Section I.3. Cyclic Groups

Note. Cyclic groups should be your favorite kind of group! They are easily classified, familiar, and they make up all finitely generated abelian groups.

Note. First, a preliminary result.

Theorem I.3.1. Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$ where m is the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.

Note. Notice that Theorem I.3.1 implies that the subgroups of $\mathbb{Z}$ are precisely the groups $\langle m \rangle \cong m\mathbb{Z}$ where $m \in \mathbb{N} \cup \{0\}$. Now we classify cyclic groups.

Theorem I.3.2. Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Definition I.3.3. Let G be a group and $a \in G$. The *order* of a is the order of the cyclic subgroup $\langle a \rangle$, denoted $|a|$.

Note. We now explore the properties of elements of finite and infinite order.

Theorem I.3.4. Let G be a group and $a \in G$. If a has infinite order then

(i) $a^k = e$ if and only if $k = 0$;

(ii) the elements a^k are all distinct as the values of k range over $\mathbb{Z}$.

If a has finite order $m > 0$ then

(iii) m is the least positive integer such that $a^m = e$;

(iv) $a^k = e$ if and only if $m \mid k$;

(v) $a^r = a^s$ if and only if $r \equiv s \pmod{m}$;

(vi) $\langle a \rangle$ consists of the distinct elements $a, a^2, \ldots, a^{m-1}, a^m = e$.

(vii) for each k such that $k \mid m$, $|a^k| = m/k$.

Theorem I.3.5. Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

Note. The following classifies generators of cyclic groups.

Theorem I.3.6. Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G if and only if $(k, m) = 1$ (i.e., the greatest common divisor of k and m is 1; k and m are relatively prime).