Chapter 9

Cyclic groups

A group $(G, \cdot, e)$ is called *cyclic* if it is generated by a single element g. That is if every element of G is equal to

$$g^n = \begin{cases} gg \dots g \,(n \text{ times}) & \text{if } n > 0 \\ e & \text{if } n = 0 \\ g^{-1}g^{-1} \dots g^{-1} \;\; (|n| \text{ times}) & \text{if } n < 0 \end{cases}$$

Note that if the operation is $+$, instead of exponential notation, we use $ng = g + g + \dots$

Example 9.1. *$\mathbb{Z}$ is cyclic. It is generated by* 1.

Example 9.2. *$\mathbb{Z}_n$ is cyclic. It is generated by* 1.

Example 9.3. *The subgroup of $\{I, R, R^2\}$ of the symmetry group of the triangle is cyclic. It is generated by R.*

Example 9.4. *Let $R_n = \{e^{\frac{2\pi ik}{n}} \mid k = 0, 1 \dots n-1\}$ be the subgroup of $(\mathbb{C}^*, \cdot, 1)$ consisting of* nth roots of unity*. This is cyclic. It is generated by* $e^{\frac{2\pi i}{n}}$.

We recall that two groups H and G are *isomorphic* if there exists a one to one correspondence $f : H \to G$ such that $f(h_1h_2) = f(h_1)f(h_2)$. The function f is called an *isomorphism*. A function $f : H \to G$ is called a *homomorphism* if $f(h_1h_2) = f(h_1)f(h_2)$. This is more general than an isomorphism because we do not require it to be one to one or onto. Here are some basic examples.

Example 9.5. *The function $f : \mathbb{Z} \to R_n$ defined by $f(x) = e^{2\pi ix}$ is a homomorphism because $f(x + y) = f(x)f(y)$ from highschool algebra.*

Example 9.6. *The function $f : \mathbb{Z}_n \to R_n$ defined by $E(x) = e^{2\pi ix}$ is an isomorphism.*

Example 9.7. *The function $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = x\, mod\, n$ is a homomorphism. Reverting to $\oplus$ notation, we observe that we need $f(x+y) = f(x) \oplus f(y)$, and this comes down to fact that*

$$(x+y)\, mod\, n = (x\, mod\, n) \oplus (y\, mod\, n)$$

which we verified back in chapter 5. Alternatively, we can reduce this to the first example by using the fact that $\mathbb{Z}_n$ and R_n are isomorphic.

Theorem 9.8. *Any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$.*

Proof. Let $(G, \cdot, e)$ be a cyclic group with generator g. There are two cases. The first case is that $g^n \neq e$ for any positive n. We say that g has infinite order. Then we define $f : \mathbb{Z} \to G$ by $f(m) = g^m$. Since $f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$, it is a homomorphism. It is also onto, because $G = \{g^m = f(m) \mid m \in \mathbb{Z}\}$ by assumption. Suppose that $f(n_1) = f(n_2)$ with $n_1 > n_2$. Then $g^{n_1} = g^{n_2}$ implies that $g^{n_1 - n_2} = e$, which contradicts the fact that g has infinite order.

In the second case, g has finite order which means that $g^n = e$ for some $n > 0$. Let us assume that n is the smallest such number (this is called the order of g). We claim that $G = \{e, g, \ldots, g^{n-1}\}$ and that all the elements as written are distinct. By distinctness we mean that if $m_1 > m_2$ lie in $\{0, 1, \ldots n-1\}$ then $g^{m_1} \neq g^{m_2}$. If not then $g^{m_1 - m_2} = e$ would contradict the fact that n is the order of g. To finish the proof of the claim, use the division algorithm to write any integer m as $m = nq + r$, where $r = m\, mod\, n$. Then $g^m = (g^n)^q g^r = g^r = g^{m\, mod\, n}$. We define $f : \mathbb{Z}_n \to G$ by $f(m) = g^m$. This is onto, and therefore also a one to one correspondence because the sets have the same cardinality. Finally, we note that it is an isomorphism because

$$f(m_1)f(m_2) = g^{m_1} g^{m_2} = g^{m_1+m_2} = g^{(m_1+m_2)\, mod\, n} = f(m_1 \oplus m_2)$$

□

Theorem 9.9. *A subgroup of a cyclic group is cyclic.*

Proof. We may assume that the group is either $\mathbb{Z}$ or $\mathbb{Z}_n$. In the first case, we proved that any subgroup is $\mathbb{Z}d$ for some d. This is cyclic, since it is generated by d. In the second case, let $S \subset \mathbb{Z}_n$ be a subgroup, and let $f(x) = x\, mod\, n$ as above. We define

$$f^{-1}S = \{x \in \mathbb{Z} \mid f(x) \in S\}$$

We claim that this is a subgroup. Certainly, $0 \in f^{-1}S$ because $f(0) = 0$. Also if $x, y \in f^{-1}S$ then $f(x+y) = f(x) + f(y) \in S$, and therefore $x + y \in f^{-1}S$. Finally, if $x \in S$, then $f(-x) = -x\, mod\, n = \ominus x \in S$. Therefore $-x \in f^{-1}S$. Thus $f^{-1}S$ is a subgroup as claimed. This implies that $f^{-1}S = \mathbb{Z}d$ for some d. It follows that S is generated by $f(d)$. □

9.10 Exercises

1. Let $\mathbb{Z}_7^*$ be the set of nonzero elements in $\mathbb{Z}_7$ regarded as a group using (modular) multiplication. Show that it is cyclic by finding a generator.

2. Given a homomorphism $f : H \to G$, prove that f takes the identity to the identity.