

---

**Definition 1.** A *group* is a set  $G$  together with a function  $\mu : G \times G \rightarrow G$  called a *binary operation*, defined as  $(x, y) \mapsto xy$ , that satisfies the following properties:

1. (Associativity) For all  $x, y, z \in G$ ,  $(xy)z = x(yz)$ .
2. (Identity element) There exists an element  $1 \in G$ , called the *identity*, such that  $1x = x = x1$  for all  $x \in G$ .
3. (Existence of Inverses) For all  $x \in G$  there exists an element  $y \in G$  (denoted by  $x^{-1}$ , see property 2) such that  $xy = 1 = yx$ .

A group is called an *abelian group* if furthermore the operation is commutative, that is  $xy = yx$  for all  $x, y \in G$ . In this case the

**Properties.**

1. Identity elements are necessarily unique: if  $1, 1' \in G$  are identity elements then  $1 = 1'1 = 11' = 1'$  where the first two equalities hold because  $1'$  is an identity element and the third equality holds because  $1$  is an identity.
2. .