Lecture 5: Cyclic Groups

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Cyclic Subgroups

Theorem

Let $(G,\cdot)$ be a group and let $a \in G$.Then $H = \{a^n \mid n \in \mathbb{Z}\} \leq G$.
Similarly, if $(G,+)$ is a group, then $H = \{na \mid n \in \mathbb{Z}\} \leq G$.

Remark: The subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ is the smallest subgroup of G that contains a.

Definition

Let $(G,\cdot)$ be a group and let $a \in G$.Then the subgroup $H = \{a^n \mid n \in \mathbb{Z}\}$ of G is called the (cyclic) **subgroup generated by** a and denoted by $\langle a \rangle$.

If the cyclic subgroup $\langle a \rangle$ of G is finite, then $\circ(a) = |\langle a \rangle|$. Otherwise we say that a is infinite order.

Definition (Cyclic group)

Let $(G, \cdot)$ be a group and $a \in G$.

$$\text{If } \langle a \rangle = G \Rightarrow G \text{ is called } \textbf{cyclic group}.$$

In this case, the element $a \in G$ is called a **generator** for G and it is said that a **generates** G.

If G is a finite cyclic group $\Leftrightarrow \exists a \in G$ such that $\circ(a) = |G|$.

Examples:

1. $(\mathbb{Z}, +)$ is cyclic group. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

2. $(\mathbb{Z}_6, +_6)$ is cyclic group. $\mathbb{Z}_6 = \langle \overline{1} \rangle = \langle \overline{5} \rangle$.

3. $(\mathbb{Z}_n, +_n)$ is cyclic group. $\mathbb{Z}_n = \langle \overline{a} \rangle$ where $\gcd(a, n) = 1$.

4. $(n\mathbb{Z}, +)$ is cyclic subgroup of $\mathbb{Z}$. $n\mathbb{Z} = \langle n \rangle$.

5. Klein-4 group is not cyclic. Since no element of order 4.

6. $(\mathbb{Q}, +)$ is not cyclic.

Our goal is describe all cyclic grous and all subgroups of them. Cyclic groups can be seen as the fundamental building blocks for all finite abelian groups.

Theorem

1. *Every cyclic group is abelian.*
2. *A subgroup of a cyclic group is also cyclic.*
3. *Let $(G, \cdot)$ be a cyclic group. If*

$$|G| \text{ is infinite} \Rightarrow G \simeq \mathbb{Z}$$

$$|G| = n \Rightarrow G \simeq \mathbb{Z}_n.$$

Properties of cyclic groups

Theorem

Let $G = \langle a \rangle$ *and* $|\langle a \rangle| = n$. *Then*

1. $\langle a^s \rangle = H \leq G$ *such that* $|\langle a^s \rangle| = \frac{n}{\gcd(n,s)}$.
2. $G = \langle a^m \rangle \Leftrightarrow \gcd(n, m) = 1$.
3. *The number of generators of* G *is* $\phi(n)$.

Remark:

For finite cyclic groups, we have the following result which is a special case of the Lagrange Theorem.

- Let $(G, \cdot)$ be a cyclic group and $|G| = n$. If $H < G \Rightarrow |H| \mid |G|$. Note that $H = \langle a^s \rangle$ for $s \in \mathbb{Z}$ such that $s \mid n$.

The converse of this result also holds for all finite cyclic groups.

- Let $(G, \cdot)$ be a cyclic group and $|G| = n$. Then every positive divisor d of n, there exists a unique subgroup of G of order d.

Example: Find the subgroups and generators of $\mathbb{Z}_6$.

Since the positive divisors of $|\mathbb{Z}_6| = 6$ are $1, 2, 3, 6$. Thus the subgroups of $\mathbb{Z}_6$ are

$$\begin{aligned}
\langle\overline{1}\rangle &= \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\} = \mathbb{Z}_6 \\
\langle\overline{2}\rangle &= \{\overline{0},\overline{2},\overline{4}\} \\
\langle\overline{3}\rangle &= \{\overline{0},\overline{3}\} \\
\langle\overline{6}\rangle &= \langle\overline{0}\rangle = \{\overline{0}\}
\end{aligned}$$

Since $m = 1, 5$ such that $\gcd(m, 6) = 1$, the generators of $\mathbb{Z}_6$ are $\langle\overline{1}\rangle = \langle\overline{5}\rangle$.

Remarks:

1. Let $G = \langle a \rangle$ be a cyclic group and the order of G is infinite. Then

- The order of all subgroups of G are infinite.
- All generators are a and a^{-1}.

Example: $(\mathbb{Z}, +)$ is an infinite cyclic group and $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

2. For positive integers n, m, we have

- $\langle n \rangle \cap \langle m \rangle = \langle \operatorname{lcm}(n, m) \rangle$
- $\langle n \rangle + \langle m \rangle = \langle \gcd(n, m) \rangle$

Example:

$$\begin{aligned} \langle 2 \rangle \cap \langle 3 \rangle &= \langle 6 \rangle = 6\mathbb{Z} \\ \langle 2 \rangle + \langle 3 \rangle &= \{2a + 3b \mid a, b \in \mathbb{Z}\} = \langle 1 \rangle = \mathbb{Z}. \end{aligned}$$

3. Consider the direct product

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}.$$

- $\circ((g_1, g_2)) = \operatorname{lcm}(\circ(g_1), \circ(g_2))$
- If G_1 and G_2 are cyclic, then $G_1 \times G_2$ need not be cyclic.

Examples:

1. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic since $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle(\bar{1}, \bar{1})\rangle$

2. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic since there is no element of order 4.

3. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic since there is no element of order 8.

- Let G_1 and G_2 are finite cyclic groups. Then

$$G_1 \times G_2 \text{ is cyclic} \Leftrightarrow \gcd(|G_1|, |G_2|) = 1.$$

- $$\mathbb{Z}_m \times \mathbb{Z}_n \text{ is cyclic} \Leftrightarrow \gcd(m, n) = 1.$$

4. Every group is the union of its cyclic subgroups. Since every element of the group generates a cyclic subgroup that contains itself.

Example: The Klein-4 group $\left(V_4 = \left\{e, a, b, c \mid a^2 = b^2 = c^2 = e\right\}, \cdot\right)$ is a union of its cyclic subgroups

$$\begin{aligned} \langle a \rangle &= \{e, a\} \\ \langle b \rangle &= \{e, b\} \\ \langle c \rangle &= \{e, c\}, \end{aligned}$$

that is

$$V_4 = \langle a \rangle \cup \langle b \rangle \cup \langle c \rangle .$$

Note that the subgroups of V_4 is cyclic, but V_4 is not cyclic.

Generating Sets

Let G be a group.

- For $a \in G$, $\langle a \rangle \leq G$ is the smallest subgroup that containing a.
- For $a_1, a_2 \in G$, $\langle a_1, a_2 \rangle \leq G$ is the smallest subgroup that containing a_1, a_2.
- In general, let $S \subseteq G$. Then $\langle S \rangle \leq G$ is the smallest subgroup that containing S, that is,

$$\langle S \rangle := \bigcap_{i \in I} G_i, \;\; G_i \leq G, S \subseteq G_i \text{ for all } i \in I.$$

Note that

$$\begin{aligned} S &= \emptyset \Rightarrow \langle \emptyset \rangle = \{e\} \\ S &= \emptyset \Rightarrow \langle S \rangle = \{a_1^{n_1} a_2^{n_2} ... a_r^{n_r} \mid a_i \in S, n_i \in \mathbb{Z}, r \in \mathbb{N}, \} \end{aligned}$$

where a_i may occur several times.

- If $G = \langle a \rangle \Rightarrow G$ is cyclic group
- If $G = \langle a_1, a_2, ..., a_n \rangle \Rightarrow G$ is **finitely generated group.**