Abstract Algebra : A Brief Review

Jeongbin Jo

Department of Physics, Yonsei University, jeongbin033@yonsei.ac.kr

Abstract

This document provides a comprehensive review of the fundamental concepts in abstract algebra, with a specific focus on group theory. It outlines the axiomatic definition of groups and distinguishes between abelian and non-abelian structures based on the law of composition. A variety of concrete examples, including the group of integers, all six rigid symmetries of an equilateral triangle (D_3), general linear groups with matrix operations, integers modulo n, and the quaternion group, are systematically explored to bridge abstract definitions with concrete mathematical objects. Finally, basic properties such as the order of a finite group and the formal proof regarding the uniqueness of the identity element are discussed.

Contents

1 Groups

1.1 Definition of a Group

The concept of a group is central to abstract algebra, providing a unified framework for studying symmetries and generalized arithmetic operations.

Definition 1.1 (Group)**.** A group (G, f) is a set G equipped with a map $f : G \times G \to G$, called a binary operation or law of composition, satisfying the following three axioms [1, 2]:

1. *Associativity:* For all $a, b, c \in G$, $f(f(a, b), c) = f(a, f(b, c))$ [1].
2. *Identity Element:* There exists an element $e \in G$ such that for all $a \in G$, $f(e, a) = a$ and $f(a, e) = a$ [2].
3. *Inverse Element:* For each $a \in G$, there exists an element $b \in G$ such that $f(a, b) = e$ and $f(b, a) = e$ [1].

Remark. It is a common and convenient convention to denote the binary operation $f(a, b)$ simply as $a \cdot b$ or ab [1]. Furthermore, a group (G, f) is said to be *abelian* (or commutative) if $f(a, b) = f(b, a)$ for all $a, b \in G$ [3].

1.2 Examples of Groups

The following examples illustrate various abstract group structures, expanding deeply into matrix groups and geometric symmetries.

Example 1.1 (The Integers)**.** The set of integers $\mathbb{Z}$ together with standard addition forms a group denoted by $(\mathbb{Z}, +)$ [2]. The identity element is 0, since $a + 0 = 0 + a = a$ [1]. The inverse of any integer a is $-a$, yielding $a + (-a) = 0$ [1]. This group is abelian [3].

Example 1.2 (Symmetries of an Equilateral Triangle)**.** Symmetries are rigid transformations mapping the shapes back to itself, preserving both angle and distance. The set of all such symmetries for an equilateral triangle forms a group under the binary operation of composition [3].

Let the initial vertices of the triangle be A (bottom-left), C (bottom-right), and B (top). The group $G = \{id, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$ consists of exactly 6 elements [1]:

- **Reflections (μ):** μ_2 fixes B and swaps A, C. μ_1 fixes A and swaps B, C. μ_3 fixes C and swaps A, B.
- **Rotations (ρ):** ρ_1 is a clockwise rotation by 120°. ρ_2 is a counter-clockwise rotation by 120°.
- **Identity (id):** Leaves the triangle completely unchanged.

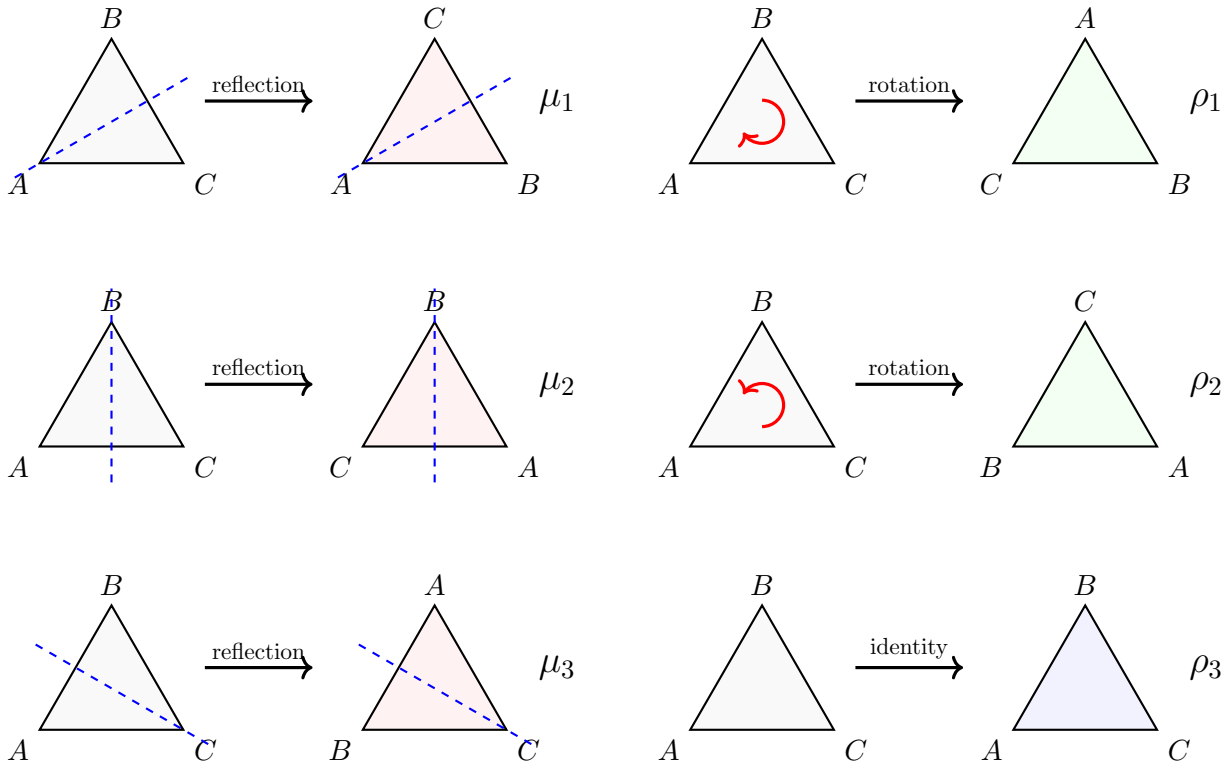


Figure 1: The six symmetry operations of an equilateral triangle, composing the Dihedral group D_3. Reflections (μ) are arranged on the left, and rotations (ρ) are on the right.

The composition of these operations is non-abelian. For example, $\mu_1 \circ \rho_1 \neq \rho_1 \circ \mu_1$. The operation $G \times G \to G$ ensures closure within the set [1].

Example 1.3 (General Linear Group)**.** Let $M_2(\mathbb{R})$ denote the set of 2×2 matrices with real coefficients [1]. The general linear group, denoted as $GL_2(\mathbb{R})$, is the set of all invertible matrices in $M_2(\mathbb{R})$ [3].

Formally, a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belongs to $GL_2(\mathbb{R})$ if and only if its determinant is non-zero ($\det A = ad - bc \neq 0$) [1]. If $\det A \neq 0$, the inverse element exists and is strictly defined as:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tag{1}$$

Under matrix multiplication, $(GL_2(\mathbb{R}), \cdot)$ is a non-abelian group [2]. The identity element is the identity matrix $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ [3]. Notice that $(M_2(\mathbb{R}), \cdot)$ is *not* a group because singular matrices (where $ad - bc = 0$) lack multiplicative inverses [1].

Example 1.4 (The Integers Modulo n)**.** The set of integers modulo n under addition modulo n forms a group $(\mathbb{Z}_n, +)$ [2]. Under multiplication, an element $x \in \mathbb{Z}_n \setminus \{0\}$ has an inverse if and only if $\gcd(x, n) = 1$ [3]. The subset $U(n) = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$ forms a group under multiplication modulo n, known as the group of units of $\mathbb{Z}_n$ [1, 3].

Example 1.5 (The Quaternion Group)**.** The quaternion group, denoted as Q_8, is a non-abelian group of order 8. Abstractly, it is defined by the standard set of elements (following William Rowan Hamilton's notation):

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\} \tag{2}$$

The group operations are governed by the fundamental defining relations:

$$i^2 = j^2 = k^2 = ijk = -1 \tag{3}$$

From these elegant relations, we can derive the cyclic and anti-commutative properties that strictly demonstrate the non-abelian nature of the group [1]:

$$ij = k, \quad jk = i, \quad ki = j \tag{4}$$

$$ji = -k, \quad kj = -i, \quad ik = -j \implies ij = -ji \tag{5}$$

The abstract group Q_8 can be explicitly represented using 2×2 complex matrices in $GL_2(\mathbb{C})$. A standard isomorphic representation maps the fundamental elements to the following matrices [3]:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \tag{6}$$

In physics, this mathematical structure is deeply connected to the **Pauli matrices** $(\sigma_x, \sigma_y, \sigma_z)$, which are the observable operators for spin-1/2 particles in quantum mechanics. The Pauli matrices are defined as:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7}$$

By multiplying the Pauli matrices by the imaginary unit i (where $i = \sqrt{-1}$), we recover the exact algebraic structure of the quaternions. Specifically, the relationship can be beautifully expressed as:

$$\mathbf{i} = i\sigma_z, \quad \mathbf{j} = i\sigma_y, \quad \mathbf{k} = i\sigma_x \tag{8}$$

This direct mapping illustrates that the elements of Q_8 are fundamentally proportional to the generators of the Special Unitary group $SU(2)$, forming a crucial bridge between abstract algebra and modern theoretical physics [1].

Example 1.6 (Non-zero Complex Numbers)**.** Defining $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, the structure $(\mathbb{C}^*, \cdot)$ is a group with the multiplicative identity 1 [2, 1]. The inverse of any complex number $a + ib$ is explicitly calculated by multiplying the numerator and denominator by the complex conjugate:

$$(a + ib)^{-1} = \frac{1}{a + ib} = \frac{a - ib}{(a + ib)(a - ib)} = \frac{a - ib}{a^2 + b^2} \tag{9}$$

This confirms that every non-zero complex number has a valid inverse in $\mathbb{C}^*$ [3].

1.3 Basic Properties of Groups

These abstract properties allow us to systematically apply algebraic tools to a wide variety of mathematical structures [2].

Definition 1.2 (Order of a Group)**.** A group (G, f) is of finite order if G is a finite set; otherwise, it is an infinite group [1]. The order of a finite group is the total number of elements in G, denoted by $|G|$ [3]. For example, $|\mathbb{Z}_n| = n$, whereas $|\mathbb{Z}| = \infty$ [2].

Proposition 1.0.1 (Uniqueness of Identity)**.** *Let G be a group. There is exactly one identity element in G.*

Proof. Let e and e' be two elements in G that both satisfy the definition of an identity element [2]. Since e is an identity element, for any $g \in G$, we have $e \cdot g = g \cdot e = g$. If we choose $g = e'$, this yields $e \cdot e' = e'$ [1, 2].

Similarly, since e' is an identity element, for any $g \in G$, $e' \cdot g = g \cdot e' = g$. Choosing $g = e$ yields $e' \cdot e = e$ [2].

By associativity and the properties above, $e = e' \cdot e = e \cdot e' = e'$. Therefore, $e = e'$, proving the uniqueness of the identity element [1]. □

2 Subgroups

2.1 Definition and Examples

A group can contain smaller structures within it that also behave as groups. Understanding these subsets is essential for analyzing the internal structure of groups and their symmetries [2].

Definition 2.1 (Subgroup)**.** A subset H of a group G is called a subgroup if H itself forms a group under the exact same binary operation defined on G [1]. We denote this relationship as $H \leq G$.

Remark. If a group G has at least two elements, it inherently contains at least two subgroups [2]. These are the group G itself, and the *trivial subgroup* consisting only of the identity element, $H = \{e\}$. Any subgroup H that is strictly different from G (i.e., $H \subsetneq G$) is referred to as a *proper subgroup* [3].

Example 2.1 (Non-zero Rational Numbers)**.** Consider the set of non-zero real numbers $\mathbb{R}^*$ under multiplication, which forms a group with the identity 1. The set of non-zero rational numbers $\mathbb{Q}^* = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, p \neq 0, q \neq 0\}$ is a subset of $\mathbb{R}^*$ [3]. Since the product of two rational numbers $\frac{p}{q} \times \frac{r}{s} = \frac{pr}{qs}$ is also a non-zero rational number, and the inverse $(\frac{p}{q})^{-1} = \frac{q}{p}$ is strictly in $\mathbb{Q}^*$, it follows that $\mathbb{Q}^*$ is a valid subgroup of $\mathbb{R}^*$ [1].

Example 2.2 (Special Linear Group)**.** Let $GL_2(\mathbb{R})$ be the general linear group of invertible 2×2 matrices. The special linear group, denoted as $SL_2(\mathbb{R})$, is defined as the set of all real 2×2 matrices with a determinant equal to 1 [1]. For any $A, B \in SL_2(\mathbb{R})$, the determinant of their product is calculated as:

$$\det(A \cdot B) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1 \tag{10}$$

Since the identity matrix I has a determinant of 1 and the subset is closed under matrix multiplication, $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$ [3].

Example 2.3 (General Linear Group under Addition)**.** Let $M_2(\mathbb{R})$ be the group of all 2×2 real matrices under matrix addition. Although the set $GL_2(\mathbb{R}) \subset M_2(\mathbb{R})$, $GL_2(\mathbb{R})$ is *not* a subgroup of $M_2(\mathbb{R})$ [2]. This is because they do not share the same valid binary operation for closure; $GL_2(\mathbb{R})$ is not closed under addition. For instance, the identity matrix I and its additive inverse $-I$ are both invertible matrices, but their sum $I + (-I) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is the zero matrix, which is singular and therefore not in $GL_2(\mathbb{R})$ [1].

Example 2.4 (Comparing $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$)**.** Consider the group $\mathbb{Z}_4$ and the Cartesian product $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ under component-wise addition [3]. Both are abelian groups of order 4. However, they are fundamentally distinct algebraic structures (not isomorphic) [1]. A structural distinction can be explicitly made by counting their proper subgroups: $\mathbb{Z}_4$ has different subgroup generating patterns compared to the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2$, proving they cannot be the same group [3].

2.2 Subgroup Tests

To verify whether a given subset is a subgroup, it is not strictly necessary to check all abstract group axioms from scratch. The following algebraic propositions provide highly efficient criteria [2].

Proposition 2.0.1 (Three-Step Subgroup Test)**.** *A subset H of a group G is a subgroup of G if and only if it satisfies the following three conditions [1]:*

1. *The identity element e of G is in H.*
2. *Closure under the operation: For all $h_1, h_2 \in H$, $h_1 h_2 \in H$.*
3. *Closure under inverses: For all $h \in H$, $h^{-1} \in H$.*

Proof. If H is a subgroup, it must possess its own unique identity, say $e_H \in H$ [2]. By definition within H, $e_H e_H = e_H$. However, within the larger group G, multiplying by the identity e yields $e e_H = e_H$. Therefore, $e e_H = e_H e_H$. By applying the cancellation law in G, we deduce $e = e_H$, proving that the identity in H is identical to the identity in G [2].

Furthermore, if $h \in H$, it has an inverse $h' \in H$ such that $hh' = h'h = e$. Since the inverse of any element in a group G is strictly unique, h' must be the exact same element as h^{-1} in G [1].

The converse statement is straightforward: if the three conditions hold, the standard group axioms are naturally satisfied, making H a subgroup [3]. □

Proposition 2.0.2 (One-Step Subgroup Test)**.** *Let H be a subset of a group G. Then H is a subgroup of G if and only if H is non-empty ($H \neq \emptyset$) and for all $h_1, h_2 \in H$, the element $h_1 h_2^{-1} \in H$ [1].*

Proof. Suppose H is a subgroup of G. Since H must contain the identity e, H is non-empty ($e \in H \implies H \neq \emptyset$) [3]. For any $h_1, h_2 \in H$, the inverse h_2^{-1} is guaranteed to be in H, and by the closure property, their product $h_1 h_2^{-1}$ must also be in H [1].

Conversely, suppose H is non-empty and the condition $h_1, h_2 \in H \implies h_1 h_2^{-1} \in H$ holds [1]. Since $H \neq \emptyset$, we can choose some arbitrary element $h \in H$. By applying the given condition to h and itself, $hh^{-1} = e \in H$, which proves the identity element is in H [2].

Now, knowing $e \in H$, we can take e and any $h \in H$ to apply the condition again: $eh^{-1} = h^{-1} \in H$, thoroughly proving closure under inverses [2].

Finally, for closure under the binary operation, take any $h_1, h_2 \in H$. Since $h_2 \in H$, we have already proven that $h_2^{-1} \in H$. Applying the initial condition to h_1 and h_2^{-1} yields $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$ [1]. Thus, all subgroup conditions are perfectly satisfied. □

3 Cyclic Groups

3.1 Definition and Examples

Cyclic groups are the simplest and most fundamental class of groups, as their entire structure is generated by the powers of a single element [2].

Definition 3.1 (Cyclic Group and Generator)**.** Let G be a group and let $a \in G$. The set of all integral powers of a, denoted by $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, is a subgroup of G called the cyclic subgroup generated by a [1]. If there exists an element $a \in G$ such that the entire group $G = \langle a \rangle$, then G is called a *cyclic group*, and the element a is called a *generator* of G [2].

Remark. For any element $a \in G$, the order of the element, denoted as $|a|$, is defined as the smallest strictly positive integer $n > 0$ such that $a^n = e$. If no such n exists, we say a has infinite order, written as $|a| = \infty$ [3].

Example 3.1 (The Integers)**.** The group of integers $\mathbb{Z}$ under addition is an infinite cyclic group [2]. Its generators are exactly 1 and -1. The subset $3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$ is a proper cyclic subgroup of $\mathbb{Z}$ generated by 3, since all its elements are uniquely determined as multiples of 3 [1].

Example 3.2 (A Multiplicative Subgroup of Rational Numbers)**.** Consider the subset $H = \{2^n \mid n \in \mathbb{Z}\}$ within the group of non-zero rational numbers $\mathbb{Q}^*$ under multiplication. For any $a = 2^n$ and $b = 2^m$ in H, applying the One-Step Subgroup Test yields $ab^{-1} = 2^n \cdot 2^{-m} = 2^{n-m}$. Since $n - m \in \mathbb{Z}$, the result is strictly in H. Thus, H is a valid cyclic subgroup generated by 2 [1].

Example 3.3 (Group of Units $U(9)$)**.** The group of units $U(9) = \{1, 2, 4, 5, 7, 8\}$ under multiplication modulo 9 is a cyclic group [3]. We can verify that 2 is a generator by calculating its successive powers modulo 9:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 \equiv 7 \pmod 9, \quad 2^5 \equiv 5 \pmod 9, \quad 2^6 \equiv 1 \pmod 9 \tag{11}$$

Since $\langle 2 \rangle = U(9)$, it is formally cyclic [3]. Note that a cyclic group can have multiple generators; for instance, 5 is also a generator of $U(9)$, whereas 2 is not a generator for $\mathbb{Z}_6$ under addition [1].

Example 3.4 (A Non-Cyclic Group)**.** Not every group is cyclic. Consider the group of symmetries of an equilateral triangle, D_3 (or S_3). Every individual element generates a proper subgroup, but no single element can generate the entire non-abelian structure of D_3 [3].

3.2 Properties of Cyclic Groups

Theorem 3.1. *Every cyclic group is an abelian group [2].*

Proof. Let G be a cyclic group generated by $a \in G$, so $G = \langle a \rangle$. For any two elements $g, h \in G$, there exist integers $n, m \in \mathbb{Z}$ such that $g = a^n$ and $h = a^m$ [1]. By the exponent rules of abstract groups:

$$gh = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = hg \tag{12}$$

Therefore, the binary operation is strictly commutative, proving that G is abelian [3]. □

Theorem 3.2. *Every subgroup of a cyclic group is cyclic [1].*

Proof. Let $G = \langle a \rangle$ be a cyclic group, and let H be a subgroup of G [2]. If $H = \{e\}$, then it is trivially cyclic with $H = \langle e \rangle$.

Otherwise, suppose H contains some element other than the identity. This element must be of the form a^n for some non-zero integer $n \in \mathbb{Z}$. Since H is a subgroup, it is closed under inverses, meaning $a^{-n} \in H$. Thus, H must contain a^k for some strictly positive integer k [1].

Let m be the *smallest* positive integer such that $a^m \in H$. We claim that H is completely generated by $b = a^m$. To prove this, let $h \in H$ be an arbitrary element. Since $h \in G$, $h = a^k$ for some integer $k \in \mathbb{Z}$. By the division algorithm, there exist unique integers $q, r \in \mathbb{Z}$ such that:

$$k = qm + r, \quad 0 \leq r < m \tag{13}$$

We can rewrite h algebraically as:

$$h = a^k = a^{qm+r} = (a^m)^q a^r = b^q a^r \implies a^r = b^{-q} h \tag{14}$$

Since $b = a^m \in H$, its inverse and powers are also in H, meaning $b^{-q} \in H$. Because $h \in H$ as well, their product $a^r = b^{-q} h$ must belong to H [3].

However, r is strictly smaller than m ($0 \leq r < m$). Since m was defined as the smallest strictly positive integer for which $a^m \in H$, r cannot be positive. Therefore, it is forced that $r = 0$, which implies $k = qm$. Thus, $h = a^k = a^{qm} = (a^m)^q = b^q \in \langle b \rangle$. This proves that every element in H is generated by b, concluding that $H = \langle a^m \rangle$ is cyclic [1]. □

Remark. A direct corollary of this theorem is that the subgroups of $\mathbb{Z}$ are exactly of the form $n\mathbb{Z} = \langle n \rangle$ for $n = 0, 1, 2, \ldots$ [2].

Proposition 3.2.1. *Let G be a cyclic group of order n generated by a. Then $a^k = e$ if and only if n divides k [3].*

Proof. Suppose n divides k. Then $k = ns$ for some integer $s \in \mathbb{Z}$. It follows naturally that:

$$a^k = a^{ns} = (a^n)^s = e^s = e \tag{15}$$

Conversely, suppose $a^k = e$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that $k = qn + r$ with $0 \leq r < n$ [1]. Then:

$$e = a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r \tag{16}$$

Since n is the order of the group (defined as the smallest positive integer such that $a^n = e$), the condition $a^r = e$ with $0 \leq r < n$ mathematically forces $r = 0$ [3]. Therefore, $k = qn$, which precisely means that n divides k [2]. □

Proposition 3.2.2 (Equality of Powers)**.** *Let $G = \langle a \rangle$ be a cyclic group of order n. Then $a^k = a^l$ if and only if n divides $k - l$ [3]. Furthermore, the order of the cyclic subgroup generated by a is equal to the order of the element itself, explicitly written as $|\langle a \rangle| = |a|$ [1].*

Theorem 3.3 (Order of an Element in a Cyclic Group)**.** *Let $G = \langle a \rangle$ be a cyclic group of order n. Then the order of any element $a^k \in G$ is uniquely determined by the formula:*

$$|a^k| = \frac{n}{\gcd(k, n)} \tag{17}$$

[2].

Proof. Let $d = \gcd(k, n)$. By definition, $|a^k|$ is the smallest strictly positive integer $m > 0$ such that $(a^k)^m = e$ [1]. By Proposition 3.2.1, the condition $(a^k)^m = a^{km} = e$ holds if and only if n divides km [3]. Dividing both the divisor and the dividend by their greatest common divisor d, this statement is logically equivalent to $\frac{n}{d}$ dividing $\frac{k}{d}m$.

Since we factored out the greatest common divisor, we know that $\gcd(\frac{n}{d}, \frac{k}{d}) = 1$ [2]. By Euclid's Lemma, since $\frac{n}{d}$ divides the product but shares no common factors with $\frac{k}{d}$, it must strictly divide m [1]. Therefore, the smallest such positive integer m is exactly $m = \frac{n}{d}$. Thus, $|a^k| = \frac{n}{d}$ [3]. □

Corollary 3.3.1 (Generators of a Cyclic Group)**.** *Let $G = \langle a \rangle$ be a cyclic group of order n. An element $a^k \in G$ is a generator of G (meaning $\langle a^k \rangle = G$) if and only if $\gcd(k, n) = 1$ [1].*

Example 3.5 (Generators of $\mathbb{Z}_5$)**.** Consider the additive cyclic group $\mathbb{Z}_5$. An element $k \in \mathbb{Z}_5$ generates the entire group if and only if $\gcd(k, 5) = 1$ [2]. Since 5 is a prime number, the elements $1, 2, 3$, and 4 are all mutually coprime to 5, making them all valid generators of $\mathbb{Z}_5$ [3].

Example 3.6 (The Circle Group and n-th Roots of Unity)**.** Let $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ be the set of all complex numbers lying on the unit circle in the complex plane [1]. $\mathbb{T}$ is a continuous subgroup of $\mathbb{C}^*$ under multiplication, often called the *circle group*.

To formally prove this using the One-Step Subgroup Test, let $z, z' \in \mathbb{T}$. Using Euler's formula, we can represent them as $z = e^{i\theta}$ and $z' = e^{i\varphi}$ for some real angles $\theta, \varphi \in \mathbb{R}$ [3]. The inverse of z' is $(z')^{-1} = e^{-i\varphi}$. Computing their product yields:

$$z(z')^{-1} = e^{i\theta}e^{-i\varphi} = e^{i(\theta-\varphi)} \tag{18}$$

Since $|e^{i(\theta-\varphi)}| = 1$, the result is strictly in $\mathbb{T}$, proving it is a valid subgroup [2].

Within this circle group $\mathbb{T}$, the subset of complex numbers satisfying the polynomial equation $z^n = 1$ are called the n-th roots of unity [1]. They form a finite cyclic subgroup of order n, strictly generated by the element $e^{i\frac{2\pi}{n}}$. For instance, the 4th roots of unity ($n = 4$) are explicitly $\{1, i, -1, -i\}$, visually highlighted as the red dots in Figure 2, and they form a finite cyclic subgroup of order 4 [3].

4 Permutation Groups

4.1 Definition and The Symmetric Group

Permutation groups provide a highly concrete and fundamental way to construct and analyze finite groups through the concept of bijective mappings [2].

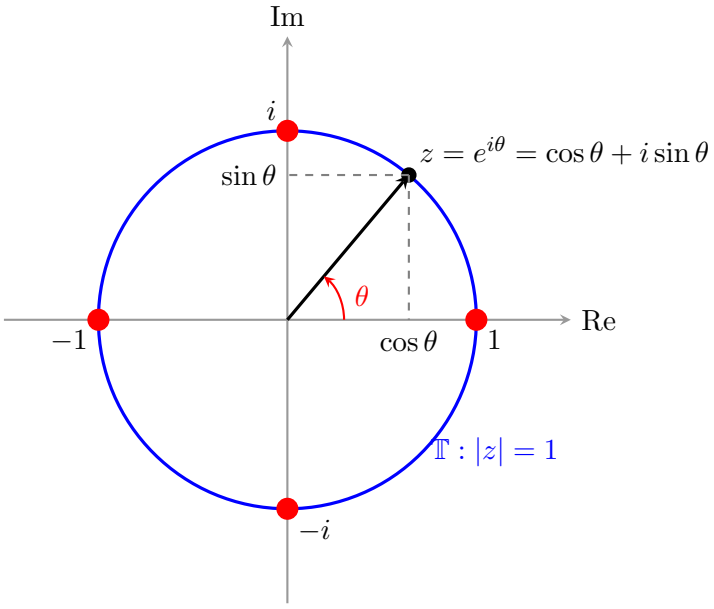


Figure 2: Geometric representation of the circle group $\mathbb{T}$ in the complex plane. Any element $z \in \mathbb{T}$ can be uniquely identified by the angle θ using Euler's formula [1]. The red dots visually highlight the 4th roots of unity, which form a cyclic subgroup of order 4 [3].

Definition 4.1 (Permutation and Symmetric Group)**.** A permutation of a set X is defined as a bijective function (one-to-one and onto) from X to itself, mapping $X \to X$ [1]. The set of all possible permutations of X, denoted by S_X, forms a group under the binary operation of function composition. If the set X is finite and consists of n elements, typically $X = \{1, 2, \ldots, n\}$, this group is denoted as S_n and is called the *symmetric group on n letters* [3].

Theorem 4.1. *The symmetric group S_n is a valid group, and its order is $|S_n| = n!$ [2].*

Proof. To verify that S_n is a group, we check the group axioms:

1. *Identity:* The identity mapping $e : X \to X$ defined by $e(k) = k$ for all $k \in X$ is a bijection, thus $e \in S_n$ [1].
2. *Inverses:* If $f : X \to X$ is a bijection, its inverse function $f^{-1} : X \to X$ mathematically exists and is also a bijection. Therefore, every permutation has an inverse in S_n [2].
3. *Closure and Associativity:* The composition of any two bijections $f, g : X \to X$ is strictly bijective. Function composition is inherently associative (i.e., $(f \circ g) \circ h = f \circ (g \circ h)$) [3].

Since there are exactly n choices for where to map the first element, $n-1$ for the second, and so forth, the total number of distinct bijective mappings is $n \times (n-1) \times \cdots \times 1 = n!$. Hence, $|S_n| = n!$ [1]. □

Remark. Any subgroup of S_n is generically referred to as a *permutation group* [3].

4.2 Two-Line Notation and Computations

Permutations are frequently expressed using a two-line matrix notation, where the top row lists the elements of the domain, and the bottom row lists their corresponding images [1]. For instance, a

permutation $f \in S_3$ where $f(1) = 2$, $f(2) = 1$, and $f(3) = 3$ is written as:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{19}$$

Example 4.1 (An Abelian Subgroup of S_5)**.** Consider a subgroup G of the symmetric group S_5 consisting of the identity id and the following three specific permutations [1]:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \tag{20}$$

By computing all possible compositions of these elements (for instance, evaluating $\sigma \cdot \tau = \mu$ and $\tau \cdot \sigma = \mu$ from right to left), we can construct the complete Cayley table for this subgroup G [2]:

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Table 1: The Cayley table for the subgroup $G = \{id, \sigma, \tau, \mu\}$.

A careful observation of Table 1 reveals two critical algebraic properties:

1. Every element is its own inverse, meaning $x \cdot x = id$ for all $x \in G$.
2. The table is perfectly symmetric strictly across its main diagonal. This geometric symmetry formally guarantees that $x \cdot y = y \cdot x$ for all $x, y \in G$.

Therefore, despite being a subgroup of the highly non-commutative group S_5, this specific subgroup G is strictly commutative (abelian) [3]. Structurally, this group is isomorphic to the Klein four-group (V_4).

Example 4.2 (Non-commutativity of S_n)**.** Generally, for $n \geq 3$, the symmetric group S_n is non-abelian [2]. Consider two permutations $\sigma, \tau \in S_4$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \tag{21}$$

We compute the composition $\sigma \cdot \tau$ by evaluating right-to-left (applying τ first, then σ) [1]:

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \tag{22}$$

Conversely, computing $\tau \cdot \sigma$ yields a different outcome:

$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \tag{23}$$

Since $\sigma \cdot \tau \neq \tau \cdot \sigma$, the group operation is strictly non-commutative [3].

4.3 Cycle Notation

Definition 4.2 (Cycle of Length k)**.** A permutation $\sigma \in S_X$ is called a cycle of length k (or a k-cycle) if there exist k distinct elements $a_1, a_2, \ldots, a_k \in X$ such that [1]:

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots, \quad \sigma(a_k) = a_1 \tag{24}$$

and $\sigma(x) = x$ for all other elements $x \in X$ not in this set. We compactly denote this as $\sigma = (a_1\ a_2\ \ldots\ a_k)$.

Example 4.3 (A 6-Cycle in S_7)**.** Consider the following permutation in S_7:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} \tag{25}$$

Tracing the mappings, we observe $1 \mapsto 6 \mapsto 2 \mapsto 3 \mapsto 5 \mapsto 4 \mapsto 1$, while 7 remains strictly fixed [3]. This forms a cycle of length 6, written as $\sigma = (1\ 6\ 2\ 3\ 5\ 4)$.

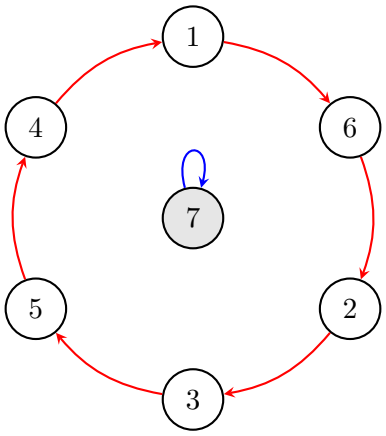


Figure 3: Visual representation of the 6-cycle $\sigma = (1\ 6\ 2\ 3\ 5\ 4)$ in S_7. The element 7 is fixed, mapping back to itself [1].

Example 4.4 (Disjoint Cycles Decomposition)**.** Not every permutation is a single cycle [2]. However, every permutation can be uniquely expressed as a product of disjoint cycles. Consider:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\ 2\ 4\ 3)(5\ 6) \tag{26}$$

Here, the domain structurally splits into two independent non-overlapping subsets: one subset cycles through $\{1, 2, 4, 3\}$ and the other merely swaps $\{5, 6\}$ [3].

Proposition 4.1.1 (Disjoint Cycles Commute)**.** *Let σ and τ be disjoint cycles in S_X. Then they strictly commute, meaning $\sigma\tau = \tau\sigma$ [2].*

Proof. Let A be the set of elements moved by σ (e.g., $A = \{a_1, \ldots, a_k\}$), and let B be the set of elements moved by τ (e.g., $B = \{b_1, \ldots, b_l\}$) [1]. Because σ and τ are disjoint cycles, their respective sets of moved elements are entirely disjoint, implying $A \cap B = \emptyset$ [3].

To formally prove $\sigma(\tau(x)) = \tau(\sigma(x))$ for all $x \in X$, we evaluate three distinct cases [1]:

1. If $x \notin A \cup B$, then both cycles fix x. Thus, $\sigma(\tau(x)) = \sigma(x) = x$ and $\tau(\sigma(x)) = \tau(x) = x$.

2. If $x \in A$, then $x \notin B$. Since $\sigma(x)$ is also contained in A, it follows that $\sigma(x) \notin B$. Therefore, the cycle τ acts as the identity on both x and $\sigma(x)$. We get $\tau(\sigma(x)) = \sigma(x)$, and $\sigma(\tau(x)) = \sigma(x)$.

3. If $x \in B$, by symmetric logic, $x \notin A$ and $\tau(x) \notin A$. Thus, $\sigma(\tau(x)) = \tau(x)$ and $\tau(\sigma(x)) = \tau(x)$.

Since the mappings are identical in all possible cases, the group operation commutes, meaning $\sigma\tau = \tau\sigma$ [2]. □

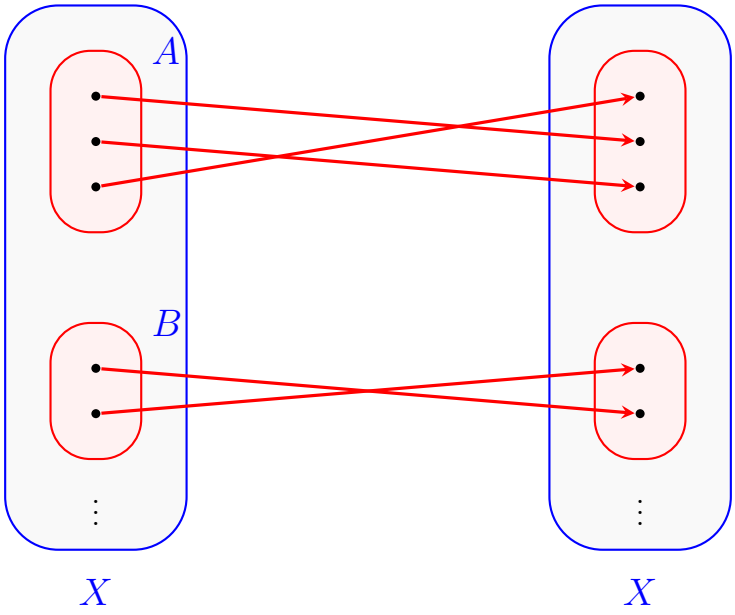


Figure 4: A bipartite mapping diagram illustrating that disjoint cycles operate on completely independent subsets A and B. Because $A \cap B = \emptyset$, their respective mappings do not interfere with each other, visually confirming the algebraic property $\sigma\tau = \tau\sigma$ [3].

4.4 Transpositions and the Parity of Permutations

Definition 4.3 (Transposition)**.** A cycle of length 2, denoted as $(a\ b) \in S_X$, is called a transposition [2]. It effectively swaps the elements a and b while leaving all other elements in X strictly fixed. A fundamental property of any transposition is that it is its own inverse, meaning $(a\ b) = (b\ a)$ and $(a\ b)^{-1} = (a\ b)$ [1].

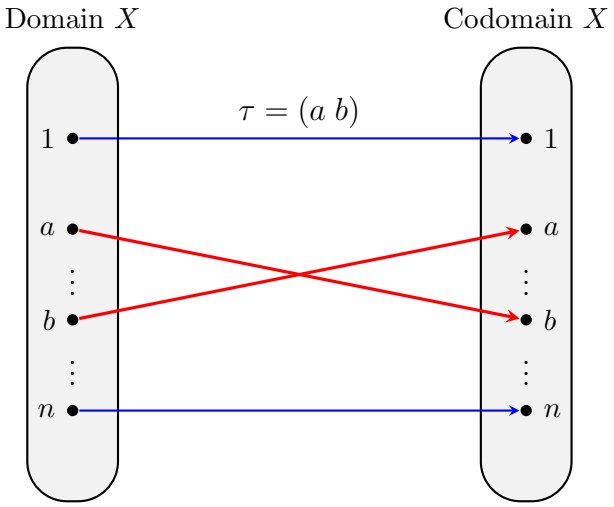


Figure 5: A bipartite mapping diagram illustrating the transposition $\tau = (a\ b)$. The elements a and b are strictly swapped (red arrows), while all other elements map directly to themselves (blue arrows) [3].

Proposition 4.1.2 (Decomposition into Transpositions)**.** *Any permutation on a set containing at least two elements can be expressed as a finite product (composition) of transpositions [2].*

Proof. Since every permutation can be written as a product of disjoint cycles, it suffices to show that any single cycle can be decomposed into transpositions [1]. A cycle of length k can be systematically decomposed as:

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\dots(a_1\ a_3)(a_1\ a_2) \tag{27}$$

By applying the transpositions from right to left, we observe that $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, and so forth, exactly reproducing the original cycle. Since every cycle can be factored this way, the proposition holds [3]. □

Remark. The decomposition into transpositions is not unique. For example, the identity permutation can be written as $id = (1\ 2)(1\ 2)$ or $id = (2\ 3)(1\ 4)(1\ 4)(2\ 3)$. However, the *parity* (even or oddness) of the number of transpositions is always invariant [1].

Lemma 4.1.1 (Parity of the Identity)**.** *If the identity permutation is written as a product of transpositions, $id = \tau_1\tau_2\dots\tau_r$, then the number of transpositions r must strictly be an even number [3].*

Definition 4.4 (Sign and Parity of a Permutation)**.** The sign (or signature/parity) of a permutation $\sigma \in S_n$, denoted as $\operatorname{sgn}(\sigma)$, is defined mathematically by the number of transpositions r required to express it:

$$\operatorname{sgn}(\sigma) = (-1)^r \tag{28}$$

If $\operatorname{sgn}(\sigma) = 1$ (meaning r is even), we say σ is an *even permutation*. If $\operatorname{sgn}(\sigma) = -1$ (meaning r is odd), we say σ is an *odd permutation* [2]. The well-definedness of this map $\operatorname{sgn} : S_n \to \{-1, 1\}$ is guaranteed by the preceding lemma [1].

Lemma 4.1.2 (Multiplicativity of the Sign)**.** *For any two permutations $\sigma, \sigma' \in S_n$, the sign function is strictly multiplicative:*

$$\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma') \tag{29}$$

Proof. Let σ and σ' be expressed as products of transpositions:

$$\sigma = \tau_1\tau_2\dots\tau_r \quad \text{and} \quad \sigma' = \tau'_1\tau'_2\dots\tau'_s \tag{30}$$

The composition $\sigma\sigma'$ is simply the concatenated product of these transpositions:

$$\sigma\sigma' = \tau_1\dots\tau_r\tau'_1\dots\tau'_s \tag{31}$$

This combined expression consists of exactly $r+s$ transpositions [1]. By the definition of the sign function, we can compute:

$$\operatorname{sgn}(\sigma\sigma') = (-1)^{r+s} = (-1)^r(-1)^s = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma') \tag{32}$$

This confirms that composing two even (or two odd) permutations yields an even permutation, while composing an even and an odd permutation yields an odd permutation [3]. □

4.5 The Alternating Group and the Dihedral Group

Definition 4.5 (The Alternating Group)**.** For any integer $n \geq 2$, the alternating group of degree n, denoted by A_n, is defined as the set of all even permutations within the symmetric group S_n [1].

Theorem 4.2. *The set of even permutations A_n forms a valid subgroup of the symmetric group S_n [2].*

Proof. We can formally prove this by verifying the standard subgroup criteria.

1. *Identity:* The identity permutation id has $\operatorname{sgn}(id) = 1$, which strictly implies $id \in A_n$ [1].
2. *Closure:* Let $\sigma, \sigma' \in A_n$. Since $\operatorname{sgn}(\sigma) = 1$ and $\operatorname{sgn}(\sigma') = 1$, their composition yields $\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma') = 1$. Thus, $\sigma\sigma' \in A_n$ [2].
3. *Inverses:* For any $\sigma \in A_n$, $\operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(id) = 1$. Since $\operatorname{sgn}(\sigma) = 1$, it algebraically forces $\operatorname{sgn}(\sigma^{-1}) = 1$, meaning $\sigma^{-1} \in A_n$ [3].

Therefore, $A_n \leq S_n$. □

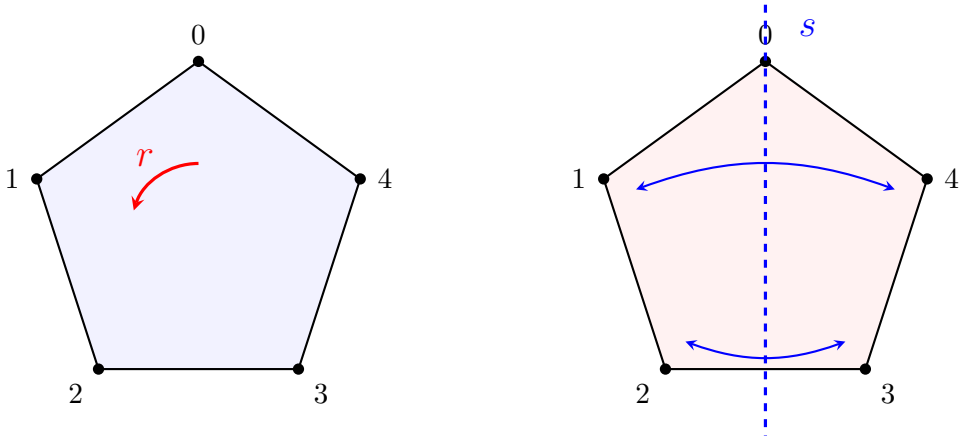
Theorem 4.3 (Order of the Alternating Group)**.** *The order of the alternating group A_n is exactly half the order of the symmetric group S_n, explicitly $|A_n| = \frac{n!}{2}$ [3].*

Proof. Let B_n be the set of all odd permutations in S_n. We construct a strict bijective mapping between A_n and B_n. Fix an arbitrary transposition $\tau \in S_n$. Define a mapping $f : A_n \to B_n$ by $f(\sigma) = \tau\sigma$. Since σ is an even permutation, composing it with one transposition τ changes its parity, ensuring the result is an odd permutation [1].

This mapping is injective because $\tau\sigma = \tau\sigma'$ implies $\sigma = \sigma'$ by left cancellation. It is surjective because any odd permutation $\mu \in B_n$ can be written as $\tau(\tau\mu)$, where $\tau\mu \in A_n$. Since f is a perfect bijection, $|A_n| = |B_n|$. Because $S_n = A_n \cup B_n$ is a disjoint union, $2|A_n| = |S_n| = n!$, which concludes the proof [2]. □

4.6 The Dihedral Group

Definition 4.6 (The Dihedral Group)**.** The n-th dihedral group D_n is defined as the group of isometries leaving a regular n-gon strictly invariant. These isometries inherently consist of spatial rotations and reflections [3].



Rotation r (72°) Reflection s (Fixes vertex 0)

Figure 6: Consider the dihedral group D_5, which algebraically represents the symmetries of a regular pentagon. The order of D_5 is precisely $2 \times 5 = 10$. Let the 5 vertices be labeled $0, 1, 2, 3, 4$ in counterclockwise order. The fundamental rotation r shifts each vertex counterclockwise by exactly 72° ($2\pi/5$). The fundamental reflection s geometrically fixes vertex 0 and symmetrically swaps the remaining vertices (e.g., $1 \leftrightarrow 4$ and $2 \leftrightarrow 3$) strictly across the vertical axis of symmetry [3].

Theorem 4.4 (Order of D_n)**.** *The dihedral group D_n is a subgroup of the symmetric group S_n, and it consists of exactly $2n$ elements [1].*

Proof. By tracking the permutations of the n distinct vertices of the regular n-gon, we can naturally embed D_n into S_n [2]. First, there are exactly n distinct rotational symmetries, which cyclically permute the vertices (e.g., mapping vertex $1 \mapsto k$, $2 \mapsto k+1$, and so on up to n). Additionally, there are exactly n distinct symmetries involving a reflection (or a reflection followed by a rotation), which reverse the sequential orientation of the vertices (e.g., mapping $1 \mapsto k$, $2 \mapsto k-1$). Summing these two disjoint sets of isometries yields exactly $n+n = 2n$ elements [3]. Therefore, $|D_n| = 2n$. □

Theorem 4.5 (Generators and Relations of D_n)**.** *For $n \geq 3$, the dihedral group D_n consists of all possible products of two fundamental elements r and s, satisfying the following algebraic relations [1]:*

$$r^n = id, \quad s^2 = id, \quad srs = r^{-1} \tag{33}$$

Proof. Let r denote a clockwise rotation by an angle of $\frac{2\pi}{n}$. Clearly, applying this rotation n times returns the polygon to its exact original position, strictly implying $r^n = id$. The cyclic subgroup $\langle r \rangle$ contains all the n purely rotational symmetries generated by r [2].

Let s denote a reflection that leaves at least one vertex strictly invariant. Applying a geometric reflection twice restores the original orientation, so clearly $s^2 = id$ [3]. Since D_n is generated

entirely by rotations and reflections, all elements of D_n can be expressed in the form $r^k s^l$, where the exponent $l \in \{0, 1\}$ [1].

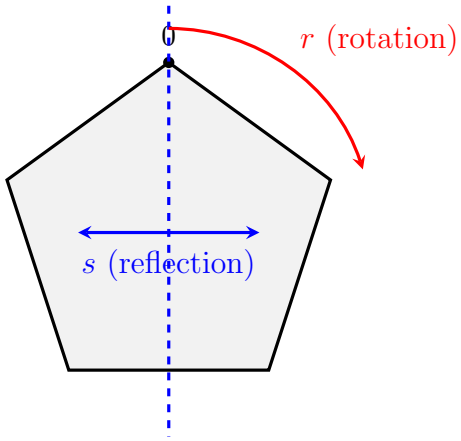


Figure 7: Geometric visualization of the generators r and s on a regular polygon (illustrated here with $n = 5$). The clockwise rotation r shifts the vertices by $\frac{2\pi}{n}$, while the reflection s mirrors the polygon across the axis of symmetry explicitly passing through vertex 0 [3].

To rigorously prove the non-abelian relation $srs = r^{-1}$, let us label the vertices of the n-gon using the integers modulo n, forming the set $\mathbb{Z}_n$. Without loss of generality, let the vertex fixed by the reflection s be labeled "0" [3]. The mathematical actions of r and s on any arbitrary vertex $k \in \mathbb{Z}_n$ are formally defined as:

$$r(k) = k + 1 \pmod{n}, \quad s(k) = -k \equiv n - k \pmod{n} \tag{34}$$

We now systematically evaluate the composition $srsr$ acting on the vertex k [1]:

$$\begin{aligned} (srsr)(k) &= srs(k+1) && (35)\\ &= sr(n-(k+1)) && (36)\\ &= s(n-k-1+1) && (37)\\ &= s(n-k) && (38)\\ &= n-(n-k) = k && (39) \end{aligned}$$

Since the result is $(srsr)(k) = k$ for all possible vertices $k \in \mathbb{Z}_n$, the combined transformation acts completely identically to the identity mapping, meaning $srsr = id$ [2]. Multiplying both sides of this equation by r^{-1} on the right yields the final relation:

$$srs = r^{-1} \tag{40}$$

[1]. □

4.7 Symmetry Group of the Cube

Theorem 4.6 (Rotational Symmetries of a Cube)**.** *The group of strictly rotational symmetries leaving a solid cube invariant is isomorphic to the symmetric group S_4 [1].*

Proof. A cube intrinsically possesses exactly 4 main body diagonals connecting opposite vertices. Any spatial rotation of the cube uniquely and validly permutes these 4 distinct diagonals [3].

To calculate the exact order of this rotational group G, observe that any of the 6 square faces can be chosen to face "upward." For each chosen top face, there are exactly 4 possible rotational orientations around the vertical axis [2]. Thus, the total number of rotational symmetries is exactly $|G| = 6 \times 4 = 24$. Since $|S_4| = 4! = 24$, and every rotation induces a unique permutation of the diagonals, the group of rotations is isomorphic to S_4 [1]. □

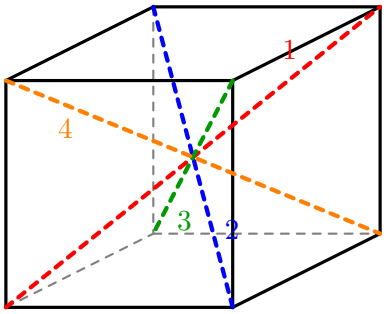


Figure 8: The 4 main diagonals of a cube. Any 3D rotation of the cube corresponds to a valid permutation of these 4 distinct diagonals, geometrically demonstrating the isomorphism to S_4 [3].

Remark (The Full Symmetry Group of the Cube). While the group of strictly rotational symmetries (orientation-preserving isometries) is isomorphic to S_4 with an order of 24, the *full* symmetry group of the cube additionally includes reflections and the central inversion (orientation-reversing isometries) [1].

Since the central inversion mathematically commutes with all possible geometric rotations in 3D space, the full symmetry group has exactly $24 \times 2 = 48$ elements. Algebraically, this full group is strictly isomorphic to the direct product $S_4 \times \mathbb{Z}_2$ [3]. The rigorous mathematical proof of this structural isomorphism, along with a detailed analysis of the central inversion's role, will be thoroughly discussed in a later section.

5 Cosets and Lagrange's Theorem

5.1 Definition of Cosets

Definition 5.1 (Left and Right Cosets)**.** Let H be a subgroup of a group G, and let $g \in G$. The *left coset* of H in G containing g is formally defined as the set [2]:

$$gH = \{gh \mid h \in H\} \tag{41}$$

Similarly, the *right coset* of H in G containing g is defined as $Hg = \{hg \mid h \in H\}$ [1].

Example 5.1 (Cosets in $\mathbb{Z}_6$)**.** Let $G = \mathbb{Z}_6$ under addition, and consider the subgroup $H = \{0, 3\}$ [3]. Because G is an abelian group, the left and right cosets perfectly coincide ($g + H = H + g$). The distinct cosets are iteratively calculated as:

$$0 + H = 3 + H = \{0, 3\} = H \tag{42}$$
$$1 + H = 4 + H = \{1, 4\} \tag{43}$$
$$2 + H = 5 + H = \{2, 5\} \tag{44}$$

Example 5.2 (Equality of Left and Right Cosets)**.** Let $G = S_3$, and consider the subgroup $H = \{(1), (123), (132)\}$, which is the alternating group A_3. We evaluate the left and right cosets containing the specific element (12) [1]:

$$\begin{aligned} \text{Left Coset: } (12)H &= \{(12)(1), (12)(123), (12)(132)\} \\ &= \{(12), (23), (13)\} \end{aligned} \tag{45}$$

$$\begin{aligned} \text{Right Coset: } H(12) &= \{(1)(12), (123)(12), (132)(12)\} \\ &= \{(12), (13), (23)\} \end{aligned} \tag{46}$$

Since $(12)H = H(12)$ (and this holds true for any element in G), the left and right cosets perfectly coincide. Such a subgroup where left and right cosets are always equal is geometrically and algebraically symmetric, and is formally called a *normal subgroup* [3].

Example 5.3 (Non-equality of Left and Right Cosets)**.** Let $G = S_3$, and consider the non-normal subgroup $K = \{(1), (12)\}$. We rigorously evaluate all distinct left and right cosets by computing the disjoint cycle multiplications strictly from right to left [2]:

Left Cosets:

$$(1)K = (12)K = \{(1), (12)\} \tag{47}$$

$$(13)K = (123)K = \{(13)(1), (13)(12)\} = \{(13), (123)\} \tag{48}$$

$$(23)K = (132)K = \{(23)(1), (23)(12)\} = \{(23), (132)\} \tag{49}$$

Right Cosets:

$$K(1) = K(12) = \{(1)(1), (12)(1)\} = \{(1), (12)\} \tag{50}$$

$$K(13) = K(132) = \{(1)(13), (12)(13)\} = \{(13), (132)\} \tag{51}$$

$$K(23) = K(123) = \{(1)(23), (12)(23)\} = \{(23), (123)\} \tag{52}$$

Comparing the fully computed results, we can observe that $(13)K = \{(13), (123)\}$ whereas $K(13) = \{(13), (132)\}$. Since $(13)K \neq K(13)$, this explicitly demonstrates that left and right cosets are not necessarily equal in a non-abelian group [1].

5.2 Properties and Partition of a Group

Lemma 5.0.1 (Equivalence of Coset Properties)**.** *Let H be a subgroup of a group G, and let $g_1, g_2 \in G$. The following algebraic propositions are perfectly equivalent [1]:*

1. $g_1 H = g_2 H$
2. $g_1 H \subseteq g_2 H$
3. $g_2 \in g_1 H$
4. $g_1^{-1} g_2 \in H$

Theorem 5.1 (Partition of a Group by Cosets)**.** *Let H be a subgroup of a group G. Then the family of all distinct left cosets of H forms a complete and disjoint partition of G [2].*

Proof. By definition, every element $g \in G$ belongs to at least one left coset, namely gH, because the identity $e \in H$ implies $g = ge \in gH$. Thus, the union of all left cosets tightly constitutes the entirety of the group G [3].

To rigorously prove that they form a partition, we must show that any two left cosets are either perfectly identical or strictly disjoint [2]. Suppose g_1H and g_2H have a non-empty intersection. Let $x \in g_1H \cap g_2H$. By definition, $x = g_1h_1 = g_2h_2$ for some elements $h_1, h_2 \in H$ [1].

Multiplying the equation by h_1^{-1} on the right yields $g_1 = g_2h_2h_1^{-1}$. Since H is a subgroup, it is algebraically closed, meaning $h_2h_1^{-1} \in H$. This strictly dictates that $g_1 \in g_2H$. By applying the equivalences established in Lemma 5.0.1, we conclude that $g_1H = g_2H$ [3]. Therefore, any two intersecting cosets must be completely identical, proving that left cosets perfectly partition the group. □

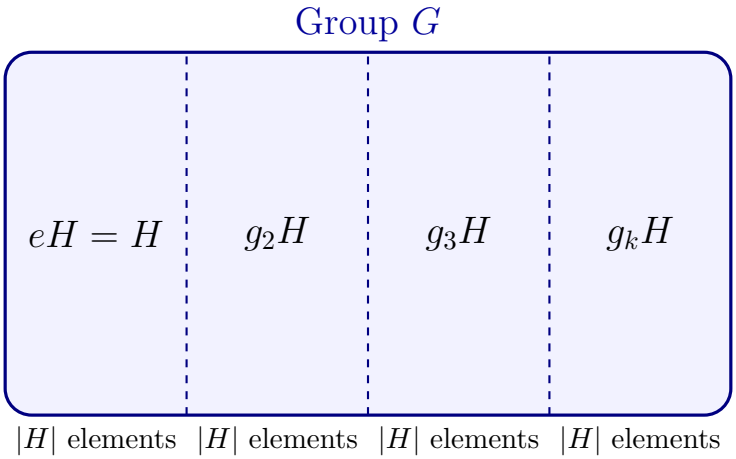


Figure 9: A visual representation of Lagrange's Theorem foundation: The distinct left cosets perfectly partition the entire group G into mutually disjoint subsets of identically equal size [2].

5.3 Index of a Subgroup and Lagrange's Theorem

Definition 5.2 (Index of a Subgroup)**.** Let H be a subgroup of a group G. The *index* of H in G, denoted by $[G : H]$, is defined mathematically as the total number of distinct left cosets of H in G [1].

Before proving Lagrange's Theorem, we establish two critical lemmas regarding the size and number of cosets [2].

Lemma 5.1.1 (Equivalence of Left and Right Coset Cardinality)**.** *Let H be a subgroup of G. Let $\mathcal{L}_H$ denote the set of all left cosets of H, and $\mathcal{R}_H$ denote the set of all right cosets of H. There exists a strict bijection between $\mathcal{L}_H$ and $\mathcal{R}_H$, implying that the number of left cosets equals the number of right cosets [3].*

Proof. We define a mapping $\phi : \mathcal{L}_H \to \mathcal{R}_H$ by $\phi(gH) = Hg^{-1}$ for all $g \in G$.

1. *Well-defined and Injective:* Suppose $g_1H = g_2H$. By coset equivalence, this is true if and only if $g_2^{-1}g_1 \in H$. Since H is closed under inverses, $(g_2^{-1}g_1)^{-1} = g_1^{-1}(g_2^{-1})^{-1} = g_1^{-1}g_2 \in H$. This strictly implies that $Hg_1^{-1} = Hg_2^{-1}$ [1]. Thus, ϕ is both perfectly well-defined and strictly injective.

2. *Surjective:* For any arbitrary right coset $Hg \in \mathcal{R}_H$, we can rewrite it as $H(g^{-1})^{-1}$. This is the exact image of the left coset $g^{-1}H$ under our mapping ϕ, meaning $\phi(g^{-1}H) = Hg$ [2].

Since ϕ is a valid bijection, the cardinalities are strictly equal. □

Lemma 5.1.2 (Size of a Coset)**.** *Let H be a subgroup of G. For any $g \in G$, the cardinality of the left coset gH is exactly equal to the cardinality of H, meaning $|gH| = |H|$ [3].*

Proof. Define a mapping $\psi : H \to gH$ by $\psi(h) = gh$ [1]. The map is clearly surjective by the very definition of a coset. To check injectivity, suppose $\psi(h_1) = \psi(h_2)$. Then $gh_1 = gh_2$. By the left cancellation law in group G, we immediately obtain $h_1 = h_2$. Thus, ψ is a bijection, and $|gH| = |H|$ [2]. □

Theorem 5.2 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of H strictly divides the order of G [3]. Furthermore, the exact relationship is given by:*

$$|G| = [G : H] \cdot |H| \tag{53}$$

Proof. By the foundational property of cosets, the collection of all distinct left cosets of H forms a disjoint partition of the entire group G. By definition, there are exactly $[G : H]$ such disjoint cosets [1]. By our previous lemma, every single left coset contains exactly $|H|$ elements. Since G is the disjoint union of these $[G : H]$ equivalent-sized blocks, the total number of elements in G must simply be the product of the number of blocks and the size of each block [2]. Therefore, $|G| = [G : H] \cdot |H|$. □

5.4 Corollaries to Lagrange's Theorem

Corollary 5.2.1 (Order of an Element)**.** *Let G be a finite group and let $g \in G$. Then the order of the element g strictly divides the order of G [1].*

Proof. The order of the element g, denoted $|g|$, is exactly equal to the order of the cyclic subgroup it generates, $|\langle g \rangle|$. Since $\langle g \rangle$ is a subgroup of G, Lagrange's Theorem dictates that its order must strictly divide $|G|$ [3]. □

Corollary 5.2.2 (Groups of Prime Order)**.** *Let G be a group with $|G| = p$, where p is a prime number. Then G is strictly a cyclic group [2].*

Proof. Since $p \geq 2$, there exists an element $g \in G$ such that $g \neq e$. Consider the cyclic subgroup $\langle g \rangle$. By Lagrange's Theorem, the order $|\langle g \rangle|$ must divide the prime p. The only strictly positive divisors of p are 1 and p. Since $g \neq e$, $|\langle g \rangle| > 1$. This mathematically forces $|\langle g \rangle| = p$, which directly implies that $\langle g \rangle = G$. Thus, G is cyclic [1]. □

Theorem 5.3 (Multiplicativity of the Index)**.** *Let G be a finite group, and let H and K be subgroups such that $K \subset H \subset G$. Then:*

$$[G : K] = [G : H][H : K] \tag{54}$$

[3].

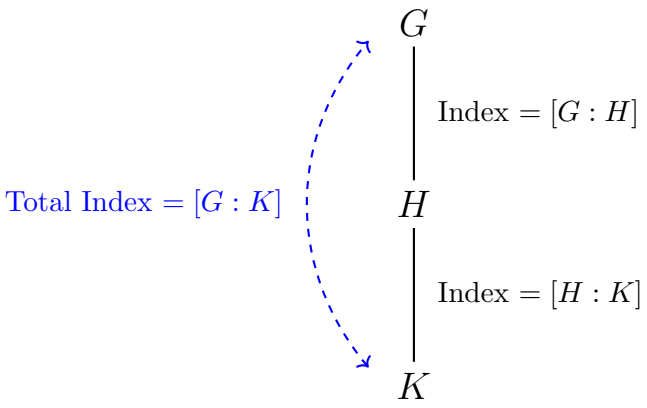


Figure 10: A subgroup lattice (or tower) illustrating the multiplicativity of the index. By Lagrange's Theorem, $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]$ [1].

5.5 The Converse of Lagrange's Theorem is False

Lagrange's Theorem guarantees that the order of any subgroup strictly divides the order of the group. However, the converse statement—"If d divides $|G|$, then G must have a subgroup of order d"—is generally false [2].

Example 5.4 (The Alternating Group A_4)**.** Consider the alternating group $A_4 \subset S_4$, which has an order of $|A_4| = \frac{4!}{2} = 12$. The divisors of 12 are $1, 2, 3, 4, 6$, and 12. We will rigorously prove by contradiction that A_4 contains no subgroup of order 6 [1].

Suppose there exists a subgroup $H \subset A_4$ such that $|H| = 6$. The index of this hypothetical subgroup would be $[A_4 : H] = \frac{12}{6} = 2$. Because the index is exactly 2, H has exactly two left cosets: H itself, and gH for some $g \notin H$. Since cosets partition the group, the right cosets must also be H and Hg. This strictly forces $gH = Hg$, meaning H is a normal subgroup [3]. Consequently, for any element $x \in A_4$, its square must inherently fall into H (i.e., $x^2 \in H$).

Now, observe that A_4 contains all 3-cycles of 4 elements. The total number of distinct 3-cycles in A_4 is exactly 8 (computed via combinatorics: choosing 3 elements from 4 yields $\binom{4}{3} \times 2 = 8$) [2]. Let x be any of these 3-cycles. The order of a 3-cycle is 3, so $x^3 = id$. Since $x^2 \in H$, it follows that $(x^2)^2 = x^4 = x \cdot x^3 = x \cdot id = x$. Because H is algebraically closed, $(x^2)^2 \in H$, which necessitates that $x \in H$ [1].

This logic dictates that H must contain *all* eight 3-cycles of A_4. However, this requires $|H| \geq 8$, which violently contradicts our foundational assumption that $|H| = 6$ [3]. Thus, no such subgroup can exist.

6 Isomorphisms and Cayley's Theorem

6.1 Cyclic Groups and Isomorphisms

Theorem 6.1 (Classification of Finite Cyclic Groups)**.** *If G is a finite cyclic group of order n, then G is strictly isomorphic to the additive group $\mathbb{Z}_n$ [1].*

Proof. Let $G = \langle a \rangle$ with $|a| = n$. We define a mapping $\phi : \mathbb{Z}_n \to G$ by $\phi(k) = a^k$ [2]. By the properties of exponents in cyclic groups, this mapping is both well-defined and bijective. Furthermore, it inherently preserves the group operation since $\phi(k + l) = a^{k+l} = a^k a^l = \phi(k)\phi(l)$ [3]. Thus, $G \cong \mathbb{Z}_n$. □

Corollary 6.1.1 (Groups of Prime Order)**.** *If G is a group of order p, where p is a prime number, then G is isomorphic to $\mathbb{Z}_p$ [2].*

Proof. By a previous corollary to Lagrange's theorem, any group of prime order is strictly cyclic [1]. Applying the preceding theorem directly yields $G \cong \mathbb{Z}_p$ [3]. □

6.2 Cayley's Theorem

Theorem 6.2 (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations [3].*

Proof. Let G be an arbitrary group. For any element $g \in G$, we define a function $\lambda_g : G \to G$ by $\lambda_g(x) = gx$ for all $x \in G$. This specific mapping is formally called the *left regular representation* of G [1].

First, we must prove that λ_g is a valid permutation on the set G (meaning $\lambda_g \in S_G$):

1. *Injectivity:* Suppose $\lambda_g(a) = \lambda_g(b)$. Then $ga = gb$. By the left cancellation law in G, we rigorously obtain $a = b$ [2].
2. *Surjectivity:* For any arbitrary element $y \in G$, we can strategically choose $x = g^{-1}y \in G$. Evaluating the function yields $\lambda_g(x) = g(g^{-1}y) = (gg^{-1})y = y$, proving the map is strictly onto [1].

Next, consider the set of all such permutations: $\bar{G} = \{\lambda_g \mid g \in G\}$. We must show that $\bar{G}$ forms a subgroup of S_G [3]. Evaluating the composition of two such functions λ_g and λ_h on an element $x \in G$ gives:

$$(\lambda_g \circ \lambda_h)(x) = \lambda_g(hx) = g(hx) = (gh)x = \lambda_{gh}(x) \tag{55}$$

This mathematically proves that $\lambda_g \circ \lambda_h = \lambda_{gh}$, ensuring closure [1]. The identity element is clearly λ_e (since $\lambda_e(x) = ex = x$), and the inverse of λ_g is strictly $\lambda_{g^{-1}}$ [2]. Thus, $\bar{G} \leq S_G$.

Finally, we construct an isomorphism $\phi : G \to \bar{G}$ defined by $\phi(g) = \lambda_g$. The mapping is surjective by the very definition of $\bar{G}$, and it is injective because $\lambda_g = \lambda_h \implies \lambda_g(e) = \lambda_h(e) \implies ge = he \implies g = h$ [3]. It structurally preserves the operation since $\phi(gh) = \lambda_{gh} = \lambda_g \circ \lambda_h = \phi(g)\phi(h)$ [1]. Consequently, $G \cong \bar{G}$, completing the proof. □

Example 6.1 (Left Regular Representation of $\mathbb{Z}_3$)**.** Consider the additive group $G = \mathbb{Z}_3 = \{0, 1, 2\}$. We explicitly compute its left regular representations to find the isomorphic permutation group $\bar{G} \leq S_3$ [2]:

$$\lambda_0(x) = 0 + x \pmod 3 \implies \lambda_0 = id \tag{56}$$

$$\lambda_1(x) = 1 + x \pmod 3 \implies \lambda_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (0\ 1\ 2) \tag{57}$$

$$\lambda_2(x) = 2 + x \pmod 3 \implies \lambda_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (0\ 2\ 1) \tag{58}$$

Thus, $\mathbb{Z}_3 \cong \bar{G} = \{id, (0\ 1\ 2), (0\ 2\ 1)\}$, which perfectly corresponds to the alternating group A_3 [3].

7 Direct Products

Given two independent groups, we can constructively mathematically synthesize a new group using their Cartesian product [1].

Definition 7.1 (External Direct Product)**.** Let $(G, \cdot)$ and $(H, *)$ be groups. The *external direct product* of G and H, denoted by $G \times H$, is the set of all ordered pairs (g, h) where $g \in G$ and $h \in H$, equipped with the component-wise binary operation [3]:

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 * h_2) \tag{59}$$

Proposition 7.0.1. *The Cartesian product $(G \times H, \cdot)$ strictly forms a group [2].*

Proof. If e_G and e_H are the identities in G and H respectively, then the ordered pair (e_G, e_H) is strictly the identity in $G \times H$ [1]. The inverse of any element (g, h) is unequivocally (g^{-1}, h^{-1}) [3]. Associativity is naturally inherited directly from the constituent groups G and H [2]. □

Example 7.1 (The Klein Four-Group via Direct Product)**.** Consider the external direct product $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ under component-wise modulo 2 addition [1]. The full Cayley table is seamlessly constructed as:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Table 2: The Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ [3].

Notice that for any element $x \in \mathbb{Z}_2 \times \mathbb{Z}_2$, adding it to itself yields the identity: $x + x = (0,0)$. This strictly implies that every non-identity element has an order of exactly 2. Consequently, this group is not cyclic, structurally proving that $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$ [2].

Theorem 7.1 (Order of Elements in a Direct Product)**.** *Let $(g, h) \in G \times H$. If $|g| = r$ and $|h| = s$, then the order of the ordered pair (g, h) is exactly the least common multiple of r and s [1]:*

$$|(g, h)| = \operatorname{lcm}(r, s) \tag{60}$$

Proof. Let $m = \operatorname{lcm}(r, s)$ and let $k = |(g, h)|$. By evaluating the element to the power of m, we acquire:

$$(g, h)^m = (g^m, h^m) = (e_G, e_H) \tag{61}$$

because m is a multiple of both r and s [3]. This forces the true order k to divide m, hence $k \leq m$ [2]. Conversely, by the strict definition of order, $(g, h)^k = (g^k, h^k) = (e_G, e_H)$. This necessitates that $g^k = e_G$ (meaning r divides k) and $h^k = e_H$ (meaning s divides k) [1]. Since k is a common multiple of both r and s, and m is explicitly defined as the *least* common multiple, it must be that $m \leq k$. Combining both inequalities rigorously yields $m = k$, successfully concluding the proof [3]. □

7.1 Internal Direct Products

Definition 7.2 (Internal Direct Product)**.** Let G be a group, and let H and K be subgroups of G. The group G is formally called the *internal direct product* of H and K if it precisely satisfies the following three conditions [1]:

1. $G = HK = \{hk \mid h \in H, k \in K\}$
2. $H \cap K = \{e\}$
3. $hk = kh$ for all $h \in H$ and $k \in K$

Theorem 7.2. *If a group G is the internal direct product of subgroups H and K, then G is structurally isomorphic to the external direct product $H \times K$ [2].*

Proof. We construct a mapping $\phi : H \times K \to G$ mathematically defined by $\phi(h, k) = hk$. First, we must meticulously verify that ϕ is a valid bijection [3].

- *Surjectivity:* By the first defining condition of internal direct products, $G = HK$, any element $g \in G$ can be intrinsically written as $g = hk$ for some $h \in H, k \in K$. Thus, ϕ is naturally surjective [1].
- *Injectivity:* Suppose $\phi(h_1, k_1) = \phi(h_2, k_2)$. Then $h_1k_1 = h_2k_2$. By multiplying h_2^{-1} on the left and k_1^{-1} on the right, we algebraically yield $h_2^{-1}h_1 = k_2k_1^{-1}$. The left side explicitly belongs to H, while the right side strictly belongs to K. Therefore, the element $h_2^{-1}h_1$ resides in the intersection $H \cap K$. By the second defining condition, $H \cap K = \{e\}$, which mathematically forces $h_2^{-1}h_1 = e \implies h_1 = h_2$ and $k_2k_1^{-1} = e \implies k_1 = k_2$. This thoroughly proves injectivity [2].

Finally, we confirm that ϕ preserves the group operation. Since elements from H and K universally commute (the third condition), we evaluate [3]:

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2) \tag{62}$$

Consequently, the internal direct product is perfectly isomorphic to the external direct product $H \times K$. □

8 Normal Subgroups and Factor Groups

8.1 Definition and Equivalence of Normal Subgroups

Definition 8.1 (Normal Subgroup)**.** A subgroup N of a group G is formally defined as *normal* if its left and right cosets precisely coincide for every element in G. That is, for all $g \in G$, $gN = Ng$ [2]. If N is normal in G, we frequently denote it as $N \triangleleft G$.

Theorem 8.1 (Equivalent Conditions for Normality)**.** *Let N be a subgroup of a group G. The following three mathematical statements are perfectly equivalent [1]:*

1. *N is normal in G ($gN = Ng$ for all $g \in G$).*
2. *$gNg^{-1} \subseteq N$ for all $g \in G$.*
3. *$gNg^{-1} = N$ for all $g \in G$.*

Proof. We will construct a cyclic chain of implications: (1) $\implies$ (2) $\implies$ (3) $\implies$ (1) [3].

Proof of (1) $\implies$ (2)*:* Let N be normal, so $gN = Ng$. For any arbitrary $n \in N$, the element $gn \in gN$. Because $gN = Ng$, there necessarily exists an element $n' \in N$ such that $gn = n'g$ [2]. Multiplying by g^{-1} on the right strictly yields $gng^{-1} = n' \in N$. Therefore, the entire set $gNg^{-1} \subseteq N$ [1].

Proof of (2) $\implies$ (3)*:* Assume $gNg^{-1} \subseteq N$ for all $g \in G$. Since this holds universally for *all* elements, it inherently must hold for the element g^{-1} [3]. Thus, $(g^{-1})N(g^{-1})^{-1} \subseteq N$, which radically simplifies to $g^{-1}Ng \subseteq N$. Multiplying this set inclusion by g on the left and g^{-1} on the right mathematically forces $N \subseteq gNg^{-1}$ [1]. Since we have both $gNg^{-1} \subseteq N$ and $N \subseteq gNg^{-1}$, the sets are perfectly identical: $gNg^{-1} = N$.

Proof of (3) $\implies$ (1)*:* Assume $gNg^{-1} = N$ for all $g \in G$. Multiplying both sides by the element g strictly on the right yields the classic relation $gN = Ng$ [2]. This thoroughly concludes the equivalence. □

8.2 Factor Groups (Quotient Groups)

Theorem 8.2 (Construction of a Factor Group)**.** *Let N be a normal subgroup of a group G. The collection of all left cosets of N in G forms a rigorously valid algebraic group under the defined operation $(aN)(bN) = (ab)N$. This specific structure is called the* factor group *(or quotient group) and is denoted as G/N, with an order of exactly $[G : N]$ [3].*

Proof. The most pivotal and non-trivial step is proving that this coset multiplication is mathematically *well-defined*—meaning the result fundamentally depends exclusively on the respective cosets themselves, not merely on the specific representatives chosen [1].

Suppose we choose different representatives for the same identical cosets, such that $aN = a'N$ and $bN = b'N$. We must meticulously verify that $(ab)N = (a'b')N$ [2]. By coset properties, $a \in a'N$, so there exists $n_1 \in N$ such that $a = a'n_1$. Similarly, $b \in b'N$, so $b = b'n_2$ for some $n_2 \in N$ [3].

We algebraically evaluate the product ab [1]:

$$ab = (a'n_1)(b'n_2) = a'(n_1b')n_2 \tag{63}$$

Because N is rigorously normal, the left coset $b'N$ equals the right coset Nb'. The element n_1b' strictly belongs to Nb', so it can be cleanly rewritten as $b'n_3$ for some $n_3 \in N$ [2]. Substituting this back gives:

$$ab = a'(b'n_3)n_2 = (a'b')(n_3n_2) \tag{64}$$

Since N is a subgroup and inherently closed, the product n_3n_2 is definitively an element of N. This clearly shows that ab structurally belongs to the coset $(a'b')N$. By coset equivalence, this mathematically guarantees that $(ab)N = (a'b')N$, proving the operation is impeccably well-defined [3].

The remaining group axioms follow naturally [1]:

- *Identity:* The coset $eN = N$ acts perfectly as the identity, since $(aN)(eN) = (ae)N = aN$.
- *Inverses:* The absolute inverse of aN is $a^{-1}N$, since $(aN)(a^{-1}N) = (aa^{-1})N = eN = N$.
- *Associativity:* It is inherited directly from G, as $((aN)(bN))(cN) = (ab)NcN = ((ab)c)N = (a(bc))N = aN((bN)(cN))$ [2].

□

A The Division Algorithm

The Division Algorithm is a fundamental theorem in number theory and abstract algebra. It serves as the logical mathematical foundation for understanding cyclic groups, greatest common divisors,

and Euclidean domains [1, 3]. The rigorous proof of this theorem relies fundamentally on the Well-Ordering Principle of the integers.

Theorem A.1 (Well-Ordering Principle)**.** *Every non-empty subset of the non-negative integers contains a least element [2].*

Theorem A.2 (The Division Algorithm)**.** *Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r, \quad 0 \leq r < b \tag{65}$$

The integer q is traditionally called the quotient, and r is called the remainder [2].

Proof. **Existence:**
Consider the set S defined by all non-negative remainders of the form $a - bk$ for any integer $k \in \mathbb{Z}$:

$$S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \geq 0\} \tag{66}$$

First, we must formally show that S is non-empty. If $a \geq 0$, choosing $k = 0$ yields $a - b(0) = a \geq 0$, which means $a \in S$. If $a < 0$, choosing $k = a$ yields $a - ba = a(1 - b)$. Since $b \geq 1$, we have $1 - b \leq 0$. Multiplying two non-positive numbers gives $a(1 - b) \geq 0$, ensuring $a(1 - b) \in S$. Thus, S is always a non-empty subset of the non-negative integers [1].

By the Well-Ordering Principle (Theorem A.1), S must contain a strictly least element. Let us denote this least element as r. Since $r \in S$, there exists some integer q such that $r = a - bq$, which naturally rearranges to $a = bq + r$. Furthermore, by the very definition of S, $r \geq 0$ [3].

We must now prove that $r < b$. Suppose, for the sake of contradiction, that $r \geq b$. Then we can constructively define a new integer r' such that:

$$r' = r - b = (a - bq) - b = a - b(q + 1) \tag{67}$$

Since $r \geq b$, it clearly follows that $r' \geq 0$. Furthermore, r' is exactly of the form $a - bk$ (with $k = q + 1$), which dictates that $r' \in S$. However, $r' = r - b < r$ because $b > 0$. This directly contradicts our foundational assumption that r is the least element of S [2]. Therefore, our assumption $r \geq b$ must be strictly false, conclusively proving that $0 \leq r < b$.

Uniqueness:
To prove that q and r are algebraically unique, suppose there exist another pair of integers q' and r' satisfying the theorem:

$$a = bq + r = bq' + r', \quad 0 \leq r, r' < b \tag{68}$$

Without loss of generality, we may assume $r \geq r'$. Subtracting the two algebraic equations yields:

$$b(q - q') = r' - r \implies b \mid (r' - r) \tag{69}$$

Since $0 \leq r < b$ and $0 \leq r' < b$, the difference $r' - r$ is strictly bounded by the inequality $-b < r' - r \leq 0$. The only integer multiple of b that strictly falls within this narrow range is 0 [1].

Therefore, $r' - r = 0$, which dictates $r = r'$. Substituting this result back into the prior equation gives $b(q - q') = 0$. Since $b > 0$, we are mathematically forced to conclude that $q = q'$. This completely proves that the quotient and the remainder are uniquely determined [3]. □

B The Cayley-Hamilton Theorem and Matrix Groups

While primarily a foundational result in linear algebra, the Cayley-Hamilton Theorem provides a powerful algebraic tool for analyzing matrix groups such as the General Linear Group $GL_n(\mathbb{R})$ [1].

Theorem B.1 (Cayley-Hamilton Theorem)**.** *Let A be an $n \times n$ matrix over a commutative ring (such as $\mathbb{R}$ or $\mathbb{C}$). If $p(\lambda) = \det(\lambda I - A)$ is the characteristic polynomial of A, then substituting the matrix A into its own characteristic polynomial yields the zero matrix:*

$$p(A) = 0 \tag{70}$$

Remark (Application to Group Inverses in $GL_2(\mathbb{R})$). In abstract algebra, this theorem offers an elegant and explicit method to compute the inverse of an element within a matrix group without relying on Gaussian elimination [3].

Consider an arbitrary matrix $A \in GL_2(\mathbb{R})$. Its characteristic polynomial is strictly given by $p(\lambda) = \lambda^2 - \mathrm{Tr}(A)\lambda + \det(A)$. By applying the Cayley-Hamilton Theorem, we establish the fundamental matrix equation:

$$A^2 - \mathrm{Tr}(A)A + \det(A)I = 0 \tag{71}$$

Since $A \in GL_2(\mathbb{R})$, we are mathematically guaranteed that its determinant is non-zero ($\det(A) \neq 0$). We can algebraically rearrange the terms and factor out the matrix A:

$$A\left(\mathrm{Tr}(A)I - A\right) = -\det(A)I \implies A\left[\frac{1}{\det(A)}\left(\mathrm{Tr}(A)I - A\right)\right] = I \tag{72}$$

By the definition of an inverse in a group, this strictly demonstrates that the inverse element A^{-1} can be expressed purely as a linear combination of A and the identity matrix I [2]:

$$A^{-1} = \frac{1}{\det(A)}\left(\mathrm{Tr}(A)I - A\right) \tag{73}$$

References

[1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Hoboken, NJ, 3rd edition, 2004.

[2] John B. Fraleigh. *A First Course in Abstract Algebra*. Pearson, Boston, MA, 7th edition, 2002.

[3] Joseph A. Gallian. *Contemporary Abstract Algebra*. Cengage Learning, Boston, MA, 9th edition, 2016.