Proceedings of CONF-APMM 2025 Symposium: Simulation and Theory of Differential-Integral Equation in Applied Physics
DOI: 10.54254/2753-8818/2025.DL27546

Proof and Applications of Lagrange's Theorem in Deriving Fermat's Little Theorem and Euler's Theorem

Siyi Liu

Raffles Institution, Singapore, Singapore
26YLIUS158W@student.ri.edu.sg

Abstract. The group theory, as one of the cornerstones of the modern algebra, has a profound historical trajectory that reflects the evolution of the mathematical thought. This comprehensive paper analyses the historical development of the group theory and provides an overview of the interconnectedness of the several key theorems in the group theory: The Lagrange's Theorem, the Fermat's Little Theorem and the Euler's Theorem. This paper begins by establishing the modern group-theoretical framework within the Lagrange's Theorem on the link between the order of groups and that of its subgroups. Then, an extension onto other related theorems are provided. In all, this paper is highly interlinking among the ideas in group theory. Ultimately, this study not only demonstrates the beauty of mathematical interconnections but also highlights their continuing relevance for the modern applications, showing how the classical results remain relevant to guide contemporary explorations in algebra, number theory, and related disciplines.

Keywords: Group theory, Lagrange's Theorem, Fermat's Little Theorem, Euler's Theorem

1. Introduction

Group Theory is fundamentally about the algebraic formalization of symmetric structures, with wide application in both the physics and chemistry fields. It was first brought up in the 1770s, then had several major breakthroughs in the 19th century by mathematicians such as Cauchy, Cayley and Hölder [1]. Up to the 18th century, mathematicians mainly focused on the study of polynomials [1]. The 19th century marked a pivotal transition for algebra, which by the 20th century had become a discipline primarily concerned with abstract, axiomatic structures [1]. Modern group theory development thus began in the 20th centuries even though World War I has caused a temporary cease in the study of group theory [2]. In 1932, Wilhelm Magnus solved the world problem for one-relator groups, and combinatorial group theory flourished throughout the 1930s to 1960s, setting the foundations for modern research in geometric and probabilistic group theory, as well as in regions such as cryptography and group theory [2].

The Italian French mathematician Joseph-Louis Lagrange, perhaps, contributed the most in the analysis field [3]. His contribution to the theory of equations has deeply influenced the development of group theory and Galois theory as well [3]. Lagrange's Theorem was initially not aimed at developing the group theory but rather to solve polynomials with degree 5 or above, since when Lagrange himself launched the results, the concept of group theory was yet to be established [4].

DOI: 10.54254/2753-8818/2025.DL27546

Lagrange's theorem has wide applications. Modern studies have been done on its analog for continued fractions on the Heisenberg Group [5], as well as its substantiation in for hom-groups which is useful in the regions of nonassociative Hopf algebras, combinatorics and cryptography [6].

With the recognition of the importance of these theorems, Section 2 provides the proof for Lagrange's Theorem and section 3 provides extensions onto Fermat's Little Theorem and Euler's Theorem.

2. Lagrange's Theorem

2.1. Relevant definitions and lemmas

Definition of subgroup

If $\mathcal{V} \subseteq \mathcal{R}$, $\mathcal{V}$ is considered a subgroup of $\mathcal{R}$ if and only if $\mathcal{V}$ is closed under production and inversion.

Definition of Coset

Let $\mathcal{V}$ represent a group, and $\mathcal{H} \leq \mathcal{V}$. A left coset of $\mathcal{H}$ in $\mathcal{V}$ is defined as a subset satisfying

$v\mathcal{H} = \{vj : j \in \mathcal{H}\}$ and $v\mathcal{H} \in \mathcal{V}$ for a fixed v.

Proposition 1

Let $v\mathcal{H}$ and $v'\mathcal{H}$ be two cosets of $\mathcal{H}$ in $\mathcal{V}$, if $v\mathcal{H} \neq v'\mathcal{H}$, then the cosets disjoint and have the same cardinality as $\mathcal{H}$.

Proof for proposition 1

Let $v \in \mathcal{V}$ and $v' \in \mathcal{V}$ and $v\mathcal{H}$ and $v'\mathcal{H}$ both be cosets of $\mathcal{H}$ in $\mathcal{V}$.

Assume that the two cosets are not disjoint, then there definitely exist $x \in v\mathcal{H} \cap v'\mathcal{H}$, and $\varkappa, \varkappa' \in \mathcal{H}$ such that $x = v\varkappa = v'\varkappa'$.

Thus, $v = v'\varkappa'\varkappa^{-1}$ and $\varkappa'\varkappa^{-1} \in \mathcal{H}$, which means that $v \in v'\mathcal{H}$.

Similarly, it can be shown that $v' \in v\mathcal{H}$.

Thus, $\forall b \in \mathcal{H} : vb = v'\varkappa'\varkappa^{-1}b$, indicating $\varkappa'\varkappa^{-1}b \in \mathcal{H}$.

Hence, $vk \in v'\mathcal{H}$ and $v\mathcal{H} \subseteq v'\mathcal{H}$ since b is arbitrary.

By symmetry, the proof for $v'\mathcal{H} \subseteq v\mathcal{H}$ can be done similarly, and by double inclusion, $v\mathcal{H} = v'\mathcal{H}$.

2.2. Proof of lagrange's Theorem

Theorem

For a finitely defined group $\mathcal{V}$ and $\mathcal{H} \leq \mathcal{V}$, the cardinality of $\mathcal{H}$ is a factor the cardinality of $\mathcal{V}$, meaning $|\mathcal{H}| \mid |\mathcal{V}|$.

Proof

$\mathcal{V}$ sits in the union of $v\mathcal{H}$ where $v \in \mathcal{V}$, i.e. $\mathcal{V} = Uv\mathcal{H}$, and $v = e \cdot v \in v\mathcal{H}$.

Let $v1, v2, v3 \ldots vn$ be elements of $\mathcal{V}$ such that $\mathcal{V} = Uivi\mathcal{H}$.

Note that $vi\mathcal{H} = vj\mathcal{H}$ holds if and only if $i = j$, Then $|\mathcal{V}| = \sum_{i=1}^{n} |vi\mathcal{H}| = \sum_{i=1}^{n} |\mathcal{H}| = n\,|\mathcal{H}|$, Thus, $|\mathcal{H}| \mid |\mathcal{V}|$.

3. Application

Lagrange's Theorem is of high significance in the field of number theory [7,8]. It provides a powerful and beautiful bridge between the abstract structure of groups and the fundamental

DOI: 10.54254/2753-8818/2025.DL27546

arithmetic properties of integers. One can easily and directly apply Lagrange's theorem to derive several fundamental results in the number theory field such as Euler's Theorem and Fermat's Little Theorem.

3.1. Relevant definitions, corollaries and proofs

Binary operation

Let $\mathscr{A}$ be a set; a function $\mathscr{A} \times \mathscr{A} \to \mathscr{A}$ is a binary operation and its image (a, b) is denoted as ab.

Symmetric groups

Sym(A) is the set of bijections from A to A, i.e., $Sym(A) \times Sym(A) \to Sym(A)$ is a binary operation.

Properties of symmetric groups

1) Associative; $\forall \mathrm{i}, \mathrm{j}, \mathrm{k} \in \varkappa$, $(\mathrm{ij})\mathrm{k} = \mathrm{i}(\mathrm{jk})$.

2) There exists a unit $\mathrm{e} \in \varkappa$, $\forall \mathrm{i} \in \varkappa$: $\mathrm{e} \bullet \mathrm{i} = \mathrm{i} \bullet \mathrm{e} = \mathrm{i}$.

3) Inversible; $\forall \mathrm{i} \in \varkappa, there\ exists\ i^{'} \in \varkappa : ii^{'} = i^{'}i = e.$

4) Inverse on $\varkappa$ is unique.

Cyclic subgroup

A subgroup of Sym(A) is cyclic if and only if it is generated by one single element, i.e., $H =< \{a\} >$, $a \in Sym(A)$.

Euler's totient function

The number of $t \in \mathbb{Z}$ satisfying $1 \le t \le j$ and $gcd(t, j) = 1$, denoted by $\varphi(j)$

Equivalence relation

For a set $\mathscr{T}$, a relation $\mathscr{R}$ on $\mathscr{T}$ is a subset of $\mathscr{T} \times \mathscr{T}$. It is defined that $i \in \mathscr{T}$ is $\mathscr{R}$-related to $j \in \mathscr{T}$ if and only if $(i, j) \in \mathscr{R}$ and is written as $i\mathscr{R}j$.

Properties of equivalence relation

1) R is reflective if and only if $\forall \mathrm{i} \in \mathscr{A}$, $\mathrm{i}\mathscr{R}\mathrm{i}$.

2) R is symmetric if and only if $\forall \mathrm{i}, \mathrm{j} \in \mathscr{A}$, $\mathrm{i}\mathscr{R}\mathrm{j}$ gives $\mathrm{j}\mathscr{R}\mathrm{i}$.

3) R is transitive if and only if $\forall \mathrm{i}, \mathrm{j}, \mathrm{k} \in \mathscr{A}$, $(\mathrm{i}\mathscr{R}\mathrm{j}, \mathrm{j}\mathscr{R}\mathrm{k})$ gives $\mathrm{i}\mathscr{R}\mathrm{k}$.

A relation satisfying all 3 criteria is said to be an equivalence relation, denoted by " ~ ".

Lying in the same coset

Let $H \le g$. Define $i \sim_H p$ if and only if $i^{-1}u \in H$ for $i, u \in g$.

Proof for lying in the same coset

Take $u \in g$. $u \bullet u^{-1} = 1 \in G$, hence $u \sim_H u$.

Take $u, p \in g$. If $u^{-1}p \in H$, thus $\left(u^{-1}p\right)^{-1} \in H$. Hence $u^{-1}p \in H$ and $p \sim_H u$.

Take $i, u, k \in g$. Assume $i^{-1}u \in H$ and $j^{-1}k \in H$, then $\left(i^{-1}u\right)\left(j^{-1}u\right) \in H$. Hence $i^{-1}k \in H$ and $i \sim_H k$.

Equivalent class

Denoted by $[a] = \{b \in A : a \sim b\}$.

Corollary

For a finitely defined group $\mathscr{V}$ with identity e and $v \in \mathscr{V}$ then $o(v) \mid |\mathscr{V}|$ and $v^{|\mathscr{V}|} = e$.

Proof

$o(v)$ equals to the cardinality of $< v >$ where $< v >$ is the cyclic subgroup generated by v.

DOI: 10.54254/2753-8818/2025.DL27546

Since $< v >$ $\leq \mathcal{V}$, by Lagrange's Theorem, $o(v) \mid |\mathcal{V}|$. Thus, $|\mathcal{V}| = b \times o(v)$ where $b \in \mathbb{Z}$. Thus, $v^{|\mathcal{V}|} = v^{b \times o(v)} = \left(v^{o(v)}\right)^b = e^b = e$.

3.2. Fermat's little Theorem

Definition

Let g be a prime number while $j \in \mathbb{Z}$ that does not share any common factor as g. Thus, $j^{g-1} \equiv 1 \left(mod\ g\right)$.

Proof

$[a]_g \in \mathbb{Z}_g^{\times}$ which is a group of size $g-1$, so $[a]_g = [1]_g$, so $\left([a]_g\right)^{g-1}$ equals to $[1]_g$, so $\left[a^{g-1}\right]_g = [1]_g$, so $a^{g-1} \equiv 1 \left(mod\ g\right)$.

3.3. Euler's Theorem

Definition

Let $m \in \mathbb{Z}^+$. If $k \in \mathbb{Z}^+$ and does not possess a common factor as m, then $k^{\varphi(m)} \equiv 1 \left(mod\ m\right)$.

Proof

Since $a^{|G|} = e = \left(a^{o(a)}\right)^{|G|/o(a)}$ and $\left|\frac{Z}{n\mathbb{Z}}\right| = \varphi\left(n\right)$, $[a]^{\varphi(n)} = e = [1]$, hence $\left[a^{\varphi(n)}\right] = \left[1\right]$, hence $a^{\varphi(n)} \equiv 1 \left(mod\ n\right)$.

4. Conclusion

This paper provides basic insights on how Lagrange's Theorem can be extended and applied not only in the region of group theory itself but also in other areas, especially in group theory. Lagrange Theorem provides alternative proofs for Fermat's Little Theorem and Euler's Theorem, integrating these mathematical concepts and forming a more comprehensive picture altogether. It is in hope that further developments can be made on Lagrange's Theorem. In particular, its applications may extend beyond classical number theory to modern fields such as cryptography, algebraic coding theory, and computational mathematics, where group theory methods are increasingly used. These directions highlight the enduring value of Lagrange's theorem as a foundational tool and a bridge for interdisciplinary exploration.

References

[1] Kleiner, I. (1986). The evolution of group theory: A brief survey. Mathematics Magazine, 59(4), 195-215.
[2] Hobbs, M., & Mallory, E. (2025). A Biography of Vilhjalmur Stefansson, Canadian Arctic Explorer (Vancouver: UBC Press, 1986); Gísli Pálsson, Travelling Passions: The Hidden Life of Vilhjalmur Stefansson, trans. Keneva Kunz (Winnipeg: University of Manitoba Press, 2005); and Janice Cavell and Jeff Noakes, Acts of Occupation: Canada and Arctic Sovereignty, 1918–25 (Vancouver: UBC Press, 2010). 20 On Stefansson's anthropological fieldwork in northern Canada, see Gísli Pálsson, ed., Writing. A Cold Colonialism: Modern Exploration and the Canadian North, 275.
[3] Roth, R. L. (2001). A history of Lagrange's theorem on groups. Mathematics Magazine, 74(2), 99-108.
[4] Lienert, C. (2023). Lagrange's Proof of Wilson's Theorem—and More!.
[5] Joseph Vandehey. 2018. Lagrange's Theorem for Continued Fractions on the Heisenberg Group.
[6] Hassanzadeh, M. (2019). Lagrange's theorem for Hom-groups.

DOI: 10.54254/2753-8818/2025.DL27546

[7] Armstrong, M. A. (1988). Lagrange’s theorem. In Groups and Symmetry (pp. 57-60). New York, NY: Springer New York.
[8] Johnson, W. (1983). A note on Lagrange's theorem. The American Mathematical Monthly, 90(2), 132-133.