Introduction to Sylow's Theorem

Bella Chen, Ziyao Ma, Alice Yin

May 17, 2026

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Group Definition

Definition

A **group** is a pair $(G, \star)$, where G is a set and $\star$ is a binary operation $\star : G \times G \to G$, satisfying the following axioms:

1. **Associativity:** For all $a, b, c \in G$,
$$(a \star b) \star c = a \star (b \star c).$$
2. **Identity:** There exists an element $e \in G$ such that for all $a \in G$,
$$a \star e = e \star a = a.$$
3. **Inverses:** For each $a \in G$, there exists an element $a^{-1} \in G$ such that
$$a \star a^{-1} = a^{-1} \star a = e.$$

Group Example

Example

The set $\mathbb{Z}$ is a group under addition.
Identity: 0 : For each $a \in \mathbb{Z}$, $a + 0 = a$.
Inverse: The inverse of a is $-a$: For each $a \in \mathbb{Z}$, $a + (-a) = 0$.
Associativity: Addition is associative.

Similarly, $(\mathbb{Q}, +), (\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are groups.

A Few Results

Let $(G, \star)$ be a group. Then:

1. The identity element of G is unique.
2. For each $a \in G$, the inverse of a is unique.
3. For each $a \in G$, $(a^{-1})^{-1} = a$
4. For all $a, b \in G$,

$$(a \star b)^{-1} = b^{-1} \star a^{-1}$$

5. **Left and Right cancellation laws.** For all $a, u, v \in G$,

$$a \star u = a \star v \implies u = v$$

$$u \star a = v \star a \implies u = v$$

Generators

Definition

G is **cyclic** if there exists an element $a \in G$ such that every element of G can be written as a power of a. In this case, we write

$$G = \langle a \rangle$$

and call a a **generator** of G.

Group Example

Example

The group $\mathbb{Z}_n$ under addition modulo n is cyclic. In particular,

$$\mathbb{Z}_n = \langle \overline{1} \rangle$$

since every element of $\mathbb{Z}_n$ can be written as

$$\overline{k} = k\overline{1}$$

for some integer k.

Order of a Group

Definition

The **order** of a group G, denoted $|G|$, is the number of elements in G. If G has infinitely many elements, then G is said to have infinite order.

Order of an Element

Definition

Denoted as $|a| = n$, the **order** of a is the smallest

$$a^n = e$$

provided such an integer exists. If no positive integer n satisfies $a^n = e$, then a is said to have infinite order.

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Subgroup Definition

Definition

Let G be a group, and let $H \subseteq G$. We say that H is a **subgroup** of G if H is nonempty and is closed under the operation and inverses; that is, for all $x, y \in H$,

$$xy \in h \qquad \text{and} \qquad x^{-1} \in H.$$

Denote $H \leq G$.

Subgroup Example

Example

Consider the group $\mathbb{Z}_{12}$ under addition modulo 12.

$$H = \langle \overline{3} \rangle$$

$$\langle \overline{3} \rangle = \{ n\overline{3} \mid n \in \mathbb{Z} \} = \{ \overline{0}, \overline{3}, \overline{6}, \overline{9} \}.$$

Therefore,

$$H \leq \mathbb{Z}_{12}$$

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Definition of Group Action

Definition

A **group action** of a group G on a set A is a map $G \times A \to A$ (denoted $g \cdot a$) satisfying:

- $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \quad \forall g_1, g_2 \in G, a \in A$
- $1 \cdot a = a \quad \forall a \in A$

Examples of Group Actions

Example

Left Regular Action: Let $A = G$. Define $g \cdot a = ga$ using the group operation.

Examples of Group Actions

Example

Left Regular Action: Let $A = G$. Define $g \cdot a = ga$ using the group operation.

Example

Translation on $\mathbb{Z}$: The additive group $(\mathbb{Z}, +)$ acts on itself by:

$$z \cdot a = z + a \quad \text{for } z, a \in \mathbb{Z}$$

Examples of Group Actions

Example

Left Regular Action: Let $A = G$. Define $g \cdot a = ga$ using the group operation.

Example

Translation on $\mathbb{Z}$: The additive group $(\mathbb{Z}, +)$ acts on itself by:

$$z \cdot a = z + a \quad \text{for } z, a \in \mathbb{Z}$$

Example

Shear on the Plane: The additive group $(\mathbb{R}, +)$ acts on $\mathbb{R}^2$ by:

$$r \cdot (x, y) = (x + ry, y)$$

Conjugation

The Conjugation Action

G acts on the set of its own subsets by **conjugation**. For $g \in G$ and $A \subseteq G$:

$$g \cdot A = gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Definition of Cosets

Definition

For any $N \leq G$ and any $g \in G$, define

- **Left Cosets:** $gN = \{gn \mid n \in N\}$
- **Right Cosets:** $Ng = \{ng \mid n \in N\}$

Any element in a coset is called a **representative** of the coset.

Definition of Cosets

Definition

For any $N \leq G$ and any $g \in G$, define

- **Left Cosets:** $gN = \{gn \mid n \in N\}$
- **Right Cosets:** $Ng = \{ng \mid n \in N\}$

Any element in a coset is called a **representative** of the coset.

Theorem

Let N be a subgroup of G. The set of left cosets of N form a partition of G.

Definition of Normal Subgroup

Definition

A subgroup N of G is a **normal** if

$$\forall g \in G,\ gNg^{-1} = N$$

Denote $N \trianglelefteq G$.

Definition of Normal Subgroup

Definition

A subgroup N of G is a **normal** if

$$\forall g \in G,\ gNg^{-1} = N$$

Denote $N \trianglelefteq G$.

Example

Let $H \leq \mathbb{Z}_{12}$, and $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.
For all $a \in \mathbb{Z}_{12}, b \in H$,

$$a + b + (-a) \pmod{12} = b \pmod{12}.$$

Thus, $H \trianglelefteq \mathbb{Z}_{12}$.

Operation of Cosets in Normal Subgroups

Definition

Define the following operation on the left cosets of N in G:

$$uN \cdot vN = (uv)N.$$

The operation is well-defined if and only if $N \trianglelefteq G$.

Definition of Quotient Groups

Definition

If $N \trianglelefteq G$, then there exists a **quotient group** G/N (read G mod N) which contains all left (or right) cosets N in G.

Definition of Quotient Groups

Definition

If $N \trianglelefteq G$, then there exists a **quotient group** G/N (read G mod N) which contains all left (or right) cosets N in G.

Example

One example of quotient group is $\mathbb{Z}/5\mathbb{Z}$. The left cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are:

- $0 + 5\mathbb{Z} = \{\cdots, -5, 0, 5, 10, 15, \cdots\}$
- $1 + 5\mathbb{Z} = \{\cdots, -4, 1, 6, 11, 16, \cdots\}$
- $2 + 5\mathbb{Z} = \{\cdots, -3, 2, 7, 12, 17, \cdots\}$
- $3 + 5\mathbb{Z} = \{\cdots, -2, 3, 8, 13, 18, \cdots\}$
- $4 + 5\mathbb{Z} = \{\cdots, -1, 4, 9, 14, 19, \cdots\}$

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Lagrange's Theorem

Theorem

Let G be a finite group, and let $H \leq G$. Then $|H|$ divides $|G|$. Moreover, the number of left cosets of H in G is

$$\frac{|G|}{|H|}.$$

Immediate Consequences of Lagrange's

Corollary

Let G be a finite group, and let $x \in G$. Then the order of x divides the order of G. In particular,

$$x^{|G|} = e$$

for all $x \in G$.

Corollary

Let G be a group of prime order p. Then G is cyclic, $G \cong \mathbb{Z}_p$.

Table of Contents

1 Groups

2 Subgroups

3 Group Actions

4 Normal Subgroups and Quotient Groups

5 Lagrange's Theorem

6 Sylow's Theorem

Definitions

Definition

Let G be a finite group, and let p be a prime.

1. **p-group**: A group whose order is p^α for some integer $\alpha \geq 1$.
2. **p-subgroup**: A subgroup of G that is a p-group.
3. **Sylow p-subgroup**: A subgroup of G of order p^α, where $|G| = p^\alpha m$, and p does not divide m.
4. $\mathrm{Syl}_p\, G$: set of Sylow p-subgroups
5. $n_p(G) = |\mathrm{Syl}_p\, G|$

Sylow's Theorem

Theorem

Let G be a finite group with

$$|G| = p^{\alpha} m,$$

where p is prime, $\alpha \geq 1$, and $p \nmid m$. Then:

1. G has at least one Sylow p-subgroup.
2. Any two Sylow p-subgroups of G are conjugate.
3. If n_p denotes the number of Sylow p-subgroups of G, then

$$n_p \equiv 1 \pmod{p} \qquad \text{and} \qquad n_p \mid m.$$

Application of Sylow's Theorem

Example (Groups of order pq, p and q primes, $p < q$)

Let $|G| = pq$ for primes p and q, where $p < q$. Let $P \in Syl_p(G)$, and $Q \in Syl_q(G)$. We can show that Q is a normal subgroup of G, and if P is also normal in G, then G is cyclic.

Cauchy's Theorem

We can use Sylow's Theorem to prove Cauchy's Theorem.

Theorem

If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Cauchy's Theorem

We can use Sylow's Theorem to prove Cauchy's Theorem.

Theorem

If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Proof Sketch.

By Sylow's Theorem, there exists a Sylow p-subgroup. By Lagrange's Theorem, there exists an element x in the Sylow p-subgroup with a prime-power order. If x in G has order p, then we are done. Else, if the order of x is p^k with $k > 1$, then $x^{p^{k-1}}$ has an order p. □

Thanks for listening!

Thank you to Max Lu, Paige Bright, and Mary Stelow for supporting our work and providing suggestions.