Propositions about cyclic groups and orders of elements.

1. Assume that G is a finite group and that $a \in G$. Then a has finite order.

2. Assume that G is a finite abelian group and that $a \in G$. Then the order of a divides the order of G. (We will eventually be able to prove this proposition without the assumption that G is abelian.)

3. If G is a cyclic group, then G is an abelian group.

4. Assume that G is a group and that $a \in G$. We let $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$. Then $\langle a \rangle$ is a subgroup of G and is called the *cyclic subgroup of G generated by a*. If a has finite order, then $\big|\langle a \rangle\big| = |a|$.

5. Suppose that G is a group and that $a \in G$. Suppose also that a has finite order. Let $m = |a|$. Suppose that $k_1, \ k_2 \in \mathbb{Z}$. We have

$$a^{k_1} = a^{k_2} \iff k_1 \equiv k_2 \pmod{m} \ .$$

In particular, if $k \in \mathbb{Z}$, then $a^k = e$ if and only if m divides k.

6. Suppose that G is a cyclic group and that H is a subgroup of G. Then H is also a cyclic group. Let a be a generator for G. If $H \neq \{e\}$, then H is generated by a^t where t is the smallest positive integer in the set $K = \{ k \in \mathbb{Z} \mid a^k \in H \}$. For that positive integer t, we have $K = t\mathbb{Z}$ and $H = \langle a^t \rangle = \{ a^k \mid k \in t\mathbb{Z} \}$.

7. Suppose that G is a finite cyclic group. Let $n = |G|$. If u is a positive integer which divides n, then G has exactly one subgroup H of order u. If a is a generator of G, then $H = \langle a^t \rangle$ where $t = n/u$.

8. Suppose that G is a finite cyclic group of order n and suppose that a is a generator of G. Suppose that $r \in \mathbb{Z}$. Let $b = a^r$. Let $d = gcd(r, n)$. Then

$$|b| = \frac{n}{d} \ .$$

In particular, b is a generator of G if and only if $gcd(r, n) = 1$.