Algebraic Structures

A Lecture on Group Theory

John Rick Dolor Manzanares

Baguio City, Philippines

December 3, 2023

For Instructors

Math Communication

Inquiry-Based Learning (IBL)

Definition

Inquiry-based learning is a learning process that engages students by making real-world connections through exploration and high-level questioning.

Instructors can run inquiry activities in the form of:

- Case Studies
- Group Projects
- Research Projects
- Field Work
- Unique Exercises (tailored to the students)

Types of IBL

- Confirmation Inquiry
  1. Give students the question and the answer.
  2. Students investigate the method of reaching the answer.
- Structured Inquiry
  1. Give students an open question and an investigation method.
  2. Students use the method to craft an evidence-backed conclusion.
- Guided Inquiry
  1. Give students an open question.
  2. Typically in groups, students design an investigation methods to reach a conclusion.
- Open Inquiry
  1. Give students time and support.
  2. Students pose questions that they investigate through their own methods, and present the results to discuss and expand.

1. Reinforces Curriculum Content
2. Warms Up the Brain
3. Promotes a Deeper Understanding of Content
4. Helps Make Learning Rewarding
5. Builds Initiative and Self-Direction
6. Offers Differenttated Instruction

1. Demonstrate How to Participate
2. Surprise Students
3. Use Inquiry When Traditional Methods Won’t Work
4. Understand When Inquiry Won’t Work
5. Don’t Wait for the Perfect question
6. Run a Check-In Afterwards

Pillars of IBL

1. Students deeply engaged in rich mathematical sense making.
2. Regular opportunities for students to collaborate with peers and instructors.
3. Instructor inquiry into student thinking.
4. Instructor focus on equity.

Pillars of Grading for Equity

1. Clearly defined standards
2. Helpful feedback
3. Marks indicate progress
4. Reattempts without penalty

1. Use inclusive teaching practices and frameworks that encourage more students to be engaged more often.
2. Add an equity statement to signify the importance of inclusion and equity. This helps create a positive learning environment in your class. Imaging a student of different nationality, sitting in a room full of people not like her.
3. Use the students' preferred pronouns.

Reminders for Small Group Discussions and Think-Pair-Share

1. Visit the groups the same number of times.
2. Raise softer voices and redirect louder voices.
   - Rather than asking for volunteers, let the students talk among the group first.
3. Avoid the question "Are there any questions...?" as it focuses more on the louder voices.
4. "What did your group discuss?" is more inviting than questions putting the students in a higher stakes scenario. For example, "What's the right answer?" where it puts a student to a right or wrong scenario rather than just sharing a though.

Introduction

Notations

Notations

$\emptyset$	Empty Set
$\mathbb{Z}$	Set of Integers
$\mathbb{Q}$	Set of Rational Numbers
$\mathbb{R}$	Set of Real Numbers
$\mathbb{C}$	Set of Complex Numbers
$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$	Positive Elements of $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$
$\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	Nonzero Elements of $\mathbb{Z}, \mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Introduction

History of Group Theory

- The definition of a group is credited to Evariste Galois in his study of *symmetries* among the roots of polynomials.
- Let $n \geq 3$ be an integer and P_n be a regular n-sided polygon. We denote $V_n := \{v_1, \ldots, v_n\}$ as the set of vertices of P_n contained in the Euclidean plane $\mathbb{R}^2$.

- The definition of a group is credited to Evariste Galois in his study of *symmetries* among the roots of polynomials.
- Let $n \geq 3$ be an integer and P_n be a regular n-sided polygon. We denote $V_n := \{v_1, \dots, v_n\}$ as the set of vertices of P_n contained in the Euclidean plane $\mathbb{R}^2$.

Definition

A **symmetry** of a regular n-gon is a bijection $\sigma : V_n \to V_n$ such that if the unordered pair $\{v_i, v_j\}$ consists of the end points of an edge of the n-gon, then $\{\sigma(v_i), \sigma(v_j)\}$ also contains the endpoints of an edge.

For simplicity, we let V_n be the set

$$\{1, 2, \ldots, n\}.$$

Example and Non-Example

Consider a regular quadrilateral with edges $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, and $\{1, 4\}$. Let f be the function from V_4 into V_4 where

$$1 \to 3, 2 \to 1, 3 \to 2, \text{ and } 4 \to 4.$$

Also, let g be the function from V_4 into V_4 where

$$1 \to 1, 2 \to 3, 3 \to 2, \text{ and } 4 \to 4.$$

Consider a regular quadrilateral with edges $\{1,2\}$, $\{2,3\}$, $\{3,4\}$, and $\{1,4\}$. Let f be the function from V_4 into V_4 where

$$1 \to 3, 2 \to 1, 3 \to 2, \text{ and } 4 \to 4.$$

Also, let g be the function from V_4 into V_4 where

$$1 \to 1, 2 \to 3, 3 \to 2, \text{ and } 4 \to 4.$$

Observe that f is not a symmetry, while g is a symmetry.

There are six symmetries of a triangle. These are the bijections from V_3 onto V_3 given by:

ρ_0: $1 \to 1, 2 \to 2,$ and $3 \to 3.$

ρ_1: $1 \to 2, 2 \to 3,$ and $3 \to 1.$

ρ_2: $1 \to 3, 2 \to 1,$ and $3 \to 2.$

μ_1: $1 \to 1, 2 \to 3,$ and $3 \to 2.$

μ_2: $1 \to 3, 2 \to 2,$ and $3 \to 1.$

μ_3: $1 \to 2, 2 \to 1,$ and $3 \to 3.$

Property

We denote the set of symmetries of the regular n-gon as D_{2n} and call it the set of *dihedral* symmetries.

We denote the set of symmetries of the regular n-gon as D_{2n} and call it the set of *dihedral* symmetries.

Theorem

The cardinality of D_{2n} is $2n$. In symbols, $|D_{2n}| = 2n$.

We denote the set of symmetries of the regular n-gon as D_{2n} and call it the set of *dihedral* symmetries.

Theorem

The cardinality of D_{2n} is $2n$. In symbols, $|D_{2n}| = 2n$.

Proof.

Consider any element v_1 from V_n. For a symmetry σ, suppose that $\{v_1, v_2\}$ is an edge. A symmetry can map n elements to v_1. However, σ must map v_2 to a vertex adjacent to $\sigma(v_1)$. Note that there are only two possible ways. Once $\sigma(v_1)$ and $\sigma(v_2)$ are known, all remaining $\sigma(v_i)$ for $3 \leq i \leq n$ are determined. $\square$

The elements of D_{2n} are composed of

- n rotations, and
- n reflection symmetries.

We can compose two functions from D_{2n}. Observe the compositions of the elements of D_{2n} by looking at the table below.

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

Exercise

Find the symmetries of a square. Construct the operation table between elements of D_4 with function composition as the operation.

Introduction

Clock Arithmetic

- Consider the set $\mathbb{Z}_{12} := \{0, 1, \ldots, 11\}$ of integers between zero (0) and eleven (11). For any $a, b \in \mathbb{Z}_{12}$, the operation **addition modulo 12** $+_{12}$ is defined as

$$a +_{12} b = c \quad \text{or} \quad a + b = c \pmod{12}$$

  where c is the remainder when $a + b$ is divided by 12.
- This resembles finding the time after n hours, where 0 represent 12:00 AM or PM.

Exercise

Construct the operation table between elements of $\mathbb{Z}_{12}$ with addition modulo 12 as the operation.

Groups

Binary Operation

Definition

A **binary operation** on a set S is a function that assigns each ordered pair of elements of S to an element of S.

Definition

A **binary operation** on a set S is a function that assigns each ordered pair of elements of S to an element of S.

Definition (Restated)

A **binary operation** or **law of composition** on a set S is a function from $S \times S$ into S.

Definition

A **binary operation** on a set S is a function that assigns each ordered pair of elements of S to an element of S.

Definition (Restated)

A **binary operation** or **law of composition** on a set S is a function from $S \times S$ into S.

The condition which maps an ordered pair from S to an element in S is called the **closure property**. In this case, we say that S is **closed under the binary operation**.

Remarks

Let $\star$ be a binary operation on S. We denote the image $\star((a, b))$ of each ordered pair $(a, b) \in S \times S$ by $a \star b$.

1. Addition of integers is a binary operation.
2. Subtraction of integers is ________ binary operation.
3. Subtraction of positive integers is ________ binary operation.
4. Multiplication of integers is ________ binary operations.
5. The integers from the previous examples can be replaced by ________ numbers or ________ numbers.
6. Division of integers is ________ binary operation.

1. Addition of integers is a binary operation.
2. Subtraction of integers is a binary operation.
3. Subtraction of positive integers is not a binary operation.
4. Multiplication of integers are binary operations.
5. The integers from the previous examples can be replaced by rational numbers or real numbers.
6. Division of integers is not a binary operation.

1. The operations addition modulo n and multiplication modulo n on
$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$
are binary operations.

1. The operations addition modulo n and multiplication modulo n on
$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$
are binary operations.
2. Let $M(\mathbb{R})$ be the set of all matrices with real entries. The usual matrix addition is not a binary operation on $M(\mathbb{R})$. The set $M_{m\times n}(\mathbb{Q})$, containing all $m \times n$ matrices with rational entries, is closed under the usual matrix addition.

Other Examples of Binary Operations

1. The operations addition modulo n and multiplication modulo n on
$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$
are binary operations.
2. Let $M(\mathbb{R})$ be the set of all matrices with real entries. The usual matrix addition is not a binary operation on $M(\mathbb{R})$. The set $M_{m\times n}(\mathbb{Q})$, containing all $m \times n$ matrices with rational entries, is closed under the usual matrix addition.
3. We define an operation $*$ on $\mathbb{Z}^+$ by $a * b = \min\{a, b\}$. The set $\mathbb{Z}^+$ is closed under $*$. (This operation is programmed into modern GPS systems.)

1. The operations addition modulo n and multiplication modulo n on
$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$$
are binary operations.
2. Let $M(\mathbb{R})$ be the set of all matrices with real entries. The usual matrix addition is not a binary operation on $M(\mathbb{R})$. The set $M_{m\times n}(\mathbb{Q})$, containing all $m \times n$ matrices with rational entries, is closed under the usual matrix addition.
3. We define an operation $*$ on $\mathbb{Z}^+$ by $a * b = \min\{a, b\}$. The set $\mathbb{Z}^+$ is closed under $*$. (This operation is programmed into modern GPS systems.)
4. We also define $*'$ as an operation on $\mathbb{Z}^+$ such that $a *' b = a$. The set $\mathbb{Z}^+$ is also closed under $*'$.

Definition

Let $*$ be a binary operation on S and H be a subset of S. The binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H.

Definition

Let $*$ be a binary operation on S and H be a subset of S. The binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H.

Definition (Restated)

Let $*$ be a binary operation on S. We say that $*$ is an **induced operation** on $H \subset S$ if H is closed under $*$.

1. The set $\mathbb{Z}$ is __________ under ordinary subtraction $-$ but $\mathbb{Z}^+ \subset \mathbb{Z}$ is __________ under $-$.

1. The set $\mathbb{Z}$ is __________ under ordinary subtraction $-$ but $\mathbb{Z}^+ \subset \mathbb{Z}$ is __________ under $-$.
2. The set $3\mathbb{Z}$ containing integer multiples of 3 under the induced operation on $(\mathbb{Z}, +)$ is __________ induced operation on $3\mathbb{Z}$.

1. The set $\mathbb{Z}$ is closed under ordinary subtraction $-$ but $\mathbb{Z}^+ \subset \mathbb{Z}$ is not closed under $-$.

Examples

1. The set $\mathbb{Z}$ is closed under ordinary subtraction $-$ but $\mathbb{Z}^+ \subset \mathbb{Z}$ is not closed under $-$.
2. The set $3\mathbb{Z}$ containing integer multiples of 3 under the induced operation on $(\mathbb{Z}, +)$ is an induced operation on $3\mathbb{Z}$.

1. The set $\mathbb{Z}$ is closed under ordinary subtraction $-$ but $\mathbb{Z}^+ \subset \mathbb{Z}$ is not closed under $-$.
2. The set $3\mathbb{Z}$ containing integer multiples of 3 under the induced operation on $(\mathbb{Z}, +)$ is an induced operation on $3\mathbb{Z}$.

Exercise

Let $+$ and $\cdot$ denote addition and multiplication respectively on $\mathbb{Z}$. Define the set

$$H = \{n^2 : n \in \mathbb{Z}^+\}.$$

Prove that H is closed under $\cdot$ but not closed under $+$.

Definition

A binary operation $*$ on a set S is **commutative** if

$$a * b = b * a$$

for all a and b in S.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are __________ commutative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a *' b = a$. The binary operation $*'$ is __________ commutative.
3. Let $+$ be a binary operation defined on $\mathbb{R} \times \mathbb{R}$ such that

$$(a, b) + (c, d) = (a + c, b + d).$$

   Show that $+$ is commutative.
4. Let $*$ be a binary operation defined on $\mathbb{Z}$ such that

$$a * b = 2ab + 3.$$

   Is $*$ commutative?

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are commutative binary operations.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are commutative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a *' b = a$. The binary operation $*'$ is not commutative.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are commutative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a *' b = a$. The binary operation $*'$ is not commutative.
3. Let $+$ be a binary operation defined on $\mathbb{R} \times \mathbb{R}$ such that

$$(a, b) + (c, d) = (a + c, b + d).$$

Commutativity of $+$ follows from the commutativity of $+$ in $\mathbb{R}$.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are commutative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a *' b = a$. The binary operation $*'$ is not commutative.
3. Let $+$ be a binary operation defined on $\mathbb{R} \times \mathbb{R}$ such that

$$(a, b) + (c, d) = (a + c, b + d).$$

   Commutativity of $+$ follows from the commutativity of $+$ in $\mathbb{R}$.
4. Let $*$ be a binary operation defined on $\mathbb{Z}$ such that

$$a * b = 2ab + 3.$$

   The operation $*$ is commutative.

Definition

A binary operation on a set S is **associative** if

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

for all a, b, and c in S.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are __________ binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a * b = \min\{a, b\}$. The binary operation $*$ is __________.
3. Let F be the set of all real-valued functions with domain $\mathbb{R}$. The operations addition, subtraction, multiplication, and composition for functions are __________ binary operations.
4. Let $*$ be the binary operation on $\mathbb{R}$ where $a * b = ab + a + b$. Is $*$ associative?

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are associative binary operations.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are associative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a*b = \min\{a, b\}$. The binary operation $*$ is associative.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are associative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a * b = \min\{a, b\}$. The binary operation $*$ is associative.
3. Let F be the set of all real-valued functions with domain $\mathbb{R}$. The operations addition, multiplication, and composition for functions are associative binary operations.

1. The operations addition and multiplication on the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{R}^+$, and $\mathbb{R}$ are associative binary operations.
2. Consider the binary operation $*'$ on $\mathbb{Z}^+$ where $a*b = \min\{a, b\}$. The binary operation $*$ is associative.
3. Let F be the set of all real-valued functions with domain $\mathbb{R}$. The operations addition, multiplication, and composition for functions are associative binary operations.
4. Let $*$ be the binary operation on $\mathbb{R}$ where $a * b = ab + a + b$. Is $*$ associative?

Identity Element for a Binary Operation

Definition

Let $*$ be a binary operation on a set S. An element $e \in S$ is called an **identity element** for $*$ if

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

for all $a \in S$.

1. The element __________ is an identity element for $\times$ while the element __________ is an identity element with respect to $+$.
2. The set Z^* has __________ with respect to $+$.
3. The set $M_{m\times n}(\mathbb{R})$ under the usual matrix addition has __________.
4. The operation $*'$ on $\mathbb{Z}^+$ where $a *' b = a$ has __________.

1. The element $1 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element for $\times$ while the element $0 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element with respect to $+$.

1. The element $1 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element for $\times$ while the element $0 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element with respect to $+$.
2. However, the set Z^* has no identity element with respect to $+$.

1. The element $1 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element for $\times$ while the element $0 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element with respect to $+$.
2. However, the set Z^* has no identity element with respect to $+$.
3. The set $M_{m\times n}(\mathbb{R})$ under the usual matrix addition has an identity element given by **zero matrix** defined as a matrix whose entries are all zero.

1. The element $1 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element for $\times$ while the element $0 \in \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is an identity element with respect to $+$.
2. However, the set Z^* has no identity element with respect to $+$.
3. The set $M_{m\times n}(\mathbb{R})$ under the usual matrix addition has an identity element given by **zero matrix** defined as a matrix whose entries are all zero.
4. The operation $*'$ on $\mathbb{Z}^+$ where $a*'b = a$ has no identity element.

Theorem

A set with binary operation $*$ has at most one identity element.

Theorem

A set with binary operation $*$ has at most one identity element.

Proof.

Let S be a set closed under $*$. If there is no identity element for $*$, then the conclusion holds. Suppose that e_1 is an identity element for $*$. Furthermore, we assume that e_2 is another identity element for $*$. By definition, e_1 and e_2 must be in S. Also, for all $a \in S$,

$$a * e_1 = e_1 * a = a$$

and

$$e_2 * a = a * e_2 = a.$$

Thus, $e_1 = e_2 * e_1 = e_1 * e_2 = e_2$. $\square$

Let A be a set which is called an **alphabet**. We define

$$A^n = \{a_1 a_2 \dots a_n : a_i \in A\}$$

to be the set of all sequences (or strings) of n elements of A. Elements of A^n are called **words** of length n over A. The empty sequence, denoted by Λ, is a word of length 0. Moreover, we denote the set of all words over A as

$$FM(A) = \bigcup_{n=0}^{\infty} A^n$$

where $A^0 = \{\Lambda\}$.

We define the operation $*$ on $FM(A)$, called **string concatenation**, by

$$a_1 a_2 \dots a_n * b_1 b_2 \dots b_m = a_1 a_2 \dots a_n b_1 b_2 \dots b_m.$$

Exercise

Show that the operation string concatenation $*$ on the set $FM(A)$ is an associative binary operation with an identity element. The set $FM(A)$ equipped with $*$ is called the **free monoid generated by the set A**.

Definition

Let x be an element in a set S and $*$ be a binary operation on S. Suppose that e is an identity element with respect to $*$. The **inverse** of x is an element $x' \in S$ such that $x * x' = x' * x = e$.

1. The inverse of the element $2 \in \mathbb{Z}$ under usual addition is __________. Moreover, the inverse of the same element in $\mathbb{Z}_n$ under addition modulo n is __________. In general, the inverse of any $a \in \mathbb{Z}$ is __________ and any $a \in \mathbb{Z}_n$ is __________.
2. The inverse of the element $2 \in \mathbb{Z}$ under usual multiplication __________. However, the inverse of the same element in $\mathbb{Q}$ under usual multiplication is __________. In general, the inverse of any $a \in \mathbb{Q}$ is __________.
3. Any matrix M in $M_{m\times n}(\mathbb{R})$ has inverse, with respect to the usual matrix addition, given by __________.

1. The inverse of the element $2 \in \mathbb{Z}$ under usual addition is -2. Moreover, the inverse of the same element in $\mathbb{Z}_n$ under addition modulo n is $n-2$. In general, the inverse of any $a \in \mathbb{Z}$ is $-a$ and any $a \in \mathbb{Z}_n$ is $n-a$.

1. The inverse of the element $2 \in \mathbb{Z}$ under usual addition is -2. Moreover, the inverse of the same element in $\mathbb{Z}_n$ under addition modulo n is $n-2$. In general, the inverse of any $a \in \mathbb{Z}$ is $-a$ and any $a \in \mathbb{Z}_n$ is $n-a$.
2. The inverse of the element $2 \in \mathbb{Z}$ under usual multiplication does not exist. However, the inverse of the same element in $\mathbb{Q}$ under usual multiplication is $1/2$. In general, the inverse of any $a \in \mathbb{Q}$ is $1/a$.

1. The inverse of the element $2 \in \mathbb{Z}$ under usual addition is -2. Moreover, the inverse of the same element in $\mathbb{Z}_n$ under addition modulo n is $n-2$. In general, the inverse of any $a \in \mathbb{Z}$ is $-a$ and any $a \in \mathbb{Z}_n$ is $n-a$.
2. The inverse of the element $2 \in \mathbb{Z}$ under usual multiplication does not exist. However, the inverse of the same element in $\mathbb{Q}$ under usual multiplication is $1/2$. In general, the inverse of any $a \in \mathbb{Q}$ is $1/a$.
3. Any matrix M in $M_{m\times n}(\mathbb{R})$ has inverse, with respect to the usual matrix addition, given by the matrix whose entries consists of the inverse of each entry in M.

Other Terminologies

1. A set S, together with one or more operations on S, is called **algebraic system** or **algebraic structure**. The set S is called the **underlying set** of the structure.
2. A set equipped with one binary operation $*$ is referred to as a **magma** or a **groupoid** or **quasigroup**, denoted by $(S, *)$.
3. A **semigroup** is an algebraic structure consisting of a non-empty set equipped with an associative binary operation.
4. A **monoid** is a semigroup having an identity element.
5. The identity element may also be called the **unit element**.

Groups

Terminologies and Examples

Definition

A (nonempty) set G together with a binary operation $*$ is a **group**, denoted by $(G, *)$, under $*$ if the following properties holds:

- $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$,
- there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$, and
- for each $a \in G$, there exists $a^{-1} \in G$ where $a * a^{-1} = a^{-1} * a = e$.

The four defining postulates for a group are referred to as the **group axioms**. A group with only one element (or consisting only of the identity element) is called a **trivial group**.

Definition (Restated)

A **group** is a nonempty set G under an associative binary operation, such that G contains an identity element for the operation, and each element of G has an inverse in G.

Definition (Restated)

A **group** is a nonempty set G under an associative binary operation, such that G contains an identity element for the operation, and each element of G has an inverse in G.

Definition

Let $(G, *)$ be a group. The cardinality of G is called the **order** of G. We say that G is a **finite group** if its order is finite; otherwise, it is an **infinite group**.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are __________ under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are __________ under the usual multiplication.
2. The set $\mathbb{Z}$ under ordinary multiplication is __________. The same set under ordinary subtraction is __________.
3. The set $(\mathbb{R}^+ - \mathbb{Q}) \cup \{1\}$ under usual multiplication is __________.
4. The set

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

consisting of 2×2 matrices with real entries and nonzero determinants is __________ under matrix multiplication.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are infinite groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are infinite groups under the usual multiplication.
2. The set $\mathbb{Z}$ under ordinary multiplication is not a group. The same set under ordinary subtraction is also not a group.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are infinite groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are infinite groups under the usual multiplication.
2. The set $\mathbb{Z}$ under ordinary multiplication is not a group. The same set under ordinary subtraction is also not a group.
3. The set $(\mathbb{R}^+ - \mathbb{Q}) \cup \{1\}$ under usual multiplication is not a group.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are infinite groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are infinite groups under the usual multiplication.
2. The set $\mathbb{Z}$ under ordinary multiplication is not a group. The same set under ordinary subtraction is also not a group.
3. The set $(\mathbb{R}^+ - \mathbb{Q}) \cup \{1\}$ under usual multiplication is not a group.
4. The set

$$GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

consisting of 2×2 matrices with real entries and nonzero determinants is an infinite group under matrix multiplication. This is called the **general linear group** of degree 2 over $\mathbb{R}$.

1. Consider the set F consisting of all real-valued functions defined on $\mathbb{R}$. The algebraic structures $(F, +)$, $(F, -)$, $(F, \cdot)$, and $(F, \circ)$ are infinite groups.

1. Consider the set F consisting of all real-valued functions defined on $\mathbb{R}$. The algebraic structures $(F, +)$, $(F, -)$, $(F, \cdot)$, and $(F, \circ)$ are infinite groups.
2. For each positive integer n, $\mathbb{Z}_n$ is a finite group of order n under addition modulo n.

1. Consider the set F consisting of all real-valued functions defined on $\mathbb{R}$. The algebraic structures $(F, +)$, $(F, -)$, $(F, \cdot)$, and $(F, \circ)$ are infinite groups.
2. For each positive integer n, $\mathbb{Z}_n$ is a finite group of order n under addition modulo n.
3. Let $U(n) := \{x : \gcd(x, n) = 1 \text{ and } x < n\}$ where $n \in \mathbb{Z}^+$. The set $U(n)$ under multiplication modulo n is a finite group of order $\phi(n)$ where ϕ is the Euler-phi number theoretic function. This group is called the **group of units** of $\mathbb{Z}_n$.

1. Consider the set F consisting of all real-valued functions defined on $\mathbb{R}$. The algebraic structures $(F, +)$, $(F, -)$, $(F, \cdot)$, and $(F, \circ)$ are infinite groups.
2. For each positive integer n, $\mathbb{Z}_n$ is a finite group of order n under addition modulo n.
3. Let $U(n) := \{x : \gcd(x, n) = 1 \text{ and } x < n\}$ where $n \in \mathbb{Z}^+$. The set $U(n)$ under multiplication modulo n is a finite group of order $\phi(n)$ where ϕ is the Euler-phi number theoretic function. This group is called the **group of units** of $\mathbb{Z}_n$.
4. We can form a new group from two groups $(A, \oplus)$ and $(B, \otimes)$ through the **direct product** $(A \times B, \cdot)$ whose elements belong in the Cartesian product $A \times B$. The operation $\cdot$ on the direct group is defined as follows:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \oplus a_2, b_1 \otimes b_2).$$

Exercise

Let S be a set with at least one element. The *power set* $\mathcal{P}(S)$ of S is defined as the collection of all subsets of S. In other words,

$$\mathcal{P}(S) = \{A : A \subset S\}.$$

Identify the group axioms not satisfied by the pair $(\mathcal{P}(S), \cup)$ where $\cup$ is the union operation of sets.

Exercise

Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, and $K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ where $i^2 = -1$.

1. Verify that the relations $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, and $IK = -J$ hold.
2. Show that the set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is a group. This group is called the **quaternion group**.

Definition

An **Abelian** or **commutative group** is a group G that has a commutative binary operation. Otherwise, we say that G is **non-Abelian** or **noncommutative**.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are __________ groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are __________ group under the usual multiplication.
2. The general linear group of degree 2 over $\mathbb{R}$ is __________ group.
3. The groups $(F, +)$, $(F, -)$, $(F, \cdot)$, and $(F, \circ)$ are __________.
4. The groups $(\mathbb{Z}_n, +_n)$ and $(\mathbb{Z}_n, \cdot_n)$, where $+_n$ and $\cdot_n$ denotes addition modulo n and multiplication modulo n respectively, are __________.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are Abelian groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are Abelian groups under the usual multiplication.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are Abelian groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are Abelian groups under the usual multiplication.
2. The general linear group of degree 2 over $\mathbb{R}$ is a non-Abelian group.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are Abelian groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are Abelian groups under the usual multiplication.
2. The general linear group of degree 2 over $\mathbb{R}$ is a non-Abelian group.
3. The groups $(F, -)$ and $(F, \circ)$ are non-Abelian.

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are Abelian groups under the usual addition. Moreover, the set $\mathbb{Q}^+$ and the set of nonzero real numbers R^* are Abelian groups under the usual multiplication.
2. The general linear group of degree 2 over $\mathbb{R}$ is a non-Abelian group.
3. The groups $(F, -)$ and $(F, \circ)$ are non-Abelian.
4. The groups $(\mathbb{Z}_n, +_n)$ and $(\mathbb{Z}_n, \cdot_n)$, where $+_n$ and $\cdot_n$ denotes addition modulo n and multiplication modulo n respectively, are Abelian.

1. Let $G = \mathbb{R}^+ - \{1\}$. Let $*$ be a function on G defined by $a * b = a^{\ln b}$ for all a and b in G. Prove that G is an Abelian group with respect to $*$.
2. Let $f_{m,b} : \mathbb{R} \to \mathbb{R}$ be a function where $f_{m,b}(x) = mx + b$. Show that the set $A = \{f_{m,b} : \mathbb{R} \to \mathbb{R} \mid m \neq 0\}$ of **affine functions** from $\mathbb{R}$ into $\mathbb{R}$ forms a non-Abelian group under composition of functions. Furthermore, show that the group $(A, \circ)$ is Abelian when $m = 1$.

- The set of complex numbers $\mathbb{C} := \{a + bi : a, b \in \mathbb{R}\}$ under addition $+$ and multiplication $\cdot$ defined by

  $$(a + bi) + (c + di) = (a + c) + (b + d)i$$

  and

  $$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$

  is an Abelian group. [Enroll Complex Analysis]
- A vector space V over a field F is an algebraic system with two operations vector addition $+$ and scalar multiplication $\cdot$ that satisfies many properties similar to the field axioms. $(V, +)$ being an Abelian group is one of those properties. [Enroll Linear Algebra Courses]

Where Do We See Abelian Groups?

- A ring $(R, +, \cdot)$ is a set R under a collection of two operations, $+$ and $\cdot$, namely **addition** and **multiplication** that also satisfies a certain number of conditions. One of the conditions states that $(R, +)$ must be Abelian. [Enroll Algebraic Structures]

Groups

Cayley Tables

For a finite set G, a binary operation $*$ on G can be defined by a table. We list the elements in the top (left to right) and left side (top to bottom) in the same order. For instance, consider the table below which defines a binary operation $*$ on $G = \{a, b, c\}$ that follows the rule, $x * y$ where x is an element in the left and y is an element in the top, in computing the image under $*$.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

.

- Operation $*$ is not commutative since $a * b = c \neq a = b * a$.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

.

- Operation $*$ is not commutative since $a * b = c \neq a = b * a$.
- There is no identity element for $*$ since there exists no $e \in G$ such that $x * e = e * x = x$ for all x in G.

- The binary operation $*$ is commutative if and only if the Cayley table is symmetric with respect to the main diagonal.

- The binary operation $*$ is commutative if and only if the Cayley table is symmetric with respect to the main diagonal.
- If the operation has an identity element, which is unique, then there exists a column and a row similar to the left and top sides respectively.

- The binary operation $*$ is commutative if and only if the Cayley table is symmetric with respect to the main diagonal.
- If the operation has an identity element, which is unique, then there exists a column and a row similar to the left and top sides respectively.
- Verifying whether the operation is associative is a tedious process. We may use Light's associativity test but we omit it here since it is also a tedious approach.

- The binary operation $*$ is commutative if and only if the Cayley table is symmetric with respect to the main diagonal.
- If the operation has an identity element, which is unique, then there exists a column and a row similar to the left and top sides respectively.
- Verifying whether the operation is associative is a tedious process. We may use Light's associativity test but we omit it here since it is also a tedious approach.
- The identity element and inverse of each element may be glanced through the Cayley table.

Example (Klein 4-Group)

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Let $V = \{e, a, b, c\}$. The Cayley table shows the Abelian group $(V, *)$ under the binary operation $*$. The group is known as the **Klein four-group**.

1. Construct the Cayley table for the group $U(9)$ under multiplication modulo 9 denoted by $\times_9$[1].
   1.1 What is the identity element?
   1.2 Determine the inverse of each element under $\times_9$.
   1.3 Determine whether the group is Abelian or not.

[1] The remainder when the product of the two numbers are divided by 9.

Groups

Properties of a Group

Theorem

A nonempty set G under an associative binary operation, such that G contains a left identity element, and each element of G has a left inverse in G is a group.

Proof.

Let g^{-1} be the left inverse of every $g \in G$ and e be a left identity. Observe that

$$\begin{aligned} g * g^{-1} &= (e * g) * g^{-1} = \left[\left(g^{-1}\right)^{-1} * g^{-1}\right] * g] * g^{-1} \\ &= \left(g^{-1}\right)^{-1} * \left(g^{-1} * g\right) * g^{-1} = \left(g^{-1}\right)^{-1} * g^{-1} = e. \end{aligned}$$

This shows that g^{-1} is also the right inverse for g. Moreover,

$$g * e = g * \left(g^{-1} * g\right) = e * g = g.$$

Thus, e is also the right identity. The conclusion follows. $\square$

Theorem

Let $(G, *)$ be a group. Suppose a and b are any elements of G. The linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G. In particular, the inverse of every element in a group are unique.

Theorem

Let $(G, *)$ be a group. Suppose a and b are any elements of G. The linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G. In particular, the inverse of every element in a group are unique.

Proof.

The linear equations $a*x = b$ and $y*a = b$ has respective solutions given by $x = a^{-1}b \in G$ and $y = ba^{-1} \in G$. Let x_1 and x_2 be solutions of $a * x = b$. Hence, $a * x_1 = a * x_2$. Thus, $a^{-1} * (a * x_1) = a^{-1} * (a * x_2)$ or $x_1 = x_2$. Similar arguments can be made for the linear equation $y * a = b$. Therefore, the linear equations have unique solutions in G. In particular, if we let $b = e$, where e is the identity element of $(G, *)$, then $a * x = y * a = e$ has unique solutions in G. $\square$

- For simplicity, we omit the operation $*$ and write ab to denote $a * b$. We also write a group $(G, *)$ simply as G assuming the binary operation is well-understood.
- Moreover, the expression a^n for a positive integer n and an element $a \in G$ denotes the repeated application of the binary operation

$$aa \cdots a \ \ (n \text{ factors})$$

and $a^n = e$ for $n = 0$. When n is negative,

$$a^n = \left(a^{-1}\right)^{|n|}.$$

Exponential Laws

Theorem

Let G be a group. Suppose that $a \in G$. For any integers n and m, we have

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

Theorem

For a group G, $ba = ca$ implies $b = c$ and $ca = cb$ implies $a = b$ for all a, b, and c in G. In other words, the ***left*** *and* ***right cancellation laws*** *hold.*

Theorem

For a group G, $ba = ca$ implies $b = c$ and $ca = cb$ implies $a = b$ for all a, b, and c in G. In other words, the ***left*** *and* ***right cancellation laws*** *hold.*

Proof.

Since a and c are in G, their inverses exists. Hence,

$$(ba) * a^{-1} = (ca) * a^{-1} \text{ and } c^{-1} * (ca) = c^{-1} * (cb)$$

holds. Using the associative law and simplifying, we must have $b = c$ and $a = b$ respectively. □

- A magma is **left cancellative** (or **right cancellative**) if the left cancellation (or right cancellation) law holds.
- The previous theorem states that a group must be left and right cancellative.
- This result shows that an element must only appear once each column and each row for a Cayley table representation of a group.
- In combinatorics, a **Latin square** is an $n \times n$ array filled with n different symbols such that each symbol appears exactly once in each column and exactly once in each row.

Theorem

For each element a in a group G, the inverse $(a^{-1})^{-1}$ of a^{-1} is a.

Theorem

For each element a in a group G, the inverse $(a^{-1})^{-1}$ of a^{-1} is a.

Proof.

The theorem follows from the definition and the uniqueness of the inverse of a group element. $\square$

Theorem

For any elements $a_1, a_2, \ldots, a_n \in (G, *)$ where $(G, *)$ is a group under the binary operation $*$, the value $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed.

Theorem (Socks-Shoes Property)

For any elements a and b of a group, $(ab)^{-1} = b^{-1}a^{-1}$.

Socks-Shoes Property

Theorem (Socks-Shoes Property)

For any elements a and b of a group, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

Note that

$$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aea^{-1} = aa^{-1} = e$$

and

$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}\left(a^{-1}a\right)b = b^{-1}eb = b^{-1}b = e.$$

Since the inverse of a group element is unique, $(ab)^{-1} = b^{-1}a^{-1}$. $\square$

1. Let $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and assume that G is a group under a binary operation $*$ that satisfies the following properties:
   - $a * b \leq a + b$ for all $a, b \in G$, and
   - $a * a = 0$ for all $a \in G$.

   Write out the Cayley table for G.

Subgroups

Terminologies and Examples

Definition

A subset H of a group G is a **subgroup** of G if H is a group under the induced operation from G. We let $H \leq G$ denote that H is a subgroup of G. Also, let $H < G$ denote that $H \leq G$ and $H \neq G$.

1. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
2. $(\mathbb{Q}^+, \cdot)$ is a subgroup of $(\mathbb{R}^+, \cdot)$.
3. The set of continuous real-valued functions with domain $\mathbb{R}$ is a subgroup of F under function addition.

- The largest subgroup of a group G is G itself. We call this subgroup the **improper** subgroup of G.

Remarks

- The largest subgroup of a group G is G itself. We call this subgroup the **improper** subgroup of G.
- Any subgroup H of G such that $H \neq G$ are called **proper subgroups**.

- The largest subgroup of a group G is G itself. We call this subgroup the **improper** subgroup of G.
- Any subgroup H of G such that $H \neq G$ are called **proper subgroups**.
- The smallest subgroup of G is the group $\{e\}$ consisting of the identity element for the operation. This subgroup is referred to as the **trivial subgroup** of G.

- The largest subgroup of a group G is G itself. We call this subgroup the **improper** subgroup of G.
- Any subgroup H of G such that $H \neq G$ are called **proper subgroups**.
- The smallest subgroup of G is the group $\{e\}$ consisting of the identity element for the operation. This subgroup is referred to as the **trivial subgroup** of G.
- Any subgroup of G not equal to the trivial subgroup is a **non-trivial subgroup**.

Recall that a **partial order relation** is a reflexive (or homogeneous) relation that is both antisymmetric and transitive.

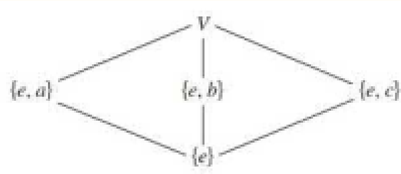
Recall that a **partial order relation** is a reflexive (or homogeneous) relation that is both antisymmetric and transitive.

Observe that the relation $\leq$ defined for subgroups is a partial order relation. Hence, we can construct a Hasse diagram relating the subgroups of a group G. We also call this diagram as the **lattice diagram for subgroups**.

The subgroups of the Klein-4 group V are $\{e\}, \{e, a\}, \{e, b\}, \{e, c\}$, and V.

The subgroups of the Klein-4 group V are $\{e\}, \{e, a\}, \{e, b\}, \{e, c\}$, and V.

The lattice diagram is given by



Find the subgroups of the group $(Z_4, +_4)$ and construct the lattice diagram for subgroups of $(Z_4, +_4)$.

Subgroups

Subgroup Tests

Definition

Let H be a subset of a group G. We say that H is **closed under taking inverses** if $a^{-1} \in H$ for any $a \in H$ under the induced operation on H.

Definition

Let H be a subset of a group G. We say that H is **closed under taking inverses** if $a^{-1} \in H$ for any $a \in H$ under the induced operation on H.

Theorem (Two-Step Subgroup Test)

A subset H of a group G is a subgroup of G if and only if

1. *H is non-empty,*
2. *H is closed under the binary operation defined on G, and*
3. *H is closed under taking inverses.*

Proof of the Two-Step Subgroup Test

Proof.

Note that associative law holds for any elements in a subset of G. Thus, the theorem is proven. $\square$

Theorem

A nonempty subset H of the group G is a subgroup of G under the induced operation on H if and only if $ab^{-1} \in H$ for any a and b in H.

Theorem

A nonempty subset H of the group G is a subgroup of G under the induced operation on H if and only if $ab^{-1} \in H$ for any a and b in H.

Proof.

Proof for the necessary part of the theorem clearly follows. Suppose $ab^{-1} \in H$ for all $a, b \in H$. Associative law clearly holds in H. Since H is non-empty, there exists an element $x \in H$. Hence $xx^{-1} = e \in H$. Moreover, $ex^{-1} = x^{-1} \in H$. Thus, H is closed under taking inverses. Lastly, suppose that $y \in H$. Therefore, $x\left(y^{-1}\right)^{-1} = xy \in H$ and H is closed under the induced operation from G. □

Theorem

Let H be any non-empty finite subset of a group G. If H is closed under the binary operation on G, then H is a subgroup of G.

Finite Subgroup Test

Theorem

Let H be any non-empty finite subset of a group G. If H is closed under the binary operation on G, then H is a subgroup of G.

Proof.

Suppose that H is closed under the binary operation on G. We only need to prove H is closed under taking inverses. If $a = e$, then $a^{-1} = a \in H$. Suppose $a \neq e$. Consider the set $\{a^n : n \in \mathbb{Z}^+\}$. Since H is closed, $a^n \in H$ for each $n \in \mathbb{Z}^+$. By the assumption that H is finite, $a^x = a^y$ for some $x, y \in \mathbb{Z}^+$ such that $x \neq y$. Without loss of generality, we assume that $x > y$. Thus, $a^{x-y} = e$ where $x - y > 1$ since $a \neq e$. It follows that $aa^{x-y-1} = e$ or $a^{-1} = a^{x-y-1}$. Observe that $x - y - 1 \geq 1$. Hence, $a^{x-y-1} \in \{a^n : n \in \mathbb{Z}^+\}$. By the two-step subgroup test, the conclusion follows. $\square$

1. The **center** $Z(G)$ of a group G is a subset of G containing elements that commute with every element of G. That is,

$$Z(G) := \{a \in G : ag = ga \text{ for all } g \in G\}.$$

   Prove that the center of a group G is a subgroup of G.

2. The **centralizer** $C(a)$ of an element a of a group G is a subset of G containing elements that commute with a. In symbols,

$$C(a) := \{g \in G : ag = ga\}.$$

   Prove that the centralizer of a is a subgroup of G for each element a in a group G.

3. Let G be a group and A be a non-empty subset of G. The **normalizer** of A in G is defined as

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

where $gAg^{-1} = \{gag^{-1} : a \in A\}$. Prove that the normalizer of A in G is a subgroup of G.
4. Let H and K be subgroups of an abelian group G. Show that the set $\{hk : h \in H, k \in K\}$ under the induced operation from G is a subgroup of G.

5. Prove that the intersection $H \cap K$ of two subgroups H and K of a group G is a subgroup of G.
6. Prove that D is a subgroup of $(F, +)$ where D consists of differentiable real-valued functions with domain $\mathbb{R}$. Moreover, show that $\{f \in D : {}^{df}/_{dx} \text{ is constant}\}$ is a subgroup of D.

- In the Two-Step Subgroup Test, some references replace the requirement for a subgroup H of a group G to be non-empty by showing that the identity element in G also lies in H.
- A finite group G cannot be written as a union of two finite proper subgroups of G.

Cyclic Groups

Cyclic Groups

Terminologies and Examples

Theorem

Let G be a group. Suppose that a is any element of G. The set

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

is a subgroup of G under the binary operation on G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a, that is, every subgroup containing a contains $\langle a \rangle$. The subgroup $\langle a \rangle$ is called the ***cyclic subgroup generated by*** *a.*

Proof.

Note that $e = a^0 \in G$. Suppose that $x, y \in \langle a \rangle$. Then $x = a^m$ and $y = a^n$ for some $m, n \in \mathbb{Z}$. Since

$$xy^{-1} = a^m \left(a^n\right)^{-1} = a^{m-n}$$

and $a^{m-n} \in \langle a \rangle$, $xy^{-1} \in \langle a \rangle$. Thus, $\langle a \rangle$ is a subgroup of G.
Now, suppose that H is a subgroup containing a. This implies that a^{-1} is also in H. By the closure property, $a^n \in H$ for any $n \in \mathbb{Z}$. Therefore, H contains $\langle a \rangle$. $\square$

1. What is the cyclic subgroup generated by 3 in $\mathbb{Z}_{12}$?
2. What is the cyclic subgroup generated by 4 in $\mathbb{Z}_{18}$?
3. What is the cyclic subgroup generated by 5 in $U(12)$?
4. What is the cyclic subgroup generated by 5 in $U(7)$?

Examples

1. $\{0, 3, 6, 9\}$

1. $\{0, 3, 6, 9\}$
2. $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

1. $\{0, 3, 6, 9\}$
2. $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
3. $\{1, 5\}$

1. $\{0, 3, 6, 9\}$
2. $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
3. $\{1, 5\}$
4. $U(7)$

Definition

An element a of a group G **generates** G if $\langle a \rangle = G$. We also say that $a \in G$ is a **generator** for G.

Definition

A group G is said to be **cyclic** if there exists an element that generates G.

1. The group $\mathbb{Z}_8$ is ________.
2. The Klein four-group is ________.
3. The group of units $U(9)$ in $\mathbb{Z}_9$ is ________.

Examples

1. The group $\mathbb{Z}_8$ is cyclic with generator 1. The elements $3, 5,$ and 7 are also generators of the group.

1. The group $\mathbb{Z}_8$ is cyclic with generator 1. The elements $3, 5$, and 7 are also generators of the group.
2. The Klein four-group is not cyclic.

Examples

1. The group $\mathbb{Z}_8$ is cyclic with generator 1. The elements $3, 5$, and 7 are also generators of the group.
2. The Klein four-group is not cyclic.
3. The group of units $U(9)$ in $\mathbb{Z}_9$ is cyclic with generator 2.

Definition

Let S be a non-empty subset of a group G. We define $\langle S\rangle$ as the subset of **words** made from elements in S. In symbols,

$$\langle S\rangle = \{s_1^{\alpha_1}\cdots s_n^{\alpha_n} : n \in \mathbb{Z}_{\geq 1}, s_i \in S, \alpha_i \in \mathbb{Z}\}.$$

Subgroup Generated by a Subset

Theorem

*For any non-empty subset S of a group G, $\langle S \rangle \leq G$. The subgroup $\langle S \rangle$ is called the **subgroup generated** by S.*

Example

Definition

A group is said to be **finitely generated** if it is generated by a finite subset.

Cyclic Groups

Properties of Cyclic Groups

Cyclic Groups are Commutative

Theorem

Every cyclic group is Abelian.

Theorem

Every cyclic group is Abelian.

Proof.

Suppose that G is generated by a. Let $x, y \in \langle a \rangle$. Then $x = a^m$ and $y = a^n$ for some $m, n \in \mathbb{Z}$. Observe that

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx.$$

Therefore, G is Abelian. $\square$

Definition

The **order** $|a|$ of an element a from a group G is the smallest positive integer n such that $a^n = e$. If no such positive integer exist, then a is said to be of infinite order.

1. Consider the group $\mathbb{Z}_4$. The order of 3 is _________ while the order of 2 is _________.
2. The element $5 \in U(7)$ has order _________.
3. The element $7 \in \mathbb{Z}$ has _________.

1. Consider the group $\mathbb{Z}_4$. The order of 3 is 4 while the order of 2 is 2.

Examples

1. Consider the group $\mathbb{Z}_4$. The order of 3 is 4 while the order of 2 is 2.
2. The element $5 \in U(7)$ has order 6.

1. Consider the group $\mathbb{Z}_4$. The order of 3 is 4 while the order of 2 is 2.
2. The element $5 \in U(7)$ has order 6.
3. The element $7 \in \mathbb{Z}$ has an infinite order.

Lemma

The order of an element a from a group G is the order of the cyclic subgroup generated by a. More specifically,

1. *if $|\langle a\rangle| = n < \infty$ then $a^n = e$ and $e, a, \ldots, a^{n-1}$ are the distinct elements of $\langle a\rangle$, and*
2. *if $|\langle a\rangle| = \infty$ then $a^n \neq e$ and $a^x \neq a^y$ for all positive integers n, x, and y such that $x \neq y$.*

Lemma

The order of an element a from a group G is the order of the cyclic subgroup generated by a. More specifically,

1. *if $|\langle a \rangle| = n < \infty$ then $a^n = e$ and $e, a, \ldots, a^{n-1}$ are the distinct elements of $\langle a \rangle$, and*
2. *if $|\langle a \rangle| = \infty$ then $a^n \neq e$ and $a^x \neq a^y$ for all positive integers n, x, and y such that $x \neq y$.*

Proof.

The proof is left as an exercise to the reader. □

Theorem

Let G be a group. Suppose that $a \in G$ and $k \in \mathbb{Z} - \{0\}$. The following statements hold:

1. *If $|a| = \infty$ then $|a^k| = \infty$.*
2. *If $|a| = n < \infty$ then $|a^k| = {}^{n}/_{\gcd(n,k)}$.*

Corollary

Let G be a group of order n. Suppose that $a \in G$ and $k \in \mathbb{Z} - \{0\}$. Then $G = \langle a^k \rangle$ if and only if $\gcd(k, n) = 1$.

Lemma

Let G be a cyclic group of order n. Suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Alternative Lemma for the Theorem

Lemma

Let G be a cyclic group of order n. Suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Proof.

Suppose that $a^k = e$. There exists integers q, r where $0 < r < n$ and

$$k = nq + r.$$

Hence, $a^k = a^{nq+r} = a^{nq}a^r$. Since n is the order of a, we must have $r = 0$. Thus, n divides k. On the other hand, if n divides k then $k = nq$ for some integer q. Therefore,

$$a^k = a^{nq} = (a^n)^q = e^q = e.$$

$\square$

Theorem

Let G be a group. Suppose that $a \in G$ and $k \in \mathbb{Z} - \{0\}$. The following statements hold:

1. *If $|a| = \infty$ then $|a^k| = \infty$.*
2. *If $|a| = n < \infty$ then $|a^k| = n/\gcd(n,k)$.*

Theorem

Let G be a group. Suppose that $a \in G$ and $k \in \mathbb{Z} - \{0\}$. The following statements hold:

1. *If $|a| = \infty$ then $|a^k| = \infty$.*
2. *If $|a| = n < \infty$ then $|a^k| = n/\gcd(n,k)$.*

Proof.

The proof for the infinite case is trivial. Suppose that $|a| = n < \infty$. Note that the order of a^k is the smallest integer m such that

$$\left(a^k\right)^m = e \text{ or } a^{km} = e.$$

Using the previous lemma, n must divide km. If $d = \gcd(n,k)$ then n/d divides $m\,(k/d)$. Thus, n/d divides m. Therefore, $m = n/d$. □

Corollary

Let G be a group of order n. Suppose that $a \in G$ and $k \in \mathbb{Z} - \{0\}$. Then $G = \langle a^k \rangle$ if and only if $\gcd(k, n) = 1$.

Corollary

The order of an element in a finite cyclic group G divides the order of G.

Theorem

Let $G = \langle a \rangle$ be a cyclic group. Suppose that $|G| = n < \infty$. Every subgroup of a cyclic group is cyclic. Furthermore, the order of any subgroup of G divides n. In addition, for each positive integer k dividing n, there exists a unique subgroup of G of order k. This subgroup is the cyclic group $\langle a^d \rangle$ where $d = n/k$.

Proof.

Let G be a cyclic group generated by a, and H be a subgroup of G. If H is a trivial subgroup then the conclusion follows. Suppose that H is non-trivial. This implies that there exists $b \in H$ where $b \neq e$. Note that b is also in G. Hence, $b = a^r$ for some nonzero $r \in \mathbb{Z}$. Since H is a subgroup, a^{-r} is also in H. This shows that H contains positive powers of a since exactly one of r or $-r$ is positive. From the collection of positive powers of a, let m be the smallest element. Such element exists using the Well-Ordered Principle.

Proof.

We claim that a^m is a generator for H. Consider $h \in H \subset G$. We can also write h as a^k for some $k \in \mathbb{Z}$. By the Division Algorithm, there exists integers q and r such that $k = mq + r$ where $0 \leq r < m$. Observe that

$$a^k = a^{mq+r} = a^{mq}a^r = (a^m)^q \, a^r.$$

Hence, $a^r = a^k (a^m)^{-q}$ and $a^r \in H$. Note that m is the smallest positive element such that $a^m \in H$. Thus, $r = 0$ and

$$h = (a^m)^q \, .$$

Therefore, H is cyclic with generator a^m.

Proof.

Let H be a subgroup of G. Then H is cyclic and $H = \langle a^m \rangle$ where m divides n. Also H satisfies

$$|H| = |\langle a^m \rangle| = \frac{n}{\gcd(n, m)} = \frac{n}{m}.$$

Hence, the order of any subgroup of G divides n. Now, let k be a divisor of n. Note that

$$\left| \left\langle a^{n/k} \right\rangle \right| = \frac{n}{\gcd\left(n, \frac{n}{k}\right)} = \frac{n}{n/k} = k.$$

This shows that G has a subgroup of order k.

Proof.

Suppose that K is another subgroup of order k. Then K must also be cyclic and has generator a^s where s divides n. Also,

$$k = |K| = |a^s| = \frac{n}{\gcd(n, s)} = \frac{n}{s}.$$

Therefore, $s = \dfrac{n}{k}$. $\square$

Corollary

Let G be a finite cyclic group and $H \leq G$. The order $|H|$ of H must divide that $|G|$ of G. In other words, $|G|$ is a multiple of $|H|$.

Corollary

For each integer k dividing n, the set $\langle \frac{n}{k} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ with order k. Moreover, these are only the subgroups of $\mathbb{Z}_n$.

Corollary

Let d be a divisor of n. The number of elements of order d in a cyclic group of order n is $\phi(d)$, the number of positive integers less than d relatively prime to d.

Corollary

In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

1. Find all generators and draw the lattice diagram of subgroups for $\mathbb{Z}_{16}$, $\mathbb{Z}_{28}$, $U(18)$, and $U(24)$.
2. Suppose that a and b are elements of a finite group such that $ab = ba$. Show that the order $|ab|$ of ab divides the product $|a||b|$ of the orders of a and b. In addition, show that $|ab| = |a||b|$ if and only if $\gcd(|a|, |b|) = 1$.
3. Prove that a group of order 3 is always cyclic.

Examples of Non-Abelian Groups

Examples of Non-Abelian Groups

Symmetric Group

Definition

A **permutation** of a set A is a function $\phi : A \to A$ from a set into itself that is both one-to-one and onto.

Definition

A **permutation** of a set A is a function $\phi : A \to A$ from a set into itself that is both one-to-one and onto.

Definition (Restated)

A **permutation** of a set A is a bijective function from A onto itself.

Theorem

The collection of all permutations of a set A into itself is a group under function composition.

Theorem

The collection of all permutations of a set A into itself is a group under function composition.

Proof.

The proof follows from the definition and properties of a bijective function. □

The collection of all permutations on a set A under function compositio forms a group called the **symmetric group** on A. By letting A be the set $Q_n := \{1, \ldots, n\}$, we call the symmetric group S_n on Q_n as the **symmetric group on *n* letters**.

What are the elements of the symmetric group S_3 on 3 letters?

What are the elements of the symmetric group S_3 on 3 letters?

Consider a function from the set $\{1, 2, 3\}$ onto $\{1, 2, 3\}$. The only possible bijective functions are those functions whose mappings are given by:

1. $1 \mapsto 1, 2 \mapsto 2$, and $3 \mapsto 3$,
2. $1 \mapsto 1, 2 \mapsto 3$, and $3 \mapsto 2$,
3. $1 \mapsto 3, 2 \mapsto 2$, and $3 \mapsto 1$,
4. $1 \mapsto 2, 2 \mapsto 1$, and $3 \mapsto 3$,
5. $1 \mapsto 2, 2 \mapsto 3$, and $3 \mapsto 1$, and
6. $1 \mapsto 3, 2 \mapsto 1$, and $3 \mapsto 2$.

A permutation σ on Q_n can be expressed in the two-line notation shown below

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

A permutation σ on Q_n can be expressed in the two-line notation shown below

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

With this notation, the inverse of a permutation is given by

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Example (Revisited)

Using the two-line notation, the elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

EXAMPLE (REVISITED)

Using the two-line notation, the elements of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Now, we use the notation to easily compute for the composition of permutations. Let

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

We compute for $f \circ g$. Note that finding composition of two permutations shall be read from right to left.

Given the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$ on Q_6, it can be expressed simply as

$$(1\,2)(3\,4\,6)(5)$$

where the objects $(a_1\ a_2\ \ldots\ a_{n-1}\ a_n)$, referred to as **cycles of length *n*** or ***n*-cycles**, satisfies $\sigma(a_1) = a_2, \ldots, \sigma(a_{n-1}) = a_n$, and $\sigma(a_n) = a_1$. The product of cycles is called the **cycle decomposition** of σ.

Cycle Decomposition Algorithm

1. Select the smallest element a which has not appeared in a previous cycle.
2. Find the image b of the element to obtain an initial cycle $(a\ b$. Repeat this step until we reach an element k which is mapped to a.
3. We close the cycle with a right parenthesis. For instance, we have the cycle $(a\ b\ \ldots k)$.
4. Repeat the first step until all elements of S_n are considered.
5. Remove all cycles of length one (1).

1. Consider the permutations in S_6 given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 4 & 3 \end{pmatrix} \text{ and } \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 6 & 5 & 3 \end{pmatrix}.$$

   What are $\sigma \circ \delta$ and $\delta \circ \sigma$?

2. Evaluate all powers of the permutation $\sigma \in S_5$ given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

- For all integers $n \geq 3$, the symmetric group on n letters is non-Abelian.
- For any cycle $(a_1\ a_2\ \ldots\ a_n)$ of length n,

$$(a_1\ a_2\ \ldots\ a_n) = (a_2\ \ldots\ a_n\ a_1) = \cdots = (\ldots\ a_n\ a_1\ a_2).$$

Disjoint Cycles

Cycles that have no entries in common are said to be **disjoint**.

Cycles that have no entries in common are said to be **disjoint**.

For instance, the cycles $(1\ 4\ 7)$ and $(6\ 5)$ are disjoint while $(2\ 5\ 3)$ and $(3\ 7)$ are not disjoint.

Disjoint Cycles

Cycles that have no entries in common are said to be **disjoint**.

For instance, the cycles $(1\ 4\ 7)$ and $(6\ 5)$ are disjoint while $(2\ 5\ 3)$ and $(3\ 7)$ are not disjoint.

The inverse of a permutation $(a_1\ \dots\ a_n)(b_1\ \dots\ b_k)\cdots$, where the cycles are pairwise disjoint, is then given by

$$\cdots(b_k\ \dots\ b_1)(a_n\ \dots\ a_1).$$

Examples

1. Write the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ and its inverse using disjoint cycles.
2. Consider the permutations in S_7 given by $\sigma = (1\ 3\ 4)(5\ 6\ 2)$ and $\delta = (2\ 4)(3\ 6)$. Compute for $\sigma\delta$ and $\delta\sigma$.

Theorem

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Proof.

The proof is left as an exercise to the reader. $\square$

Theorem

Given any pair of disjoint cycles σ and δ, we must have $\sigma\delta = \delta\sigma$.

Disjoint Cycles Commute

Theorem

Given any pair of disjoint cycles σ and δ, we must have $\sigma\delta = \delta\sigma$.

Proof.

Let x be an entry in σ. Then $\sigma(x)$ is an entry in σ and $\delta(y) = y$ for all entries y in σ. Hence, $\sigma(\delta(x)) = \sigma(x) = \delta(\sigma(x))$. Similar arguments follow when x is an entry in δ. $\square$

Lemma

The order of a k-cycle is k.

Lemma

The order of a k-cycle is k.

Proof.

Let $\sigma = (a_1\ a_2\ \ldots\ a_k)$ be a k-cycle. Note that $\sigma(a_i) = a_{i+1}$. Hence, $\sigma^n(a_i) = a_{i+n}$ where $i + n$ is taken modulo k. This shows that $\sigma^k(a_i) = a_i$ and $\sigma^j(a_1) \neq a_1$ for $1 \leq j \leq k - 1$. Therefore, $\sigma^j \neq (1)$ whenever $1 \leq j \leq k - 1$ and $|\sigma| = k$. $\square$

Theorem

The order a permutations is the least common multiple of the lengths of the cycles in its cycle decomposition.

Theorem

The order a permutations is the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof.

Let $\alpha = \alpha_1 \dots \alpha_n$ be a cycle decomposition where the length of α_i is l_i. Suppose that k is the order of α and l be the least common multiple of l_1, ..., and l_n. Then $\alpha^k = \alpha_1^k \cdots \alpha_n^k = (1)$ because disjoint cycles commute. It follows that $\alpha_i^k = (1)$ for all i since α_i^k are disjoint. Thus, each l_i divides k which implies that l divides k. Moreover, $\alpha^l = (1)$ since $\alpha_i^{l_i} = (1)$. This means that k divides l. Therefore, $k = l$. $\square$

Find the order of the following permutations.

1. $(1\ 3\ 4)(2\ 5)$
2. $(1\ 7\ 3)(4\ 8)(2\ 5\ 6\ 9)$
3. $(1\ 5\ 4\ 2)(2\ 5\ 7\ 9)$

Transposition

Definition

A cycle of length 2 is called a **transposition**.

Definition

A cycle of length 2 is called a **transposition**.

Theorem

Every permutation of a finite set containing at least two elements is a product of 2-cycles.

Definition

A cycle of length 2 is called a **transposition**.

Theorem

Every permutation of a finite set containing at least two elements is a product of 2-cycles.

Proof.

The proof follows from the fact that any cycle $(a_1\ a_2\ \ldots\ a_k)$ can be written as $(a_1\ a_k)\ldots(a_1\ a_3)(a_1\ a_2)$. $\square$

Lemma

If $\sigma_1 \dots \sigma_k = (1)$ then k must be even.

Lemma

If $\sigma_1 \ldots \sigma_k = (1)$ then k must be even.

Proof.

The proof is left as an exercise to the reader. $\square$

Theorem

No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Theorem

No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof.

Let $\alpha = \alpha_1 \dots \alpha_k$ and $\beta = \beta_1 \dots \beta_j$. If $\alpha = \beta$ then

$$\alpha_1 \dots \alpha_k \beta_j^{-1} \dots \beta_1^{-1} = \alpha_1 \dots \alpha_k \beta_j \dots \beta_1 = (1).$$

Thus, $s + r$ must be even. Therefore, s and r must be both odd or both even. $\square$

Definition

A permutation of a finite set is **even** or **odd** if it can be written as a product of an even or odd number of transpositions, respectively.

Definition

Let n be an integer with $n \geq 2$. Define T_n as the set of ordered pairs given by

$$T_n = \{(i, j) \in Q_n^2 : i < j\}.$$

The number of *inversions* of $\sigma \in S_n$ is the number

$$\mathrm{inv}(\sigma) = |\{(i, j) \in T_n : \sigma(i) > \sigma(j)\}|\,.$$

Observe that

$$|T_n| = \sum_{i=1}^{n}(n-i) = n(n-1) - \sum_{i=1}^{n} i = \frac{n(n-1)}{2}.$$

Consider the permutation $\sigma = (1\ 3\ 2)(4\ 5)$ in S_5. To find $\mathrm{inv}(\sigma)$, we must find pairs $(i, j) \in Q_5^2$ such that $\sigma(i) > \sigma(j)$. These are the pairs

$$(1,2), (1,3), \text{ and } (4,5).$$

Hence, $\mathrm{inv}(\sigma) = 3$.

Theorem

A permutation $\sigma \in S_n$ is even (odd) if and only if $\mathrm{inv}(\sigma)$ is an even (odd) integer.

Proof.

The proof is left as an exercise. $\square$

Theorem

*Let $n \geq 2$ be an integer. The collection of all even permutations of $\{1, 2, \ldots, n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n. This subgroup is called the **alternating group on n letters**.*

Alternating Group on n Letters

Theorem

*Let $n \geq 2$ be an integer. The collection of all even permutations of $\{1, 2, \ldots, n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n. This subgroup is called the **alternating group on n letters**.*

Proof.

Consider the function $f : A_n \to S_n - A_n$ defined by $f(\sigma) = \alpha\sigma$ where α is a fixed element of $S_n - A_n$. We claim that f is bijective. Suppose that $f(\sigma) = f(\beta)$. Then $\alpha\sigma = \alpha\beta$. Hence, $\sigma = \beta$ and f is one-to-one. Now, we consider $\delta \in S_n - A_n$. Then $\alpha^{-1}\delta$ is an even permutation and $f(\alpha^{-1}\delta) = \delta$. Thus, f is onto. Therefore, f is bijective and $|A_n| = |S_n - A_n| = \frac{n!}{2}$. $\square$

1. What are the possible orders for the elements of S_5?
2. Let $H = \{\beta \in S_5 : \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5. Find the order of H.
3. Prove that for any permutation σ, $\sigma\tau\sigma^{-1}$ is a transposition if and only if τ is a transposition.

- Symmetric groups on n letters are also called **symmetric groups of degree *n***.
- Any subgroup of a symmetric group of a set is called a **permutation group**.
- The product of all cycles relating to a permutation σ is called the **cycle decomposition** of σ.

Examples of Non-Abelian Groups

Dihedral Group

The elements of D_{2n} are composed of

- n rotations, and
- n reflection symmetries.

These rotation and reflection symmetries can be written in terms of permutations.

For instance, the elements of D_8 are subsets of S_4 given by the rotations

1. (1)
2. $(1\,2\,3\,4)$
3. $(1\,3)(2\,4)$ and
4. $(1\,4\,3\,2)$,

and the reflection symmetries

1. $(1\,2)(3\,4)$
2. $(2\,4)$
3. $(1\,3)$ and
4. $(1\,4)(2\,3)$.

Theorem

For any $n \geq 3$, $(D_{2n}, \circ)$ is a group under function composition.

Theorem

For any $n \geq 3$, $(D_{2n}, \circ)$ is a group under function composition.

Theorem

The proof follows from the definition of a symmetry.

Definition

Let $n \geq 3$. The **dihedral group** D_{2n} of order $2n$ is the set D_{2n} under the function composition.

Definition

Let $n \geq 3$. The **dihedral group** D_{2n} of order $2n$ is the set D_{2n} under the function composition.

Definition (Restated)

The **dihedral group** D_{2n} of order $2n$, where $n \geq 3$, is the group consisting of all rigid motions of a regular polygon with n sides under the function composition.

Lemma

The dihedral group D_{2n} can be expressed as

$$\{1, \rho, \rho^2, \ldots, \rho^{n-1}, \mu\rho, \mu\rho^2, \ldots, \mu\rho^{n-1}\}$$

where ρ is the clockwise rotation about the origin through $2\pi/n$ radians and μ is the reflection about the line of symmetry passing through vertex 1 and the origin.

Lemma

The dihedral group D_{2n} can be expressed as

$$\{1, \rho, \rho^2, \ldots, \rho^{n-1}, \mu\rho, \mu\rho^2, \ldots, \mu\rho^{n-1}\}$$

where ρ is the clockwise rotation about the origin through $2\pi/n$ radians and μ is the reflection about the line of symmetry passing through vertex 1 and the origin.

Proof.

The proof is left as an exercise to the reader. $\square$

Theorem

Let D_{2n} be the dihedral group of order $2n$. The following statements hold:

1. *The order of ρ and μ is n and 2 respectively.*
2. *For any integers i and j, $\rho^i \rho^j = \rho^{i+j}$.*
3. *For any $1 \leq i \leq n-1$, $\mu \neq \rho^i$.*
4. *For $0 \leq i \leq n$, $\rho^i \mu = \mu \rho^{-i}$ holds.*

Theorem

Let D_{2n} be the dihedral group of order $2n$. The following statements hold:

1. *The order of ρ and μ is n and 2 respectively.*
2. *For any integers i and j, $\rho^i \rho^j = \rho^{i+j}$.*
3. *For any $1 \leq i \leq n-1$, $\mu \neq \rho^i$.*
4. *For $0 \leq i \leq n$, $\rho^i \mu = \mu \rho^{-i}$ holds.*

Proof.

The proof is left as an exercise to the reader. $\square$

- The dihedral group of order $2n$ is also called the ***n*th dihedral group**.

Group Isomorphism

Group Isomorphism

Cayley's Theorem

Definition

Let $(G, *)$ and $(H, \star)$ be groups, and $f : G \to H$. We say that f is a **group isomorphism** if f is a bijective homomorphism, that is,

1. The function f is one-to-one and maps onto H.
2. For all $a, b \in G$, $f(a * b) = f(a) \star f(b)$.

We say that $(G, *)$ is **isomorphic** to $(H, \star)$ if there exists an isomorphism between $(G, *)$ and $(H, \star)$. We denote these statement by $G \cong H$.

Consider a group $(G, *)$ with three elements say $\{e, a, b\}$. Since a group needs an identity element, we assume that the identity element is e. We can construct a Cayley table as follows:

$$\begin{array}{c|c|c|c} * & \mathrm{e} & \mathrm{a} & \mathrm{b} \\ \hline \mathrm{e} & \mathrm{e} & \mathrm{a} & \mathrm{b} \\ \hline \mathrm{a} & \mathrm{a} & \mathrm{b} & \mathrm{e} \\ \hline \mathrm{b} & \mathrm{b} & \mathrm{e} & \mathrm{a} \end{array}.$$

The Cayley table of another group with three elements must be similar to the previous table. Hence, up to an isomorphism, there is a unique group of order 3.

1. The additive group $(\mathbb{R}, +)$ of real numbers is isomorphic to multiplicative group $(\mathbb{R}, \cdot)$ of real numbers.
2. The groups $U(8)$ and $U(12)$ are isomorphic.
3. The groups $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$ are not isomorphic.
4. The groups $\mathbb{Z}_6$ and S_3 are not isomorphic.

Lemma

Let $f : G \to H$ be a group isomorphism between $(G, *)$ and $(H, \star)$. Then $f^{-1} : H \to G$ is also a group isomorphism and $|G| = |H|$.

Lemma

Let $f : G \to H$ be a group isomorphism between $(G, *)$ and $(H, \star)$. Then $f^{-1} : H \to G$ is also a group isomorphism and $|G| = |H|$.

Proof.

The proof is left as an exercise to the reader. $\square$

Theorem

The isomorphism of groups determines an equivalence relation on the class of all groups.

Theorem

The isomorphism of groups determines an equivalence relation on the class of all groups.

Proof.

The proof is left as an exercise to the reader. □

Theorem

Let $f : G \to H$ be a group isomorphism. Then the following statements hold:

1. *G has generator a if and only if H has generator $\phi(a)$.*
2. *The elements a in G and $\phi(a)$ in H have the same order.*
3. *If G is Abelian, then H is Abelian.*
4. *If G has a subgroup of order n, then H has a subgroup of order n.*

Let G and H be groups. Then G is not isomorphic to H whenever

1. $|G| \neq |H|$,
2. G (H) is Abelian and H (G) is non-Abelian,
3. the largest order of any element in G is not equal to the largest order of any element in H, or
4. the number of elements of some specific order in G is not the same as the number of elements of the same order in H.

1. The groups $\mathbb{Z}_{12}$ and D_{12} are not isomoprhic.
2. The group $\mathbb{Q}$ of rational numbers under addition is not isomorphic to the group $\mathbb{Q}^*$ of nonzero rational numbers under multiplication.

Theorem

Let G be a cyclic group. If the order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$. However, If G has finite order n then G is isomorphic to $(\mathbb{Z}_n, +_n)$.

Theorem

Let G be a cyclic group. If the order of G is infinite, then G is isomorphic to $(\mathbb{Z}, +)$. However, If G has finite order n then G is isomorphic to $(\mathbb{Z}_n, +_n)$.

Proof.

The proof is left as an exercise to the reader. $\square$

1. The groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic.
2. The groups $(\mathbb{Z}_n, +_n)$ and $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \oplus\right)$ are isomorphic.

Theorem

Every group is isomorphic to a group of permutations.

Theorem

Every group is isomorphic to a group of permutations.

Proof.

The proof is left as an exercise to the reader. $\square$

Definition

Let G be a group. The function $\phi : G \to S_G$, where $S_G := \{\lambda_g : g \in G\}$ and $\lambda_g(x) = gx$ for all $x \in G$ is called the **left regular representation** of G. Moreover, the map $\tau : G \to S_G$ given by $\tau(x) = \sigma_{x^{-1}}$ where $\sigma_g = xg$ for all $x \in G$ is called the **right regular representation** of G.

Group Isomorphism

Automorphism

Definition

An isomorphism from a group G onto itself is called an **automorphism** of G.

Theorem

Let G be a group, and a be a fixed element of G. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is an automorphism, called the ***inner automorphism*** *of G induced by a.*

Theorem

Let G be a group, and a be a fixed element of G. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is an automorphism, called the ***inner automorphism*** *of G induced by a.*

Proof.

The proof is left as an exercise to the reader. $\square$

1. The function $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $\phi(a, b) = (b, a)$ is an automorphism of $\mathbb{R}^2$ under componentwise addition.

1. Suppose that $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities of $\phi(x)$?
2. Compute $\text{Aut}(\mathbb{Z}_{10})$.

Theorem

The set $\mathrm{Aut}(G)$ of automorphism of a group G and the set $\mathrm{Inn}(G)$ of inner automorphisms of G are groups under the operation of function composition.

Theorem

The set $\mathrm{Aut}(G)$ of automorphism of a group G and the set $\mathrm{Inn}(G)$ of inner automorphisms of G are groups under the operation of function composition.

Proof.

The proof is left as an exercise to the reader. $\square$

Theorem

For every positive integer n, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.

Theorem

For every positive integer n, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.

Proof.

The proof is left as an exercise to the reader. $\square$

1. Suppose that a group G is isomoprhic to a group H. Show that $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{Aut}(H)$.

Group Isomorphism

Direct Product

Theorem

Let G and H be groups. The set $G \times H$ is a group under the operation

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

*where $g_1, g_2 \in G$ and $h_1, h_2 \in H$. The group is called the **external direct product** of G and H.*

Theorem

Let G and H be groups. The set $G \times H$ is a group under the operation

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

*where $g_1, g_2 \in G$ and $h_1, h_2 \in H$. The group is called the **external direct product** of G and H.*

Corollary

Let $G_1, G_2, \ldots, G_n$ be groups. The set $\prod_{i=1}^{n} G_i$ is a group under the operation

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$$

where $g_i, h_i \in G_i$ for each integer $1 \leq i \leq n$.

Examples

1. The external direct product of a finite number of the group of real numbers under addition.
2. The external direct product of a finite number of $\mathbb{Z}_2$.
3. The external direct product of $U(8)$ and $U(10)$.

Order of External Direct Products

Theorem

Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) is the least common multiple of r and s.

Theorem

Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) is the least common multiple of r and s.

Corollary

Let $(g_1, \ldots, g_n) \in \prod_{i=1}^{n} G_i$. If g_i has finite order r_i in G_i, then the order of $(g_1, \ldots, g_n)$ is the least common multiple of $r_1, \ldots, r_n$.

Theorem

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Theorem

The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Corollary

Let $n_1, \ldots, n_k$ be positive integers. Then

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Corollary

Suppose that $p_1, \ldots, p_k$ are distinct primes. If $m = p_1^{e_1} \cdots p_k^{e_k}$ then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

1. Let G, H, G', and H' be groups such that $G \cong G'$ and $H \cong H'$. Show that $G \times H \cong G' \times H'$.

Let H and K be subgroups of a group G such that

1. $G = HK = \{hk : h \in H, k \in K\}$,
2. $H \cap K = \{e\}$, and
3. $hk = kh$ for all $h \in H$ and $k \in K$.

The group G is called the **internal direct product** of H and K.

Examples

Let $\{H_i : 1 \leq i \leq n\}$ be a collection of n subgroups of a group G such that

1. $G = H_1 \cdots H_k = \{h1 \cdots h_n : h_i \in H_i\}$,
2. $H_i \cap \left(\bigcup_{j \neq i} H_j \right) = \{e\}$, and
3. $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

Theorem

Let G be the internal direct product of subgroups H and K. Then G is isomorphic to $H \times K$.

Theorem

Let G be the internal direct product of subgroups H and K. Then G is isomorphic to $H \times K$.

Theorem

Let G be the internal direct product of subgroups H_i, where $1 \leq i \leq n$ is an integer. Then G is isomorphic to $\prod_{i=1}^{n} H_i$.

Cosets

Cosets

Equivalence Relation on Groups

Theorem

Let H be a subgroup of a group G. The relation $\sim_L$ defined on G where

$$a \sim_L b \text{ if and only if } ab^{-1} \in H$$

is an equivalence relation on G.

Theorem

Let H be a subgroup of a group G. The relation $\sim_L$ defined on G where

$$a \sim_L b \text{ if and only if } ab^{-1} \in H$$

is an equivalence relation on G.

Observe that the equivalence class $[a]$ containing a can be written as

$$\begin{aligned}
[a] &= \{b \in H : b \sim_L a\} = \{b \in H : ba^{-1} \in H\} \\
&= \{b \in H : ba^{-1} = h \text{ for some } h \in H\} \\
&= \{b \in H : b = ha \text{ for some } h \in H\} \\
&= \{ha : h \in H\}.
\end{aligned}$$

Cosets

Definition

Definition

Let H be a subgroup of a group G. The subsets $aH = \{ah : h \in H\}$ and $Ha = \{ha : h \in H\}$ of G are respectively called the **left coset** and **right coset** of H containing $a \in G$. Any element of a coset is called a **representative** of a coset.

1. Consider the subgroup $\{0, 3\}$ of $\mathbb{Z}_6$. Find the following cosets $0H, 1H, 4H, 5H, H1$, and $H2$.
2. Consider the subgroup $H = \{(1), (1\,2\,3), (1\,3\,2)\}$ of S_3. Find all the left and right cosets of K.
3. Consider the subgroup $K = \{(1), (1\,2)\}$ of S_3. Find all the left and right cosets of K.

Lemma

Let H be a subgroup of a group G. Suppose that $g_1, g_2 \in G$. The following conditions are equivalent:

1. $g_1H = g_2H$
2. $Hg_1^{-1} = Hg_2^{-1}$
3. $g_1H \subset g_2H$
4. $g_2 \in g_1H$
5. $g_1^{-1}g_2 \in H$

Theorem

Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.

Definition

Let H be a subgroup of a (possibly infinite) group G. The number of left cosets of H in G is the **index** of H in G, denoted by $(G : H)$.

Lemma

Let H be a subgroup of a group G. The cardinality of H is equal to the cardinality of any left coset gH of H in G.

Theorem

Let H be a subgroup of a finite group G. Then the order of H divides the order of G. In particular,

$$|G| = \frac{(G : H)}{|H|}.$$

Corollary

Every group G of prime order is cyclic. In addition, any element of G is a generator for G.

Corollary

The order of an element in a finite group G divides the order of G.

Corollary

If G is a group of prime order p, then G is cyclic. Specifically, G is isomorphic to $\mathbb{Z}_p$.

Corollary

Let H and K be subgroups of a group G such that $K \leq H \leq G$. Suppose that $(H : K)$ and $(G : H)$ are both finite. Thus, $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$.

1. Suppose that $(G : H) = 2$. If a and b are not in H, then $ab \in H$.
2. If $(G : H) = 2$, then $gH = Hg$.
3. Let H and K be subgroups of a group G. Prove that $gH \cap gK$ is a coset of $H \cap K$ in G.

Normal and Quotient Groups

Normal and Quotient Groups

Normal Subgroup

Definition

Let H be a subgroup of a group G. We say that H is **normal** in G or H is a **normal subgroup** of G if $gH = Hg$ for all $g \in G$. We write $H \trianglelefteq G$ to mean that H is normal in G.

Theorem

For a subgroup H of a group G, the following statements are equivalent:

1. *For all $g \in G$, $gH = Hg$.*
2. *For all $g \in G$ and $h \in H$, $ghg^{-1} \in H$ (or $gHg^{-1} \subset H$).*
3. *For all $g \in G$, we have $gHg^{-1} = H$.*

Theorem

For a subgroup H of a group G, the following statements are equivalent:

1. *For all $g \in G$, $gH = Hg$.*
2. *For all $g \in G$ and $h \in H$, $ghg^{-1} \in H$ (or $gHg^{-1} \subset H$).*
3. *For all $g \in G$, we have $gHg^{-1} = H$.*

Definition (Normal Subgroup (Restated))

Let G be a group. The element ghg^{-1} is called the **conjugate** of $h \in H$ by $g \in G$. The set $gHg^{-1} := \{ghg^{-1} : h \in H\}$ is called the **conjugate** of H by g. The element g is said to **normalize** H if $gHg^{-1} = H$. A subgroup H of G is **normal** in G if every element of G normalizes N.

Normal and Quotient Groups

Quotient Group

Let H be a subgroup of a group G. The **left coset multiplication** is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Theorem

Let H be a normal subgroup of a group G. The cosets of H form a group G/H of order $(G : H)$ under left coset multiplication. This group is called the ***quotient group*** *(or* ***factor group****) of G by H.*

Theorem

If G is a cyclic group and H is a normal subgroup of G, then G/H is cyclic.

Normal and Quotient Groups

Other Groups Related to Normal Subgroups*

Definition

A group is **simple** if it has no proper nontrivial normal subgroups.

Definition

A group is **simple** if it has no proper nontrivial normal subgroups.

Theorem

The alternating group A_n is simple for $n \geq 5$.

Definition

A **maximal normal subgroup** of a group G is a proper normal subgroup M of G such that there exists no other proper normal subgroup N of G containing M.

Theorem

Let M be a subgroup of G. Then M is a maximal normal subgroup of G if and only if G/M is simple.

1. If a group G has exactly one subgroup H or order k then H is normal in G.

Group Homomorphism

Group Homomorphism

Definition and Properties

Definition

Let $(G, *)$ and $(H, \otimes)$ be semigroups. A function $\phi : G \to H$ is a **homomorphism** provided that

$$\phi(a * b) = \phi(a) \otimes \phi(b)$$

holds for all a, b in G. The range of ϕ is sometimes called the **homomorphic image** of ϕ.

Let $\phi : G \to H$ be a homomorphism from a semigroup G into another semigroup H.

- If ϕ is injective as a map of sets, then ϕ is called a **monomorphism**.
- If ϕ is surjective, then ϕ is called an **epimorphism**.
- If ϕ is bijective, then ϕ is called an **isomorphism**.
- If $H = G$, then ϕ is called an **endomorphism** of G.
- If $H = G$ and ϕ is bijective, then ϕ is called an **automorphism** of G.

Theorem

Let ϕ be a homomorphism of a group G with identity e into a group G' with identity e'.

1. *The element $\phi(e)$ is the identity element in G'. That is, $e' = \phi(e)$.*
2. *If $a \in G$, then $\phi(a^{-1}) = [\phi(a)]^{-1}$.*
3. *If H is a subgroup of G, then $\phi(H)$ is a subgroup of G'.*
4. *If H' is a subgroup of G', then $\phi^{-1}(H')$ is a subgroup of G.*

Theorem

Let $\phi : G \to G'$. If H is normal subgroup of G, then $\phi(N)$ is a normal subgroup of G'. Also, if H' is a normal subgroup of $\phi(G)$, then $\phi^{-1}(H')$ is a normal subgroup of G.

Group Homomorphism

Kernel of a Group Homomorphism

Definition

Let $\phi : G \to H$ be a homomorphism of groups. The **kernel** of f, denoted by $\ker(f)$, is defined as

$$\{a \in G : \phi(a) = e'\}$$

where e' is the identity element for H.

Theorem

Let $\phi : G \to G'$ be a group homomorphism. Then the left and right cosets of $\ker(\phi)$ are identical. Furthermore, the elements a and b in G are in the same coset of $\ker(\phi)$ if and only if $\phi(a) = \phi(b)$.

Theorem

Let $\phi : G \to H$ be a homomorphism of groups,

1. *The function ϕ is a monomorphism if and only if the kernel of f is trivial.*
2. *The function ϕ is an isomorphism if and only if there exists a homomorphism $\delta : H \to G$ such that the compositions $\phi\delta$ and $\delta\phi$ are equal to the appropriate identity functions.*

Theorem

Let $\phi : G \to H$ be a group homomorphism. Then the kernel of ϕ is a normal subgroup of G.

Theorem

Let $\phi : G \to H$ be a group homomorphism. Then the kernel of ϕ is a normal subgroup of G.

Theorem

Let H be a subgroup of a group G. Then H is a normal subgroup of G if and only if there exists a group homomorphism $\phi : G \to H$ such that $\ker(\phi) = H$.

Theorem

*Let H be a normal subgroup of a group G. Then $\phi : G \to {}^{G}/_{H}$ given by $\phi(x) = xH$ is a homomorphism with kernel H. The function ϕ is called the **natural projection** of G onto ${}^{G}/_{H}$. It is also called the **canonical homomorphism**.*

Theorem

Let $\phi : G \to H$ be a group homomorphism with kernel K. If $\gamma : G \to G/K$ is the canonical homomorphism, then there exists a unique isomorphism $\mu : G/K \to \phi(G)$ such that $\phi = \mu \circ \gamma$.

A **commutative diagram** is a collection of mappings where all compositi starting from the same set and ending with the same set lead to the same result.

Theorem

Let H be a subgroup of G, and N be a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

Theorem

Let N and H be normal subgroups of G where $N \subset H$. Then

$$\frac{G}{H} \cong \frac{G/N}{H/N}.$$

Theorem

Let N be a normal subgroup of a group G. Then there is a bijection from the set of subgroups H of G containing N onto the set of subgroups of G/N such that, for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

1. *$A \leq B$ if and only if $A/N \leq B/N$,*
2. *if $A \leq B$ then $(B : A) = (B/N : A/N)$,*
3. *$(A \cap B)/N = A/N \cap B/N$, and*
4. *$A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.*

Theorem

Let $G = H \times K$ be the external direct product of groups H and K. Then $\overline{H} = \{(h, e) : h \in H\}$ is a normal in G. Moreover, $G/\overline{H}$ is isomorphic to K in a natural way. Analogously, $G/\overline{K}$ is isomorphic to H in a natural way.

Structure of Groups

Goal of Group Theory

The ultimate goal of group theory is to classify all groups up to isomorphism; that is, given a particular group, we should be able to match it up with a known group via an isomorphism.

Definition

Let $\{g_i\}$ be a collection of elements of a group G. The smallest subgroup containing each g_i is the **subgroup of G generated by the g_i's**. In this case, the g_i's are the **generators** for G. Furthermore, if $\{g_i\}$ is a finite set that generates G, then G is **finitely generated**.

Theorem

Let H be a subgroup of a group G that is generated by $\{g_i\}$. Then $h \in H$ when it is a product of the form

$$h = g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$$

where the g_{i_k}'s are not necessarily distinct.

Definition

Let p be a prime number. A group G is a ***p*-group** if every element in G has as its order a power of p.

Theorem

Every finite Abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1}^{\alpha_1} \times \mathbb{Z}_{p_2}^{\alpha_2} \times \cdots \times \mathbb{Z}_{p_n}^{\alpha_n}$$

where each p_i are primes (not necessarily distinct).

Lemma

Let G be a finite Abelian group of order n. If p is a prime that divides n, then G contains an element of order p.

Lemma

Let G be a finite Abelian group of order n. If p is a prime that divides n, then G contains an element of order p.

Lemma

A finite Abelian group is a p-group if and only if its order is a power of p.

Lemma

Let G be a finite Abelian group of order n. If p is a prime that divides n, then G contains an element of order p.

Lemma

A finite Abelian group is a p-group if and only if its order is a power of p.

Lemma

Let G be a finite Abelian group of order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where each p_i is prime and each α_i is a positive integer. Then G is the internal direct product of subgroups $G_1, G_2, \ldots, G_k$, where G_i is the subgroup of G consisting of all elements of order p_i^r for some integer r.

Lemma

Let G be a finite Abelian p-group and suppose that $g \in G$ has maximal order. Then G is isomorphic to $\langle g \rangle \times H$ for some subgroup H of G.

Lemma

Let G be a finite Abelian p-group and suppose that $g \in G$ has maximal order. Then G is isomorphic to $\langle g \rangle \times H$ for some subgroup H of G.

Theorem

Every finitely generated Abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1}^{\alpha_1} \times \mathbb{Z}_{p_2}^{\alpha_2} \times \cdots \times \mathbb{Z}_{p_n}^{\alpha_n} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where each p_i are primes (not necessarily distinct).

Frame Title

Definition

A **subnormal series** of a group G is a finite sequence of subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

where H_i is a normal subgroup of H_{i+1}. If each subgroup H_i is normal in G, then the series is called a **normal series**. The **length** of a subnormal or normal series is the number of proper inclusions.

Definition

A **subnormal series** of a group G is a finite sequence of subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

where H_i is a normal subgroup of H_{i+1}. If each subgroup H_i is normal in G, then the series is called a **normal series**. The **length** of a subnormal or normal series is the number of proper inclusions.

Definition

A subnormal series $\{K_j\}$ is a **refinement of a subnormal series** $\{H_i\}$ if $\{H_i\} \subset \{K_j\}$.

Definition

Two subnormal series $\{H_i\}$ and $\{K_j\}$ of a group G are **isomorphic** if there is a bijection between the collection of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$.

Definition

Two subnormal series $\{H_i\}$ and $\{K_j\}$ of a group G are **isomorphic** if there is a bijection between the collection of factor groups $\{{}^{H_{i+1}}/_{H_i}\}$ and $\{{}^{K_{j+1}}/_{K_j}\}$.

Definition

A subnormal series of a group is a **composition series** if all the factor groups are simple. A normal series of a group is a **principal series** if all the factor groups are simple.

Theorem

Any two composition series of G are isomorphic.

Theorem

Any two composition series of G are isomorphic.

Definition

A group is **solvable** if it has a subnormal series $\{H_i\}$ such that all the factor groups H_{i+1}/H_i are Abelian.

Group Action on a Set

Definition

Let X be a set and G be a group. A **(left) action** of G on X is a map $G \times X \to X$ given by $(g, x) \to gx$, where

1. $ex = x$ for all $x \in X$, and
2. $(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and $g_1, g_2 \in G$.

The set X is called a ***G*-set**.

Definition

If G acts on a set X and $x, y \in X$, then x is said to be ***G*-equivalent** to y if there exists $g \in G$ such that $gx = y$. We write $x \sim_G$ or $x \sim y$ if two elements are G-equivalent.

Theorem

Let X be a G-set. Then G-equivalence is an equivalence relation on X.

Definition

Suppose that G is a group acting on a set X. Let $g \in G$. The **fixed point set** of g in X, denoted by X_g, is the set of all $x \in X$ such that $gx = x$. The **stabilizer subgroup** or **isotropy subgroup** of $x \in X$ consists of all group elements g such that $gx = x$.

Frame Title

Theorem

Let G be a group acting on a set X and $x \in X$. The stabilizer subgroup of x is a subgroup of G.

Theorem

Let G be a group acting on a set X and $x \in X$. The stabilizer subgroup of x is a subgroup of G.

Theorem

Let G be a finite group and X be a finite G-set. If $x \in X$, then $|\mathcal{O}_x| = (G : G_x)$.

Let X be a finite G-set and X_G be the set of fixed points in X; that is

$$X_G = \{x \in X : gx = x \text{ for all } g \in G\}.$$

Since the orbits of the action partition X,

$$|X| = |X_G| + \sum_{i=k}^{n} |\mathcal{O}_{x_i}|$$

where $x_k, \ldots, x_n$ are representatives from the distinct nontrivial orbits of X.

Consider the case in which G acts on itself by conjugation, $(g, x) \to gxg^{-1}$. The **center** of G is the set

$$Z(G) = \{x : xg = gx \text{ for all } g \in G\}$$

of points that are fixed by conjugation. The nontrivial orbits of the action are called **conjugacy classes** of G. If $x_1, \ldots, x_k$ are representatives from each of the nontrivial conjugacy classes of G and $|\mathcal{O}_{x_i}| = n_i$, then

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

The stabilizer subgroups of each x_i,

$$C(x_i) = \{g \in G : gx_i = x_i g\}$$

are called **centralizer subgroups** of the x_i's. Thus, we obtain the **class equation** given by

$$|G| = |Z(G)| + (G : C(x_1)) + \cdots + (G : C(x_k)).$$

Frame Title

Theorem

Let G be a group of order p^n where p is prime. Then G has a nontrivial center.

Theorem

Let G be a group of order p^n where p is prime. Then G has a nontrivial center.

Corollary

Let G be a group of order p^2 where p is prime. Then G is Abelian.

Lemma

Let X be a G-set and suppose that $x \sim y$. Then G_x is isomorphic to G_y. In particular, $|G_x| = |G_y|$.

Theorem

Let G be a finite group acting on a set X. Suppose that k is the number of orbits of X. Then

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Theorem

Let G be a permutation group of X and $\tilde{X}$ be the set of functions from X to Y. Then G induces a group $\tilde{G}$ that permutes the elements of $\tilde{X}$, where $\tilde{\sigma} \in \tilde{G}$ is defined by $\tilde{\sigma} = f \circ \sigma$ for $\sigma \in G$ and $f \in \tilde{X}$. Furthermore, if n is the number of cycles in the cycle decomposition of σ, then $|X_\sigma| = |Y|^n$.

Sylow Theorems

Definition

A group G is a ***p*-group** if every element in G has its order a power of a prime number p. A subgroup of a group G is a ***p*-subgroup** if it is a p-group.

Frame Title

Theorem

Let G be a finite group and p be a prime such that p divides the order of G. Then G contains a subgroup of order p.

Theorem

Let G be a finite group and p be a prime such that p divides the order of G. Then G contains a subgroup of order p.

Corollary

Let G be a finite group. Then G is a p-group if and only if $|G| = p^n$.

First Sylow Theorem

Theorem

Let G be a finite group and p be a prime such that p^r divides $|G|$. Then G contains a subgroup of order p^r.

Definition

A **Sylow p-subgroup** of a group G is a maximal p-subgroup of G.

Definition

The set $N(H) = \{g \in G : gHg^{-1} = H\}$ is a subgroup of G called the **normalizer** of H in G.

Frame Title

Lemma

Let P be a Sylow p-subgroup of a finite group G. Suppose that the order of x is a power of p. If $x^{-1}Px = P$, then $x \in P$.

Lemma

Let P be a Sylow p-subgroup of a finite group G. Suppose that the order of x is a power of p. If $x^{-1}Px = P$, then $x \in P$.

Lemma

Let H and K be subgroups of G. The number of distinct H-conjugates of K is $(H : N(K) \cap K)$.

Second Sylow Theorem

Theorem

Let G be a finite group and p be a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.

Theorem

Let G be a finite group and p be a prime dividing $|G|$. Then the number of Sylow p-subgroups is congruent to 1 modulo p and divides $|G|$.

Frame Title

Theorem

If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence, G cannot be simple. Furthermore, if q is not congruent to 1 modulo p, then G is cyclic.

Theorem

Let $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ be the subgroup consisting of all finite products of elements of the form $aba^{-1}b^{-1}$ in a group G. Then G' is a normal subgroup of G and ${}^{G}/_{G'}$ is Abelian.

The subgroup G' of G is called the **commutator subgroup** of G.

Lemma

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Theorem

Every finite simple group of nonprime order must be of even order.

Thank You!

Bibliography I