Abstract algebra

Lecture note 2. Subgroups

Lecturer : O-joung Kwon
Spring, 2019

Convenient notations : consider a binary operation as a summation : $a+b$, $-a$, $5a+2b$...

consider a binary operation as a multiplication : ab, a^{-1}, a^5b^2 ...

Definition 1. *For a group G, the order $|G|$ of G denotes the number of elements in G.*

Definition 2 (Subgroup)**.** *Let H be a subset of a group G that is closed under the binary operation of G such that H with the induced operation from G is itself a group, then H is a* subgroup *of G. We denote by $H \leq G$. In particular $H < G$ means that $H \leq G$ but $H \neq G$.*

Example 1. $< \mathbb{Q}^+, + >$ is not a subgroup of $< \mathbb{R}, + >$ because $< \mathbb{Q}^+, + >$ itself is not a group.

Definition 3. *G is an* improper subgroup *of G, and all other subgroups are called* proper subgroups *of G. $\{e\}$ is a* trivial subgroup *of G.*

Theorem 1. *A subset H of a group G is a subgroup of G if and only if*

(1) H is closed under the binary operation of G,
(2) the identity element e of G is in H,
(3) for all $a \in H$, a^{-1} is also in H.

PROOF.

Cyclic subgroups
$\mathbb{Z}_n$ is a group on $\{0, 1, \ldots, n-1\}$, where $a + b = c \pmod{n}$.

Question : What is the largest subgroup of $\mathbb{Z}_{12}$ containing 3?

Easy to observe that $3, 6, 9, 0$ are contained in any subgroup. Since $\{3, 6, 9, 0\}$ is a subgroup, it is the smallest one.

In general, all of a^x's form the smallest subgroup containing a.

Theorem 2. *Let G be a group and $a \in G$. Then $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G, and is the smallest subgroup of G containing a.*

PROOF

Definition 4. *Let G be a group and $a \in G$. Then the subgroup $\{a^n : n \in \mathbb{Z}\}$ is called the* cyclic subgroup *of G generated by a. It is denoted by $< a >$.*

Definition 5. *An element a of a group G is a* generator *of G if $G =< a >$. We also say that a generates G. A group G is* cyclic *if it has a generator.*

Example 2. $< 1 >=< 3 >= \mathbb{Z}_4$. So, $\mathbb{Z}_4$ is cyclic.

Example 3. $\mathbb{Z}$ is cyclic. Both 1 and -1 are generators. The group $\mathbb{Z}_n$ under addition modulo n is cyclic.