6 Cyclic Groups

Review: If $G = \{b^n \mid n \in \mathbb{Z}\}$ then the element b is a **generator** of G, the group $G = \langle b \rangle$ is **cyclic**, and we say G is **generated** by b.

If $\langle b \rangle$ is finite, then the **order** of b is the order $|\langle b \rangle|$ of this cyclic group. Otherwise, b is of **infinite order**.

6.1 Elementary Properties of Cyclic Groups

Theorem. *Every cyclic group is abelian.*

Theorem (Division Algorithm for $\mathbb{Z}$)**.** *If $m \in \mathbb{Z}^+, n \in \mathbb{Z}$, then there exist unique integers q, r such that*

$$n = mq + r, \quad 0 \leq r < m.$$

In the division algorithm, q is called the quotient and r is the remainder.

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

Corollary. *The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.*

Definition 1. *Let $r, s \in \mathbb{Z}^+$. The positive generator d of the cyclic group*

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

*under addition is the **greatest commond divisor** (abbreviated gcd) of r and s. We write $d = \gcd(r, s)$.*

Relatively prime integers have gcd= 1, that is, they have no common prime factors.

Remark. *If r, s are relatively prime and $r \mid sm$, then $r \mid m$. (The vertical line is notation for "divides")*

6.2 The Structure of Cyclic Groups

Theorem. *Let $G = \langle b \rangle$ be a cyclic group. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order, then G is isomorphic to $\langle \mathbb{Z}_n, + \rangle$.*

6.3 Subgroups of Finite Cyclic Groups

Theorem. *Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$. Let $b = a^s$ for some integer s. Then $H = \langle b \rangle \leq G$ is a cyclic subgroup of G with $|H| = n/\gcd(n, s)$. Also,*

$$\langle a^s \rangle = \langle a^t \rangle \quad \Longleftrightarrow \quad \gcd(n, s) = \gcd(n, t)$$

Corollary. *If b is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form b^r, where r is relatively prime to n.*

Example 1. *An isomorphism of a group with itself is an **automorphism** of the group. Find the number of automorphisms of $\mathbb{Z}_8$.*

Example 2. *Find the number of elements in the cyclic subgroup of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication, generated by $(1 + i)/\sqrt{2}$.*

Example 3. *Find all orders of subgroups of $\mathbb{Z}_8$.*

Example 4. *Either give an example of an infinite cyclic group having four generators, or explain why no such group exists.*

Example 5. *Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the* unique *such element. Show that $ax = xa$ for all $x \in G$. [Hint: Consider $(xax^{-1})^2$.]*