A Brief Survey of Key Topics in Group Theory

Angela Zhao, Sophie Strey, Niva Sethi

May 2023

1. Basics of Group Theory
   - Definitions
   - What is a group?
   - Isomorphisms and Homomorphisms
   - Commutativity
   - Order of a Group
   - Order of an Element

2. Symmetry

3. Subgroups, Groups, and Cosets

4. Applications

Before introducing groups, we must first understand binary operations.

Definition (Binary Operation)

If G is a nonempty set, a binary operation μ on G is a function $\mu : G \times G \to G$.

Definition (Associativity)

A binary operation $*$ on set G is associative if

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

for all $a, b, c \in G$.

Before introducing groups, we must first understand binary operations.

Definition (Binary Operation)

If G is a nonempty set, a binary operation μ on G is a function $\mu : G \times G \to G$.

Definition (Associativity)

A binary operation $*$ on set G is associative if

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

for all $a, b, c \in G$.

Before introducing groups, we must first understand binary operations.

Definition (Binary Operation)

If G is a nonempty set, a binary operation μ on G is a function $\mu : G \times G \to G$.

Definition (Associativity)

A binary operation $*$ on set G is associative if

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

for all $a, b, c \in G$.

Examples of Binary Operations

1. Division on the set of integers is not a binary operation, but addition, multiplication, and subtraction are.
2. Matrix multiplication.
3. Function composition.

Examples of Binary Operations

1. Division on the set of integers is not a binary operation, but addition, multiplication, and subtraction are.
2. Matrix multiplication.
3. Function composition.

Examples of Binary Operations

1. Division on the set of integers is not a binary operation, but addition, multiplication, and subtraction are.
2. Matrix multiplication.
3. Function composition.

Definition (Group)

A group $(G, *)$ is a set G with binary operation $* : G \times G \to G$ that satisfies:

1. *Closure:* $g * h \in G$. We say that G is closed under $*$.
2. *Associativity:* for any $g, h, i \in G$ we have $(g * h) * i = g * (h * i)$.
3. *Identity:* $e * g = g * e = g$ for all $g \in G$.
4. *Inverse:* Every element $g \in G$ has an inverse g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Examples

Some examples include:

1. The integers under addition, subtraction, and multiplication.
2. The set $GL_2(\mathbb{R})$ of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation.
3. Function composition.

Examples

Some examples include:

1. The integers under addition, subtraction, and multiplication.
2. The set $GL_2(\mathbb{R})$ of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation.
3. Function composition.

Examples

Some examples include:

1. The integers under addition, subtraction, and multiplication.
2. The set $GL_2(\mathbb{R})$ of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation.
3. Function composition.

Obervations

- The identity element has to be unique.
- The inverse is unique.
- The inverse of the inverse is unique.

Obervations

- The identity element has to be unique.
- The inverse is unique.
- The inverse of the inverse is unique.

Obervations

- The identity element has to be unique.
- The inverse is unique.
- The inverse of the inverse is unique.

Proof that the Identity is Unique

Proof.

Let there be group G such that $a \in G$ and e_1 and e_2 are both identity elements of G. Then:

$$a^{-1} * a = e_1$$

$$a^{-1} * a = e_2$$

$$e_1 = a^{-1} * a = e_2$$

$$e_1 = e_2$$

$\square$

Isomorphisms

Definition (Isomorphism)

Two groups $(G, *)$ and $(H, \circ)$ are said to be isomorphic if there is a one-to-one correspondence $\theta : H \to G$ such that

$$\theta(g_1 * g_2) = \theta(g_1) \circ \theta(g_2)$$

for all $g_1, g_2 \in G$. The mapping θ is called an isomorphism and we say that G is isomorphic to H (written as $G \cong H$).

Homomorphisms

Definition (Homomorphism)

If θ satisfies the previously mentioned property but is not a one-to-one correspondence, we say θ is homomorphism.

Definition (Commute)

If G is a group and $g, h \in G$, if $gh = hg$ we say that g and h commute.

Definition (Abelian)

$g * h = h * g$ for all $g, h \in G$, then we say G is an abelian group. Some examples include:

- The group of integers under addition.
- Every cyclic group (we will learn about these a bit later).

Definition (Commute)

If G is a group and $g, h \in G$, if $gh = hg$ we say that g and h commute.

Definition (Abelian)

$g * h = h * g$ for all $g, h \in G$, then we say G is an abelian group. Some examples include:

- The group of integers under addition.
- Every cyclic group (we will learn about these a bit later).

Definition (Commute)

If G is a group and $g, h \in G$, if $gh = hg$ we say that g and h commute.

Definition (Abelian)

$g * h = h * g$ for all $g, h \in G$, then we say G is an abelian group. Some examples include:

- The group of integers under addition.
- Every cyclic group (we will learn about these a bit later).

Definition (Commute)

If G is a group and $g, h \in G$, if $gh = hg$ we say that g and h commute.

Definition (Abelian)

$g * h = h * g$ for all $g, h \in G$, then we say G is an abelian group. Some examples include:

- The group of integers under addition.
- Every cyclic group (we will learn about these a bit later).

1. Basics of Group Theory
   - Definitions
   - What is a group?
   - Isomorphisms and Homomorphisms
   - Commutativity
   - Order of a Group
   - Order of an Element
2. Symmetry
3. Subgroups, Groups, and Cosets
4. Applications

Definition (Finite Group)

A finite group is one with only a finite number of elements.

Definition (Order of a Group)

The order of a finite group, written $|G|$, is the number of elements in G.

Definition (Finite Group)

A finite group is one with only a finite number of elements.

Definition (Order of a Group)

The order of a finite group, written $|G|$, is the number of elements in G.

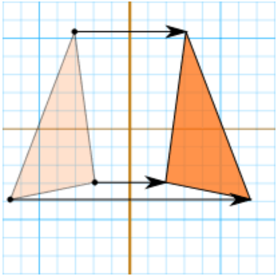
Order of an Element

Definition (Order of an Element)

The order of an element $g \in G$, written as $o(g)$, is the smallest natural number n, such that $g^n = e$. If no n exists we say the element has an infinite order.

Definition (Symmetry)

A symmetry is a transformation of a figure under which the figure is invariant.

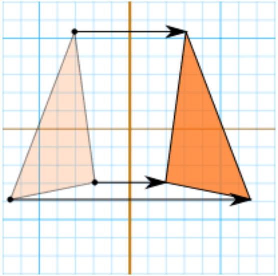


Definition (Symmetry group)

A symmetry group G is a set of all symmetries of a shape under the binary operation of composition of transformations.

Definition (Symmetry)

A symmetry is a transformation of a figure under which the figure is invariant.

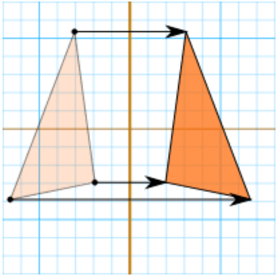


Definition (Symmetry group)

A symmetry group G is a set of all symmetries of a shape under the binary operation of composition of transformations.

Definition (Symmetry)

A symmetry is a transformation of a figure under which the figure is invariant.



Definition (Symmetry group)

A symmetry group G is a set of all symmetries of a shape under the binary operation of composition of transformations.

Proof of the 5th Quadratic

Theorem (Abel-Ruffini Theorem)

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

- Uses roots of unity
- Requires proof that the symmetric group of the 5th polynomial is not solvable and that there are polynomials with symmetric Galois groups.

$$P(x) = x^n + b_1 x^{n-1} + b_{n-1}x + b_n = (x - x_1)\cdots(x - x_n)$$

Proof of the 5th Quadratic

Theorem (Abel-Ruffini Theorem)

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

- Uses roots of unity
- Requires proof that the symmetric group of the 5th polynomial is not solvable and that there are polynomials with symmetric Galois groups.

$$P(x) = x^n + b_1 x^{n-1} + b_{n-1} x + b_n = (x - x_1) \cdots (x - x_n)$$

Proof of the 5th Quadratic

Theorem (Abel-Ruffini Theorem)

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

- Uses roots of unity
- Requires proof that the symmetric group of the 5th polynomial is not solvable and that there are polynomials with symmetric Galois groups.

$$P(x) = x^n + b_1 x^{n-1} + b_{n-1} x + b_n = (x - x_1) \cdots (x - x_n)$$

Proof of the 5th Quadratic

Theorem (Abel-Ruffini Theorem)

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

- Uses roots of unity
- Requires proof that the symmetric group of the 5th polynomial is not solvable and that there are polynomials with symmetric Galois groups.

$$P(x) = x^n + b_1 x^{n-1} + b_{n-1} x + b_n = (x - x_1) \cdots (x - x_n)$$

Wallpaper Groups

Definition (Fundamental Region, Wallpaper group)

A Fundamental Region is a pattern or region that repeats in many directions.
A Wallpaper Group is the group of symmetries of a fundamental region, under the binary operation of composition.

Wallpaper groups include rotations, reflections, translations, and glide reflections. With these transformations, there are 17 possible wallpaper groups in $\mathbb{R}^2$

Wallpaper Groups

Definition (Fundamental Region, Wallpaper group)

A Fundamental Region is a pattern or region that repeats in many directions.
A Wallpaper Group is the group of symmetries of a fundamental region, under the binary operation of composition.

Wallpaper groups include rotations, reflections, translations, and glide reflections. With these transformations, there are 17 possible wallpaper groups in $\mathbb{R}^2$

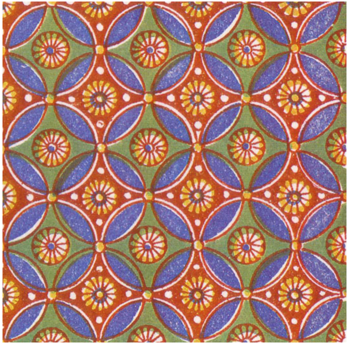
Wallpaper Groups

Definition (Fundamental Region, Wallpaper group)

A Fundamental Region is a pattern or region that repeats in many directions.
A Wallpaper Group is the group of symmetries of a fundamental region, under the binary operation of composition.

Wallpaper groups include rotations, reflections, translations, and glide reflections. With these transformations, there are 17 possible wallpaper groups in $\mathbb{R}^2$

Wallpaper Group Example



Definition (Subgroup, Proper Subgroup)

A subset $H \subseteq G$ is a subgroup of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G. If also $H \neq G$, we say that H is a proper subgroup and write $H < G$.

Definition (Subgroup, Proper Subgroup)

A subset $H \subseteq G$ is a subgroup of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G. If also $H \neq G$, we say that H is a proper subgroup and write $H < G$.

Definition (Subgroup, Proper Subgroup)

A subset $H \subseteq G$ is a subgroup of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G. If also $H \neq G$, we say that H is a proper subgroup and write $H < G$.

Definition (Subgroup, Proper Subgroup)

A subset $H \subseteq G$ is a subgroup of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G. If also $H \neq G$, we say that H is a proper subgroup and write $H < G$.

Definition (Subgroup, Proper Subgroup)

A subset $H \subseteq G$ is a subgroup of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

We write $H \leq G$ if H is a subgroup of G. If also $H \neq G$, we say that H is a proper subgroup and write $H < G$.

Lattices of subgroups

Definition (Lattice)

The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of "visualizing" a group.

Lattices of subgroups

Definition (Lattice)

The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of "visualizing" a group.

Lattices of subgroups

Definition (Lattice)

The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of “visualizing” a group.

Lattices of subgroups

Definition (Lattice)

The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of "visualizing" a group.

Lattices of subgroups

Definition (Lattice)

The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of "visualizing" a group.

Lattices of subgroups

Definition (Lattice)

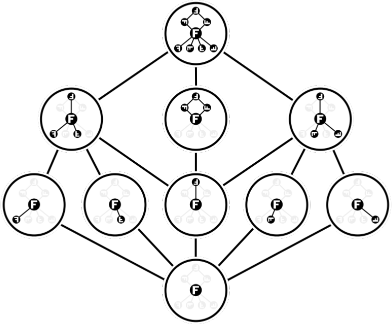
The lattice of subgroups of a group G is the graph where subgroups are nodes.
To construct the lattices of a finite subgroup:

- Plot subgroups starting at the bottom of the lattice with identity subgroup $\{1\}$.
- Plot subgroups of larger order progressively higher in the lattice.
- End at the top of the lattice with G.
- Draw a line upwards from A to B if $A \leq B$ and no subgroups exist properly between A and B.

Lattices of subgroups are a good way of “visualizing” a group.

Lattices of subgroups

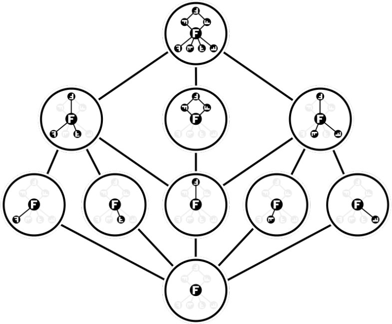
The Dihedral group of order 4 has ten subgroups:



This group has five subgroups of order 2 and three subgroups of order 4, including a cyclic subgroup and two subgroups of form $Z_2 \times Z_2$

Lattices of subgroups

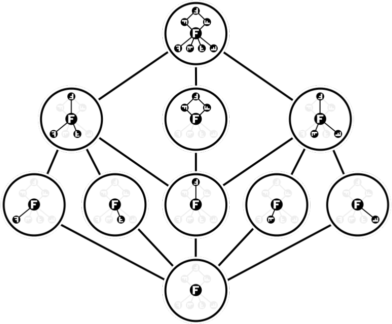
The Dihedral group of order 4 has ten subgroups:



This group has five subgroups of order 2 and three subgroups of order 4, including a cyclic subgroup and two subgroups of form $Z_2 \times Z_2$

Lattices of subgroups

The Dihedral group of order 4 has ten subgroups:



This group has five subgroups of order 2 and three subgroups of order 4, including a cyclic subgroup and two subgroups of form Z_2 x Z_2

Cyclic Groups

Definition (Cyclic)

A group H is cyclic if it can be generated by a single element, i.e, there is some element $x \in H$ such that

$$H = \{x^n | n \in \mathbb{Z}\},$$

where as usual the operation is multiplication.

If using additive notation, H is cyclic if it can be written as

$$H = \{nx | n \in \mathbb{Z}\}.$$

Cyclic Groups

Definition (Cyclic)

A group H is cyclic if it can be generated by a single element, i.e, there is some element $x \in H$ such that

$$H = \{x^n | n \in \mathbb{Z}\},$$

where as usual the operation is multiplication.

If using additive notation, H is cyclic if it can be written as

$$H = \{nx | n \in \mathbb{Z}\}.$$

Cyclic Groups

We denote the fact that H is generated by x as:

$$H = \langle x \rangle$$

A cyclic group can have more than one generator.

Example

We can also write $H = \langle x^{-1} \rangle$ since both n and $-n$ run over all integers and

$$(x^{-1})^n = x^{-n}$$

$$\implies \{x^n | n \in \mathbb{Z}\} = \{(x^{-1})^n | n \in \mathbb{Z}\}$$

Cyclic Groups

We denote the fact that H is generated by x as:

$$H = \langle x \rangle$$

A cyclic group can have more than one generator.

Example

We can also write $H = \langle x^{-1} \rangle$ since both n and $-n$ run over all integers and

$$(x^{-1})^n = x^{-n}$$

$$\implies \{x^n | n \in \mathbb{Z}\} = \{(x^{-1})^n | n \in \mathbb{Z}\}$$

Cyclic Groups

We denote the fact that H is generated by x as:

$$H = \langle x \rangle$$

A cyclic group can have more than one generator.

Example

We can also write $H = \langle x^{-1} \rangle$ since both n and $-n$ run over all integers and

$$(x^{-1})^n = x^{-n}$$

$$\implies \{x^n | n \in \mathbb{Z}\} = \{(x^{-1})^n | n \in \mathbb{Z}\}$$

Order of Cyclic Groups

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$.

- *if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H.*
- *if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

Order of Cyclic Groups

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$.

- *if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H.*
- *if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

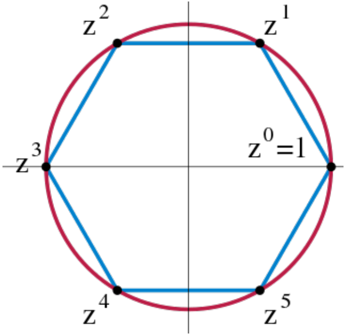
Order of Cyclic Groups

Proposition

If $H = \langle x \rangle$, then $|H| = |x|$.

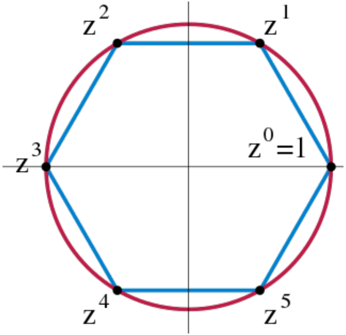
- *if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, ..., x^{n-1}$ are all distinct elements of H.*
- *if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

Cyclic Groups Example



This is a cyclic group under multiplication. Note that z is a generator but z^2 is not.

Cyclic Groups Example



This is a cyclic group under multiplication. Note that z is a generator but z^2 is not.

Dihedral Groups

Definition (dihedral)

A dihedral group is the group of symmetries of a regular polygon.
This includes rotations and reflections.

For a n-gon, the algebraic way of representing this group is D_{2n} and the geometric way is D_n.

Dihedral groups play an important role within and outside of group theory. They are one of the simplest finite groups.

Dihedral Groups

Definition (dihedral)

A dihedral group is the group of symmetries of a regular polygon.
This includes rotations and reflections.

For a n-gon, the algebraic way of representing this group is D_{2n} and the geometric way is D_n.

Dihedral groups play an important role within and outside of group theory. They are one of the simplest finite groups.

Dihedral Groups

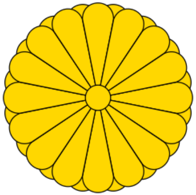
Definition (dihedral)

A dihedral group is the group of symmetries of a regular polygon.
This includes rotations and reflections.

For a n-gon, the algebraic way of representing this group is D_{2n} and the geometric way is D_n.
Dihedral groups play an important role within and outside of group theory. They are one of the simplest finite groups.

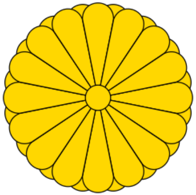
Dihedral Groups

This is a 2D example of the dihedral group of a 16-gon.



Dihedral Groups

This is a 2D example of the dihedral group of a 16-gon.



Tarski Groups

Definition (Tarski Monster group)

A Tarski Monster group is an infinite group G with the property:

- Every proper subgroup (not including the identity subgroup) is a cyclic group of order p, where p is a fixed prime number.

Tarski Groups

Definition (Tarski Monster group)

A Tarski Monster group is an infinite group G with the property:

- Every proper subgroup (not including the identity subgroup) is a cyclic group of order p, where p is a fixed prime number.

Tarski Group

Properties

- *The Tarski Monster Group is non-abelian*
- *Although the group is infinite, all the proper subgroups are finite cyclic groups*

Tarski Group

Properties

- *The Tarski Monster Group is non-abelian*
- *Although the group is infinite, all the proper subgroups are finite cyclic groups*

Signifiance

Problem (Burnside's Problem)

Must a finitely generated group in which every element has finite order necessarily be finite group?

The existence of a Tarski group for a prime p provides a negative answer to the Burnside problem for that prime p.
Satisfies

- the minimal condition: every strictly descending chain of subgroups is finite.
- the maximal condition: every strictly ascending chain of subgroups is finite.

Signifiance

Problem (Burnside's Problem)

Must a finitely generated group in which every element has finite order necessarily be finite group?

The existence of a Tarski group for a prime p provides a negative answer to the Burnside problem for that prime p.
Satisfies

- the minimal condition: every strictly descending chain of subgroups is finite.
- the maximal condition: every strictly ascending chain of subgroups is finite.

Cosets

Definition (Left Coset)

Given a subgroup $H \leq G$ and element $g \in G$, the left coset is a subset of G of the form $gH := \{gh : h \in H\}$.

Definition (Right Coset)

Similarly, the right coset would be $Hg := \{hg : h \in H\}$.

Cosets

Definition (Left Coset)

Given a subgroup $H \leq G$ and element $g \in G$, the left coset is a subset of G of the form $gH := \{gh : h \in H\}$.

Definition (Right Coset)

Similarly, the right coset would be $Hg := \{hg : h \in H\}$.

Lagrange's Theorem

Lagranges Theorem is one of the central theorems of Abstract Algebra and its proof uses several important ideas. Let's look at Lagrange's Theorem and then try to prove it.

Theorem (Lagrange's Theorem)

If G is a finite group and $H \leq G$, then $|H|$ will divide $|G|$.

Lagrange's Theorem

Lagranges Theorem is one of the central theorems of Abstract Algebra and its proof uses several important ideas. Let's look at Lagrange's Theorem and then try to prove it.

Theorem (Lagrange's Theorem)

If G is a finite group and $H \leq G$, then $|H|$ will divide $|G|$.

Lagrange's Theorem Proof

Before we prove Lagrange's Theorem, we need to look at some lemmas.

Lemma

If $H \leq G$ there is a one-to-one correspondence between H in any coset of H.

Lemma

If $H \leq G$, then the left coset relation, $g_1 \sim g_2$ if $g_1 H = g_2 H$ is an equivalence relation.

Lemma

Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.

Lagrange's Theorem Proof

Before we prove Lagrange's Theorem, we need to look at some lemmas.

Lemma

If $H \leq G$ there is a one-to-one correspondence between H in any coset of H.

Lemma

If $H \leq G$, then the left coset relation, $g_1 \sim g_2$ if $g_1 H = g_2 H$ is an equivalence relation.

Lemma

Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.

Lagrange's Theorem Proof

Before we prove Lagrange's Theorem, we need to look at some lemmas.

Lemma

If $H \leq G$ there is a one-to-one correspondence between H in any coset of H.

Lemma

If $H \leq G$, then the left coset relation, $g_1 \sim g_2$ if $g_1 H = g_2 H$ is an equivalence relation.

Lemma

Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.

Lagrange's Theorem Proof

Before we prove Lagrange's Theorem, we need to look at some lemmas.

Lemma

If $H \leq G$ there is a one-to-one correspondence between H in any coset of H.

Lemma

If $H \leq G$, then the left coset relation, $g_1 \sim g_2$ if $g_1 H = g_2 H$ is an equivalence relation.

Lemma

Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes with $A \cap B \neq \emptyset$, then $A = B$.

Lagrange's Theorem Proof

With these lemmas in mind, we can prove Lagrange's Theorem.

Proof.

Let $\sim$ be the left coset equivalence relation we defined in the second lemma. The last lemma states that any two distinct cosets of $\sim$ are disjoint. This means we can say

$$G = (g_1 H) \cup (g_2 H) \cup \ldots \cup (g_n H)$$

The first lemma shows that the order of each coset is the same as the order of H, so

$$|G| = |g_1 H| + |g_2 H| + \ldots + |g_n H| = n|H|$$

$$|G| = n|H|$$

showing that $|G|$ is divisible by $|H|$. □

Extension to Number Theory

Theorem (Fermat's Little Theorem)

Let p be a prime number and let a be an integer not divisible by p. Then,

$$a^p \equiv a \pmod{p}.$$

Proof.

Let set $G = (1, 2, \cdots, p-1)$ form a group with the operation of multiplication. Let us assume that a is in the range $1 \geq a \geq p-1$, that, a is an element of G. Let k be of the order of a, that is, k is the smallest positive integer such that $a^k \equiv 1 \pmod{p}$. Then the numbers $1, a, a^2, \cdots, a^{k-1}$ reduced modulo p form a subgroup of G whose order is k and therefore by Lagrange's theorem, k divides the order of G, which is $p-1$. $\square$

Extension to Geometry

Theorem

There are only three polygons that can tile the plane: equilateral triangles, squares, and regular hexagons.

Proof.

Let G be the symmetry group of the tiling, which must contain at least one n-fold rotational symmetry. If G has any reflections, then the vertex figure of the tiling must be a regular polygon of $2-n$ sides. This is impossible. Therefore, G can only consist of rotations, which implies that the angles around each vertex must sum to a multiple of $\frac{360}{n}$ degrees. This is only possible for $n = 3, 4, 6$ which correspond to the 3 regular tilings that we identified. $\square$

References

Dummit, David Steven, and Richard M. Foote. *Abstract Algebra.* Third ed., John Wiley & Sons, Inc., 2004.

Acknowledgments

- Thank you so much to our mentor Gabrielle Liu and the PRIMES CIRCLE program and the MIT Math Department!
- We also want to thank our parents, family, and friends for providing us with the support we needed.

Thank you! Any Questions?