Symmetry and Simplicity in Finite Group Theory

Gracie Sheng[1] Evelyn Zhu[2]

[1]Massachusetts Academy of Math and Science at WPI

[2]Boston Trinity Academy

PRIMES Conference 2022

Roadmap

What is Group Theory?

- Branch of abstract algebra that studies algebraic structures called groups
- Foundation for other interests in mathematics such as representation theory
- Model patterns in nature, manipulations, and puzzles
- Forces, public key cryptography, Rubik's cube

Groups

Definition

A *group* is a finite or infinite set G together with a binary group operation $\circ : G \times G \to G$ that fulfill the group axioms:

i *Closure:* For all $g, h \in G$, the element $g \circ h \in G$.

ii *Associativity:* For $f, g, h \in G$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

iii *Identity:* There exists an *identity* element $e \in G$, such that $e \circ g = g = g \circ e \quad \forall g \in G$.

iv *Inverse:* For each $g \in G$, there exists an *inverse* element $g^{-1} \in G$ such that $g \circ g^{-1} = e = g^{-1} \circ g$.

Subgroups

Definition

Let G be a group. The subset H of G is a *subgroup* of G if it satisfies the group axioms under the binary operation of G. This relation is denoted as $H \leq G$.

- Subgroups help to "shrink" and simplify groups
- Smaller structures give insight to the whole

Injection, Surjection, and Bijection

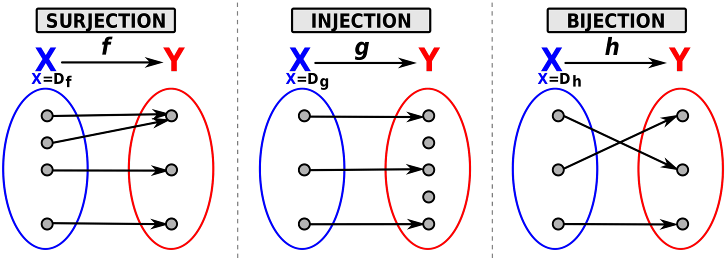
- The function $f : X \to Y$ is *injective* if for all $x, x^{'} \in X$, $f(x) = f(x^{'}) \Rightarrow x = x^{'}$.

Injection, Surjection, and Bijection

- The function $f : X \to Y$ is *injective* if for all $x, x^{'} \in X$, $f(x) = f(x^{'}) \Rightarrow x = x^{'}$.
- The function $f : X \to Y$ is *surjective* if for all $y \in Y$, there is $x \in X$ such that $f(x) = y$.

Injection, Surjection, and Bijection

- The function $f : X \to Y$ is *bijective* if for all $y \in Y$, there is a unique $x \in X$ such that $f(x) = y$.



Homomorphisms and Isomorphisms

- The Greek roots "homo" and "morph" mean "same shape."
- A *homomorphism* is a special correspondence between elements of two groups.
- A *isomorphism* is a function that captures a one-to-one relationship between two groups.

Homomorphisms and Isomorphisms

Definition

A *homomorphism* is a map $\phi : G \to H$ between two groups satisfying $\phi(ab) = \phi(a)\phi(b)$, for all $a, b \in G$.

Definition

A group *isomorphism* is a group homomorphism which is a bijection.

Roadmap

Symmetries in Life

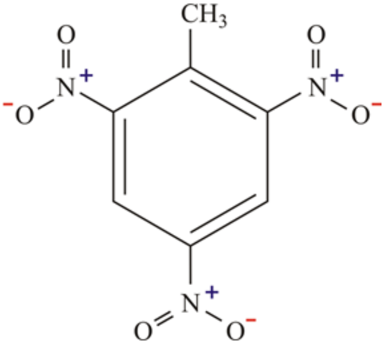


Figure 1: Symmetry in chemistry - Trinitrotoluene (TNT)

Figure 2: Symmetry in architecture - Taj Mahal in Agra, India built in marble from 1634 to 1656

Symmetric Group

Definition (Symmetric Group)

- The elements of the group are permutations on the given set (i.e., bijective maps from the set to itself).
- The product of two elements is their composite as permutations, i.e., function composition.
- The identity element of the group is the identity function from the set to itself.
- The inverse of an element in the group is its inverse as a function.

A group is said to be a *symmetric group* if it is isomorphic to the symmetric group on some set.

Example of Symmetric Groups: log and exp

Example

- Let $\mathbb{R}^x$ be the multiplicative group of positive real numbers, and let $\mathbb{R}$ be the additive group of real numbers.
- The logarithm function $\log : \mathbb{R}^x \to$ satisfies that $\log(xy) = \log(x) + \log(y)$ for all $x, y \in \mathbb{R}^x$, so log is a group homomorphism.

Example of Symmetric Groups: log and exp

Example

- The exponential function exp : $\mathbb{R} \to \mathbb{R}^x$ satisfies $exp(x + y) = exp(x) + exp(y)$ for all x, $y \in \mathbb{R}$ so exponential function is also a homomorphism.
- Logarithm and exponential function are *inverses* of each other. Since log is a homomorphism that has an inverse exp that is also a homomorphism
- So, both log and (exp) are isomorphisms between $\mathbb{R}^x$ and $\mathbb{R}$.

Cayley Table

	$\mathbf{e}$	$\mathbf{R_1}$	$\mathbf{R_2}$	$\mathbf{S_1}$	$\mathbf{S_2}$	$\mathbf{S_3}$
$\mathbf{e}$	e	R_1	R_2	S_1	S_2	S_3
$\mathbf{R_1}$	R_1	R_2	e	S_3	S_1	S_2
$\mathbf{R_2}$	R_2	e	R_1	S_2	S_3	S_1
$\mathbf{S_1}$	S_1	S_2	S_3	e	R_1	R_2
$\mathbf{S_2}$	S_2	S_3	S_1	R_2	e	R_1
$\mathbf{S_3}$	S_3	S_1	S_2	R_1	R_2	e

Cayley Table: describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table reminiscent of an addition or multiplication table.

Cayley's Theorem

Theorem (Cayley)

Every group G is isomorphic to a subgroup of a symmetric group. Specifically, G is isomorphic to a subgroup of the symmetric group whose elements are the permutations of the underlying set of G.

Cayley's Theorem

Proof.

To prove Cayley's theorem we need to find a subgroup H of $Sym(G)$ and a bijective homomorphism $f : G \to H$. The roadmap for the proof is:

- Define $\phi_a : G \to G$ for each a $\in G$ and show that ϕ_a is a bijection
- Define H - ϕ_a $|a \in G$ and show that $H \leq Sym(G)$
- Define $f : G \to H$ and show that f is both a bijection and homomorphism

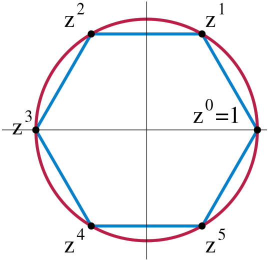
$\square$

Roadmap

Cyclic Groups

Definition

A group G is *cyclic* if G can be generated by a single element, that is, if there is some element $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. We say that G is *generated* by g.



Cyclic Groups

Definition

A group G is *cyclic* if G can be generated by a single element, that is, if there is some element $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. We say that G is *generated* by g.

Theorem

Any two cyclic groups of the same order are isomorphic.

We often express the cyclic group of order n as Z_n. Every infinite cyclic group is isomorphic to the additive group of $\mathbb{Z}$, the integers. Every finite cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n.

Cyclic Groups

Theorem (Lagrange)

If G is a finite group and $H \leq G$, then the order of H divides the order of G.

Cyclic Groups

Theorem (Lagrange)

If G is a finite group and $H \leq G$, then the order of H divides the order of G.

Corollary

If G is a group of prime order p, then G is cyclic. Then $G \cong Z_p$.

Cyclic Groups

Theorem (Lagrange)

If G is a finite group and $H \leq G$, then the order of H divides the order of G.

Corollary

If G is a group of prime order p, then G is cyclic. Then $G \cong Z_p$.

Proof.

Let $g \in G$, $g \neq e_G$. Thus $|\langle g \rangle| > 1$ and $|\langle g \rangle|$ divides $|G|$. Since $|G|$ is prime we must have $|\langle g \rangle| = |G|$. Hence $G = \langle g \rangle$ is cyclic. Since cyclic groups of equal order are isomorphic, we have $G \cong Z_p$. □

Roadmap

Normal Subgroups

Definition

The element gng^{-1} is the *conjugate* of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the *conjugate* of N by g. If $gNg^{-1} = N$, the element g is said to *normalize* N.

Definition

The subgroup N of a group G is *normal* if $gNg^{-1} = N$, or equivalently $gN = Ng$, for all $g \in G$, i.e. if every element of G normalizes N. This relation is denoted as $N \trianglelefteq G$.

Simple Groups

Definition

A nontrivial group G is *simple* if its only normal subgroups are the identity and itself.

Theorem (Feit-Thompson)

If G is a simple group of odd order, then $G \cong Z_p$ for some prime p.

Classification of Finite Simple Groups

Theorem (Classification Theorem, Gorenstein)

Every finite simple group is isomorphic to one of the following:

i *A cyclic group of prime order;*

ii *An alternating group;*

iii *A member of one of sixteen infinite families of groups of Lie type; or*

iv *One of twenty-six sporadic groups not isomorphic to any of the above groups.*

Roadmap

Abelian Simple Groups

Theorem

Abelian simple groups are cyclic groups of prime order.

Abelian Simple Groups

Theorem

Abelian simple groups are cyclic groups of prime order.

Lemma

Every subgroup of an abelian group is normal.

Abelian Simple Groups

Theorem

Abelian simple groups are cyclic groups of prime order.

Lemma

Every subgroup of an abelian group is normal.

Proof.

Let G be an abelian group and let $H \leq G$. Consider an element $x \in gHg^{-1}$. Since G is abelian and $g, h \in G$, we have

$$x = (gh)g^{-1} = (hg)g^{-1} = h \in H \Rightarrow gHg^{-1} \subseteq H \Rightarrow H \trianglelefteq G$$

Abelian Simple Groups

Theorem

Abelian simple groups are cyclic groups of prime order.

Proof.

($\Rightarrow$) *If G is a simple abelian group, then the order of G is prime.*

- Suppose that G is a simple abelian group and consider $\langle g \rangle \leq G$ where $g \in G$ is a nonidentity element.
- Since G is abelian, every subgroup of G is normal. Since G is simple, we must have $\langle g \rangle = G$ and G be of finite order.
- Let $|g| = |G| = p$. FSOC assume that $p = mn$ is a composite number. Then $\langle g^m \rangle \trianglelefteq G$, but G is simple, so p must be prime.

Abelian Simple Groups

Proof.

($\Leftarrow$) *If the order of G is prime, then G is a simple abelian group.*

- Similar to the forward direction

Abelian simple groups are cyclic groups of prime order.

Acknowledgements

We would like to acknowledge

- Prof. Pavel Etingof, PRIMES Chief Research Advisor
- Dr. Slava Gerovitch, PRIMES Program Director
- Marisa Gaetz and Mary Stelow, PRIMES Circle Coordinators
- Gabrielle Kaili-May Liu, PRIMES Circle Mentor

for providing us the opportunity to deeply explore complex topics in math.

Thank you for listening!