Proceedings of CONF-APMM 2026 Symposium: Applied Mathematics and Quantitative Modeling
DOI: 10.54254/2753-8818/2026.PU36747

A Concise Survey of Group Theory: Fundamental Theorems and Reaching Applications

Chenyu Yang

Shanghai Experimental Foreign Language School, Shanghai, China
ychenyu2709@outlook.com

Abstract. Group theory is a basic part of contemporary abstract algebra that offers an organised system for studying symmetry and structure in mathematics and science. Galois studied polynomial equations in the 19th century and provided a basis for this work. The first section of this paper is a general introduction to group theory. First, present the basic concepts of groups, subgroups, cosets and group actions, and then briefly review Lagrange's Theorem and the Orbit-Stabilizer Theorem. It also studies the relationship between the above results and normal subgroups, quotient groups, homomorphisms and isomorphism theorems. To show the practical value of group theory, typical applications are presented in this paper to demonstrate how abstract ideas of symmetry can be used to describe physical laws, molecular and crystal structures, and algebraic systems in modern cryptography. Finally, the article introduces the connections among the above problems and proposes future research directions.

Keywords: Group Theory, Group Actions, Orbit-Stabilizer Theorem, Abstract Algebra

1. Introduction

Group theory offers a general language for expressing symmetry and structure in mathematics and other sciences. In the early 19th century, the French mathematician Évariste Galois first presented the idea of a "group" in his seminal but unpublished notes, and these notes were not published during his lifetime [1]. Galois showed that the difficulty of solving general fifth-degree equations by radicals is closely related to the symmetry relations among their roots, which are described by what is now known as the Galois group. Building on this foundation, related algebraic structures such as rings, fields, and ideals subsequently developed, which becomes central components of both pure and applied mathematics [2].

Formally, a group is a non-empty set G equipped with a binary operation satisfying four axioms. From this minimal definition, a rich theoretical framework emerges. One of the earliest and most fundamental results is Lagrange's theorem, first implicitly used by Joseph-Louis Lagrange in the study of permutations of polynomial roots and later formalized in group-theoretic terms: for any finite group G and any subgroup $H \leq G$, the order of H divides the order of G [3, 4]. Another central result arises from the theory of group actions.

Apart from the pure mathematical field, group theory has also become indispensable in the natural sciences. The Symmetry Group in Physics provides the foundation for expressing laws of

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-8818/2026.PU36747

nature. Lie groups are used to describe the gauge symmetries of the Standard Model of particle physics, and these Lie groups are responsible for all fundamental forces [5]. The Poincaré group is a group of symmetries for Minkowski space that describes the structure of special relativity [6]. Point groups and space groups are frequently employed in the fields of chemistry and materials science to predict the spectral features and other physical properties of these materials [7]. The other is that group theory is the basis for modern cryptography and coding theory. For example, the difficulty assumptions of some public-key cryptosystems are based on the structure of algebraic groups over finite fields [8].

No new theoretical results will be proposed in this paper; instead, a short introduction to group theory and its internal logical structure and various applications will be given. Section 2 of this paper provides the basic definitions and fundamental theorems of group theory. Section 3 introduces the deep theoretical connections among the above concepts and their significance in abstract algebra; Section 4 explores typical applications of group theory to demonstrate how the abstract algebraic structure can be realised in specific scientific fields; and finally, Section 5 presents the conclusion of this paper.

2. Basic definitions and fundamental theorems

The axiomatic definition of a group abstracts the common features of symmetry transformations, permutations, and arithmetic structures. A group is a pair $(G, \cdot)$ where G is a non-empty set and $\cdot : G \times G \to G$ is a binary operation such that:

1. Closure: $a \cdot b \in Gforalla, b \in G$;
2. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)foralla, b, c \in G$;
3. Identity: there exists $e \in Gwithe \cdot a = a \cdot e = aforalla \in G$;
4. Inverses: for each $a \in G$ there exists $a^{-1} \in Gwitha \cdot a^{-1} = a^{-1} \cdot a = e$.

If the operation is additionally commutative, the group is called abelian. Standard examples include $(\mathbb{Z}, +)$, the symmetric group $S_nonnletters$, and the general linear group $GL_n(\mathbb{R})$ under matrix multiplication.

2.1. Lagrange's theorem

Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$, and the index $[G : H] = |G|/|H|$ equals the number of distinct left cosets of H in G.

Sketch of proof. The relation $a \sim b \iff a^{-1}b \in H$ is an equivalence relation on G ; its equivalence classes are exactly the left cosets gH, all of which have cardinality $|H|$. Since G is partitioned into disjoint cosets $|G| = [G : H] \cdot |H|$.

Lagrange's theorem is historically rooted in Lagrange's study of permutations of roots of polynomials, and was later recast in abstract group language in the 19th century. It immediately implies that the order of every element divides the group order, and that groups of prime order are cyclic.

2.2. Group actions and the orbit–stabilizer theorem

A group action of G on a set X is a map $G \times X \to X$, $(g, x) \mapsto g \cdot x$, satisfying $e \cdot x = x$ and $g \cdot (h \cdot x) = (gh) \cdot x$. For $x \in X$, the orbit is $Orb(x) = \{g \cdot x \mid g \in G\}$ and the stabilizer is $Stab(x) = \{g \in G \mid g \cdot x = x\} \leq G$.

DOI: 10.54254/2753-8818/2026.PU36747

Theorem (Orbit–Stabilizer). Let G act on X and $x \in X$. Then there is a bijection $G/Stab(x) \longrightarrow Orb(x) \qquad gStab(x) \mapsto g \cdot x$.

Consequently, if G is finite, $|G| = |Orb(x)| \cdot |Stab(x)|$.

Proof idea. Define $\varphi : G \to Orb(x)$ by $\varphi(g) = g \cdot x$. Its fibers are exactly the left cosets of $Stab(x)$, so the induced map from the coset space is bijective.

This theorem unifies counting arguments in group theory: it yields Cauchy's theorem (existence of elements of prime order dividing $|G|$), bounds on conjugacy class sizes, and Burnside's lemma for counting orbits under a finite group action.

2.3. Place within the survey

These two results are not isolated facts. Lagrange's theorem operates at the level of subgroup indices; the Orbit–Stabilizer theorem refines it by linking subgroup structure to the geometry of a group action. Both appear repeatedly in later sections: in Section 3 this study examines how they connect to normal subgroups, quotient groups, and the isomorphism theorems; in Section 4 this paper uses them to explain symmetry counts in chemistry, conserved quantities in physics, and subgroup-based constructions in cryptography.

3. Theoretical connections within group theory

The results presented in Section 2 are not isolated facts of finite-group combinatorics; they are the first manifestations of a single structural principle: the size and shape of a group are controlled by how it acts on itself and on external sets, and by which subgroups survive quotienting. In this section this paper makes that principle explicit by tracing the logical chain from Lagrange's theorem to the isomorphism theorems.

3.1. From cosets to normal subgroups

Lagrange's theorem rests on the partition of G into left cosets gH , all of size $|H|$. This already suggests that the index $[G : H]$ is a flexible invariant than the order alone. However, left and right cosets need not coincide. When they do that is, when $gH = Hg$ for all $g \in G$ the subgroup H is called normal, denoted $H \trianglelefteq G$. Normality is exactly the condition that allows one to define a group structure on the set of cosets to form the quotient group G/H.

Group actions bridge this via conjugation $(x \mapsto gxg^{-1})$: H is normal if and only if its orbit under conjugation is a single point $(Orb(H) = \{H\})$. Thus, the Orbit–Stabilizer theorem frames normal subgroups as those with trivial conjugacy motion.

3.2. Orbit–stabilizer refines lagrange

Let G act transitively on a set X. For a Fixed $x \in X$. The Orbit-Stabilizer theorem gives $|G| = |Orb(x)| \cdot |Stab(x)| = |X| \cdot |Stab(x)|$.

Special Case Alignment: Lagrange's theorem emerges when G acts by left multiplication on the coset space $G/H(where X = G/H, |X| = [G : H]$, and $Stab(H) = H)$

Core Insight: Index counting is not a separate combinatorial trick, but a specific instance of orbit counting under canonical group actions.

DOI: 10.54254/2753-8818/2026.PU36747

3.3. Homomorphisms, kernels, and the First Isomorphism Theorem

For a group homomorphism $\varphi : G \to K$, the kernel $ker\varphi$ is normal in G, and the image $\varphi(G)$ is a subgroup of K. The map $\bar{\varphi} : G/ker\varphi \to \varphi(G) defined by gker\varphi \mapsto \varphi(g)$ yields the First Isomorphism Theorem: $G/ker\varphi \cong \varphi(G)$.

Isomorphism Theorems & Quotient Calculus. The First Isomorphism Theorem subsumes Lagrange's theorem (via projection maps) and demonstrates that quotient groups are the canonical, structure-preserving way to evaluate homomorphic images while eliminating normal subgroups. The remaining isomorphism theorems extend this foundation shown in Table 1:

Table 1. Isomorphism theorems and their structural roles

Theorem statement structural role	Theorem statement structural role	Theorem statement structural role
Second(Diamond) $\mathrm{HN/N} \cong \mathrm{H/(H \cap N)}$ Relates the interaction of a subgroup $H \leq G$ and a normal subgroup $N \trianglelefteq G$	Second(Diamond) $\mathrm{HN/N} \cong \mathrm{H/(H \cap N)}$ Relates the interaction of a subgroup $H \leq G$ and a normal subgroup $N \trianglelefteq G$	Second(Diamond) $\mathrm{HN/N} \cong \mathrm{H/(H \cap N)}$ Relates the interaction of a subgroup $H \leq G$ and a normal subgroup $N \trianglelefteq G$
Third $(G/N)/(K/N) \cong G/K$ Simplifies nested quotients for normal subgroups	Third $(G/N)/(K/N) \cong G/K$ Simplifies nested quotients for normal subgroups	Third $(G/N)/(K/N) \cong G/K$ Simplifies nested quotients for normal subgroups
$N \trianglelefteq K \trianglelefteq G$	$N \trianglelefteq K \trianglelefteq G$	$N \trianglelefteq K \trianglelefteq G$

Systematized by Emmy Noether and popularized in van der Waerden's Moderne Algebra, these theorems transform early coset counting into a systematic calculus of quotients, providing a unified framework for structural algebra.

3.4. Why this matters inside abstract algebra

The chain: *Lagrange* $\Rightarrow$ *cosetpartition* $\Rightarrow$ *groupaction/Orbit-Stabilizer* $\Rightarrow$ *normalsubgroups* $\Rightarrow$ *quotientgroups* $\Rightarrow$ *isomorphismtheorems* is the backbone of group theory. The three functions are as follows:

1. All the counting problems (orders, exponents, group sizes, etc.) can be expressed by a single formula.

2. It can be seen that "maintaining the collapse of structure" (i.e., taking quotients of normal subgroups) is algebraically equivalent to operations of taking remainders or eliminating symmetries.

3. Using the unified framework of isomorphism theorems, finite group theory can be connected with representation theory, Sylow theory, and ring and module theory.

From this perspective, Lagrange's theorem is not merely a conclusion about divisibility, but rather an entry point to the modern perspective of group theory, that is, the best way to understand a group is by examining its group action and the lattice of normal subgroups.

DOI: 10.54254/2753-8818/2026.PU36747

3.5. Transition to applications

In Section 4 this paper leaves the internal architecture of group theory and show that the same objects—stabilizers, quotient groups, orbit decompositions reappear as physical conservation laws, molecular symmetry classes, and cryptographic hardness assumptions. The theoretical connections drawn here are precisely what make those applications non-accidental: a point group in chemistry is a stabilizer subgroup; a gauge group in physics is a normal subgroup modded out in the quotient space of field configurations; a finite-field multiplicative group in cryptography is a cyclic quotient whose order-divisibility is Lagrange's theorem in disguise.

4. Applications of group theory

The structural concepts developed in Sections 2 and 3 coset partitions, orbit–stabilizer counting, normal subgroups, and quotient groups are not merely abstract constructions. They reappear, often verbatim, as organizing principles in physics, chemistry, and cryptography. This section illustrates how the same algebraic machinery governs symmetry in physical laws, molecular structure, and modern cryptosystems.

4.1. Physics: symmetry groups and conservation laws

In theoretical physics, symmetries are formalized through group actions on physical systems. The cornerstone is Noether's theorem.These symmetries are described by Lie groups smooth manifolds that are also groups—whose local structure is captured by Lie algebras [5].

A paradigmatic example is the Standard Model of particle physics, where fundamental interactions are governed by gauge symmetries associated with the Lie group $SU(3) \times SU(2) \times U(1)$. The quotient group construction appears explicitly: the Higgs mechanism breaks $SU(2) \times U(1)$ to a $U(1)$ subgroup, and the resulting quotient structure explains how gauge bosons acquire mass while preserving local gauge invariance [5, 6].

At a more foundational level, the Poincaré group the semidirect product of translations and Lorentz transformations encodes the symmetries of Minkowski spacetime in special relativity. The irreducible representations of this group classify elementary particles by mass and spin, a direct application of the orbit–stabilizer principle: the orbit of a momentum vector under the Poincaré group determines the particle's mass shell, while the stabilizer subgroup (the little group) determines its spin degrees of freedom [6]. Thus, what physicists call "particle classification" is, algebraically, the decomposition of a group representation into orbits and stabilizers.

4.2. Chemistry and materials science: point groups and space groups

In chemistry, molecular symmetry is described by point groups, which are finite subgroups of $O(3)$ that leave at least one point fixed. The symmetry of a water molecule (H_2O), for instance, is captured by the point group C_{2v}. The Orbit Stabilizer theorem provides a systematic way to count vibrational modes: the number of distinct vibrational states equals the number of orbits of the atomic displacement space under the molecular point group action [7]

For crystalline solids, the relevant structures are space groups, which combine point symmetries with translational symmetry. There are exactly 230 distinct space groups in three dimensions, a classification result that relies fundamentally on Lagrange's theorem: the translational subgroup is a normal subgroup of the space group, and the quotient group is a finite point group. The order of this

DOI: 10.54254/2753-8818/2026.PU36747

quotient divides the index of the translational subgroup, constraining the possible symmetry types [7]. This algebraic constraint is what allows chemists to predict X-ray diffraction patterns and optical activity from symmetry alone.

4.3. Cryptography: algebraic groups over finite fields

Modern cryptography increasingly relies on the hardness of computational problems in algebraic groups. A canonical example is ECC. The security of ECC rests on the ECDLP, whose difficulty is tied to the group's order. Lagrange's theorem ensures that the order of any element divides the total number of points on the curve, a fact that cryptographers exploit to select secure curve parameters [8-10].

Similarly, the multiplicative group $\mathbb{F}_p^{\backslash\backslash}$ times of a finite field plays a central role in the Diffie Hellman key exchange. This group is cyclic of order p-1, and Lagrange's theorem guarantees that for any divisor d of p-1, there exists a subgroup of order d. This property is used to construct safe primes and to ensure that discrete logarithms are well-defined within the chosen subgroup [8]. In this context, the abstract notion of a quotient group also appears: protocols such as ElGamal encryption implicitly work in the quotient of the multiplicative group by the subgroup generated by the public key, ensuring semantic security.

4.4. Synthesis: why group theory works across domains

What unites these diverse applications is not analogy but mathematical identity. A molecular point group is literally a stabilizer subgroup; a gauge symmetry is literally a normal subgroup being quotiented out; a cryptographic group is literally a finite abelian group whose order divisibility is governed by Lagrange's theorem. The Orbit–Stabilizer theorem, introduced in Section 2 as an abstract counting principle, becomes in physics a tool for particle classification, in chemistry a tool for spectroscopic prediction, and in cryptography a tool for parameter validation.

This cross-domain utility is precisely why group theory is often described as the "language of symmetry." It provides a single set of axioms that, once internalized, unlock structural insights across disciplines without requiring domain-specific modifications.

5. Conclusion

This paper briefly introduced group theory and traced the development of its first ideas by Galois to its present application as a unifying language in mathematics and science. Based on the axiomatic definition of a group, this paper explored how Lagrange's Theorem and the Orbit-Stabilizer Theorem arise naturally from the interplay between a group and its action on a set. These results were shown not as isolated combinatorial facts, but as the entry point to a deeper structural theory: the identification of normal subgroups, the construction of quotient groups, and the systematic framework of the isomorphism theorems.

A central theme of this survey has been that the power of group theory lies in its double life. On one hand, it is a purely abstract discipline, concerned with the internal architecture of algebraic objects. On the other, it is a practical toolkit, whose concepts stabilizers, orbits, cosets, quotients appear verbatim in the description of physical laws, molecular symmetries, and cryptographic protocols. The Poincaré group's role in classifying elementary particles, the use of point and space groups in predicting spectroscopic behavior, and the reliance of elliptic curve cryptography on

DOI: 10.54254/2753-8818/2026.PU36747

Lagrange's theorem all testify to the same underlying principle: symmetry, when formalized through group theory, becomes a computable and predictive property of a system.

From a pedagogical perspective, this survey highlights the value of teaching group theory not as a self-contained algebraic curiosity, but as a bridge to other disciplines. The logical chain from cosets to quotient groups to representations provides students with a template for translating abstract definitions into concrete calculations a skill that transfers well beyond mathematics.

Looking ahead, several directions naturally extend the scope of this work. One is the study of representation theory, which builds on group actions to linearize group elements and is indispensable in quantum mechanics and chemistry. Another is the exploration of infinite and topological groups, such as Lie groups and Galois groups, which underpin modern number theory and differential geometry. Finally, the growing role of group-theoretic hardness assumptions in post-quantum cryptography suggests that the interplay between abstract algebra and information security will only deepen in the coming decades.

References

[1] Edwards, H. M. (1984). *Galois theory*. Springer.
[2] Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (3rd ed.). Wiley.
[3] Lagrange, J.-L. (1771). Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*.
[4] Rotman, J. J. (1995). *An introduction to the theory of groups* (4th ed.). Springer.
[5] Georgi, H. (1999). *Lie algebras in particle physics* (2nd ed.). Westview Press.
[6] Weinberg, S. (1995). *The quantum theory of fields, Vol. 1: Foundations*. Cambridge University Press.
[7] Cotton, F. A. (1990). *Chemical applications of group theory* (3rd ed.). Wiley.
[8] Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An introduction to mathematical cryptography*. Springer.
[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017, November). Quantum resource estimates for computing elliptic curve discrete logarithms. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 241-270). Springer International Publishing.
[10] Zhang, Z., & Zhao, Y. (2024). Enhanced elliptic curve cryptography (EECC). *Procedia Computer Science, 247*, 1324-1330.