Introduction to Group Theory

Jianing Huang, Sylvia Lee

MIT PRIMES Circle

May 18, 2025

How Can We Understand the Symmetry of this Shape?

What is the set of all the symmetries of this square, and how can they be composed?

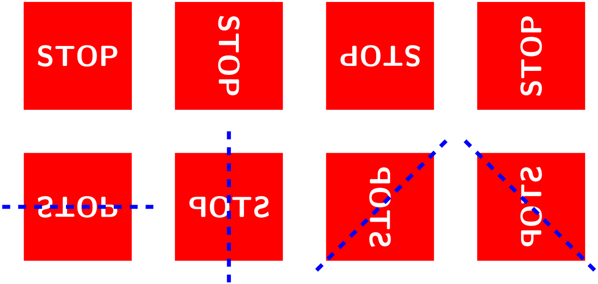


Figure: A beautiful red square

Definition of Groups

Definition

A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

Definition of Groups

Definition

A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

1. *Closure*. For all elements $a, b \in G$, $ab \in G$.

Definition of Groups

Definition

A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

1. *Closure*. For all elements $a, b \in G$, $ab \in G$.
2. *Associativity*. $(ab)c = a(bc)$ for all $a, b, c \in G$.

Definition of Groups

Definition

A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

1. *Closure*. For all elements $a, b \in G$, $ab \in G$.
2. *Associativity*. $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. *Identity*. There exists an identity $e \in G$ such that $ae = ea = a$.

Definition of Groups

Definition

A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

1. *Closure*. For all elements $a, b \in G$, $ab \in G$.
2. *Associativity*. $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. *Identity*. There exists an identity $e \in G$ such that $ae = ea = a$.
4. *Inverse*. For all $a \in G$, there is an element $b \in G$ such that $ab = ba = e$. b is the inverse of a, denoted $b = a^{-1}$.

Definition of Order

Definition

The **order of a group** G, denoted $|G|$, is the number of elements in G.

Definition of Order

Definition

The **order of a group** G, denoted $|G|$, is the number of elements in G.

Definition

The **order of an element** a, denoted $|a|$, is the smallest positive integer n such that $a^n = e$.

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

- Closure: The sum of two integers is always an integer.

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

- Closure: The sum of two integers is always an integer.
- Associativity: Addition is associative.

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

- Closure: The sum of two integers is always an integer.
- Associativity: Addition is associative.
- Identity: 0

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

- Closure: The sum of two integers is always an integer.
- Associativity: Addition is associative.
- Identity: 0
- Inverse: $n^{-1} = -n$

Examples of Groups

Examples

The set of integers $\mathbb{Z}$ under addition.

- Closure: The sum of two integers is always an integer.
- Associativity: Addition is associative.
- Identity: 0
- Inverse: $n^{-1} = -n$

The group $\mathbb{Z}$ has infinite order.

Examples of Groups

Examples

The dihedral group D_4 is the set of all symmetries of a square $\{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$ with composition as the operation.

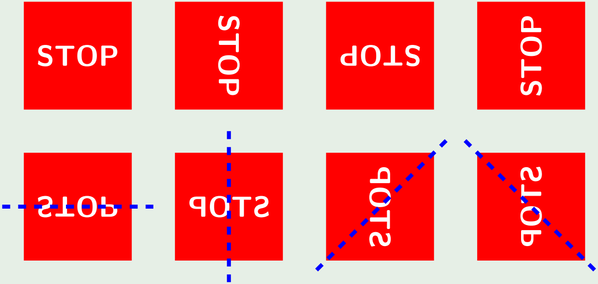


Figure: D_4 has order 8.

Examples of Groups

Examples

The dihedral group D_4 is the set of all symmetries of a square $\{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$ with composition as the operation.

- Closure: The composition of any two transformations always results in another transformation that preserves the square's shape.

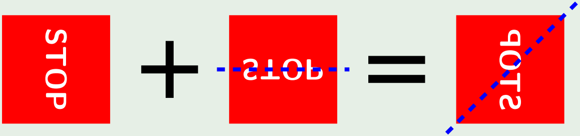


Figure: $R_{90} + H = D_1$.

Examples

- Associativity: Composition is associative.

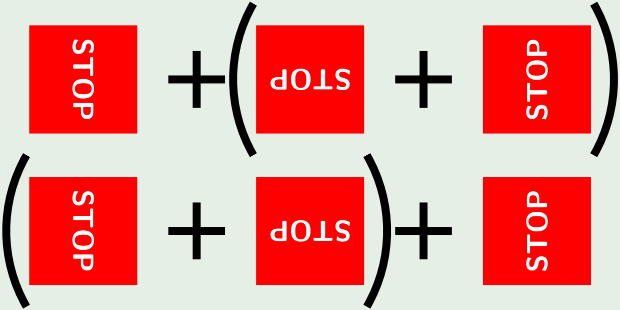


Figure: $R_{90} + (R_{180} + R_{270}) = (R_{90} + R_{180}) + R_{270} = I$.

Examples of Groups

Examples

- Identity: The identity I is the original, untransformed square.

Figure: The "do nothing" operation.

Examples of Groups

Examples

- Identity: The identity I is the original, untransformed square.

Figure: The “do nothing” operation.

- Inverse: Each transformation can be “undone” by the opposite transformation.

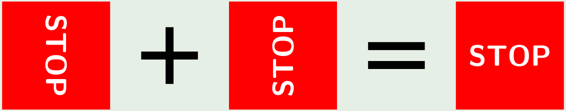


Figure: $R_{90} + R_{270} = I$, so $(R_{90})^{-1} = R_{270}$.

Definition of Subgroups

Definition

A subgroup H of a group G is a group such that all elements of H are also elements of G, and the operation is the same.

Definition of Subgroups

Definition

A subgroup H of a group G is a group such that all elements of H are also elements of G, and the operation is the same.

Example

The set of rotations $\{I, R_{90}, R_{180}, R_{270}\}$ in the group of transformations $D_4 = \{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$ on a square is a subgroup, where the operation is composition.

Definition of Subgroups

Definition

A subgroup H of a group G is a group such that all elements of H are also elements of G, and the operation is the same.

Example

The set of rotations $\{I, R_{90}, R_{180}, R_{270}\}$ in the group of transformations $D_4 = \{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$ on a square is a subgroup, where the operation is composition.

Example

The set $\{1, 2, 4\}$ under multiplication is a subgroup of $\mathbb{Z}/7\mathbb{Z}^{\times} = \{1, 2, 3, 4, 5, 6\}$.

Definition of Cyclic Groups

Definition

A group G is **cyclic** if $G = \{a^n \mid a \in G, n \in \mathbb{Z}\}$, i.e. the powers of one element a in G covers the whole group. We can denote this as $G = \langle a \rangle$, where element a is a **generator** of G.

Definition of Cyclic Groups

Definition

A group G is **cyclic** if $G = \{a^n \mid a \in G, n \in \mathbb{Z}\}$, i.e. the powers of one element a in G covers the whole group. We can denote this as $G = \langle a \rangle$, where element a is a **generator** of G.

Example

The integers $\mathbb{Z}$ under addition is an infinite cyclic group $\mathbb{Z} = \langle 1 \rangle$. Negative integers can be generated by the element $1^{-1} = -1$. The order of $\mathbb{Z}$ is infinite.

Examples of Cyclic Groups

Example

The set of nonzero remainders mod 7, $\mathbb{Z}/7\mathbb{Z}^{\times}$, is the cyclic group $\langle 3 \rangle$ with generator 3.

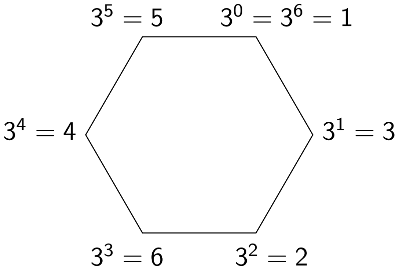


Figure: All nonzero remainders mod 7 are generated by every set of six consecutive powers of 3.

Main Theorem

Theorem (Fundamental Theorem of Cyclic Groups)

Let G be a finite cyclic group $\langle a \rangle$ with order n, then every subgroup H of G must satisfy the following:

1. *H is also cyclic. Specifically, $H = \langle a^m \rangle$.*
2. *$|H|$ is a divisor of n. In particular, if $H = \langle a^m \rangle$, then $|H| = \frac{n}{m}$.*
3. *If the order of H is known, then H is unique.*

Statement 1 - Subgroup of Cyclic Group is Cyclic

Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.

Statement 1 - Subgroup of Cyclic Group is Cyclic

Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.
Consider any element $b \in H$. Since $H \subseteq G$, $b = a^k$ for some k.

Statement 1 - Subgroup of Cyclic Group is Cyclic

Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.
Consider any element $b \in H$. Since $H \subseteq G$, $b = a^k$ for some k.
Express $k = mq + r$, where $r < m$.

Statement 1 - Subgroup of Cyclic Group is Cyclic

Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.
Consider any element $b \in H$. Since $H \subseteq G$, $b = a^k$ for some k.
Express $k = mq + r$, where $r < m$. Then $a^k = a^r \cdot a^{mq}$. By closure $a^r \in H$.

Statement 1 - Subgroup of Cyclic Group is Cyclic

Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.
Consider any element $b \in H$. Since $H \subseteq G$, $b = a^k$ for some k.
Express $k = mq + r$, where $r < m$. Then $a^k = a^r \cdot a^{mq}$. By closure $a^r \in H$.
Wait! m was the smallest positive number such that $a^m \in H$.
Thus, $r = 0$ and $k = mq$.

Statement 1 - Subgroup of Cyclic Group is Cyclic

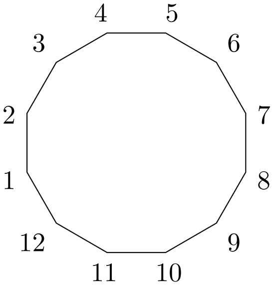
Proof.

Let $G = \langle a \rangle$, then H must contain some power of a.
Let m be the smallest such non-zero power.
Consider any element $b \in H$. Since $H \subseteq G$, $b = a^k$ for some k.
Express $k = mq + r$, where $r < m$. Then $a^k = a^r \cdot a^{mq}$. By closure $a^r \in H$.
Wait! m was the smallest positive number such that $a^m \in H$.
Thus, $r = 0$ and $k = mq$.
So for all $b \in H$, $b = a^k = a^{mq} = (a^m)^q$ for some q.
i.e. all elements in H is a power of a^m, so $H = \langle a^m \rangle$. $\square$

Theorem in Application - D_{12}

Example

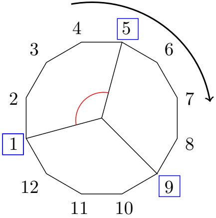
Consider a regular dodecagon (12 sides) and its dihedral group D_{12}, which includes all potential transformations, where the subgroup of rotations is a cyclic group of order 12, let's call this G.



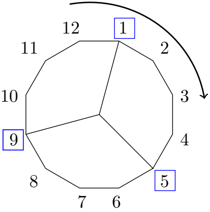
Theorem in Application - D_{12}

Example

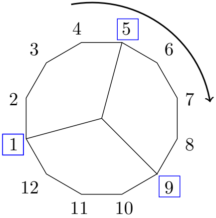
Can you find a subgroup of G with order 3? Let's verify that it is also cyclic, and that it is unique.



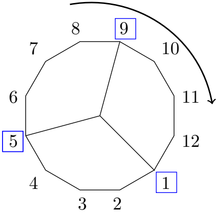
I



R_{120}



$I = (R_{120})^3$



$R_{240} = (R_{120})^2$

This is the cyclic subgroup $\langle R_{120} \rangle$. Note that R_{240} would generate the same group. $R_{120} = (R_{30})^4$, where R_{30} is the generator of the whole group, and $4 = 12 \div 3$.

Theorem in Application - D_{12}

Example

Can you find a subgroup of G with order 5?

Theorem in Application - D_{12}

Example

Can you find a subgroup of G with order 5?

The answer is no!

Theorem in Application - D_{12}

Example

Can you find a subgroup of G with order 5?

The answer is no!
Since 5 is not a divisor of 12, you cannot find a subgroup with order 5 in a cyclic group with order 12, as shown by the Fundamental theorem.

Works Cited

Gallian, Joseph A. Contemporary Abstract Algebra. Brooks/Cole, 2010.

Robertson, Edmund, and John J. O'Connor. "Abstract Groups." MacTutor History of Mathematics Archive, University of St. Adrews.

Kleiner, Israel. A History of Abstract Algebra, 2007.

Credits

Thank you to the PRIMES CIRCLE program and to our mentor June Kayath for providing us with this opportunity!
Thank you all for listening!