Introduction to Sylow's Theorem

Bella Chen, Ziyao Ma, Alice Yin

Abstract

This paper introduces the fundamental concepts of group theory, a branch of abstract algebra motivated by the study of symmetry. We begin by defining a group and introducing subgroups and normal subgroups, which are subsets of groups that allow us to form quotient groups and kernels. Building upon these ideas, we define group actions and the specific action of conjugation. This allows us to build toward Sylow's Theorem, which deals with the existence and properties of subgroups with a prime power order. We conclude by discussing the applications of Sylow's Theorem in studying the structure of finite groups.

1 Introduction

A group is a fundamental algebraic structure used to study symmetry and structures. While many mathematicians have used the notions of groups, the formal definition of an abstract group first appeared in the work of Walter Dyck in 1882.

2 Groups

2.1 Definitions

To define a group, we first introduce some background.

Definition 2.1. Let G be a set.

1. A **binary operation** on G is a map
$$\star : G \times G \to G.$$
For $a, b \in G$, we denote $\star(a, b)$ by $a \star b$.

2. A binary operation $\star$ on G is **associative** if, for all $a, b, c \in G$
$$a \star (b \star c) = (a \star b) \star c.$$

Using the terminology above we now define a group.

Definition 2.2. A **group** is a pair $(G, \star)$, where G is a set and $\star$ is a binary operation on 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

$$a \star a^{-1} = a^{-1} \star a = e.$$

Notice that by Property 2, a group always contains an identity element $e \in G$, thus every group is nonempty. Additionally, when the operation $\star$ is clear from context, we often refer to the group $(G, \star)$ simply as G. In this case, we say that G is a group under $\star$.

Definition 2.3. Given $a, b \in G$, we say that a and b **commute** under $\star$ if

$$a \star b = b \star a.$$

The operation $\star$ is **commutative** if every pair of elements of G commutes under $\star$. A group $(G, \star)$ is called **abelian** if $\star$ is commutative.

Example 2.1. The set $\mathbb{Z}$ is a group under addition. The identity element is 0, since

$$a + 0 = 0 + a = a$$

for all $a \in \mathbb{Z}$. For each $a \in \mathbb{Z}$, the inverse of a is $-a$, which is also an integer, since

$$a + (-a) = (-a) + a = 0.$$

Since addition is associative, all group axioms are satisfied. Moreover, because addition is commutative, the group $\mathbb{Z}, +$ is abelian.

Similarly, $(\mathbb{Q}, +), (\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are groups, each with identity 0 and inverse $-a$ for every element a.

Definition 2.4. Let $(G, \star)$ be a group. We say that 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.

Example 2.2. The group $\mathbb{Z}_n$ consists of the congruence classes modulo n, written

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}.$$

Here, $\overline{k}$ denotes the equivalence class of integers congruent to k modulo n. Under addition modulo n, $\mathbb{Z}_n$ is cyclic. In particular,

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

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

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

for some integer k. Thus, $\overline{1}$ generates of all of $\mathbb{Z}_n$.

We now establish several basic properties that follow from the group axioms.

Proposition 2.1. 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 $a, b \in G$,
$$(a \star b)^{-1} = b^{-1} \star a^{-1}.$$

Proof.

1. Suppose e and f are both identity elements of G. Since e and f are identities,
$$e = e \star f = f.$$
Therefore $e = f$, so the identity element is unique.

2. Let $a \in G$, and suppose $b, c \in G$ are both inverses of a. Then
$$a \star b = e \qquad \text{and} \qquad c \star a = e.$$
Thus,
$$c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b.$$
Hence the inverse of a is unique.

3. Since a^{-1} is the inverse of a, we have
$$a \star a^{-1} = a^{-1} \star a = e.$$
Thus a is an inverse of a^{-1}. By uniqueness of inverses,
$$(a^{-1})^{-1} = a.$$

4. Finally, let $a, b \in G$. We show that $b^{-1} \star a^{-1}$ is the inverse of $a \star b$. Indeed,
$$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = a \star a^{-1} = e.$$
Similarly,
$$(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star e \star b = b^{-1} \star b = e.$$
Therefore $b^{-1} \star a^{-1}$ is the inverse of $a \star b$, so
$$(a \star b)^{-1} = b^{-1} \star a^{-1}.$$
□

Proposition 2.2. Let $(G, \star)$ be a group. Then the left and right cancellation laws hold in G. That is, for all $a, u, v \in G$,

$$(1) \quad a \star u = a \star v \implies u = v$$
$$(2) \quad u \star a = v \star a \implies u = v.$$

Note that G may not be commutative, thus cancellation laws (1) and (2) are distinct.

Proof. Suppose $a \star u = a \star v$. Multiplying both sides on the left by a^{-1} gives

$$a^{-1} \star (a \star u) = a^{-1} \star (a \star v).$$

By associativity,

$$(a^{-1} \star a) \star u = (a^{-1} \star a) \star v$$
$$e \star u = e \star v.$$

Thus $u = v$.

Similarly, suppose $u \star a = v \star a$. Multiplying both sides on the right by a^{-1} gives:

$$(u \star a) \star a^{-1} = (v \star a) \star a^{-1}.$$

By associativity,

$$\begin{aligned} u = u \star e &= u \star (a \star a^{-1}) \\ &= v \star (a \star a^{-1}) \\ &= v \star e \\ &= v. \end{aligned}$$

Thus $u = v$. □

Definition 2.5. 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.

Definition 2.6. Let $(G, \star)$ be a group, and let $a \in G$. The **order** of a is the smallest

$$a^n = e$$

provided such an integer exists. In this case, we say that a has order n and write

$$|a| = n.$$

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

Example 2.3. Consider the group $(\mathbb{Z}_6, +)$. The identity element is 0. The element 2 has order 3 because

$$2 + 2 = 4 \not\equiv 0 \pmod 6, \text{but}$$
$$2 + 2 + 2 = 6 \equiv 0 \pmod 6.$$

Therefore 3 is the smallest positive integer such that $3 \cdot 2 \equiv 0 \pmod 6$, so $|2| = 3$.

Definition 2.7. A relation $\sim$ on A is said to be an equivalence relation if it is reflexive, symmetric, and transitive. The relation $\sim$ on A is said to be:

1. reflexive if $a \sim a$, for all $a \in A$,
2. symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$,
3. transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

2.2 Subgroups

Definition 2.8. 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 $x, y \in H$,

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

If H is a subgroup of G, we write $H \leq G$.

Proposition 2.3 (Subgroup Criterion)**.** Let G be a group, and let $H \subseteq G$. Then H is a subgroup of G if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$.

Note that from this point forward, we will use multiplicative notation and omit the $\star$ notation for clarity.

Proof. Suppose first that H is a subgroup of G. Then H is nonempty, and since H is closed under taking inverses and under the group operation, for all $x, y \in H$ we have $y^{-1} \in H$ and therefore $xy^{-1} \in H$.
Conversely, suppose that $H \neq \emptyset$ and that for all $x, y \in H$, $xy^{-1} \in H$. Since H is nonempty, choose some element $x \in H$. Taking $y = x$, we obtain $xx^{-1} = e \in H$. Thus H contains the identity element.
Now let $x \in H$. Since $e \in H$ and $x \in H$, the assumed condition gives $ex^{-1} = x^{-1} \in H$. Therefore H is closed under inverses.

Finally, let $x, y \in H$. Since we have shown that $y^{-1} \in H$, it follows that $(y^{-1})^{-1} = y$. Applying the assumed condition to x and y^{-1} gives $x(y^{-1})^{-1} = xy \in H$. Thus H is closed under the group operation. Therefore H is a subgroup of G. □

Example 2.4. Consider the group $\mathbb{Z}_{12}$ under addition modulo 12. The subset $H = \langle \overline{3} \rangle$ is a cyclic subgroup of $\mathbb{Z}_{12}$. Its elements are obtained by taking integer multiples of $\overline{3}$:

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

Thus H is a subgroup of $\mathbb{Z}_{12}$ generated by $\overline{3}$. Note that the subgroup H has order 4, and element $\overline{3}$ also has order 4.

3 Normal Subgroups, Quotient Groups, and Kernels

In this section, we will use subgroups to partition a group G into disjoint cosets. Then, we will discuss when the collection of such cosets form a group, and how the resulting groups enhance our understanding of homomorphisms of G.

Definition 3.1. For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid n \in N\}$$

be the **left cosets** and **right cosets** of N in G, respectively. Any element in a coset is called a **representative** of the coset.

Cosets are useful in partitioning the group.

Theorem 3.1. Let N be a subgroup of G. The set of left cosets of N form a partition of G.

Proof. Since $N \leq G$, $1 \in N$. Thus, $g = g \cdot 1 \in gN, \forall g \in G$. i.e. the union of left cosets contain all elements of G. Moreover, we show that

$$uN \neq vN \implies uN \cap vN = \emptyset.$$

We proceed by proving the contrapositive. If there exists an $x \in uN \cap vN$, and $n_1, n_2 \in N$,

$$x = un_1 = vn_2$$

Thus,

$$u = vn_2n_1^{-1}, \quad \text{where } n_2n_1^{-1} \in N \text{ by group axioms.}$$

For every element $un \in uN$, where $n \in N$, we have that

$$un = (vn_2n_1^{-1})n = v(n_2n_1^{-1}n) \in vN.$$

Thus, $uN \subseteq vN$ and we can similarly show $vN \subseteq uN$. Therefore,

$$uN = vN.$$ □

This proof also demonstrates why the representatives can be chose arbitrarily: Given any $g \in G$, for any element $x \in gN$,

$$xN = gN.$$

Another property of cosets is that they have the same size. This property leads to Lagrange's Theorem and will be proved in section 5.

Definition 3.2. If $H \leq G$, the number of left cosets of H in G is called the **index** of H in G and is denoted by $|G : H|$.

Definition 3.3. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the **conjugate** of N by g. The element g normalizes N if $gNg^{-1} = N$. A subgroup N of G is a **normal subgroup** if

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

We denote this by $N \trianglelefteq G$.

Let N be a subgroup of G. The statement N is a normal subgroup of G is equivalent to the following:

1. $N_G(N) = G$. (Recall that $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$.)
2. $\forall g \in G, gN = Ng$.
3. $gNg^{-1} \subseteq N$.
4. The operation on the left cosets of N in G ($uN \cdot vN = (uv)N$) is well defined.

We will prove the last equivalence in Proposition 3.1, the rest is left to the reader.

Below is an example for normal subgroup.

Example 3.1. Consider $2\mathbb{Z} \leq \mathbb{Z}$, the subgroup of even integers. For any integer $g \in \mathbb{Z}$,

$$g + 2\mathbb{Z} = \{\cdots, g + (-6), g + (-4), g + (-2), g + 0, g + 2, g + 4, g + 6, \cdots\}$$

$$2\mathbb{Z} + g = \{\cdots, (-6) + g, (-4) + g, (-2) + g, 0 + g, 2 + g, 4 + g, 6 + g, \cdots\}$$

By the commutativity of integer addition, for all $g \in \mathbb{Z}$, $g + 2\mathbb{Z} = 2\mathbb{Z} + g$. Therefore, $2\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Note that the commutativity of integer addition is crucial in showing the $2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. Since all abelian groups possess the commutativity of group operation, it is natural to conjecture that any subgroup of an abelian group is normal. We will prove it formally in the following lemma.

Lemma 3.1. Let G be an abelian group. Any subgroup of G is normal.

Proof. Let H be an arbitrary subgroup of G. Since G is abelian, for any $g \in G, h \in H$,

$$gh = hg.$$

By the definition of left and right cosets, this implies that

$$gH = Hg.$$

Therefore, $H \trianglelefteq G$. □

Next we will introduce an important property cosets in a normal subgroup possess in the following proposition.

Proposition 3.1. Define the following operation on the left cosets of N in G:

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

The operation is well-defined if, for any arbitrary $u_1, u_2 \in uN$ and $v_1, v_2 \in vN$, $u_1v_1N = u_2v_2N$. In particular, the operation is well-defined if and only if $N \trianglelefteq G$.

Proof. ($\Rightarrow$) Assume the operation is well-defined, let $u_1 = g$, $u_2 = gn$, and $v_1 = v_2 = g^{-1}$. Thus, $u_1N = u_2N, v_1N = v_2N$. Hence,

$$u_1N \cdot v_1N = (u_1v_1)N = (gg^{-1})N = N.$$
$$u_2N \cdot v_2N = (u_2v_2)N = (gng^{-1})N.$$

Since the operation is well-defined, we obtain

$$gng^{-1}N = N \quad \text{and} \quad gng^{-1} \in N.$$

Therefore, $gNg^{-1} \subseteq N$, for all $g \in G$ and $N \trianglelefteq G$.

($\Leftarrow$) If $N \trianglelefteq G$, $gng^{-1} \in N$, for every $n \in N$ and $g \in G$. Given $u_1, u \in uN$, $v_1, v \in vN$, there exists $n, m \in N$, such that

$$u_1 = un, \quad \text{and} \quad v_1 = vm.$$

Thus,

$$u_1v_1 = (un)(vm) = u(vv^{-1})nvm = uv(v^{-1}nv)m = uv(n_1m) \in uvN, \text{ where } v^{-1}nv = n_1 \in N.$$

Since $u_1v_1N \cap uvN \neq \emptyset$, from Theorem 3.1, we conclude that $u_1v_1N = uvN$, and the operation is well-defined. □

Using Proposition 3.1, we define the quotient group.

Proposition 3.2. 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.

Proof. Let $N \trianglelefteq G$. We verify that the set of left (or right) cosets of N in G satisfies the axioms of group through Proposition 3.1.

- Closure: The quotient group is closed under the operation $uN \cdot vN = (uv)N$. Since $uv \in G, uvN$ is a left coset of N in G.
- Associativity: The associativity naturally holds from the associativity in G.
- Identity: The identity of the group is $1N$. For every left cosets gN of N in G,

$$gN \cdot 1N = 1N \cdot gN = gN.$$

- Inverse: For every left cosets gN of N in G, its inverse is $g^{-1}N$, such that

$$gN \cdot g^{-1}N = g^{-1}N \cdot gN = 1N.$$

Since $H \trianglelefteq G$, the left cosets of H in G is equal to the right cosets. Therefore, the set of left (or right) cosets form a group. □

Example 3.2. Consider $5\mathbb{Z} \leq \mathbb{Z}$. One example of quotient group is $\mathbb{Z}/5\mathbb{Z}$. The left cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ are:

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

We can verify that $(a+5\mathbb{Z}) + (b+5\mathbb{Z}) = (a+b)+5\mathbb{Z}$ using modular arithmetic, or apply the conclusion that subgroups of an abelian group are normal to prove $5\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Definition 3.4. Let $(G, \star)$ and $(H, \diamond)$ be groups. A **homomorphism** is a map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \quad \text{for all } x, y \in G.$$

Proposition 3.3. Here are some useful properties for a homomorphism $\varphi : G \to H$:

1. $\varphi(1_G) = 1_H$, where 1_G and 1_H are identity of group G and group H, respectively.
2. $\varphi(g^n) = (\varphi(g))^n, \forall n \in \mathbb{Z}$.

Proof. To prove that $\varphi(1_G) = 1_H$,

$$\varphi(1_G)\varphi(1_G) = \varphi(1_G).$$

Multiplying both sides by $\varphi(1_G)^{-1}$, we obtain that,

$$\varphi(1_G) = 1_H.$$

We will use mathematical induction to prove the second part of the proposition. We first show that the claim holds for n being a nonnegative integer.
Base Case: When $n = 0$,

$$\varphi(g^0) = 1_H = \varphi(g)^0$$

Thus, the base case holds.
Inductive Hypothesis: Assume that the claim holds for some $n = k$, $k \geq 0$.
Inductive Step: For $n = k + 1$,

$$\varphi(g^{k+1}) = \varphi(g^k)\varphi(g) = \varphi(g)^k\varphi(g) = \varphi(g)^{k+1}.$$

Thus, the claim holds by induction on n, $n \in \mathbb{Z}, n \geq 0$. For n as a negative integer, we first prove that $\varphi(g^{-1}) = \varphi(g)^{-1}$. By the definition of homomorphism,

$$\varphi(1_G) = \varphi(g^{-1})\varphi(g) = 1_H$$

Multiplying both sides by $\varphi(g)^{-1}$,

$$\varphi(g^{-1}) = \varphi(g)^{-1}.$$

Now, we show that the claim holds for every negative integer n:

$$\varphi(g^n) = \varphi((g^{-1})^{-n}) = \varphi(g^{-1})^{-n} = (\varphi(g)^{-1})^{-n} = \varphi(g)^n.$$

Therefore, $\varphi(g^n) = \varphi(g)^n$, $\forall n \in \mathbb{Z}$. □

Definition 3.5. A homomorphism $\varphi : G \to H$ is an **isomorphism** if and only if the map is bijective. We denote G is isomorphic to H by $G \cong H$. Note that isomorphism is an equivalence relation.

Definition 3.6. If $\varphi : G \to H$ is a homomorphism, the **kernel** of φ is the set

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}.$$

We will now discuss the relation between quotient group and homomorphism through the fundamental theorem of homomorphisms.

Theorem 3.2 (First Isomorphism Theorem)**.** If $\varphi : G \to H$ is a homomorphism of groups with kernel K, then $K \trianglelefteq G$ and $G/K \cong \varphi(G)$.

Proof. To show that $K \trianglelefteq G$, we first show that K is a subgroup of G.
Since φ is a homomorphism, $\varphi(1_G) = 1_H$ and the kernel is nonempty.
For any $k_1, k_2 \in K$,

$$\varphi(k_1k_2^{-1}) = \varphi(k_1)\varphi(k_2^{-1}) = 1_H \cdot 1_H = 1_H.$$

Thus, $k_1k_2^{-1} \in K$, and $K \leq G$.
Next, we prove that for any $k \in K$, $g \in G$, we have $gkg^{-1} \in K$:

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H.$$

Therefore, $gkg^{-1} \in K$, for any $k \in K$, $g \in G$. Hence, $K \trianglelefteq G$.
Next, we define a map $\psi : G/K \to \varphi(G)$ by

$$\psi(gK) = \varphi(g).$$

We first show ψ is well-defined. If $uK = vK$, we have that

$$v^{-1}u \in K$$

Thus, we have

$$\varphi(v^{-1}u) = 1_H$$

Since φ is a homomorphism,

$$\varphi(v^{-1})\varphi(u) = 1_H.$$

By Proposition 3.3,

$$\varphi(v)^{-1}\varphi(u) = 1_H.$$

Hence,

$$\varphi(v) = \varphi(u), \quad \text{and} \quad \psi(uK) = \psi(vK).$$

Then, we show that ψ is a homomorphism. Since φ is a homomorphism,

$$\psi(uK)\psi(vK) = \varphi(u)\varphi(v) = \varphi(uv) = \psi(uvK) = \psi(uK \cdot vK).$$

Thus, ψ is a homomorphism. Finally, we prove that the map is bijective. By the definition of $\varphi(G)$, the map is surjective. To prove the map is injective, suppose $\psi(uK) = \psi(vK)$, thus $\varphi(u) = \varphi(v)$. Hence, similar to proof of well-definedness of ψ,

$$\varphi(v)^{-1}\varphi(u) = \varphi(v^{-1})\varphi(u) = \varphi(v^{-1}u) = 1_H.$$

Therefore, $v^{-1}u \in K$, and $uK = vK$. Since ψ is a well-defined, bijiective homomorphism,

$$G/K \cong \varphi(G). \qquad \square$$

4 Group Actions

Definition 4.1. A **group action** of a group G on a set A is a map from $G \times A$ to A written as $g \cdot a$, for all $g \in G$ and $a \in A$ satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$ and
2. $1 \cdot a = a$, for all $a \in A$.

For each fixed $g \in G$ we also define a map σ_g where $\sigma_g : A \to A$ where $\sigma_g(a) = g \cdot a$. Two important facts about σ_g is as follows:

1. for each fixed $g \in G$, σ_g is a permutation of A where a permutation is an ordered arrangement of all of the elements in set A, and

2. the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism. Note that S_A is the symmetric group on set A which is the set of all bijections from A to itself. In other words, it's the group under function composition of all of the permutations of A.

Example 4.1. The set of all permutations of the set $\{1, 2, 3\}$ under function composition is S_3. The six permutations of this set are the identity, the 3 permutations formed by swapping any two elements, the cycle that sends 1 to 2, 2 to 3, and 3 to 1, and finally the cycle that sends 1 to 3, 3 to 2, and 2 to 1.

To see that σ_g is a permutation of A we show that as a set map from A to A, it has a 2-sided inverse, namely $\sigma_{g^{-1}}$. For all $a \in A$,

$$\begin{aligned}
(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) && \text{(by definition of function composition)} \\
&= g^{-1} \cdot (g \cdot a) && \text{(by definition of } \sigma_{g^{-1}} \text{ and } \sigma_g) \\
&= (g^{-1}g) \cdot a && \text{(by property (1) of an action)} \\
&= 1 \cdot a = a && \text{(by property (2) of an action).}
\end{aligned}$$

This proves that $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map from A to A. Since g was arbitrary, we can interchange the roles of g and g^{-1} to obtain that $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on A. Thus σ_g has a 2-sided inverse. Therefore it is a permutation of A.

To check that $\varphi : G \to S_A$ where $\varphi(g) = \sigma_g$ is a homomorphism, we must prove that $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$. For all $a \in A$

$$\begin{aligned}
\varphi(g_1 g_2)(a) &= \sigma_{g_1 g_2}(a) && \text{(by definition of } \varphi) \\
&= (g_1 g_2) \cdot a && \text{(by definition of } \sigma_{g_1 g_2}) \\
&= g_1 \cdot (g_2 \cdot a) && \text{(by property (1) of an action)} \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) && \text{(by definition of } \sigma_{g_1} \text{ and } \sigma_{g_2}) \\
&= (\varphi(g_1) \circ \varphi(g_2))(a) && \text{(by definition of } \varphi).
\end{aligned}$$

Example 4.2. The **trivial action** is the group action where $g \cdot a = a$ for all $g \in G$ and for all $a \in A$. If distinct elements of G induce distinct permutations of A, then the action is said to be **faithful**.

For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

Example 4.3. Let G be any group and let $A = G$. We can define a map from $G \times A$ to A by $g \cdot a = ga$, for each $g \in G$ and $a \in A$, where ga on the right hand side is the product of g and a under the group operation in G. This is a group action of G onto itself, where each $g \in G$ permutes the elements of G by left multiplication. This is the left regular action of G on itself.

We now introduce more examples of group actions.

Example 4.4. The additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Example 4.5. The additive group $\mathbb{R}$ acts on the (x, y) plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

In the following section, we introduce an important family of subgroups of an arbitrary group and apply these definitions to see how they connect with group actions. Note that G in an arbitrary group and A is a nonempty subset of G in the following section.

Definition 4.2. The **centralizer** of A in G denoted $C_G(A)$ is the set

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

The **center** $Z(G)$ is the set

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

The **normalizer** of A in G denoted $N_G(A)$ is the set

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

All three of these sets are subgroups of G and note that $C_G(A) \leq N_G(A)$. The fact that the normalizer, the centralizer, and the center are all subgroups can be deduced as special cases of results on group actions.

Definition 4.3. If G is a group acting on set S, the **stabilizer** of $s \in G$ is the set $G_s = \{g \in G \mid g \cdot s = s\}$. The **kernel** of the action of G on S is $\{g \in G \mid g \cdot s = s\}$ for all $s \in S$.

Lemma 4.1. The stabilizer and the kernel of an action are both subgroups.

We will briefly show that $G_s \leq G$. A similar argument proves that the kernel of an action is a subgroup.

Proof. First, note that $1 \in G_s$ by axiom 2 of a group action. Also, if $y \in G_s$,

$$\begin{aligned} s = 1 \cdot s &= (y^{-1}y) \cdot s \\ &= y^{-1} \cdot (y \cdot s) && \text{(by axiom (1) of an action)} \\ &= y^{-1} \cdot s && \text{(since } y \in G_s\text{)} \end{aligned}$$

This shows that $y^{-1} \in G_s$ if $y \in G_s$. Finally, to show closure, if $x, y \in G_s$, then

$$\begin{aligned} (xy) \cdot s &= x \cdot (y \cdot s) && \text{(by axiom (1) of an action)} \\ &= x \cdot s && \text{(since } y \in G_s\text{)} \\ &= s. && \text{(since } x \in G_s\text{)} \end{aligned}$$

□

Now that we know that the stabilizer and kernel are subgroups, we can use these two subgroups to show that centralizers, normalizers, and centers are just special cases.

Example 4.6. An useful group action is called **conjugation** where $g : A \to gAg^{-1}$.

Under this action, $N_G(A)$ is the stabilizer of A in G. This proves the normalizer is a subgroup by Lemma 4.1.

Next let $N_G(A)$ act on the set A by conjugation where $g : a \to gag^{-1}$ for $g \in N_G(A)$ and $a \in A$. It is clear $C_G(A)$ is the kernel of this action, hence $C_G(A) \leq N_G(A)$ by Lemma 4.1. Because being a subgroup is a transitive property, $C_G(A) \leq G$.

Finally, $Z(G)$ is the kernel of G acting on G by conjugation, so $Z(G) \leq G$ by Lemma 4.1.

Theorem 4.1. Let G be a group acting on the nonempty set A. The relation $\sim$ on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the stabilizer index of a.

Proof. We first prove $\sim$ is an equivalence relation. Since $a = 1 \cdot a$, the relation is reflexive. If $a \sim b$, then $a = g \cdot b$ for some $g \in G$, so

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = b.$$

Therefore, $b \sim a$. Finally, to prove transitivity, we show that if $a \sim b$ and $b \sim c$, then $a \sim c$. If $a \sim b$ and $b \sim c$, we can write $a = g \cdot b$ and $b = h \cdot c$ for some $g, h \in G$, so

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c.$$

Therefore, the relation is transitive.

To prove the second part of the statement, we show a bijection between the left cosets of G_a in G and the elements of the equivalence class of a. Let C_a be the class of a, so

$$C_a = \{g \cdot a \mid g \in G\}.$$

Suppose $b = g \cdot a \in C_a$, then gG_a is a left coset of G_a in G. The map $b = g \cdot a \mapsto gG_a$ is a map from C_a to the set of left cosets of G_a in G. This map is surjective, since for any $g \in G$ the element $g \cdot a$ is an element of C_a. This map is injective since $gG_a = hG_a$ if and only if $h^{-1}g \in G_a$ if and only if $g \cdot a = h \cdot a$. This completes the proof. □

Theorem 4.1 implies that a group G acting on the set A partitions A into disjoint equivalence classes.

Definition 4.4. Let G be a group that acts on the set A.

1. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the **orbit** of G containing a.
2. The action of G on A is **transitive** if there is only one orbit. In other words, given two elements a, b of A, there is some $g \in G$ such that $a = g \cdot b$.

Definition 4.5. Two subsets S and T of G are said to be **conjugate** in G if there is some $g \in G$ such that $T = gSg^{-1}$. In other words, they must be in the same orbit of G acting on its subsets by conjugation.

Theorem 4.2. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. Similarly, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Proof. The proof follows from Theorem 4.1. To see why this must be true, understand that for conjugation, the stabilizer G_S is $N_G(S)$ and that the normalizer of $\{s\}$ is $C_G(s)$. □

5 Lagrange's Theorem

We now use cosets to relate the size of a finite group to the size of its subgroups. This relationship is known as Lagrange's Theorem.

Theorem 5.1 (Lagrange's 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 given by

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

In particular, $|H|$ divides $|G|$.

Proof. Let $|H| = n$, and suppose there are k left cosets of H in G. Since the left cosets of H partition G, it remains to determine the size of each coset. For any $g \in G$, consider the map $\varphi : H \to gH$ defined by $\varphi(h) = gh$. This map is surjective by the definition of gH. It is also injective, since if $\varphi(h_1) = \varphi(h_2)$,then $gh_1 = gh_2$, and the left cancellation law gives $h_1 = h_2$. Therefore φ is a bijection, so $|gH| = |H| = n$. Thus G is partitioned into K disjoint left cosets, each containing n elements. Hence $|G| = kn$. Therefore

$$k = \frac{|G|}{n} = \frac{|G|}{|H|}.$$ □

We now record two immediate consequences of Lagrange's Theorem.

Corollary 5.1. Let G be a finite group, and let $x \in G$. Then the order of x divides the order of G. In particular,

$$x^{|G|} = e \quad \text{for all } x \in G.$$

Proof. Let $\langle x \rangle$ be the cyclic subgroup of G generated by x. By Lagrange's Theorem, $|\langle x \rangle| \mid |G|$. Now let $|\langle x \rangle| = m$. Since $m \mid |G|$, there exists an integer k such that $|G| = mk$. Therefore

$$x^{|G|} = x^{mk} = (x^m)^k = e^k = e.$$ □

Corollary 5.2. Let G be a group of prime order p. Then G is cyclic, $G \cong \mathbb{Z}_p$.

Proof. Since $|G| = p$, and p is prime, G contains some element $x \neq e$. Consider the cyclic subgroup $\langle x \rangle$ generated by x. Since $x \neq e$, we have $|\langle x \rangle| > 1$. By Lagrange's Theorem, $|\langle x \rangle|$ divides p. Because the only positive divisors of p are 1 and p, it follows that $|\langle x \rangle| = p$.
Therefore $\langle x \rangle = G$, and thus G is cyclic. □

6 Sylow's Theorem

Lagrange's Theorem shows that the order of any subgroup must divide the order of the group. However, the converse is not true in general: if d divides $|G|$, there need not exist a subgroup of G of order d. Sylow's Theorem provides an important partial converse by guaranteeing the existence of subgroups whose orders are maximal powers of primes dividing $|G|$.

Definition 6.1. Let G be a finite group, and let p be a prime.

1. A group whose order is p^α for some integer $\alpha \geq 1$ is called a p-**group**. A subgroup of G that is a p-group is called a p-**subgroup** of G.

2. Suppose $|G| = p^\alpha m$, where p does not divide m. A subgroup of G of order p^α is called a **Sylow** p-**subgroup** of G.

   The set of all Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p G$. The number of Sylow p-subgroups of G is denoted by $n_p(G)$, or simply n_p when the group G is clear from context.

Theorem 6.1 (Sylow's 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

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

Next, we will use Sylow's Theorem without proof and now present an application.

Example 6.1. 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.

Proof. We first prove that $Q \trianglelefteq G$. By the part (3) of Sylow's Theorem, we have that

$$n_q \equiv 1 \pmod{q} \quad \text{and} \quad n_q | p.$$

Thus, n_q can only be 1 or p. Since $n_q \equiv 1 \pmod{q}$, we can rewrite it in the form:

$$n_q = 1 + kq, \quad \text{where } k \in \mathbb{Z}.$$

Since $1 < p < q$, $k < 1$ and $n_q = 1$. By Sylow's Theorem, n_q is the index in G of the normalizer $N_G(Q)$. Applying Lagrange's Theorem, we have

$$n_q = |G : N_G(Q)| = \frac{|G|}{|N_G(Q)|} = 1.$$

Thus $|G| = |N_G(Q)|$, and by $N_G(Q) \leq G$, we obtain that

$$N_G(Q) = G \quad \text{and} \quad Q \trianglelefteq G.$$

We now discuss when $P \trianglelefteq G$. Since $n_p = 1$ or q, if $p \nmid q - 1$, n_p must equal 1. Hence, $P \trianglelefteq G$ if $p \nmid q - 1$.
Under this case, let $P = \langle x \rangle$, and $Q = \langle y \rangle$.
Since $Q \trianglelefteq G$,

$$xyx^{-1} \in Q \quad \text{and} \quad xyx^{-1}y^{-1} \in Q.$$

Similarly,

$$yx^{-1}y^{-1} \in P \quad \text{and} \quad xyx^{-1}y^{-1} \in P.$$

Since $\gcd(p, q) = 1$, Lagrange's Theorem gives us

$$P \cap Q = \{e\}.$$

Since $xyx^{-1}y^{-1} \in P \cap Q$,

$$xyx^{-1}y^{-1} = e.$$

As $|x| = p$ and $|y| = q$,

$$xy = yx \implies |xy| = pq.$$

Since both G and $\langle xy \rangle$ has order pq, G is a cyclic group generated by xy. □

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

Theorem 6.2. *(Cauchy's Theorem)* If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Proof. Let G be a finite group and let p be a prime such that p divides $|G|$. We can write the order of G as:

$$|G| = p^n \cdot m$$

where $n \geq 1$ and $\gcd(p, m) = 1$. Sylow's Theorem states that there exists a subgroup P such that $|P| = p^n$. By Lagrange's Theorem, every non-identity element $g \in P$ has order p^k for some $1 \leq k \leq n$. If $k = 1$, g is the element of order p we are looking for. If $k > 1$, we can construct an element of order p by taking a power of g. Specifically, let:

$$x = g^{p^{k-1}}$$

We check the order of x by raising it to the power of p:

$$x^p = (g^{p^{k-1}})^p = g^{p^k} = e$$

Since p^{k-1} is less than the order of g, $x \neq e$ due to the fact that p^k is the minimum power of g that yields the identity. Therefore, x is an element of order p. □

References

[Dummit and Foote, 2003] Dummit, D. and Foote, R. (2003). *Abstract Algebra*. Wiley.