Theorem 4.1

In a group G there is only one identity element.

Proof. If $e, e' \in G$ are two identity elements, then for every $a \in G$ we have

$$a = ea \quad \text{and} \quad ae' = a$$

This gives:

$$e' = ee' = e$$

□

Theorem 4.2 (Cancellation Property)

If G is a group, $a, b, c \in G$ and either $ac = bc$ or $ca = cb$ then $a = b$.

Proof. Assume that $ac = bc$. Then we have

$$a = (ac)c^{-1} = (bc)c^{-1} = b$$

□

Theorem 4.3

If G is a group then every element of G has only one inverse element.

Proof. Let $a \in G$ and let $b, b' \in G$ be two inverses of a:

$$ab = e = ab'$$

Then, by the cancellation property, $b = b'$. □

Theorem 4.4

If G is a group and $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We have:

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = e$$

Similarly, $(b^{-1}a^{-1})(ab) = e$. □

Exercise. Write multiplication tables of all possible groups with 1, 2 and 3 elements.

Exercise. Write multiplication tables of all possible groups with 4 elements.