Lectures in Group Theory

MOHAMMED ALABBOOD

University of Basrah-College of Science
Department of Mathematics

June 24, 2020

Cyclic group

Let G be a group and S be a subset of G. Let
$\mathcal{S} = \{H : H \text{ is a subgroup of } G \text{ and } S \subseteq H\}$.
Then $\langle S\rangle = \bigcap_{H\in\mathcal{S}} H$ is a subgroup of G which is called the **subgroup generated** by S. For $a \in G$, we use the notation $\langle a\rangle$ rather than $\langle\{a\}\rangle$ to denote the subgroup of G generated by $\{a\}$. If $G = \langle a\rangle$ for some $a \in G$, then we say G cyclic group generated by a, where $\langle a\rangle = \{a^n : n \in \mathbb{Z}\}$.

Example1: Let us find the subgroup of $(\mathbb{Z}_6, +)$ which is generated by 2: By definition, we have $\langle 2\rangle = \{2, 4, 0\}$.

Example2: As we say in previous lecture, all subgroups of $(\mathbb{Z}_n, +)$ is of the form $m\mathbb{Z}_n$ where $m|n$. In fact, all these subgroups are cyclic. Now, the following are all cyclic subgroups of $(\mathbb{Z}_6, +)$:
$\langle 6\rangle = \{0\}$,
$\langle 3\rangle = \{3, 0\}$,
$\langle 2\rangle = \{2, 4, 0\}$,
$\langle 1\rangle = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$.

Product of subgroups

Let H and K be nonempty subsets of a group G. The product of H and K is defined to be the set $HK = \{hk : h \in H, k \in K\}$.
Let $H_1, H_2, \ldots, H_n$ be nonempty subsets of a group G. We define the product, $H_1 H_2 \ldots H_n$, of $H_1, H_2, \ldots, H_n$ to be the set $H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n : h_i \in H_i, i = 1, 2, \ldots, n\}$.
In general the product of subgroups need not be a subgroup. The following theorem gives a necessary and sufficient condition for the product of subgroups to be a subgroup.
Theorem: Let H and K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$. In particular, if H and K are subgroups of a commutative group G, then HK is a subgroup of G.
Proof: First, suppose that $HK \leq G$. Want to prove $HK = KH$:
(1) $KH \subseteq HK$: Let $kh \in KH$, where $h \in H$ and $k \in K$. Now $h = he \in HK$ and $k = ek \in HK$. Because HK is a subgroup, it follows that $kh \in HK$. Hence, $KH \subseteq HK$.
(2) $HK \subseteq KH$: if $hk \in HK$, then $(hk)^{-1} \in HK$, so $(hk)^{-1} = h_1 k_1$ for some $h_1 \in H$ and $k_1 \in K$. Thus,

$$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH.$$

Product of subgroups

Conversely, suppose $HK = KH$. Let $h_1k_1, h_2k_2 \in HK$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We show that $(h_1k_1)(h_2k_2) \in HK$. Now $k_1h_2 \in KH = HK$ implies $k_1h_2 = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$. Thus,

$$(h_1k_1)(h_2k_2) = (h_1h_3)(k_3k_2) \in HK.$$

Finally, $(h_1k_1)^{-1} \in HK$, since $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK$.
Note that if G is commutative group, then $HK = KH$ and hence HK is a subgroup of G according to the argument above.

Homework:

1. Find all cyclic subgroups of $(\mathbb{Z}, +)$.
2. Find all cyclic subgroups of $(\mathbb{Z}_{24}, +)$.
3. Prove that every subgroup of a cyclic group is cyclic.