

$a * b^{-1} \in H \quad \forall a, b \in H.$

($\Rightarrow$)
- closure ← given
- Associativity
- identity ← $a * a^{-1} = e = a^{-1} * a$, $e \in H$, $\forall a \in H$.
- inverse. ← given.

* restricted to H is a binary op. on H.

To show: $(a * b) * c = a * (b * c)$ $\forall a, b, c \in H$.

$a, b, c \in H \Rightarrow a, b, c \in G$

G is a gp $\Rightarrow (a * b) * c = a * (b * c)$

$a * e = a$

Special subgps

Cyclic subgp of G generated by $a \in G$.

$a \in G$.

Consider $H = \{a^n \mid n \in \mathbb{Z}\}$

Claim: $H \leq G$.

$x \cdot y \in H$

$x = a^m$, $y = a^n$ for some $m, n \in \mathbb{Z}$.

$x * y^{-1} = a^m * a^{-n} = a^{m-n} \in H$

$\Rightarrow H \leq G$.

Ex.

$(a^n)^{-1} = a^{-n}$ $n \in \mathbb{N}$

$a^n = a * a * \cdots * a$

n-times.

$= a * (a * (\cdots (a * a)))$

Note: $H = \langle a \rangle$.

$G = \mathbb{Z}$ $\quad a = 3$.

$3\mathbb{Z} = H = \{ 3^n \mid n \in \mathbb{Z} \}$.

$= \{ 0, \pm 3, \pm 6, \pm 9, \cdots \}$.

$H \leq \mathbb{Z}$.

$\boxed{n\mathbb{Z} \leq \mathbb{Z}}$

$3^0 = 3^{1-1} = 3^1 * 3^{-1}$

$= 3 + (-3)$

$= 0$

$3^2 = 3 + 3$

$3^n = \underbrace{3 + 3 + \cdots + 3}_{n\text{-times}}$

$3^{-n} = (3^n)^{-1}$

$= -(3 + \cdots + 3)$

U_n = gp of n^{th} roots of unity.

$$= \{ e^{2\pi i \frac{k}{n}} \mid k \in \mathbb{Z} \} = \langle e^{\frac{2\pi i}{n}} \rangle.$$

$0 \le k < n$

$$e^{\frac{2\pi i 8}{7}} = e^{2\pi i \frac{7}{7}} \cdot e^{2\pi i \frac{1}{7}}$$

$k = 8$ $\qquad$ $k = 1$

$7q + 1$

$nq + r$

$\mathbb{Z}_n$

Defⁿ: A gp G is called cyclic if $\exists\, a \in G$ such that $G = \langle a \rangle$

i.e. other words every elt of G can be written as power of a.

In this case a is called generator of G.

Ex: $G = \langle a \rangle$.

$\mathbb{Z}_4 = \langle 1 \rangle$

$= \langle 3 \rangle$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$3^4 = 0 = 1+1+1+1 = 1^4$

$3^3 = 1 = 1 = 1^1$

$3^2 = 2 = 1+1 = 1^2$

$3^1 = 3 = 1+1+1 = 1^3$

$\mathbb{Z}_5 = \langle 1 \rangle$

$= \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle.$

$a \in \mathbb{Z}_n^* = \langle g \rangle$

Can you find r s.t.

$a = g^r$

DLP

Defn: Order of a gp is no of elts in the ~~underlying~~ set G.

NOTN: $|G|$ or $o(G)$.

finite gp if $o(G) < \infty$

infinite gp $o(G) = \infty$.

G : finite gp.

G is cyclic iff $\exists a \in G$ s.t.

$$o(G) = o(\langle a \rangle).$$

What if G is infinite?

Is $\mathbb{Z}$ cyclic ?

$\Leftrightarrow$ $\exists\ n \in \mathbb{Z}$ s.t. $\forall\ m \in \mathbb{Z}$, $m = n^r$ for some $r \in \mathbb{Z}$.

n = 1 or -1

$n + n + \cdots + n$ (r times)

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Is $\mathbb{Q}$ cyclic?

Is $\mathbb{R}$ cyclic?

Remark: Thm Subgp of cyclic gp is cyclic.

Ex. +5 11 Friday