



Exercise 1. Let G be a group and suppose that $x \in G$ has finite order $n \in \mathbb{N}$.

- a. Prove that for any $m \in \mathbb{Z}$, $x^m = e$ if and only if n divides m . Conclude that

$$\{m \in \mathbb{Z} \mid x^m = e\} = n\mathbb{Z},$$

where $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. [*Suggestion.* Use the Division Algorithm to divide m by n . Use the minimality of n to argue that the remainder must be 0.]

- b. Conclude that for any $\ell, m \in \mathbb{Z}$, $x^\ell = x^m$ if and only if n divides $\ell - m$.

Exercise 2. Let G be a finite group. Prove that if G has even order, then G contains an element with order 2. [*Suggestion.* Count the elements of G by pairing them with their inverses.]

Exercise 3. Let G be a group and let $a, b \in G$. Denote the order of a by $|a|$.¹ Prove the following assertions.

- a. $|a| = |a^{-1}|$
- b. $|ab| = |ba|$
- c. $|a| = |bab^{-1}|$

Exercise 4. Let G be a finite abelian group, written multiplicatively. Let $a \in G$.

- a. Explain why the value of $\prod_{x \in G} x$ is independent of the particular ordering of G used to compute it.
- b. Explain why $\prod_{x \in G} x = \prod_{x \in G} (ax) = a^{|G|} \prod_{x \in G} x$.
- c. Use part **b** and Exercise **1a** to conclude that $|a|$ divides $|G|$.

¹Do not assume that $|a|$ is necessarily finite.