Cyclic Group

The groups Z and Z_n, which are among the most familiar and easily under- stood groups, are both examples of what are called cyclic groups. In this chapter we will study the properties of cyclic groups and cyclic subgroups, which play a fundamental part in the classification of all abelian groups.

4.1 Cyclic Subgroups

Often a subgroup will depend entirely on a single element of the group; that is, knowing that particular element will allow us to compute any other element in the subgroup.

Example 1. Suppose that we consider $3 \in Z$ and look at all multiples (both positive and negative) of 3. As a set, this is

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

Sandip Chatterjee, Department of Mathematics

Example 2. If $H = \{2^n : n \in Z\}$, then H is a subgroup of the multiplicative group of nonzero rational numbers, Q*. If $a = 2^m$ and $b = 2^n$ are in H, then $ab^{-1} = 2^m 2^{-n} = 2^{m-n}$ is also in H. By Proposition 3.10, H is a subgroup of Q* determined by the element 2.

Theorem 4.1. Let G be a group and a be any element in G. Then the set $\langle a \rangle = \{a^k : k \in Z\}$ is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

Proof. The identity is in $\langle a \rangle$ since $a^0 = e$. If g and h are any two elements in $\langle a \rangle$, then by the definition of $\langle a \rangle$ we can write $g=a^m$ and $h=a^n$ for some integers m and n. So $gh = a^m a^n = a^{m+n}$ is again in $\langle a \rangle$. Finally, if $g=a^n$ in $\langle a \rangle$, then the inverse $g^{-1} = a^{-n}$ is also in $\langle a \rangle$. Which proves $\langle a \rangle$ is a subgroup of G. Clearly, any subgroup H of G containing a, must contain all the powers of a by closure; hence, H contains $\langle a \rangle$. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a.

Remark. If we are using the "+" notation, as in the case of the integers under addition, we write $\langle a \rangle = \{na : n \in Z\}$.

For $a \in G$, we call $\langle a \rangle$ the **cyclic subgroup generated by a**. If G contains some element a such that $G = \langle a \rangle$, then G is a **cyclic group**. In this case a is a **generator** of G. 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 n, we say that the order of a is infinite and write $|a| = \infty$ to denote the order of a.

Example 3. Notice that a cyclic group can have more than a single generator. Both 1 and 5 generate Z_6; hence, Z_6 is a cyclic group. Not every element in a cyclic group is necessarily a generator of the group. The order of $2 \in Z_6$ is 3. The cyclic subgroup generated by 2 is $\langle 2 \rangle = \{0, 2, 4\}$.

The groups Z and Z_n are cyclic groups. The elements 1 and −1 are generators for Z. We can certainly generate Z_n with 1 although there may be other generators of Z_n, as in the case of Z_6.

Example 4. The group of units, U(9), in Z_9 is a cyclic group. As a set, U(9) is {1,2,4,5,7,8}. The element 2 is a generator for U(9) since

$$2^1 = 2 \qquad 2^3 = 8 \qquad 2^5 = 5$$
$$2^2 = 4 \qquad 2^4 = 7 \qquad 2^6 = 1$$

Example 5. Not every group is a cyclic group. Consider the symmetry group of an equilateral triangle S_3. The multiplication table for this group is Table 3.2. (Verify!)

Theorem 4.2 Every cyclic group is abelian.

Proof. Let G be a cyclic group and $a \in G$ be a generator for G. If g and h are in G, then they can be written as powers of a, say $g=a^r$ and $h=a^s$. Since $gh=a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg$, G is abelian.

Subgroups of Cyclic Groups

We can ask some interesting questions about cyclic subgroups of a group and subgroups of a cyclic group. If G is a group, which subgroups of G are cyclic? If G is a cyclic group, what type of subgroups does G possess?

Theorem 4.3. Every subgroup of a cyclic group is cyclic.

Proof. The main tool used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If H = {e}, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n. We can assume that $n > 0$.

Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well-Ordering. We claim that $h = a^m$ is a generator for H. We must show that every $h' \in H$ can be written as a power of h. Since $h' \in H$ and H is a subgroup of G, $h' = a^k$ for some positive integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \le r < m$; hence,

$$a^k = a^{mq+r} = (am)^q a^r = h^q a^r$$

So $a^r = a^k h^{-q}$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that am was in H; consequently, r=0 and so k=mq. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h.

Sandip Chatterjee, Department of Mathematics

Corollary 4.4. The subgroups of Z are exactly nZ for $n = 0, 1, 2, \ldots$.

Proposition 4.5. 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. First suppose that $a^k = e$. By the division algorithm, $k = nq + r$ where $0 \leq r < n$; hence

$$e=a^k =a^{nq+r} =a^{nq} a^r =ea^r =a^r$$

Since the smallest positive integer m such that $am = e$ is n, $r = 0$. Conversely, if n divides k, then $k = ns$ for some integer s. Consequently,

$a^k =a^{ns} =(a^n)^s =e^s =e$.

Theorem 4.6. 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. We wish to find the smallest integer m such that $e = b^m = a^{km}$. By Proposition 4.5, this is the smallest integer m such that n divides km or, equivalently, n/d divides $m(k/d)$. Since d is the greatest common divisor of n and k, n/d and k/d are relatively prime. Hence, for n/d to divide $m(k/d)$ it must divide m. The smallest such m is n/d.

Corollary 4.7. The generators of Z_n are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.