Lagrange's Theorem in Group Theory: Proof and Applications

Peiyu Zhu*

Beijing Royal School, Beijing, China

*Corresponding author: bessie@qzml.ntesmail.com

Abstract. There are many propositions in group theory, among which Lagrange's theorem is a representative example and its own meaning can be taken as a generalization of the Euler's theorem resulting from the number theory. Lagrange's theorem can be understood as follows. Suppose that N is a group and $M \leq N$ denotes a subgroup of N. This theorem clarify that the order of a subgroup M divides that of a group N.The conjecture and discovery of Lagrange's theorem has led to the establishment of a unique framework in places such as calculus and statistics, allowing a certain interpretation for some problems. This paper presents the corollaries and applications of Lagrange's theorem, which can help to understand the properties of Lagrange's theorem easily, and can help to familiarize with how to apply Lagrange's theorem on various propositions**.** The basic concepts and fundamental theories of groups, rings and domains are the main contents of modern algebra, and the companion set and exponent are the most fundamental concepts in group theory.

Keywords: Group theory, Lagrange's theorem, Converse of Lagrange's theorem, Fermat's theorem.

1. Introduction

The earliest group theory was the symmetry of solutions summarized when solving equations. After the French mathematician Lagrange proposed the theory of permutation and substitution of roots of equations as the key to solving algebraic equations, between 1824 and 1826, mathematician Abel set out to investigate what equations that can be solved by root formulas have in common and to show that if an equation can be solved by root formulas. Then every root formula that appears in the expression can be expressed as a root of the equation and as a rational number with some unit root. This theorem was used to prove the famous Abel's theorem that it is impossible to solve equations of generally higher than fourth order algebraically [1]. However, although Abel solved the method for constructing problems that could be solved at any number of times, he failed to give a solution to the problem of whether a known equation could be solved by a root formula.

At this point, Galois, the inventor of the group, followed Abel's work and introduced the concept of the group in his posthumous work, solved the problem of solving equations by radicals completely by the method of groups, and proposed the theory of groups and domains. It was this theory that provided an important tool for the later development of mathematics - group theory [2].

The Lagrange's theorem serves as one of the most important propositions in group theory [3]. It describes an important relationship between the order of a finite group and subgroup, together with the exponent of a subgroup, thus allowing to discuss and solve many problems in finite group theory and to obtain some characteristics of finite groups. The basic concepts and fundamental theory of groups, rings and domains are the main study of modern algebra, and companion sets and exponents are the most fundamental concepts in group theory. Lagrange's theorem reveals the close relationship between the order and exponent of subgroups and the or number of groups. Thanks to Joseph Louis Lagrange, the Lagrange's theorem states that for any finite group (say N), order of the subgroup M is a factor of order N. This article uses some of the contemporary knowledge of group theory to introduce new corollaries and propositions arising from the combination of group theory on Lagrange's theorem [4]. Applications of Lagrange's theorem and its corollaries are also presented, as well as inferences and possibilities arising from converse of Lagrange's theorem.

2. Lagrange's Theorem

2.1. Definitions and Lemmas

This section is devoted to present three definitions and lemmas that will be used in the paper [5].

Definition 1 (subgroup). A subgroup is a special nonempty subset of a group. A nonempty subset M of a group N is regarded as a subgroup of N if the multiplication of N also becomes a group, denoted as $M \leq N$.

Definition 2 (Coset). A simple example illustrates that N is a group, M is a subgroup of N, and n is an element of N. Then $NM = \{m: \text{for all } m \in M\}$ denotes the left companion set of M, and $MN = \{mn: \text{for all } m \in M\}$ denotes the right companion set of M.

Only the subgroup that generates the "companion set" can form a group, and only the set that contains the unit element can form a group, and the companion set does not contain the unit element, so of course, it cannot form a group, so it is called "companion set".

Definition 3 (finite group). Let K be a group, and if n is a finite set, then it is called a finite group. The finite set consists of the set of those natural numbers less than or equal to a natural number z. It is called a line segment of the natural numbers string and is denoted by symbol $|1, z|$.

Lemma 1. If a finite order m has a group N, then each of the orders of any $a \in N$ can be figured out with the order of N, where $a^K = e$.

Proof. In group N, these elements are distinct and constitute a subgroup. Since p is the order of the subgroup, so is it the divisor. Hence, $k = np$ and $a^k = a^{zp} = (a^p)^z = e$.

Lemma 2. If the order of a finite group N is of prime order, then it has no proper subgroup.

Proof. Consider a group N and denote its prime order as m. Now, m has only two factors 1 and m. Let the prime order of the group N be m. Now, k can only find two factors, 1 and k. Therefore, it is known that the subgroups of N are $\{e\}$ and N itself. In summary, no suitable subgroup exists.

Lemma 3. A prime group with only two equal factors is a cyclic group.

Proof. Set N be a prime group containing k and $a \neq e \in N$. When k is divisible by the order of a, so it is either 1 or k, and the order of a , $0(a) \neq 1$. Since $a \neq e$, the order of $o(a) = p$ is the cyclic subgroup of N created by a can also be of order k.

2.2. Theorem and its Corollaries

Theorem (Lagrange's theorem). Let G be a finite group and N be a subgroup, then [6]

$$|N| = |Z| \cdot (N:Z) \rightarrow (N:Z) = \frac{|N|}{|Z|}. \tag{1}$$

Proof (method 1): For a given group N and subgroup Z, each chaperone set is of equal size, while at the same time they are either equal or disjoint from each other. And at the same time Z is a subgroup with unitary elements, so the right chaperone set as a whole must compose N. From this one can define an equivalence relation denoted as $a \sim b$ and denote $Za = Zb$ when and only when $ab^{-1} \in N$.

Here the equivalence relation refers to the reflexivity a~a, The symmetry relation $a \sim b \Rightarrow b \sim a$ implies that $a \sim b, b \sim c \Rightarrow a \sim c$. Thus the left companion set is an equivalence class determined by the equivalence relation ~. If the quotient group N exists, then its order is equal to the index $(N:Z)$ of Z to N, i.e., $|N| = |Z| \cdot (N:Z)$.

Proof (method 2): Let the number of elements of N and Z be z and r, respectively, and let Z have s right companion sets. At the same time, N is equal to the union of all right companion sets.

The different right companion sets have no common elements, and, the number of elements of each right companion set of s is equal to r, and r is the amount of elements of Z. Therefore, the union of all right companion sets has element rs,which is equal to the element z of N: $z = rs$ and $r/z =$ s. That is, $\frac{|N|}{|Z|} = (N:z)$.

The Lagrange's theorem has the following corollaries.

Corollary 1. Let N be a finite group and $K_1 \leq K_2 \leq \cdots \leq K_z \leq N$, and the order of each element in N is a factor of $|N|$. Then $(M : K_1) = (M : K_z) \cdot (K_z : K_{z-1}) \cdot \cdots \cdot (K_2 : K_1)$.

Proof. Since M is a finite group $K_1 \leq K_2 \leq \cdots \leq K_z \leq M$, then $|N| = |K_z| \cdot (N : K_z)$, with $|K_z| = |K_{z-1}| \cdot (K_z : K_{z-1})$, …, $K_2 = K_1 \cdot (K_2 : K_1)$. From this, one can obtain the following expansion: $|N| = |K_z|(M : K_z) = |K_{z-1}| \cdot (K_z : K_{z-1})(M : K_z) = |K_{z-2}|\,(K_{z-1} : K_{z-2})(K_z : K_{z-1})(M : K_z) = \cdots = |K_1|(K_2 : K_1) \cdots (K_z : K_{z-1})(N : K_n)$.

On the other hand, the fact that $|M| = |N| \cdot (M{:}N)$ implies that $|K_1| \cdot (M : K_1) = |K_1|(K_2 : K_1) \cdots (K_z : K_{z-1})(M : K_z)$. Noting that $|K_1| \neq 0$, then it can be proved that $(N{:}K_1) = (K_2{:}K_1) \cdots (K_z{:}K_{z-1})(N{:}K_z) \rightarrow (N{:}K_1) = (K_z{:}K_{z-1})(N{:}K_z) \cdots (K_2{:}K_1)$.

Corollary 2. If the order of a finite group N is prime, therefore it has no intrinsic subgroup.

Proof. Suppose n is a prime order of the group N. At this point N has only two factors 1 and z, which can be known by the prime group property. Therefore, N itself is a subgroup of N. So the fact that the finite group N has no proper subgroups holds.

Corollary 3. The amount of elements of each class within a finite group is a factor of the group order, which differs from the companion set in that each class does not necessarily have the same number of elements. For example, if the unit element is a class of its own, then there is only a single element in this class, but each companion set has the same number of elements.

Proof. Consider the number of elements in a class given by any g for the number of elements in the class. All elements h that are reciprocal to g $(gh = hg)$ form a subgroup, denoted as H_g.The definition of the subgroup is known, and the elements of the group are$gh = hg$. Give any two group elements in the group $h_1 g = g h_1, h_2 g = g h_2$, $h_1 h_2 g = g h_1 h_2 = h_1 g h_2$ with $h_1, h_2 \in G$, it is equivalent to prove that each element has an inverse element. Firstly, give an arbitrary group element $h \in G$, one need to prove that the inverse element is in the group $h^{-1} \in G$. That is, to prove$h^{-1} g = g h^{-1}$, $h h^{-1} g = g = g h h^{-1} = h g h^{-1}$, and $g = h g h^{-1}, h^{-1} g = g h^{-1}$. Here, using $gh = hg$ and the definition of the inverse element itself $h h^{-1} = e$, it holds for any group element h. Thus, for all elements that are reciprocal to g form the group G written as H_g.

3. Applications

3.1. Converse of Lagrange's Theorem

There is no doubt that Lagrange's theorem is one of the simplest and most important theorems in group theory. It is said that the order of a subgroup should be the order of every finite group (i.e., the divisor). By contrast, the converse of Lagrange's theorem (CLT) is that the approximate value of the divisor is the magnitude of the order of a subgroup [7].

The CLT is not necessarily always true. Let G be a finite group and assume that integer d is divisible by $|G|$, but G doesn't necessarily have a subgroup of order d. The typical counter-example is that for the 4th alternating group A (i.e., A_4) it does not satisfy the CLT [8]. This A_4 group of alternating arrangements on four objects can even be traced back to 1799, when the error of CLT was first discovered by P. Ruffini. For the group A_4, its order is 12. Hence, it has factors of 12 and 6, but there is not a subgroup of order 6. The above case shows that CLT is wrong.

Statement: Suppose A_4 has a subgroup H of order 6, then $[A_4{:}H] = 2$.

Proof. Generally, for any $x \in A_4$, if $x \in H$ then $x^2 \in H$; otherwise if $x \notin H$ then $x^{-1}x^2 = x \notin H$. Thus xH and x^2H are two different companion sets of H. Since $xH \neq H$, $x^2H = H$, then $x^2 \in H$. It follows that for any $x \in A_4$, there is $x^2 \in H$. Nothe that there are eight 3-rotations in A_4. For each 3-rotation $(abc) \in A_4$, it is known that $(a\ b\ c) = (a\ c\ b)^2 \in H$. So H contains at least 8 3-rotations of A_4, and thus $|H| \geq 8$. This contradicts the order 6 of H. So no subgroup of order 6 in A_4 is identified, and of course no element of order 6 is found.

Nevertheless, in some cases CLT holds. The class of groups that can satisfy the CLT emerges, which are called CLT groups, and the positive integers n are called CLT numbers, and the group of each order n is a CLT group [9].

3.2. Fermat's Theorem

In algebra, the Fermat's theorem states that $a^{p-1} \equiv 1(\mathrm{mod}\, p)$ holds when a is any positive integer and p is a prime [10]. Note that all nonzero elements of the congruence class of mod p form an abelian group, the Fermat's theorem can be proved with the help of Lagrange's theorem.

Remark. Let the set $X = \{(a_1, a_2, \dots, a_p) \in G^p | a_1, a_2, \dots, a_p = 1\}$ where G is a finite group and p is a prime number. Let G^p denotes the Cartesian product of pG, then $|X| = |G|^{p-1}$. The family consisting of all congruence classes of modulo m is called the modulo m integer class, denoted I_m. Now use the I_p group to act X. Define $[i]$ as $(a_1, a_2, \dots, a_p) = (a_{i+1}, a_{i+2}, \dots, a_p, a_1, a_2, \dots a_i)$. Using $a_{i+1}a_{i+2} \dots a_1a_2 \dots a_p = 1$, $a_{i+1} \dots a_p = (a_1a_2 \dots a_i)^{-1}$, and $a_{i+1}a_{i+2} \dots a_pa_1a_2 \dots a_i = 1$, one has $[i](a_1, a_2, \dots, a_p) \in X$. Also, define z: $I_m \times I_m \to I_m, z([a], [b]) = [a + b]$.

At this point, a more general conclusion than Fermat's theorem is obtained. It is stated that let G be a group of order n and let p be a prime, so $x^p = 1$ $(x \in G)$ has a number of solutions mod(p) that is congruent to n^{p-1}. On the other hand, if p is not a factor of n, then by Lagrange's theorem, G has no element of order p. Namely, $n^{p-1} = |X| = 1 + kp\,.so, n^{p-1} \equiv 1\,, mod\ p \Rightarrow n^p \equiv n$. This completes the proof of Fermat's theorem.

4. Conclusion

The Lagrange's theorem is extremely useful and significant, and it reveals a close relation between the order of a subgroup and group. The basic concepts and theories of groups, rings and fields are the main content of modern algebra, and the accompanying sets and exponents are the most fundamental concepts in group theory. Lagrange's theorem reveals the close relationship between the order of a subgroup and the exponent and group number. In this paper, by using the knowledge of modern group theory to first introduce Lagrange's theorem and the converse of Lagrange's theorem, then some basic inferences on the properties and basic concepts of Lagrange's theorem are utilized to derive more concepts. In addition, some applications of Lagrange's theorem by the inferred concepts are introduced. Finally, the Lagrange's theorem has been applied to understand the Wilson's theorem and Fermat's theorem.

References

[1] Wang efang. Fundamentals of finite group theory. Tsinghua University Press, 2002.

[2] Roth Richard L. A History of Lagrange's Theorem on Groups. Math. Mag, 2001,74(2):99-108.

[3] Cui Can, Gan Chenqin, Ren Changwang, Mo Zhangying. Lagrange's Theorem in Group Theory. J. Phys.: Conference Series, 2022, 2381: 1-6.

[4] Mamidi Sai Akash. Applications Of Lagrange's Theorem in Group Theory. Int. J. Math. Comput. Sci., 2015, 3(8): 1150-1153.

[5] 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.

[6] 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.

[7] Gallian J. A. On the Converse of Lagrange's Theorem. Am. Math. Mon., 1993,66(1): 23-23.

[8] Berger T. R. A converse to Lagrange's theorem. Cambridge University Press, 1978, Series A: 291-313.

[9] Henry Jonah N. Groups Satisfying the Converse to Lagrange's Theorem, MSU Graduate Thesis, 2019.

[10] Patil D. P., Pranesachar C. R., RafJindran Renuka. The Work of Lagrange in Number Theory and Algebra. Resonance, 2006, 11: 10-25.