Unveiling Lagrange's Theorem and its Applications in Proving other Theorems

Shenghan Lin *

Queen Ethelburga's College, York, United Kingdom

* Corresponding Author Email: slin@qe.thorpeunderwood.com

Abstract. The group theory is an essential subject in Mathematics and Physics, and the target of this paper is to prove a famous theorem in group theory, so-called Lagrange's Theorem. By using some really basic definitions of group, the exsistance of this theorem is essential for abstract algebra. In this paper, the author will focus on how to prove Lagrange's Theorem step by step from the base of group theorey, mainly by using the nature of cosets and how does each coset in the same subgroup behaves to get the final result. Ultimately, the author will demonstrate that the order of the group is divisible by the order of its subset. As mentioned ealier, the status of this theorem is unshakable. Because of this theorem, many other corollary theorem was discovered, for example Wilson's Theorem and etc. All of these corollaries are very important in modern technologys, going deep into this theorem could help discover more useful applications of it. This paper should be essential for people who are interested in the Lagrange's theorem.

Keywords: Cosets, Subgroup, Lagrange's theorem; Wilson's theorem.

1. Introduction

Lagrange's Theorem was first stated in 1770-71 by Joseph-Louise Lagrange [1**]**. He published this theorem in one of his famous article, "Reflexions sur la resolution algebrique des equarions**"** [2]. He stated that is a polynomial which has n variables that can be permuted in $n!$ ways, the number of distinct polynomial that behave like this is always a multiple of $n!$. For example, take x and y as two variables, and they permutes in all 2 ways in the equation $x - y$ then in total, there are 2 different equation $a - b$ and $b - a$, and 2 is a factor of 2. From the point view of history, the theorem was published without any proof, and the first authoritative proof was provided by Augustin-Louis Cauthy in 1844. During the past decades, it has been demonstrated that the Lagrange's theorem has many applications.

The existance of this theorem built up the base of group theorey, there are many other important corollary from Lagrange's Theorem, for example "if G is not infinite with $|G|$ prime, subsequently G is a cyclic group", "if the order of group G has a finite number n then the order of any a that belongs to G divides the order of G and in some special $a^n = e$", and also of course some famous theorems like Wilson's theorem and Fermat's Little theorem, among others. The application of Lagrange's Theorem has been used in many areas in modern society, especially on internet technology, some network security system, a famous one would be RSA Crypto System, are based on it. The key of investigating Lagrange's Theorem is to find out more useful applications for the world.

This paper is written in three sections. The first section is about a brief introduction of Lange range's Theorem and how important in abstract algebra and its status in modern science. Next section is about the proof of Lagrange's Theorem, the author will prove some basic theorems of group theory, mostly about cosets, and use them for the final prove of Lagrange's theorem later on. The last section is about some famous applications of this theorem, which contain Fermat's Little theorem and Wilson's Theorem, and the author will provide some examples of how these corollaries can be used in high level technologies.

2. Lagrange's Theorem

2.1. Introduction of Theorem and Coset

There are many important concepts in group theory. Here, for clarify, the author will present some of the major concepts.

Theorem 1: If $a \epsilon Hb$, then $Ha = Hb$.

Theorem 2: Let G be a group and $G \geq H$. The family of all cosetHa, as a ranges over G, is a partition of G [3]

Theorem 3: Every arbitrary coset Ha contains an equal number of elements as subgroup H, so all cosets of H in G possess the same cardinality.

Theorem 4: Let G be a finite group and let H be a subgroup of G. The order of G is always a multiple of the order of subgroup H.

Define a group called G and H is a subgroup of$G$. For all element x that is in G, xH denotes the set of all products xh, as x stay the same and h can be any element in H, then xh is a left coset of H in G. Namely, $xH = \{ xh \mid h \in H \}$ is a left coset, while $Hx = \{ xh \mid h \in H \}$ is a right coset [4].

2.2. Proof of Theorems

Let this paper begin with the proof of theorem 1. Let H be a subgroup of G, and two cosets $Ha\ and\ Hb$. If $a \in Hb$, then it is inferred that $a = h_1 b$.Firstly, the author will show that $Ha$is a subset of Hb. Take some $x \in Ha$, for some element of H. $x = h_2 a = h_2(h_1 b) = (h_2 h_1)b \epsilon Hb$(1), so $Ha \leq Hb$. Then take some $y \in Hb$, for some element of H. Since $a = h_1 b$, multiply both side by h_1^{-1}, thus $b = h_1^{-1} a$,

$$y = h_3 b = h_3(h_1^{-1} a) = (h_3 h_1^{-1})a \tag{1}$$

Thus, $H_b \leq H_a$ and finaly theorem 1 is proved.

Moving on to the proof of theorem 2. Begin with taking two cosets $Ha\ and\ Hb$, the aim is to show that $Ha \cap Hb = \emptyset\ or\ Ha = Hb$(they are either disjoint or equal). Assume there is an overlap between $Ha\ and\ Hb$, take some element of x where $x \in Ha \cap Hb$, since x is in the coset Ha, so $x = h_1 a$, for some element of h_1. x Is also in the coset Hb, therefore $x = h_2 b$, for some element of h_2. As $x = h_1 a$, multiply both side by h_1^{-1} $a = x h_1^{-1}$. x, as shown earlier, equals to $h_2 b$, so $a = h_1^{-1} h_2 b$, since H is a subgroup, $h_1^{-1} h_2$ shows that the subgroup is closed, so $h_1^{-1} h_2 \in H$, thus a is equals to some element of H times b.So $a \in Hb$. By applying Theorem 1 that was been proved earlier, $Ha = Hb$. Then show every element $c \in G$ is in some H. $c \epsilon Hc$, this is true because of the existence of the identity e, H is a subgroup; therefore, it must include the element e, $ec = c \epsilon Hc$ Now theorem 2 is proved.

Next is the proof of theorem 3. To prove this, it is necessary to prove there is a bijection from$H\ to\ Ha$. First, the author will define a function, $let\ f: G \to Ga$ be defined by $f(g) = ga$. To prove bijectivity, the most efficient way is to prove it is injective and surjective. To prove it is injective $let\ f(g_1) = f(g_2)$, by the definition of injective, for a function $f: A \to B$, any $a, b \in G$, $f(a) = f(b) \to a = b$ [5], by the definition of the function, $g(\alpha) = g(\beta) \to \alpha a = \beta a \to \alpha = \beta$ thus the function is injective. Moving on to surjective, by the definition of surjective, for a function $f: A \to B$, for every $b \in B$ there is some $a \in A$ for which $f(a) = b$[6],Take an arbitrary element $ga \in Ga$, since $g \in G$, it is clear that $f(g) = ga$.By showing that the function is injective and surjective at the same time, it shows that there is a bijection from G to Ga. This indicates that the order of the subgroup G and the arbitrary coset Ga are equal. By now, theorem 3 has been proved.

Lastly is the proof of theorem 4, Lagrange's theorem. Assume that G is a limited group and let H represents a subgroup of G, the number of elements in G can be express as

$$| G | = | H\alpha_1 | + | H\alpha_2 | + | H\alpha_3 | + \cdots + |H\alpha_n | \tag{2}$$

Where $\alpha_i \in G$. As proved earlier, by using theorem 3,

$$|H\alpha_1| = |H\alpha_2| = |H\alpha_3| = \cdots = |H\alpha_n| \quad (3)$$

Thus $|G| = n|H\alpha_1|$, and note that n is the number of coset in subgroup H. The order of any coset is equal to the order of the subgroup since a subgroup is itself a coset, so $|G| = n|H|$. This is prove of Lagrange's theorem using the two fundamental theorem of cosets. The converse of Lagrange's Theorem is invalid, a counter example would be an alternating group on four points, it is a group of order 12 that does not possess any subgroup of order 6 [7].

3. Application of Lagrange's Theorem

3.1. Fermat's Little Theorem

The theorem was first stated on October 18th, 1640, by Pierre de Fermat, the theorem was in a letter to his good friend Frénicle de Bessy. His original statement translate in English was "Every prime integer $[p]$ necessarily divides one of the powers minus one of any geometric progression$[a, a^2, a^3, \ldots, a^n]$, there exists a value k such that p divides a^{k-1}, and the exponent k divides $p-1$. Once the first power $[k]$ that fulfills the criteria is identified, all powers whose exponents are multiples of the initial exponent will similarly satisfy the criteria; in other words, all multiples of the initial k possess the same attribute. He did not include any proof of the theorem in the letter and never did so throughout his life. The inaugural officially published proof was presented by Euler in 1736, in a paper called "Demonstration of Certain Theorems Concerning Prime Numbers" [8]

Fermat's Little Theorem is a consequence of Lagrange's Theorem and represents a significant foundational result in number theory. It discusses that if a number p is prime and i is an integer not divisible by p, then it means

$$i^{p-1} \equiv 1(mod p) \quad (4)$$

Proof: let G be a group, $o(g) = |<g>|$ where g is a subgroup of G. By using Lagrange's Theorem, one knows that $|G|$ is divisible by $o(g)$, so $|G| = n * o(g)$, where n is any positive integer. Thus

$$g^{|G|} = g^{n*o(g)} = (g^{o(g)})^n = e^n = e \quad (5)$$

Author will now think another group $\mathbb{Z}_p^x$ which is a group of size $p-1$ $[i]^p \in \mathbb{Z}_p^x$, so$[i]_p^{p-1} = [1]^p$, so $[i^{p-1}]_p = [1]_p$, so $i^{p-1} \equiv 1 \, mod \, p$ [9].

Fermat's Little Theorem is an important number theorem. It has been widely used on many areas, for example when users visit a secure website on the browser, this theorem gets used as a part of the RSA Crypto System, which is like the basis of internet security.

3.2. Wilson's Theorem

The person who first stated this theorem was an Iraqi mathematician called Ibn al-Haytham in 1000 AD. The person who published the theorem was a British mathematician called Edward Waring in 1770 but without proving the theorem and gave credit to his student John Wilson for what they had found [10]. The first official proof was provided by Joseph-Louis Lagrange in 1771, there is evidence show that Gottfried Wilhelm Leibniz also discovered the result 100 years earlier, but never published.

The definition of Wilson's theorem is quite simple, it stated that if $n > 1$ and n is a prime number, then $(n-1)!$ is always one less than pn, where $p \in \mathbb{Z}^+$ and there is only one p that follows the theorem. The Theorem can be represented as

$$(n-1)! \equiv -1(mod\, n) \quad (6)$$

Proof. There are multiple of ways to prove this theorem, the author will used Fermat's Little Theorem since the thesis is about Lagrange's Theorem. There is no significance to talk about when $n = 2$, because $2! = 2$, and obviously it does obey the theorem, so assume n is a prime integer greater or equals to three. Think about a function

$$f(x) = (x-1)(x-2)(x-3)\dots(x-(n-1)), \tag{7}$$

So the degree of this polynomial is $n-1$, with a constant term $(n-1)!$, and the roots of this polynomial are $1, 2, 3, 4, \dots, n-1$. Consider another function $g(x) = x^{n-1} - 1$. The degree of g is also $n-1$. According to Fermat's Little Theorem, modulo n also should have $n-1$ roots.

Lastly, let $h(x) = f(x) - g(x)$, the highest degree of $h(x)$ can only be $n-2$ because the leading term in f and g cancels with each other, again modulo n has $n-1$ roots. But according to Lagrange's Theorem, modulo n could not have root number more than $n-2$. This mean function h must be equal to $0\ (mod\ n)$, thus the constant term of h is $(n-1)! + 1$ which is identically equal to $0(mod\ p)$. Since $(n-1)! + 1 \equiv 0(mod\ p)$, move one to the right, $(n-1)! \equiv -1\ (mod\ p)$ and this is Wilson's Theorem.

Finally, the author mentions that Wilson's Theorem is used in many other formulas, for example Quadratic Residues, Formulas for Prime and etc.

4. Conclusion

This paper had provide a detailed proof of Lagrange's Theorem by starting from a basic introduction of coset and a fundamental feature of coset: If $a \epsilon Hb$, then $Ha = Hb$, then by some simple calculation, the author illustrated the correlation between the number of elements in a coset and the number of elements in a subgroup. At the end of section two, the author showed if G is a group and H is a subgroup of G then the order of H must always divide the order of G, which is the main aim of this paper, demonstrate the proof of Lagrange's Theorem. In section 3, the author had introduced two famous applications of Lagrange's Theorem, Fermat's Little Theorem and Wilson's Theorem, and how are they been used. Lagrange's Theorem is great in various science areas, it had made thousands of contributions on computer science and cryptography. In the future, scientists might want to improve the current systems of cyber security by what people have already created. The author believes that Lagrange's theorem can also be use on the development of artificial intelligence, mainly on the efficiency of calculations.

Reference

[1] Roth, Richard L. A History of Lagrange's Theorem on Groups. Mathematics Magazine, 2001, 74(2): 99–108.

[2] Pierpont, James. Book Review: Leçons Sur La Résolution Algébrique Des Équations. Bulletin of the American Mathematical Society, 1900, 6(8): 344–49.

[3] Kattan Doha A., Amin Maria, Bariq Abdul. Certain Structure of Lagrange's Theorem with the Application of Interval-Valued Intuitionistic Fuzzy Subgroups. J. Funct. Spaces, 2022, 2022:1-9.

[4] Majid, Shaheen and Ai Tee Tan. Usage of Information Resources by Computer Engineering Students: A Case Study of Nanyang Technological University, Singapore. Online Information Review, 2002, 26(5): 318–25.

[5] Fripertinger Harald. On Iteration of Bijective Functions with Discontinuities. Annales Mathematicae Silesianae, 2020, 34(1): 51–72.

[6] Struik Ruth Rebekka. Partial Converses to Lagrange's Theorem. Communications in Algebra, 1978, 6(5): 421–82.

[7] Burton David M. The history of mathematics: an introduction. 7th ed, McGraw-Hill, 2011.

[8] Zhu Peiyu. Lagrange's Theorem in Group Theory: Proof and Applications. Highlights in Science, Engineering and Technology, 2023, 47: 75–78.

[9] Kenneth J. A Geometric Construction Involving Wilson's Theorem. International Journal of Computer Applications, 2017, 175(1): 6-8.

[10] Kwasi Baah Gyamfi, Abraham Aidoo, Emmanuel Akweittey. Some Applications of Lagrange's Theorem in Group Theory Using Numerical Examples. World Wide J. Multidiscip. Res. Dev., 2021, 7(2): 32-34.