Lecture 3: Elementary Properties of Groups

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

Ankara University

Let $(G, \cdot)$ be a group and $a \in G$. For $n \in \mathbb{Z}$,

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \cdots \cdot a}_{n}, & n > 0 \\ e, & n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{|n|}, & n < 0. \end{cases}$$

Let $(G, +)$ be a group and $a \in G$. For $n \in \mathbb{Z}$,

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{|n|}, & n < 0. \end{cases}$$

For conventional notation, we will use the multiplicative notation $\cdot$.

Order of an element

Definition

A group $(G, \cdot)$ is called a finite group if G has only finite number of elements. The **order**, written by $|G|$, of a group G is the number of elements of G. A group with infinite number of elements is called as an infinite group.

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

$$a \in G \overset{G \text{ group}}{\Rightarrow} a \cdot a = a^2 \in G, \ldots, a^m \in G \text{ for all } m \geq 1$$

$$\overset{G \text{ finite}}{\Rightarrow} \text{the elements } a, a^2, \ldots, a^m, \ldots \text{ can not be all distinct}$$

$$\Rightarrow a^i = a^j \text{ for some integer } 0 < i < j$$

$$\overset{j-i=:n}{\Rightarrow} a^{j-i} = a^n = e \text{ for } n \in \mathbb{Z}^+.$$

Thus for a finite group G, $a^n = e$ for some $n \in \mathbb{Z}^+$. Also if G is an infinite group, it may still possible that $a^n = e$ for some $n \in \mathbb{Z}^+$. For example, $(-1)^2 = 1$ in $(\mathbb{R}^*, \cdot)$.

Order of an element

Definition

Let $(G,\cdot)$ be a group and $a \in G$. If there exists a positive integer n such that $a^n = e$, then the smallest such positive integer is called the **order** of a, and denoted by $\circ(a)$. If no such positive integer exists, then we say that a is of infinite order.

In other words,

$$\circ(a) = n \Leftrightarrow n \text{ is the smallest positive integer such that } a^n = e.$$

If we consider the group $(G,+)$, then

$$\circ(a) = n \Leftrightarrow n \text{ is the smallest positive integer such that } na = e.$$

Remark: The order of an element helps us to determine the structure of the group itself.

Examples:

1. In $(\mathbb{R}^*, \cdot)$, $\circ(-1) = 2$, but all other elements except ± 1 are infinite order.

2. In $(\mathbb{Z}_6, +_6)$, $\circ(\bar{a}) = n \Leftrightarrow n$ is the smallest positive integer such that $n\bar{a} = \bar{0}$. Thus

$$\begin{aligned} \circ(\bar{0}) &= 0, \ \circ(\bar{1}) = 6, \ \circ(\bar{2}) = 3, \\ \circ(\bar{3}) &= 2, \ \circ(\bar{4}) = 3, \ \circ(\bar{5}) = 6. \end{aligned}$$

3. In $(Q_8, \cdot)$,

$$\begin{aligned} \circ(1) &= 1, \ \circ(-1) = 2, \ \circ(i) = 4, \ \circ(-i) = 4, \\ \circ(j) &= 4, \ \circ(-j) = 4, \ \circ(k) = 4, \ \circ(-k) = 4. \end{aligned}$$

4. In $(V, \cdot)$,

$$\circ(e) = 1, \ \circ(a) = \circ(b) = \circ(c) = 2.$$

Order of an element

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

- If $\circ(a)$ is infinite, then $\circ\left(a^k\right)$ is also infinite for all $k \in \mathbb{Z}^+$.
- If $\circ(a)$ is finite, then we can compute the $\circ\left(a^k\right)$ by using the following theorem.

Theorem

Let $(G, \cdot)$ be a group and let $\circ(a) = n$ for $a \in G$.
(i) If $a^m = e$ for some $m \in \mathbb{Z}^+$, then $n \mid m$.
(ii) For every $k \in \mathbb{Z}^+$, $\circ\left(a^k\right) = \frac{n}{\gcd(k,n)}$

Example: In $(\mathbb{Z}_6, +_6)$, $\circ\left(\overline{1}\right) = 6$. So

$$\circ\left(\overline{4}\right) = \circ\left(4.\overline{1}\right) = \frac{6}{\gcd(4,6)} = 3.$$

Torsion Group

Definition

A group $(G, \cdot)$ is called a **torsion group** if every element of G is of finite order.
If every nonidentity element of G is of infinite order, then $(G, \cdot)$ is called a **torsion-free group.**

Examples:

1. $(\mathbb{R}, +)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{Q}^+, \cdot)$ are torsion-free groups.
2. $(\mathbb{Z}_6, +_6)$ is torsion group.
3. $(\mathbb{R}^*, \cdot)$ is neither a torsion group nor a torsion-free group.

Order of an element

Remarks:

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

- If $\circ(a) = m$, $\circ(b) = n \Rightarrow \circ(ab) < \infty$ or $\circ(ab) = \infty$.

2. Let $(G, \cdot)$ be an **abelian** group and let $a, b \in G$.

- If $\circ(a) = m$, $\circ(b) = n \Rightarrow \circ(ab) \mid mn$
- If $\circ(a) = m$, $\circ(b) = n$, $\gcd(m, n) = 1 \Rightarrow \circ(ab) = mn$
- If $\circ(a) = m$, $\circ(b) = n \Rightarrow \circ(ab) \mid \operatorname{lcm}(m, n)$.