Abstract Algebra I
Chapter 1
Group Theory

Dr. Sanhan M. S. Khasraw

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

1.3 Subgroups

Definition 1.3.1:

Let $(G, *)$ be a group and H be a nonempty subset of G. The pair $(H, *)$ is said to be a **subgroup** of $(G, *)$ if $(H, *)$ is itself a group.

1.3 Subgroups

Definition 1.3.1:

Let $(G, *)$ be a group and H be a nonempty subset of G. The pair $(H, *)$ is said to be a **subgroup** of $(G, *)$ if $(H, *)$ is itself a group.

Example 1.3.2:

If $\mathbb{Z}_e$ and $\mathbb{Z}_o$ denote the sets of even and odd integers, respectively, then $(\mathbb{Z}_e, +)$ is a subgroup of the group $(\mathbb{Z}, +)$, while $(\mathbb{Z}_o, +)$ is not.

Example 1.3.3:

Consider $(\mathbb{Z}_6, +_6)$, the group of integers modulo 6. If $H = \{0, 2, 4\}$, then $(H, +_6)$ is a subgroup of $(\mathbb{Z}_6, +_6)$.

Example 1.3.3:
Consider $(\mathbb{Z}_6, +_6)$, the group of integers modulo 6. If $H = \{0, 2, 4\}$, then $(H, +_6)$ is a subgroup of $(\mathbb{Z}_6, +_6)$.

Example 1.3.4:
Every group $(G, *)$ has at least two subgroups, which are $(\{e\}, *)$ and the group $(G, *)$ itself, called the *trivial* subgroups of $(G, *)$, all subgroups between these two extremes are called *nontrivial* subgroups.
Any subgroup different from $(G, *)$ is termed *proper*.

Theorem 1.3.5:
Let $(G, *)$ be a group and $\phi \neq H \subseteq G$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if $a, b \in H$ implies $a * b^{-1} \in H$.

Theorem 1.3.5:
Let $(G, *)$ be a group and $\phi \neq H \subseteq G$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if $a, b \in H$ implies $a * b^{-1} \in H$.

Example 1.3.6:
The Klien's 4-group $(V, \cdot)$ has the following subgroups:

$$H_1 = \{e\}$$
$$H_2 = V$$
$$H_3 = \{e, a\}$$
$$H_4 = \{e, b\}$$
$$H_5 = \{e, c\}.$$

Example 1.3.7:
Find all subgroups of the group $(D_8, *)$.

Example 1.3.7:
Find all subgroups of the group $(D_8, *)$.

Example:
Find all subgroups of the group $(Q_8, *)$.

Example 1.3.7:
Find all subgroups of the group $(D_8, *)$.

Example:
Find all subgroups of the group $(Q_8, *)$.

Example:
Find all subgroups of the group $(S_3, *)$.

Definition 1.3.8:

The **center** of a group $(G, *)$, denoted by $CentG (or\ Z(G))$, is the set $CentG = \{c \in G \mid c * x = x * c, \forall x \in G\}$.

Definition 1.3.8:

The **center** of a group $(G, *)$, denoted by $CentG (or\ Z(G))$, is the set $CentG = \{c \in G \mid c * x = x * c, \forall x \in G\}$.

Example 1.3.9:

1. Consider the group $(S_3, \circ)$. Then $CentS_3 = \{()\}$.
2. Consider the klein 4-group $(V, \cdot)$. Then $CentV = \{e, a, b, c\} = V$.

Definition 1.3.8:
The **center** of a group $(G, *)$, denoted by $CentG (or\ Z(G))$, is the set $CentG = \{c \in G \mid c * x = x * c, \forall x \in G\}$.

Example 1.3.9:

1. Consider the group $(S_3, \circ)$. Then $CentS_3 = \{()\}$.
2. Consider the klein 4-group $(V, \cdot)$. Then $CentV = \{e, a, b, c\} = V$.

Example 1.3.10:
The group $(G, *)$ is commutative if and only if $CentG = G$.

Theorem 1.3.11:

The pair $(CentG, *)$ is a subgroup of each group $(G, *)$.

Theorem 1.3.11:
The pair $(CentG, *)$ is a subgroup of each group $(G, *)$.

Theorem 1.3.12:
If $(H_i, *)$ is an arbitrary indexed collection of subgroups of the group $(G, *)$, then $(\cap H_i, *)$ is also a subgroup.

Theorem 1.3.11:
The pair $(CentG, *)$ is a subgroup of each group $(G, *)$.

Theorem 1.3.12:
If $(H_i, *)$ is an arbitrary indexed collection of subgroups of the group $(G, *)$, then $(\cap H_i, *)$ is also a subgroup.

Remark 1.3.13:
The union of two subgroups $(H_1, *)$ and $(H_2, *)$ of the group $(G, *)$ need not be a subgroup of $(G, *)$, for example, $(\{0, 6\}, +_{12})$ and $(\{0, 4, 8\}, +_{12})$ are two subgroups of the group $(Z_{12}, +_{12})$, then their union is $(\{0, 4, 6, 8\}, +_{12})$ fails to be a subgroup of $(Z_{12}, +_{12})$.

Theorem 1.3.14:

Let $(H_1, *)$ and $(H_2, *)$ be subgroups of the group $(G, *)$. Then $(H_1 \cup H_2, *)$ is also a subgroup if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Theorem 1.3.14:
Let $(H_1, *)$ and $(H_2, *)$ be subgroups of the group $(G, *)$. Then $(H_1 \cup H_2, *)$ is also a subgroup if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Theorem 1.3.15:
Let $(H_i, *)$ be an indexed collection of subgroups of the group $(G, *)$. Suppose the family of subsets $\{H_i\}$ has the property that for any two of its members H_i and H_j there exists a set H_k(depending on i and j) in $\{H_i\}$ such that $H_i \subseteq H_k$ and $H_j \subseteq H_k$. Then $(\cup H_i, *)$ is also a subgroup of $(G, *)$.

Definition 1.3.16:

The group $(G, *)$ is called **cyclic** if every element of G can be expressed as the power of one element of G, that is,

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

a is called the **generator** of G.

Definition 1.3.16:

The group $(G, *)$ is called **cyclic** if every element of G can be expressed as the power of one element of G, that is,

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

a is called the **generator** of G.

Example 1.3.17:

The following are cyclic groups.

1. $(\mathbb{Z}, +)$ is a cyclic group generated by 1 and -1. That is, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2. If $G = \{1, -1, i, -i\}$, where $i^2 = -1$, then $(G, .)$ is a cyclic group generated by i and $-i$, $G = \langle i \rangle = \langle -i \rangle$.
3. $(\mathbb{Z}_5, +_5)$ is a cyclic group, $\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$.

Remark 1.3.18:

In $(\mathbb{Z}_n, +_n)$, if n is prime, then every elements is a generator except 0.

Remark 1.3.18:
In $(\mathbb{Z}_n, +_n)$, if n is prime, then every elements is a generator except 0.

Example 1.3.19:
The following groups are not cyclic.

1. $(\mathbb{R}, +)$ is not a cyclic group.
2. $(S_3, \circ)$ is not a cyclic group.

Definition 1.3.20:

By a **finite group**, we mean any group whose underlying set of elements is a finite set.

Definition 1.3.20:

By a **finite group**, we mean any group whose underlying set of elements is a finite set.

Definition 1.3.21:

The **order** of a finite group $(G, *)$ is defined to be the number of its elements, denoted by $o(G)(or\ |G|)$.

Definition 1.3.22:

Let $(G, *)$ be a group. Then the **order of an element** a in G is the least positive integer n, provided it exists, such that $a^n = e$, where e is the identity element of G, and denoted by $o(a) = n$.

Definition 1.3.22:

Let $(G, *)$ be a group. Then the **order of an element** a in G is the least positive integer n, provided it exists, such that $a^n = e$, where e is the identity element of G, and denoted by $o(a) = n$.

Example 1.3.23:

Consider the group $(\mathbb{Z}_4, +_4)$. Then

$$o(0) = 1,\ o(1) = 4,\ o(2) = 2, \text{ while } o(3) = 4.$$

Theorem 1.3.24:

Every subgroup of a cyclic group is cyclic.

Theorem 1.3.24:
Every subgroup of a cyclic group is cyclic.

Theorem 1.3.25:
Every cyclic group is abelian.

Theorem 1.3.24:
Every subgroup of a cyclic group is cyclic.

Theorem 1.3.25:
Every cyclic group is abelian.

Remark 1.3.26:
The converse of Theorem 1.3.25 is not true in general, for example, $(\mathbb{R}, +)$ is an abelian group but it is not cyclic (see Example 1.3.19(1)).

Definition 1.3.27:

Let $(G, *)$ be a group and H, K be non-empty subsets G. The **product** of H and K, in that order, is the set

$$H * K = \{h * k \mid h \in H, k \in K\}.$$

Definition 1.3.27:
Let $(G, *)$ be a group and H, K be non-empty subsets G. The **product** of H and K, in that order, is the set

$$H * K = \{h * k \mid h \in H, k \in K\}.$$

Example 1.3.28:
Consider the group $(D_8, *)$. Let $H = \{R_{360}, D_1\}$ and $K = \{R_{360}, V\}$. Then $(H, *)$ and $(K, *)$ are subgroups of $(D_8, *)$.

$$H * K = \{R_{360}, V, D_1, R_{270}\}.$$

Theorem 1.3.29:
If $(H, *)$ and $(K, *)$ are subgroups of the group $(G, *)$ such that $H * K = K * H$, then the pair $(H * K, *)$ is also a subgroup.

Subgroups

Theorem 1.3.29:
If $(H, *)$ and $(K, *)$ are subgroups of the group $(G, *)$ such that $H * K = K * H$, then the pair $(H * K, *)$ is also a subgroup.

Corollary 1.3.30:
If $(H, *)$ and $(K, *)$ are subgroups of the commutative group $(G, *)$, then $(H * K, *)$ is again a subgroup.

Theorem 1.3.29:
If $(H, *)$ and $(K, *)$ are subgroups of the group $(G, *)$ such that $H * K = K * H$, then the pair $(H * K, *)$ is also a subgroup.

Corollary 1.3.30:
If $(H, *)$ and $(K, *)$ are subgroups of the commutative group $(G, *)$, then $(H * K, *)$ is again a subgroup.

Example 1.3.31:
Consider the group $(\mathbb{Z}_{12}, +_{12})$. Let $H = \{0, 6\}$ and $K = \{0, 4, 8\}$. Then

$$H +_{12} K = \{0, 6\} +_{12} \{0, 4, 8\} = \{0, 4, 8, 6, 10, 2\}.$$

Thus, $(H +_{12} K, +_{12})$ is a subgroup of $(\mathbb{Z}_{12}, +_{12})$.

1.4 Normal Subgroups and Quotient Groups

1.4 Normal Subgroups and Quotient Groups

Definition 1.4.1:
Let $(H, *)$ be a subgroup of the group $(G, *)$ and let $a \in G$. The set $a * H = \{a * h | h \in H\}$ is called a **left coset** of H in G. The element a is **representative** of $a * H$.

$H * a = \{h * a | h \in H\}$ is called a **right coset** of H in G.

1.4 Normal Subgroups and Quotient Groups

Definition 1.4.1:
Let $(H, *)$ be a subgroup of the group $(G, *)$ and let $a \in G$. The set $a * H = \{a * h | h \in H\}$ is called a **left coset** of H in G. The element a is **representative** of $a * H$.

$H * a = \{h * a | h \in H\}$ is called a **right coset** of H in G.

Example 1.4.2:
If e is the identity element of $(G, *)$, then
$e * H = \{e * h \mid h \in H\} = \{h \mid h \in H\} = H$, so that H itself is a left coset of H.

Example 1.4.2:

Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 3\}$. Then the left cosets of H in $\mathbb{Z}_6$ are

$0 +_6 H = H$,

$1 +_6 H = \{1, 4\}$,

$2 +_6 H = \{2, 5\}$,

$3 +_6 H = \{3, 0\} = H$,

$4 +_6 H = \{4, 1\} = 1 +_6 H$, and

$5 +_6 H = \{5, 2\} = 2 +_6 H$.

There are only three distinct cosets $H, \{1, 4\}$ and $\{2, 5\}$.

Theorem 1.4.3:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Theorem 1.4.3:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Theorem 1.4.4:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = b * H$ if and only if $a^{-1} * b \in H$.

Theorem 1.4.3:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Theorem 1.4.4:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = b * H$ if and only if $a^{-1} * b \in H$.

Remark 1.4.5:
If $(H, *)$ is a subgroup of the group $(G, *)$, then $H * a = H * b$ if and only if $a * b^{-1} \in H$.

Theorem 1.4.6:

If $(H, *)$ is a subgroup of the group $(G, *)$, then either the cosets $a * H$ and $b * H$ are disjoint or else $a * H = b * H$.

Theorem 1.4.6:
If $(H, *)$ is a subgroup of the group $(G, *)$, then either the cosets $a * H$ and $b * H$ are disjoint or else $a * H = b * H$.

Theorem 1.4.7:
If $(H, *)$ is a subgroup of the group $(G, *)$, then the left(right) cosets of H in G form a partition of the set G.

Theorem 1.4.6:
If $(H, *)$ is a subgroup of the group $(G, *)$, then either the cosets $a * H$ and $b * H$ are disjoint or else $a * H = b * H$.

Theorem 1.4.7:
If $(H, *)$ is a subgroup of the group $(G, *)$, then the left(right) cosets of H in G form a partition of the set G.

Example 1.4.8:
Consider the group $(\mathbb{Z}_{12}, +_{12})$. Let $H = \{0, 4, 8\}$. Then $(H, +_{12})$ is a subgroup of $(\mathbb{Z}_{12}, +_{12})$. The left cosets of H in $\mathbb{Z}_{12}$ are

Theorem (Lagrange) 1.4.9:
The order and index of any subgroup of a finite group divides the order of the group.

Theorem (Lagrange) 1.4.9:
The order and index of any subgroup of a finite group divides the order of the group.

Corollary 1.4.10:
If $(G, *)$ is a group of order n, then the order of any element $a \in G$ is a factor of n, in addition $a^n = e$.

Theorem (Lagrange) 1.4.9:
The order and index of any subgroup of a finite group divides the order of the group.

Corollary 1.4.10:
If $(G, *)$ is a group of order n, then the order of any element $a \in G$ is a factor of n, in addition $a^n = e$.

Theorem 1.4.11:
If $(G, *)$ is a finite group of composite order, then $(G, *)$ has nontrivial subgroups.

Corollary 1.4.12:
Every group $(G, *)$ of prime order is cyclic.

Corollary 1.4.12:
Every group $(G, *)$ of prime order is cyclic.

Theorem 1.4.13:
Any noncommutative group has at least six elements.

Normal Subgroups and Quotient Groups

Definition 1.4.14:

A subgroup $(H, *)$ is **normal** in the group $(G, *)$ if and only if $a * H = H * a$ for every $a \in G$.

Normal Subgroups and Quotient Groups

Definition 1.4.14:
A subgroup $(H, *)$ is **normal** in the group $(G, *)$ if and only if $a * H = H * a$ for every $a \in G$.

Theorem 1.4.15:
The subgroup $(H, *)$ is a normal subgroup of the group $(G, *)$ if and only if for each element $a \in G$,

$$a * H * a^{-1} \subseteq H.$$

Definition 1.4.16:
If $(H, *)$ is a normal subgroup of the group $(G, *)$, then we shall denote the collection of distinct cosets of H in G by G/H:

$$G/H = \{a * H \mid a \in G\}.$$

Definition 1.4.16:
If $(H, *)$ is a normal subgroup of the group $(G, *)$, then we shall denote the collection of distinct cosets of H in G by G/H:

$$G/H = \{a * H \mid a \in G\}.$$

A rule of composition $\otimes$ may be defined on G/H by the formula

$$(a * H) \otimes (b * H) = (a * b) * H.$$

Quotient Groups

Definition 1.4.16:
If $(H, *)$ is a normal subgroup of the group $(G, *)$, then we shall denote the collection of distinct cosets of H in G by G/H:

$$G/H = \{a * H \mid a \in G\}.$$

A rule of composition $\otimes$ may be defined on G/H by the formula

$$(a * H) \otimes (b * H) = (a * b) * H.$$

Theorem 1.4.17:
If $(H, *)$ is a normal subgroup of the group $(G, *)$, then the system $(G/H, \otimes)$ forms a group, known as the **quotient group of G by H**.

Definition 1.5.1:
Let $(G, *)$ and $(G', \circ)$ be two groups and f a function from G into G', $f : G \to G'$. Then f is said to be a **homomorphism** (or operation preserving function) from $(G, *)$ into $(G', \circ)$ if and only if

$$f(a * b) = f(a) \circ f(b)$$

for every pair of clements $a, b \in G$.

Homomorphisms

Definition 1.5.1:
Let $(G, *)$ and $(G', \circ)$ be two groups and f a function from G into G', $f : G \to G'$. Then f is said to be a **homomorphism** (or operation preserving function) from $(G, *)$ into $(G', \circ)$ if and only if

$$f(a * b) = f(a) \circ f(b)$$

for every pair of clements $a, b \in G$.

Example 1.5.2:
For an arbitrary group $(G, *)$, define the function $f : G \to G$ by $f(a) = a$, the identity map on G, for every $\in G$. Then f is a homomorphism from $(G, *)$ into itself.

Example 1.5.3:

Suppose that $(G, *)$ and $(G', \circ)$ are two groups with identity elements e and e', respectively. The function $f : G \to G'$ given by $f(a) = e'$ for each $a \in G$ is a homomorphism.

Example 1.5.3:
Suppose that $(G, *)$ and $(G', \circ)$ are two groups with identity elements e and e', respectively. The function $f : G \to G'$ given by $f(a) = e'$ for each $a \in G$ is a homomorphism.

Example 1.5.4:
Consider the two groups $(\mathbb{R}, +)$ and $(\mathbb{R} - \{0\}, \cdot)$. For $a \in \mathbb{R}$, define the function f by $f(a) = 2^a$. Then f is a homomorphism.

Example 1.5.3:
Suppose that $(G, *)$ and $(G', \circ)$ are two groups with identity elements e and e', respectively. The function $f : G \to G'$ given by $f(a) = e'$ for each $a \in G$ is a homomorphism.

Example 1.5.4:
Consider the two groups $(\mathbb{R}, +)$ and $(\mathbb{R} - \{0\}, \cdot)$. For $a \in \mathbb{R}$, define the function f by $f(a) = 2^a$. Then f is a homomorphism.

Example 1.5.5:
Let $(\mathbb{Z}, +)$ be the group of integers under addition and $(\mathbb{Z}_n, +_n)$ be the group of integers modulo n. Define $f : \mathbb{Z} \to \mathbb{Z}_n$ by $f(a) = [a]$ is a homomorphism.

Theorem 1.5.6:

If f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$, then

1. $f(e) = e'$, where e is the identity element of $(G, *)$ and e' is the identity element of $(G', \circ)$.
2. $f(a^{-1}) = f(a)^{-1}$ for each $a \in G$.

Theorem 1.5.6:

If f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$, then

1. $f(e) = e'$, where e is the identity element of $(G, *)$ and e' is the identity element of $(G', \circ)$.
2. $f(a^{-1}) = f(a)^{-1}$ for each $a \in G$.

Definition 1.5.7:

Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$ and let e' be the identity element of $(G', \circ)$. The **kernel** of f, denoted by $ker(f)$, is the set

$$ker(f) = \{a \in G \mid f(a) = e'\}.$$

Theorem 1.5.8:

Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$. Then f is one-to-one if and only if $ker(f) = \{e\}$.

Homomorphisms

Theorem 1.5.8:

Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$. Then f is one-to-one if and only if $ker(f) = \{e\}$.

Theorem 1.5.9:

If f is a homomorphism from tho group $(G, *)$ into the group $(G', \circ)$, then the pair $(ker(f), *)$ is a normal subgroup of $(G, *)$.

Homomorphisms

Theorem 1.5.8:
Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$. Then f is one-to-one if and only if $ker(f) = \{e\}$.

Theorem 1.5.9:
If f is a homomorphism from tho group $(G, *)$ into the group $(G', \circ)$, then the pair $(ker(f), *)$ is a normal subgroup of $(G, *)$.

Example 1.5.10:
Consider the two groups $(\mathbb{Z}, +)$ and $(\mathbb{R} - \{0\}, \cdot)$. The mapping $f : \mathbb{Z} \to \mathbb{R} - \{0\}$ defined by

$$f(n) = \begin{cases} 1 & if \quad n \in \mathbb{Z}_e \\ -1 & if \quad n \in \mathbb{Z}_o \end{cases}$$

is a homomorphism, and $ker(f) = \mathbb{Z}_e$.