Abstract Algebra
Chapter 1
Group Theory

Dr. Sanhan M. S. Khasraw

Salahaddin University-Erbil
College of Basic Education
Department of Mathematics
Third Year
Fall 2021-2022

1.1 Groups

Definition 1.1.1: Given a nonempty set S, any function from the Cartesian product $S \times S$ into S is called a **binary operation** on S.

1.1 Groups

Definition 1.1.1: Given a nonempty set S, any function from the Cartesian product $S \times S$ into S is called a **binary operation** on S.

Note:

In practice, we shall generally use the symbol $*$ to represent a binary operation and write $a * b$, instead of $*((a, b))$, for its value at the ordered pair $(a, b) \in S \times S$.

Example 1.1.2: Ordinary subtraction is a binary operation on the set $\mathbb{Z}$ of integers. However, ordinary subtraction is not a binary operation on the set $\mathbb{Z}^+$ of positive integers

Definition 1.1.3: By a **mathematical system** (or **mathematical structure**), we shall mean a nonempty set of elements together with one or more binary operations defined on this set.

Definition 1.1.3: By a **mathematical system** (or **mathematical structure**), we shall mean a nonempty set of elements together with one or more binary operations defined on this set.

A mathematical system consisting of the set S and a single binary operation $*$ will be denoted by the ordered pair $(S, *)$; analogously, a system consisting of the set S and two binary operations $*$ and $\circ$ will be represented by the ordered triple $(S, *, \circ)$.

Example 1.1.4: If $\mathbb{Z}_e$ and $\mathbb{Z}_o$ denote the even and odd integers, respectively, then $(\mathbb{Z}_e, +, \cdot)$ is a mathematical system, while $(\mathbb{Z}_o, +, \cdot)$ does not.

Definition 1.1.5: The operation $*$ defined on the set S is said to be **associative** if

$$a * (b * c) = (a * b) * c,$$

for every triple of elements a, b and c of S.

Example 1.1.6: Ordinary addition and ordinary multiplication are an associative operations on the set $\mathbb{Z}$ of integers.

Example 1.1.6: Ordinary addition and ordinary multiplication are an associative operations on the set $\mathbb{Z}$ of integers.

Example 1.1.7: An operation $*$ defined on $\mathbb{Z}$ by $a * b = a + b + ab$ is an associative.

Definition 1.1.8: A **semigroup** is a pair $(S, *)$ consisting of a nonempty set S together with an associative binary operation $*$ defined on S.

Example 1.1.9: The pairs $(\mathbb{Z}^+, +), (\mathbb{Z}^+, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, +), (\mathbb{Q}, \cdot), (\mathbb{R}, +)$, and $(\mathbb{R}, \cdot)$ form semigroups.

Example 1.1.9: The pairs $(\mathbb{Z}^+, +), (\mathbb{Z}^+, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, +), (\mathbb{Q}, \cdot), (\mathbb{R}, +)$, and $(\mathbb{R}, \cdot)$ form semigroups.

Example 1.1.10: For any set X, each of the systems $(P(X), \cup)$ and $(P(X), \cap)$ is a semigroup, where $P(X)$ is the power set of X, that is,

$$P(X) = \{A | A \subseteq X\}.$$

Definition 1.1.11: The operation $*$ defined on the set S is called **commutative** if

$$a * b = b * a,$$

for every pair of elements $a, b \in S$.

Definition 1.1.11: The operation $*$ defined on the set S is called **commutative** if

$$a * b = b * a,$$

for every pair of elements $a, b \in S$.

Example 1.1.12: Ordinary addition $(+)$ is a commutative operation on $\mathbb{Z}$.

Definition 1.1.13: The system $(S, *)$ is said to have a *(two-sided)* **identity element** for the operation $*$ if there exists an element e in S such that

$$a * e = e * a = a$$

for every $a \in S$.

Example 1.1.14:

1. The semigroup $(\mathbb{Z}, +)$ possesses an identity element, namely, the integer 0.

Example 1.1.14:

1. The semigroup $(\mathbb{Z}, +)$ possesses an identity element, namely, the integer 0.

2. The semigroup $(\mathbb{Z}, \cdot)$ possesses an identity element, namely, the positive integer 1.

3. Both the semigroups $(P(X), \cup)$ and $(P(X), \cap)$ have identities. Here, the empty set ϕ is the identity element for the union operation $(\cup)$, since

$$A \cup \phi = \phi \cup A = A$$

for each set $A \subset X$. The universal set X is the identity element for the operation of intersection $(\cap)$, since

$$A \cap X = X \cap A = A$$

for each set $A \subset X$.

Definition 1.1.15: Let $(S, *)$ be a mathematical system with identity element e. An element $a \in S$ is said to have a *(two-sided)* **inverse** for the operation $*$ if there exists some member a' of S such that

$$a * a' = a' * a = e.$$

An element a' having this property is called an **inverse** of a and is denoted by a^{-1}.

Example 1.1.16: Let $S = \{(a, b) | a \text{ and } b \text{ are nonzero real numbers}\}$ and $*$ the binary operation defined by

$$(a, b) * (c, d) = (ac, bd).$$

Then the system $(S, *)$ forms a commutative semigroup with identity element.

Definition 1.1.17: The pair $(G, *)$ is a **group** if and only if $(G, *)$ is a semigroup with identity in which each element of G has an inverse.

Definition 1.1.18: A **group** G is a non-empty set such that the following four axioms hold.

1. There is a binary operation $* : G \times G \to G$.

Definition 1.1.18: A **group** G is a non-empty set such that the following four axioms hold.

1. There is a binary operation $* : G \times G \to G$.
2. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

Definition 1.1.18: A **group** G is a non-empty set such that the following four axioms hold.

1. There is a binary operation $* : G \times G \to G$.
2. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
3. There exists an identity element e such that for any $a \in G, e * a = a * e = a$.

Definition 1.1.18: A **group** G is a non-empty set such that the following four axioms hold.

1. There is a binary operation $* : G \times G \to G$.
2. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
3. There exists an identity element e such that for any $a \in G, e * a = a * e = a$.
4. For each $a \in G$ there exists an inverse $a' \in G$ such that $a * a' = a' * a = e$.

Example 1.1.19: The pairs
$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q} - \{0\}, \cdot), (\mathbb{R}, +), (\mathbb{R} - \{0\}, \cdot))$ form groups, while the pairs $(P(X), \cup)$ and $(P(X), \cap)$ do not.

Definition 1.1.20: A group $(G, *)$ is called **commutative** (or **abelian**) group if the binary operation $*$ is commutative, that is, $a * b = b * a$ for all $a, b \in G$.

Definition 1.1.20: A group $(G, *)$ is called **commutative** (or **abelian**) group if the binary operation $*$ is commutative, that is, $a * b = b * a$ for all $a, b \in G$.

Example 1.1.21: $(\mathbb{Z}, +)$ is an abelian group.

Example 1.1.22: Let $G = \{(a, b) \mid a, b \in \mathbb{R}, a \neq 0\}$. Define the operation $*$ on G by the formula

$$(a, b) * (c, d) = (ac, bc + d).$$

Show that $(G, *)$ is a noncommutative group.

Theorem 1.1.23: Let $(G, *)$ be a group. Then the following hold.

1. The identity element of $(G, *)$ is unique.

Theorem 1.1.23: Let $(G, *)$ be a group. Then the following hold.

1. The identity element of $(G, *)$ is unique.
2. The inverse of any element of G is unique.

Theorem 1.1.24: Suppose that $(G, *)$ is a group and $g, h, k \in G$. Then

1. $(g^{-1})^{-1} = g$.

Theorem 1.1.24: Suppose that $(G, *)$ is a group and $g, h, k \in G$. Then

1. $(g^{-1})^{-1} = g$.
2. $(g * h)^{-1} = h^{-1} * g^{-1}$.

Theorem 1.1.24: Suppose that $(G, *)$ is a group and $g, h, k \in G$. Then

1. $(g^{-1})^{-1} = g$.
2. $(g * h)^{-1} = h^{-1} * g^{-1}$.
3. The cancellation laws hold in that if $g * h = g * k$ or $h * g = k * g$ then $h = k$.

Theorem 1.1.25: Any noncommutative group has at least six elements.

Theorem 1.1.25: Any noncommutative group has at least six elements.

Definition 1.1.26: In any group $(G, *)$, the **integral powers** of an element $a \in G$ are defined by

$$a^k = a * a * \cdots * a \ (\textbf{k factors}),$$

$$a^0 = e,$$

$$a^{-k} = (a^{-1})^k,$$

where $k \in \mathbb{Z}^+$.

Theorem 1.1.27: Let $(G, *)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$. The powers of a obey the following laws of exponents:

1. $a^n * a^m = a^{n+m} = a^m * a^n$,

Theorem 1.1.27: Let $(G, *)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$. The powers of a obey the following laws of exponents:

1. $a^n * a^m = a^{n+m} = a^m * a^n$,
2. $(a^n)^m = a^{nm} = (a^m)^n$,

Theorem 1.1.27: Let $(G, *)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$. The powers of a obey the following laws of exponents:

1. $a^n * a^m = a^{n+m} = a^m * a^n$,
2. $(a^n)^m = a^{nm} = (a^m)^n$,
3. $a^{-n} = (a^n)^{-1}$,

Theorem 1.1.27: Let $(G, *)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$. The powers of a obey the following laws of exponents:

1. $a^n * a^m = a^{n+m} = a^m * a^n$,
2. $(a^n)^m = a^{nm} = (a^m)^n$,
3. $a^{-n} = (a^n)^{-1}$,
4. $e^n = e$.