Lecture 8

Reference: Judson, Chapter 4.1

Subgroups

Recall the following fundamental example of a subgroup.

Example 1

Consider group $(\mathbb{Z},+)$. Then for any fixed nonzero $m \in \mathbb{Z}$ there is a subgroup of elements divisible by m

$$m\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

It turns out that the above example provides an exhaustive list of subgroups of $(\mathbb{Z},+)$. Specifically, we have the following theorem:

Theorem 1

Let $H \subset \mathbb{Z}$ be a subgroup with respect to addition. Then either H is trivial:

$$H = \{0\}$$

or H is of the form

$$H = m\mathbb{Z}$$

for some fixed nonzero $m \in \mathbb{Z}$.

Proof. Assume that H is nontrivial. Then we have some nonzero integer $a \in H$. By subgroup property, we also have $-a \in H$, hence there is at least one positive integer in H.
Let m be the smallest positive integer in H. We claim that $H = m\mathbb{Z}$.
1. $m\mathbb{Z} \subset H$**:** Since $m \in H$, by subgroup properties, we have $-m \in H$, $2m = m + m \in H$, and, more generally, for any $k \in \mathbb{Z}$ we have $k \cdot m \in H$. This proves $m\mathbb{Z} \subset H$.
2. $H \subset m\mathbb{Z}$. Let us take any element $a \in H$. We claim that a is divisible by m without remainder.
Indeed, let us divide a by m with remainder:

$$a = m \cdot q + r, \quad r \in \{0, 1, \ldots, m-1\}.$$

Since $a \in H$ and $m \in H$, by subgroup properties we have

$$a - k \cdot m \in H$$

for any $k \in \mathbb{Z}$. In particular taking $k = q$ we conclude that

$$r \in H.$$

But m is the smallest positive element of H, therefore r must be 0. □

Cyclic subgroups

As usual, let $(G,*)$ be any abstract group. Before we introduce the notion of a cyclic subgroup let us make a trivial remark:

Remark 1

If we have a subgroup $H \subset G$ and an element $a \in H$, then for any $k \in \{1, 2, 3, \dots\}$ we also have

$$a^k := \underbrace{a * \dots * a}_{k \text{ times}} \in H.$$

Similarly, since necessarily $a^{-1} \in H$, we also have

$$a^{-k} \in H.$$

Also $a^0 = e \in H$, therefore we can write

$$\{a^k \mid k \in \mathbb{Z}\} \subset H$$

and this is true for any subgroup $H \subset G$ containing a.

Problem 1: Subset $\{a^k \mid k \in \mathbb{Z}\} \subset G$ is itself a subgroup.

This remark motivates the following definition.

Definition 1: Cyclic subgroup

A subgroup H of $(G, *)$ is called *cyclic*, if there exists an element $a \in G$ such that

$$H = \{a^k \mid k \in \mathbb{Z}\} \subset G.$$

Element a is called a *generator* of a cyclic subgroup.

Remark 2

Generator of a cyclic subgroup is not unique. For example, both [1] and [2] in $\mathbb{Z}_3$ generate the whole group $(\mathbb{Z}_3, +)$.

NB 1: In the presentation $\{a^k \mid k \in \mathbb{Z}\}$ some elements might coincide, so that possibly $a^l = a^n$ for some pairs $l, n \in \mathbb{Z}$.

Example 2

Consider group $(\mathbb{Z}_7^\times, \times)$ and an element $3 \in \mathbb{Z}_7^\times$. Consider elements 3, 3^2, 3^3,... in $\mathbb{Z}_7^\times$:

$$\begin{matrix} 3^0, & 3, & 3^2, & 3^3, & 3^4, & 3^5, & 3^6, & 3^7, & 3^8, & \dots \\ 1, & 3, & 2, & 6, & 4, & 5, & 1, & 3, & 2, & \dots \end{matrix}$$

As we can see, elements in the bottom row repeat **cyclically** with period 6.

Problem 2: Do the same calculation for $2 \in \mathbb{Z}_7^\times$ and for $6 \in \mathbb{Z}_7^\times$. What are the cyclic periods in this case?