Abstract Algebra
Judson, Thomas J.

Notes by:
Clay Curry

4 Cyclic Groups

The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are both examples of what are called cyclic groups. In this chapter, we will study the properites of cyclic groups and cyclic subgroups, which play a fundamental part in the classification of all abelian groups.

4.1 Cyclic Subgroups

Example: $3\mathbb{Z}$

Suppose we consider $3 \in \mathbb{Z}$ and look at all the multiples of 3. As a set, this is

$$3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$$

Here $3\mathbb{Z}$ is a subgroup of the integers, and this subgroup is completely determined by the element 3 since we can obtain all of the other elements of the group my taking multiples of 3. Every element in the group is said to be **generated** by 3.

Example: 2^n

The following set and law of composition $(H, \cdot)$ is a subgroup of non-zero rationals $\mathbb{Q}^*$

$$H = \{2^n : n \in \mathbb{Z}\}$$

because $H \neq \emptyset$ and for all $2^n, 2^m \in H$, we have $2^n(2^m)^{-1} = 2^n 2^{-m} = 2^{n-m} \in H$. Therefore, H is a subgroup of $\mathbb{Q}^*$ determined by 2.

Theorem: Repeated composition forms a subgroup

Let G be a group and $a \in G$. Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G containing a.

Proof: If $a \in G$, then $a^0 = e \in G$ so $\langle a \rangle \neq \emptyset$. Also if $m, n \in \mathbb{Z}$ and $a^{m+n} = a^m a^n \in \langle a \rangle$, then $a^{m-n} = a^m a^{-n} \in \langle a \rangle$, concluding that $\langle a \rangle$ is a subgroup of $\mathbb{Q}^*$.

Since any group containing a must contain all the powers a^k of a, $\langle a \rangle$ is a subgroup of all groups containing a. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a. $\square$

Definition: Cyclic Groups

For $a \in G$, the set $\langle a \rangle$ is called the **cyclic subgroup** of G generated by a. If G contains some element of a such that $G = \langle a \rangle$, then G is a **cyclic group**. In this case a is called a **generator** of G.

Definition: Order

If a is an element of a group G, we define the **order** of a to be the smallest positive integer n such that $a^n = e$, and we write $|a| = n$. If there is no such integer, we write $|a| = \infty$.

In general, a cyclic group can have more than a single generator. Both 1 and 5 generate $\mathbb{Z}_6$; hence, $\mathbb{Z}_6$ is a cyclic group. In general, not every element in a cyclic group is necessarily a generator of the group. The order of $2 \in \mathbb{Z}_6$ is 3.

In the symmetry group of an equaliateral triangle S_3, each element forms a distinct cyclic subgroup of S_3; however, no single element of S_3 generates S_3.

Theorem:

Every cyclic group is abelian

Proof: Let G be a cyclic group; therefore, $\exists a \in G$ such that $G = \langle a \rangle$. Then for any two elements $g, h \in G$, since

$$gh = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = hg$$

G is abelian. $\square$

4.2 Subgroups of cyclic groups

One interesting question we can asks about any group G is, "which subgroups of G are cyclic?" Similarly, for any cyclic subgroup, we can ask, "which subgroups for some cyclic subgroup $H \leqslant G$ are cyclic?"

Theorem:

Every subgroup of a cyclic group is cyclic

Proof: Let G be a cyclic group generated by $g \in G$ and suppose $H \leqslant G$. If $H = \{e\}$ then e generates H. If some non-identity element $h = g^n \in H$, then $h^{-1} = g^{-n} \in H$, and either n or $-n$ is positive. Let $S = \{m \in \mathbb{N} : g^m \in H\}$. Notice $n \in S$ or $-n \in S$, implying $\emptyset \neq S \subset \mathbb{N}$, which means S has a least element $m = \min(S)$. Let $h' = g^m$

Claim: $\langle h' \rangle = H$.

Since $H \leqslant G$ and G is cyclic, $\forall h \in H, \exists k \in \mathbb{Z}$, such that $h = g^k$. By the division algorithm, $\exists q, r \in \mathbb{Z}$ where $0 \leq r < m$, such that

$$h = g^k = g^{mq+r} = (g^m)^q g^r \iff g^r = h(h')^{-q} \iff (g^r \in H) \wedge (r < m)$$

and since $m = \min(S)$, we know $r = 0$. Because

$$h = g^k = (g^m)^q = h'^q$$

for all $h \in H$, H is cyclic. $\square$

Theorem:

Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Proof: $\square$

Theorem:

Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

Proof: $\square$