**Supplementary notes on finite cyclic groups**

---

**Lemma 0.1.** *Let $G = \langle a \rangle$, and suppose $a^l = a^m$ for some $l < m$. Then, letting $n = m - l > 0$, $|G| = n$ and $G = \{e, a, a^2, \ldots, a^{n-1}\}$.*

*Proof.* If $a^l = a^m$ for some $l < m$, then $a^{m-l} = a^n = e$. Let $g \in G$. Since $G$ is cyclic, $g = a^k$ for some $k \in \mathbb{Z}$. By the division algorithm, there are integers $q, r$ with $0 \leq r < n$ such that $k = nq + r$. Since $0 \leq r \leq n - 1$, we have

$$a^k = a^{nq+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r \in \{e, a, \ldots, a^{n-1}\}.$$

Therefore, $G \subseteq \{e, a, \ldots, a^{n-1}\}$. By the definition of a cyclic group, $\{e, a, \ldots, a^{n-1}\} \subseteq G$, it follows that $G = \{e, a, \ldots, a^{n-1}\}$.

□

**Proposition 0.2.** *Let $G$ be a finite cyclic group of order $n$. Then $G = \{e, a, a^2, \ldots, a^{n-1}\}$. In particular, $a^n = e$.*

*Proof.* Since $G$ is finite, there must be repetition in the sequence $e, a^1, a^2, \ldots$. Therefore there is a positive integer $k$ such that $a^k$ is equal to one of $e, a, a^2, \ldots, a^{k-1}$. Let $m$ be the smallest such positive integer. Then $e, a, a^2, \ldots, a^{m-1}$ are all distinct, and $a^m = a^l$ for some $0 \leq l < m$. Since the order of $G$ is $n$, we must have $m \leq n$. Since $m > l$, by Lemma 0.1, we conclude that $G = \{e, a, a^2, \ldots, a^{m-l-1}\}$. Therefore, $m - l = n$, and since we already showed that $m \leq n$, it must be that $m = n$ and $l = 0$. The proposition is proved. □

In a finite cyclic group, we have the following: $a^l a^k = a^m$, where $m = k + l \pmod{n}$. We typically write $a^l a^k = a^{l+k}$, but keep in mind that we think of $l + k$ modulo $n$. In particular, if $a^l a^k = e$, then $l + k = 0 \pmod{n}$.

**Proposition 0.3.** *Let $a \in G$. Then the following are equivalent:*

1. *$a$ has order $n$;*
2. *$n$ is the smallest positive integer such that $a^n = e$;*
3. *the order of $\langle a \rangle = n$.*

*Proof.* That statements 1 and 3 are equivalent follows from the definition of the order of an element. The equivalence of statements 2 and 3 follows from Lemma 0.1. □

**Proposition 0.4.** *Let $G$ be a finite cyclic group of order $n$. Then $G$ is isomorphic to $\mathbb{Z}_n$.*

*Proof.* Let $\phi : G \to \mathbb{Z}_n$ be the map defined by $\phi(a^k) = k$. By Proposition 0.2, $G = \{e, a, \ldots, a^{n-1}\}$.

- $\phi$ is well-defined: Suppose $a^l = a^m$ for some $a^l, a^m \in G$. Then since $G = \{e, a, \ldots, a^{n-1}\}$, we must have $l = m$, and so $\phi(a^l) = l = m = \phi(a^m)$.
- $\phi$ is a bijection: this follows immediately from Proposition 0.2
- $\phi$ is a homomorphism: $\phi(a^k a^l) = \phi(a^{k+l}) = k + l = \phi(k) + \phi(l)$. (Here we use the comment from above that we think of the exponent $k+l$ as $k+l \pmod{n}$.)

□