

Lecture 11

Saturday, 27/08/2022

Note Title

8/26/2022

In a group $(G, *)$, for $a, b \in G$, we often write ab to denote the element $a*b$.

Subgroup: Let $(G, *)$ be a group. A subset H of G is called a subgroup of G if $(H, *)$ is also a group.

We write $H \leq G$ to mean that H is a subgroup of G .

Example: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

$$\{-1, 1\} \leq (\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot) \leq (\mathbb{C}^*, \cdot).$$

Theorem: Let G be a group and H be a non-empty subset of G .
Then, $H \leq G \Leftrightarrow ab^{-1} \in H \quad \forall a, b \in H$.

Proof: Let $H \leq G$. Let $a, b \in H$. Since H is itself a group, so $b^{-1} \in H$ and hence $ab^{-1} \in H$.

Conversely, suppose that $ab^{-1} \in H \quad \forall a, b \in H$.

Claim: $H \leq G$. We need to prove that H is itself a group.

① Since H is a subset of G , so $x(yz) = (xy)z \quad \forall x, y, z \in H$

② $a \in H \Rightarrow a \cdot a^{-1} \in H \Rightarrow e \in H$

③ $a \in H \Rightarrow e \cdot a^{-1} \in H \Rightarrow a^{-1} \in H$

④ $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$.

In a group, $(a^{-1})^{-1} = a$.
This is because, $a \cdot a^{-1} = e$
and so $(a^{-1})^{-1} = a$.

Thus, H satisfies all the properties of groups, and hence $H \leq G$.

— x —

Theorem: Let G be a group. Then, for $a \in G$, $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G .

Proof: Let $x, y \in \langle a \rangle$. Then, $x = a^n$, $y = a^m$ for some

$$\text{Now, } xy^{-1} = a^n (a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle. \quad n, m \in \mathbb{Z}.$$

$\therefore \langle a \rangle$ is a subgroup of G . #

Definition: $\langle a \rangle$ is called the cyclic subgroup of G generated by a .

Example: (1) $G = (\mathbb{Z}, +)$. For $m \in \mathbb{Z}$, $\langle m \rangle = m\mathbb{Z}$

(2) $(\mathbb{Z}_8, +)$

$$\langle 1 \rangle = \mathbb{Z}_8 = \langle 3 \rangle = \langle 7 \rangle = \langle 5 \rangle$$

$$\langle 2 \rangle = \{0, 2, 4, 6\}, \quad \langle 4 \rangle = \{0, 4\}.$$

Subgroups of $(\mathbb{Z}, +)$: Let H be a subgroup of \mathbb{Z} .

Then, $\exists m \in \mathbb{Z}$ such that $H = m\mathbb{Z}$.

(It follows from Lemma 1 of Lecture 1)

Definition: Let G be a group. G is called cyclic if $\exists a \in G$

such that $G = \langle a \rangle$.

Example: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

• For any $n > 1$, $\mathbb{Z}_n = \langle 1 \rangle$

• $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

• $\cup(G) = \{1, 5\} = \langle 5 \rangle$.

• In a group G , $\langle a \rangle$ is cyclic for every $a \in G$.

Let $G = (\mathbb{C}^*, \cdot)$. Here, $\mathbb{C}^* = \mathbb{C} - \{0\}$, the set of non-zero complex numbers.

Let $z \in \mathbb{C}^*$ and $O(z)$ is finite, say, $O(z) = n$.

Then, $z^n = 1$. Thus, the elements of finite order in \mathbb{C}^* are the

roots of unity.

Let $M_\infty =$ Set of roots of unity in \mathbb{C}^*

$= \bigcup_{n \geq 1} M_n$, where M_n is the set of all the n th roots of unity.

$$M_n = \{z \in \mathbb{C}^* \mid z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}, \text{ where}$$

$$\zeta_n = e^{2\pi i/n}$$

$$O(\zeta_n) = n$$

- M_n is a cyclic group of order n .
- $M_n \leq \mathbb{C}^* \quad \forall n \geq 1$.
- M_∞ is a subgroup of \mathbb{C}^* .
- M_∞ is an infinite group, where every element has finite order.