Proceedings of CONF-APMM 2025 Symposium: Simulation and Theory of Differential-Integral Equation in Applied Physics
DOI: 10.54254/2753-8818/2025.DL27731

The Proof of Lagrange Theorem and Its Applications

Muyao Wang

School of Mathematics and Physics, Xi'an Jiaotong-Liverpool University, Suzhou, China
Muyao.Wang23@student.xjtlu.edu.cn

Abstract. This paper explores Lagrange's Theorem, a foundational result in abstract algebra that establishes a connection between the orders of a group and its subgroups. Initially introduced by Joseph Lagrange in the 18th century, the theorem asserts that the order of any subgroup divides the order of the entire group. This investigation begins with essential concepts of group theory, including cosets and bijections, leading to a rigorous proof of Lagrange's Theorem. The paper also highlights significant implications of the theorem, such as its role in deriving Wilson's Theorem and Fermat's Little Theorem, both of which proves pivotal in algebraic theory. Furthermore, the applications of Lagrange's Theorem in modern cryptography, particularly in the RSA public-key cryptosystem, are discussed, illustrating its relevance in contemporary mathematical practices. Despite its profound impact, there is no guarantee of the existence of subgroups for every divisor by the theorem, a limitation addressed by Sylow's Theorem. This paper concludes by emphasizing the enduring significance of Lagrange's Theorem in linking abstract algebra to practical applications and suggests avenues for future research in Galois theory and advanced cryptographic methods.

Keywords: Group theory, Lagrange Theorem, RSA

1. Introduction

In 18th century, the problem of solving polynomial equations with degree 5 and higher attracted and puzzled enormous mathematicians and one of these people was Joseph Lagrange [1]. Lagrange conducted in-depth study on permutation groups and focused on how the roots of some equations can be permuted. He realized that the permutation of the roots makes up a group, which has a close relation with the solutions of equations. Then, in 1770-1771, Lagrange first gave the statement of the relation of the order between groups and their subgroups, which are latterly called Lagrange Theorem [1]. In fact, the ideas of groups and some other concepts were not specified and well defined yet in 18th century, when Lagrange Theorem appeared. It was in 19th century that genius mathematicians Galois and Abel gave rigorous definitions and concepts to the group theory. Despite this, Lagrange Theorem remained a milestone, influencing subsequent developments of algebra.

Basically, Lagrange Theorem is so revolutionary that it reveals the close relations between groups and subgroups since it states that the order of the group can be divided by the order of the subgroup. Thus, it guides mathematicians that studying the sub-structures of some groups may help gain deeper insight into the structure of the whole group. However, there is a key limitation from the statement of the theorem, which is that it only tells the possibility of orders. But for each order, there

DOI: 10.54254/2753-8818/2025.DL27731

may not exist such a group. That drawback pushed the development of group theory, and one breakthrough is Sylow Theorem in 19th century.

In addition, some important corollaries and applications can be directly proposed from Lagrange's Theorem. One simple example is the statement that "if $|A|$ is finite and $|A|$ is a prime number, then A is a cyclic group". There are some other famous theorems which can be deduced from Lagrange Theorem, such as Fermat's Little Theorem and Wilson's Theorem [2]. Besides that, with the development of group theory, Lagrange Theorem can be applied to some modern science fields like cryptography technology to increase the safety of encryption. One specific example is the Rivest-Shamir-Adleman (RSA) system which uses Lagrange Theorem a lot [3]. The public-key and private-key used in RSA are based on the group theory and have become the most secure cryptography method since 1977 [4].

This paper aims to carry out investigations and research on the Lagrange Theorem with some related, advanced applications. To achieve this goal, this article is primarily concentrated on group theory and will start with some concepts. Then, some important propositions will be introduced. Next, strict proof of Lagrange Theorem will be deduced. Finally, there will be some famous applications or theorems to illustrate the strength of Lagrange Theorem.

2. Lagrange theorem

2.1. Basic concepts of group theory

Before the detailed proof of Lagrange theorem, many basic but important concepts of group theory should be firstly clarified [5].

Definition (coset): Let B be a subgroup of $(A,\cdot)$. The left coset of B with representative $a \in A$ to be the set $aB = \{ab \in Ab \in B\}$ [6].

Lemma: Take a group D and C is a subgroup of $(D,\cdot)$. For any $a,b \in D$, if $a \in bC$, then $aC = bC$.

Proposition (1): If G be a group and let H is a subgroup. The set $G/H = \{aH|a \in G\}$ is the set of all left cosets of H and is a partition of G.

Proposition (2): Let G be a group and H is a subgroup. For any $a, \in G$, there is a bijection $\phi : H \longrightarrow aH \ : \ h \mapsto ah.$

2.2. Proof of propositions and lemma

To prove this lemma, this paper proceeds in two steps by proving $aH \subseteq bH$ and $bH \subseteq aH$ respectively. If $a \in bH$, then, there exists $c \in H,$ such that $a = bh_1$, so $b^{-1}a = h_1 \in H$. Take any $ah \in aH$, then $ah = \left(bb^{-1}\right)ah = b(b^{-1}a\Big)h = bh_1h = b\Big(h_1h\Big) \in bH$. So, this is the first step, and it has proved that $aH \subseteq bH$. Next, since $b^{-1}a = h_1 \in H$, it can be deduced that $\left(b^{-1}a\right)^{-1} = a^{-1}b = h_1^{-1} \in H$. Similarly, take any $bh \in bH$, then $bh = \left(aa^{-1}\right)bh = a\left(a^{-1}b\right)h = ah_1^{-1}h = a\Big(h_1^{-1}h\Big) \in aH$. This means that $bH \subseteq aH$. In conclusion, $aH = bH$. The proof of lemma finishes.

Moving to the proof of proposition (1). Since it comes to the set $G/H = \{aH|a \in G\}$, three properties of the partition need to be verified:

a)$\emptyset \notin G/H$:

DOI: 10.54254/2753-8818/2025.DL27731

Let $aH \in G/H$ be an arbitrary coset. As $e \in G$, based on the definition, $a = a \cdot e \in aH$ as required.

b)$\forall a, b \in: aH \cap bH \neq \emptyset \Longrightarrow aH = bH$:

Since $x \in aH \cap bH$, then, $x \in aH$ and $x \in bH$. Using the lemma, it can be deduced that $aH = xH = bH$ as required.

c)$\forall g \in G, \exists aH \in G/H : g \in aH$:

Actually, g can be chosen since $g = g \cdot e \in gH$.

To sum up, the set G/H is a partition of G.

Finally, showing ϕ is invertible can verify that ϕ is bijective. Thus, show that $\psi : aH \to H : x \mapsto a^{-1}x$ is an inverse. Note that ψ is well-defined, that is, for every $x \in aH$, $a^{-1}x \in H$. Then, for every $h \in H \, and \, x \in aH$: $\psi \circ \phi(h) = \psi(ah) = a^{-1}(ah) = \left(a^{-1}ah\right) = h$. And $\phi \circ \psi(x) = \phi\left(a^{-1}x\right) = a\left(a^{-1}x\right) = \left(aa^{-1}\right)x = x$ as required. This shows that ϕ is a bijection.

2.3. Proof of lagrange theorem

There is a finite group N and a subgroup M. And it can be concluded that $|N| = |N/M| \cdot |M|$. In particular, the number of elements in M is the divisor of the number of elements in N. This is the famous Lagrange Theorem and can be proved by following steps: the group G is partitioned into $|N/M|$ distinct left cosets by the proposition (1). From proposition (2), since all left cosets are bijective, they have the same elements. Each cosets have $|M|$ elements. So, $|N| = |N/M| \cdot |M|$ as required.

However, it should be noted that Lagrange Theorem does not make any statement about the existence of a subgroup with a given order. For example, one can verify that the alternating group A_4 has no subgroups of order 6 although 6 divides $|A_4| = 12$.

3. Applications of lagrange theorem

3.1. Wilson's theorem

The idea of the theorem was first proposed by an Iraqi mathematician called Ibn al-Haytham around 1000 AD. Then it is the British mathematician Edward Waring who published the theorem and gave fair credit to his student John Wilson for their findings [7]. However, Lagrange published the first proof of what is known as Wilson's Theorem in the article [8]. Wilson's theorem is used in many other formulas of mathematics such as Formulas for Prime.

The basic construction of Wilson's Theorem is not complicated, which can be stated that if $p > 2$ and p is prime, then $(p-1)! \equiv -1(mod\, p)$.

Proof: Since p is an odd prime, so $\mathbb{Z}_p^{\times}$ contains $p-1$ elements. The aim is to pair elements with their inverses. Note that each element has a corresponding inverse. An element is equal to its own inverse if and only if its square is the identity element. i.e., $a \equiv a \iff a^2 \equiv 1\left(mod\, p\right)$. And this can be rewritten as $p \mid \left(a^2 - 1\right) = \left(a+1\right)\left(a-1\right)$. Thus, either $p \mid (a-1)$ or $p \mid (a+1)$. This shows that the only elements which are their own inverse are exactly 1 and $p-1$. Removing these two elements, there are left with $p-3$ (an even number) elements, which must pair up. Therefore, the product of the remaining elements is 1. Hence, $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \cdot 1 \cdots 1 \equiv p-1 \equiv -1(mod\, p)$. And this proves the theorem.

DOI: 10.54254/2753-8818/2025.DL27731

3.2. Fermat's little theorem

This theorem which belongs to enormous findings of Fermat is an important conclusion in the theory of algebra and is named after the famous French mathematician Pierre de Fermat. It has been used tremendously to simplify or convert a very large power of a number to a relatively small integer as a crucial theorem in the basic number theory [9]. Fermat first stated the theorem in a letter to his friend Bessy in 1640 without a proof. He stated that if n is a prime number, then for any integer a that is not a multiple of n, the number $(a^{n-1}-1)$ is an integer multiple of n. The first known proof was given by Gottfried Wilhelm Leibniz in an unpublished manuscript around 1683, but it remained unknown until the 19th century. The first published proof was from one of the greatest mathematicians Leonhard Euler in 1736 who generalized the theorem (known as Euler's Theorem) [6].

Proof: There are two cases to consider [10].

a) If $a \equiv 0(mod\ n)$, in this case, a is an multiple of n which means the exponential of a minus a is still the multiple of n, i.e., $a^n \equiv a\ (mod\ n) \Longleftrightarrow a^{n-1} \equiv 1\ (mod\ n)$ as required.

b) If a is not the multiple of n, in this case, a is invertible in $\mathbb{Z}_n$. The multiplicative $\mathbb{Z}_n^{\times}$ has $n-1$ elements. Before continuing the proof, there is one corollary of Lagrange Theorem to clarify: Take G which is a finite group. For any $g \in G$, there should be $g^{|G|} = e_G$. Using this corollary, $a^{n-1} \equiv 1(mod\ n)$ as required.

c) Proof of the corollary: By the Lagrange Theorem, the $|g|$ divides $|G|$, as a result, $\frac{|G|}{|g|}$ is an integer. Thus, $g^{|G|} = g^{|g|\cdot\frac{|G|}{|g|}} = {e_G}^{\frac{|G|}{|g|}} = e_G$.

In fact, Euler gave an improvement of this theorem and stated that as p is a prime number, then for any integer a, $(a^p - a)$ is the multiple of p.

4. Conclusion

This paper has stated that Lagrange Theorem, a cornerstone of the group theory, establishes that the order of a subgroup divides the order of the group with exploring the detailed proof via cosets and bijections, demonstrating its fundamental role in algebra. Key applications include two famous and vital theorems which have been discussed above, as well as its use in the RSA system. However, the theorem does not ensure the existence for every divisor, a limitation addressed by Sylow's Theorem. Future research could focus on the applications in Galois theory and modern cryptography. Despite this, Lagrange Theorem remains indispensable, linking abstract algebra to practical fields and inspiring further mathematical advancements.

References

[1] Roth, R. L. (2001). A history of Lagrange's theorem on groups. Mathematics Magazine, 74(2), 99-108.
[2] Miron, R. and Anastasiei, M., (2012). The geometry of Lagrange spaces: theory and applications, 69, Springer science & business media.
[3] Meijer, A. R. (1996). Groups, factoring, and cryptography. Mathematics Magazine, 69(2), 103-109.
[4] Kaliski, B. (2006). The mathematics of the rsa public-key cryptosystem. RSA laboratories.
[5] Kattan, D. A., Amin, M., & Bariq, A. (2022). Certain Structure of Lagrange's Theorem with the Application of Interval-Valued Intuitionistic Fuzzy Subgroups. Journal of Function Spaces, 2022(1), 3580711.
[6] Zhu Peiyu. (2023). Lagrange's Theorem in Group Theory: Proof and Applications. Highlights in Science, Engineering and Technology, 47: 75–78.

DOI: 10.54254/2753-8818/2025.DL27731

[7] Gyamfi, K. B., Aidoo, A., & Akweittey, E. (2021). Some Applications of Lagrange's Theorem in Group Theory Using Numerical Examples. WWJMRD, 7(2), 32-34.
[8] Lienert, C. (2023). Lagrange's Study of Wilson's Theorem.
[9] Samandari, N., Nazari, N. M., Olfat, J. A., Rafi, R., Azizi, Z., Ulfat, W. I., ... & Niazi, M. J. (2023). Applications of Fermat's Little Theorem. Turkish Journal of Computer and Mathematics Education, 14(3), 209-214.
[10] Kenneth J. (2017). A Geometric Construction Involving Wilson's Theorem. International Journal of Computer Applications, 175(1): 6-8.