Lecture 9

Reference: Judson, Chapter 4.1

Order of an element

The study of cyclic subgroups motivates us to introduce the following notion.

Definition 1: Order of element

Given group $(G,*)$ and an element $a \in G$ consider the set of integer powers of a

$$\{a^k \| \, k \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, a^0, a, a^2, \dots\}.$$

If this sequence is periodic with period $d \in \mathbb{Z}$, we say that element $a \in G$ has **order** d:

$$\operatorname{ord}(a) = d$$

Equivalently, order of a is the smallest positive power $\operatorname{ord}(a)$ such that

$$a^{\operatorname{ord}(a)} = e.$$

If there are no such power, we say that a has infinite order.

Example 1

1. For every integer $n \geqslant 2$, the group $(\mathbb{Z}_n, +)$ is a cyclic group of order n, since the class 1 is always a generator. The class -1 is also a generator. We therefore see that the generator of a cyclic group need not be unique.
2. The group $(\mathbb{Z}, +)$ is cyclic, with generators 1 and -1. Moreover, for every $m \in \mathbb{Z}$, $m\mathbb{Z}$ is the cyclic subgroup of $\mathbb{Z}$ generated by m. Therefore, all the subgroups of $\mathbb{Z}$ are cyclic.
3. The group of units $(\mathbb{Z}_9^\times, \cdot)$ is a cyclic group, with generator 2. Indeed, as a set, $(\mathbb{Z}_9)^\times = \{1, 2, 4, 5, 7, 8\}$, and
$$\begin{gathered} 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8, \\ 2^4 \equiv 7 \pmod 9, \\ 2^5 \equiv 5 \pmod 9, \\ 2^6 \equiv 1 \pmod 9. \end{gathered}$$
4. For every n, $(\mathbb{C}^\times, \cdot)$ has a cyclic subgroup of order n, given by the n-th roots of unity:
$$U_n = \{e^{\frac{2ik\pi}{n}},\ k \in \{0, \dots n-1\}\}.$$
For example, for $n = 2$ we get the subgroup $\{1, -1\}$, for $n = 3$ we get $\{1, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}\}$, and for $n = 4$ we get $\{1, i, -1, -i\}$. Note that the elements of U_n are the vertices of a regular n-gon in the complex plane.

Proposition 1

If a is of finite order d, then for any integer n, $a^n = e$ if and only if $d \in n\mathbb{Z}$, that is, if and only if d divides n.

Proof. If $n = dk$ is a multiple of d, then we can write

$$a^n = (a^d)^k = e^k = e.$$

In the other direction, assume $a^n = e$. Since by definition of order $a^d = e$, we have

$$a^{n-qd} = (a^n) \cdot (a^d)^{-q} = e$$

for any $q \in \mathbb{Z}$. In particular

$$a^r = e$$

where $r \in \mathbb{Z}$ is the remainder of division of n by d. Since $r < d$, we must necessarily have $r = 0$ by minimality of d in the definition of the order. $\square$

Recall that a group $(G, *)$ is called *cyclic*, if there exists an element $a \in G$ such that

$$G = \{a^k | k \in \mathbb{Z}\}.$$

In this case we write $G = \langle a \rangle$. If G has exactly n elements, we will sometimes write

$$G = \langle a \rangle_n.$$

Element $a \in G$ is called a *generator* of G. Generators are not necessarily unique, so our first goal is to answer the following questions:

Question 1

When an element $b = a^k \in \langle a \rangle_n$ can be taken as a generator of $G = \langle a \rangle_n$?

Question 2

More generally, what is the cyclic subgroup $\langle b \rangle$ generated by $b = a^k$?

Example 2

Group $(\mathbb{Z}_3, +)$ is cyclic generated by $[1]$:

$$\mathbb{Z}_3 = \langle [1] \rangle_3 = \{[0], [1], [2]\}.$$

It is easy to see that element $[2]$ can be taken as another generator.

Example 3

Group $(\mathbb{Z}_4, +)$ is cyclic. One can choose either of $[1]$ and $[3] = [-1]$ as a generator. On the other hand, element $[2]$ does not generate $\mathbb{Z}_4$ since

$$\langle [2] \rangle = \{[0], [2]\} \subsetneq \mathbb{Z}_4.$$

Proposition 2

Element $b = a^k \in \langle a \rangle_n$ can be taken as a generator of $\langle a \rangle_n$ if and only if $\gcd(n, k) = 1$.

Proof. First we note that a has order exactly n.
Element b generates the whole group, if and only if $a \in \langle b \rangle$, i.e., for some $l > 0$ we have

$$b^l = a^{lk} = a.$$

By Proposition 1 this happens if and only if $lk \equiv 1 \mod n$.
This happens if and only if element $k \in \mathbb{Z}_n$ is multiplicatively invertible (is a unit), which si equivalent to $\gcd(n, k) = 1$. $\square$

Example 4

We saw that $\mathbb{Z}_9^\times$ is a cyclic group with generator $a = 2$ and is of order $\varphi(9) = 6$. By the above example, all other generators are 2^k, where k is any number coprime with 6, i.e., $k = 1$ and $k = 5$:

$$2^1 = 2, 2^5 = 5$$

With a slight modification to the above argument, we can answer the second question

Proposition 3

Consider any element $b = a^k \in \langle a \rangle_n$. Then

$$\langle b \rangle = \langle a^{\gcd(n,k)} \rangle_{n/\gcd(n,k)} = \{a^0, a^{\gcd(n,k)}, a^{2\gcd(n,k)}, \ldots, a^{n-\gcd(n,k)}\},$$

i.e., a^k generates a cyclic subgroup of order $n/\gcd(n,k)$ which can also be generated by $a^{\gcd(n,k)}$.

Problem 1: Every cyclic subgroup is abelian.

Proposition 4

Every subgroup of a cyclic group is cyclic.

Proof. We have already proved it for infinite cyclic group (see the statement about subgroups of $\mathbb{Z}$). Now let $H \subset \langle a \rangle_n$. Choose an element $a^k \in H$ with the smallest possible $k > 0$.
It is an exercise to check that $H = \langle a^k \rangle$. □

Problem 2: Let S^3 be a group of symmetries of an equilateral triangle. Find orders of all its elements.