Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

5 Definition and Examples of Groups

In Section 3, properties of binary operations were emphasized-closure, identity, inverses, associativity. Now these properties will be studied from a slightly different viewpoint by considering systems $(S, *)$ that satisfy all four of the properties. Such mathematical systems are called *groups.*
A group may be defined as follows.

Definition 5.1
A set G is a **group** with respect to a binary operation $*$ if the following properties are satisfied:

(i) $(x * y) * z = x * (y * z)$ for all elements x, y, and z of G (the Associative Law);
(ii) there exists an element e of G (the identity element of G) such that $e * x = x = x * e$, for all elements x of G;
(iii) for each element x of G there exists an element x' of G (the inverse of x) such that $x * x' = e = x' * x$ (where e is the identity element of G).

A group G is **Abelian** (or **commutative**) if $x * y = y * x$ for all elements x and y of G.

Remark 5.1
The phrase "with respect" should be noted. For example, the set $\mathbb{Z}$ is a group with respect to addition but not with respect to multiplication (it has no inverses for elements other than ± 1.)

Example 5.1
We can obtain some simple examples of groups by considering appropriate subsets of the familiar number systems.

(a) The set of even integers is an Abelian group with respect to addition.

(b) The set $\mathbb{N}$ of positive integers is not a group with respect to addition since it has no identity element.
(c) The set $\mathbb{Z}^+ = \mathbb{N} \cup \{0\}$ is not a group with respect to addition since no element other than zero has an inverse.
(d) The set of all nonzero rational numbers is an abelian group under multiplication. ■

Example 5.2
For any nonempty set S the collection of all invertible mappings from S to S is a group with respect to composition. This is a consequence of Theorem 4.3. ■

The following examples give some indication of the great variety there is in groups.

Example 5.3
(a) Let p be a fixed point in the plane P and G_p denote the set of all rotations of the plane about the point p. By Example 4.3, G_p is an Abelian group with respect to composition.
(b) The set of 2-by-2 matrices with respect to addition is an Abelian group. (Show this) ■

Example 5.4
By Theorem 4.3, the set $\mathcal{L}$ of all linear mappings $\alpha_{a,b}$, with $a \neq 0$, from $\mathbb{R}$ into $\mathbb{R}$ is a group with respect to composition.■

Next, we look at a group given by a Cayley table. In this case, it is easy to locate the identity and inverses of elements.

Example 5.5
Let $G = \{e, a, b, c\}$ with multiplication as defined by the table below.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

From the table, we observe that

(i) G is closed under this multiplication.
(ii) e is the identity element.
(iii) $e^{-1} = e, b^{-1} = b, c^{-1} = a$, and $a^{-1} = c$.
(iv) the multiplication is commutative.
It can be checked that the multiplication is associative. Thus, $(G, .)$ is an abelian group. ■

Next, we record some simple consequences of the definition of a group in the following theorem.

Theorem 5.1
Let G be a group with respect to a binary operation $*$.

(i) The identity element is unique. That is, if $e, f \in G$ are such that $e * a = f * a = a$ and $a * e = a * f = a$ for all $a \in G$ then $e = f$.
(ii) Every element in G has a unique inverse. That is, if a, b, c are elements in G such that $a * b = a * c = e$ and $b * a = c * a = e$, where e is the identity element of G then $b = c$.

Proof.
(i) Since $a * e = a$ for all $a \in G$ then in particular $f * e = f$. Similarly, since $f * a = a$ for all $a \in G$ then in particular $f * e = e$. Thus, $e = f$.
(ii) With a, b, and c as stated, we have

$$\begin{aligned} b &= b * e \text{ (e is the identity)} \\ &= b * (a * c) \text{ (since a } * \text{ c = e)} \\ &= (b * a) * c \text{ (} * \text{ is associative)} \\ &= e * c \text{ (since b } * \text{ a = e)} \\ &= c \text{ (e is the identity)} \blacksquare \end{aligned}$$

Remark 5.2
By the theorem, it makes sense to speak of *the* identity element of a group, and *the* inverse element. It is customary to use a^{-1} for the inverse of an element a.

Definition 5.2
The **order** of a group is the number of elements in the group. It is denoted by $|G|$. If $|G|$ is finite then the group is called a **finite group.** Otherwise, the group is called **infinite group**.