Similarly, any non-zero $a \in \mathbb{Z}$ has infinite order.

The identity element $0 \in \mathbb{Z}$ has order 1.

Given an element $a \in G$ of a group G, one may consider the subgroup of G generated by $a \in G$.

Case 1: $a \in G$ has finite order m.

The subgroup of G generated by $a \in G$ is $\{1, a, a^2, \ldots, a^{m-1}\}$, which has order m. So the order of the subgroup generated by $a \in G$ is equal to the order of $a \in G$.

Exercise: use the cancellation law to show that the elements of $\{1, a, a^2, \ldots, a^{m-1}\}$ are all distinct.

Case 2: $a \in G$ has infinite order.

For each $a \in G$ and each positive integer k, define

$$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ times}}.$$

The subgroup of G generated by $a \in G$ is $\{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$, which is infinite.

Exercise: show that the elements of $\{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$ are all distinct.

Remark 4.4. It follows that one can only have an element of infinite order in an infinite group. This is equivalent to saying that every element of a finite group must have finite order.

Theorem 4.5. *The order of any element in a finite group G is finite and divides the order $o(G)$ of the group G.*

Proof Let G be a finite group and pick an element $a \in G$. Suppose that $a \in G$ has order m. Consider the subgroup $\{1, a, a^2, \ldots, a^{m-1}\}$ of G generated by $a \in G$. By Lagrange's Theorem 3.18, the order m of this subgroup divides the order $o(G)$ of the group G. Hence the order of $a \in G$ divides $o(G)$. □

Definition 4.6. The subgroup generated by an element $a \in G$ of a group G is called the *cyclic subgroup* generated by $a \in G$.

If there exists an element $a \in G$ whose cyclic subgroup is the group G itself, then G is called a *cyclic group*.