Concepts, Proof, and Applications of Lagrange's Theorem

Yemei Qiao *

Heilongjiang Experimental High School, Harbin, China

* Corresponding Author Email: floraqiao1011@gmail.com

Abstract. The theory of groups and their representation, as a branch of mathematics, is a powerful tool for dealing with physical systems with certain symmetries. By using group theory method, many properties of the system can be directly understood qualitatively, complex calculations can be simplified, and the development trend of physical processes can be predicted. Lagrange's theorem is a principle in Group Theory which is seen as the expansion of Euler's theorem in number theory. It is considered an important concept to prove further complex theories in Group Theory. This study reviews these definitions and characteristics of subgroups and cosets, and then provides proofs for them. The main goal of the paper is demonstrating Lagrange's Theorem that states that every quadratic irrationality has a periodic continued fraction. The structure of a Dirichlet group emerges from these properties of the unit group in an ordered environment. Additionally, the author shows how to use Gauss's reduction to calculate n-th roots of two-dimensional matrices method. Finally, the author will provide evidence for solutions to Lagrange's Theorem.

Keywords: Group Theory; Subgroup; Coset; Lagrange's Theorem.

1. Introduction

This paper is centered on the study of group theory, with a specific focus on subgroup cosets and Lagrange's Theorem. The purpose of this study is to confirm certain propositions and the theorem itself, while also exploring various practical applications that are relevant in everyday situations, such as scientific experiments where they form the basis of knowledge. Group Theory plays a vital role in the field of mathematics and has numerous practical applications across various fields. For example, it serves as the foundation for quantum mechanics in physics. Initially used mainly for robot kinematics, its application has expanded to encompass areas. In 1984, Vage and Margrick introduced the first public-key cryptographic system based on Combinatorial Group Theory. Since then, cryptographers have collectively developed multiple public key encryption systems and key exchange protocols using this mathematical framework [1].

Group theory is a fundamental mathematical concept within abstract algebra, focus on algebraic structures such as groups. These groups play a crucial role in abstract algebra, serving as the foundation for various other algebraic structures such as rings, fields, and modules. The concept of groups permeates many areas of mathematics and has significantly influenced other branches of abstract algebra. Moreover, group theory holds great significance in the realms of physics and chemistry, providing valuable methods for modeling diverse physical structures like crystals and hydrogen atoms. Consequently, group theory and its associated representation theory have wide-ranging applications in the fields of physics and chemistry [2].

In the field of networking, group theory is used to analyze networks with double ports and converter sets that have different ports. The effective use of group theoretical methods helps to reveal the connections between these systems. Additionally, applying group theory to atomic materials improves people's understanding of the fundamental building blocks of the material world [3].

Lagrange's theorem states that the size of a subgroup is related to the size of a group which is through cost analysis. It establishes a connection between functions and their derivatives in quantitative analysis, making it useful for studying functions. This theorem is an important tool for theoretical analysis and proof development. Furthermore, applying this result leads to showing that the order of the Hom-hopf algebra BA divides the order of A by order A in a finite-dimensional home group. Sedighi and Hosseini discuss Lagrange's theorem for polygroups and show how relations between polygroup properties can be strongly regular with suitable equivalence relations. Their main

focus in this paper is on investigating Lagrange's Theorem and other lemmas related to isomorphism theorems of groups.

2. Definitions and Propositions

2.1 Subgroup and Coset

Definition 1. A group is a set G together with a binary operation: $G \times G \rightarrow G$ such that the following conditions hold [4]

(i) Closure: for any $g, h \in G$, $g \circ h$ is a uniquely defined element of G.

(ii) Associativity: for any $f, g, h \in G$,

$$(f \circ g) \circ h = f \circ (g \circ h). \tag{1}$$

(iii) Identity: There is an identity element $e \in G$ such that for all $g \in G$,

$$e \circ g = g \circ e = g. \tag{2}$$

(iv) Inverse: for every $g \in G$ there is an inverse element $g^{-1} \in G$, then there exists.

$$g \circ g^{-1} = g^{-1} \circ g = e. \tag{3}$$

Definition 2. Let G be a group and X be a set, a group action of G on X is a map

$$\mathrm{G} \times \mathrm{X} \rightarrow \mathrm{X}, (\mathrm{g}, \mathrm{x}) \rightarrow \mathrm{g} \cdot \mathrm{x} \tag{4}$$

That satisfies the two following properties: (i) $1G \cdot x = x\, for\, all\, x \in X$, and (ii) $(g1g2) \cdot x = g1 \cdot (g2 \cdot x)$ for all $x \in x$ and all $g1, g2 \in G$.

Given an element $g \in G$ and an element $s \in S$, the image $f(g, s)$ is another element of S depending on g, and the image relies on the group structure of G. Let S_X be the group of all the bijections from X to X, so every group G can be regarded as a subgroup of S_G, each $g \in G$ can be regarded as an element in S_G, so each group G has a natural action on the set G. Furthermore, a group G can act on many different sets in different ways, which gives insight into the group itself.

Definition 3. Let G be a group. A Subgroup of G is a subset $H \subset G$ that is itself a group using$G$'s group law. Explicitly, H needs to satisfy the following [5]

(i) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2$ is in H. Mathematically, one can say that H is closed. For the group law on G.

(ii) The identity element e is in H.

(iii) For every $h \in H$, the inverse h^{-1} is in H.

Note that because H uses the same law as G, the elements of H automatically satisfy the associative law, so the author does not need to add that as a requirement. If H is finite, the author defines the order of H to be the number of elements in H.

Definition 4. Let $\emptyset$: $G \rightarrow G'$ be a group homomorphism. The $kernel$ of $\emptyset$ is the set of elements of G that are sent to the identity element of G' $ker(\emptyset) \Rightarrow g \in G : \emptyset(g) = e'$.

Definition 5. If G is a group of finite order$m$, then the order of any $a \in G$ divides the order of G and in particular $a^m = e$.

Proof: Let the order of a be p, let p be the least positive integer, so $ap = e$. Then there exists$a,\ a^2,\ a^3, \ldots.,\ a^{p-1}, ap = e$, All elements of group G are different and they form a subgroup. Since the subgroup is ordered with p, thus p the order of a is the divisor of group G. So, there exists, $m = np$ where n is a positive integer. So, $a^m = a^{np} = (a^p)^n = e$ is proved.

2.2 Selected Proposition

Proposition 1. Let $\emptyset$: $G \rightarrow G'$ be a group homomorphism. The $kernel$ of $\emptyset$ is the set of elements of G that are sent to the identity element of G', $ker(\emptyset) =) g \in G : \emptyset(g) = e'$ [6].

Definition 5. Let G be a group, and let $H \subset G$ be a subgroup of G. For each $g \in G$, the (left) cost of H attached to g is the set $gH = gh: h \in H$.

In other words, gH is the set that one can get when people multiply g by every element of H But it is important to note that different elements of G may give the same coset of H.

Proposition 2. There is a finite group G, and let $H \subset G$ be a subgroup of G.

(a) Every element in G is in some coset of H.

(b) Every cost of H has the same number of elements.

(c) Let $g_1\, g_2 \in G$, then cosets g_1H and g_2H satisfy either $g_1H = g_2H$ or $H \cap g_2H = \phi$.

Proof. (a) Let $g \in G$. The subgroup H contains the identity element e, so the coset gH contains $g \cdot e = g$.

(b) Let $g \in G$. The author is going to prove that the cosets gH and H have the same number of elements by proving that the map $F: H \to gH, F(h) = gh$ is a bijective map from H to gH.

First, check that F is injective. Assume that $h^1, h^2 \in H$ satisfy $F(h^1) = F(h^2)$,which means that$gh_1 = gh_2$, and multiplying by g^{-1}on the left shows that $h_1 = h_2$. Hence F is injective. Next, check that F is surjective. Every element of gH looks like gh for some $h \in H$, and$F(h) = gh$, so every element of gH is the image of an element of H. Hence F is surjective. Now it has been proven that $F: H \to gH$ is bijective, so the number of elements in particular H and gH are the same. Since this is true for every $g \in G$, it can be concluded that every cost of H has the same number of elements [7].

(c) If $g_1H \cap g_2H = \emptyset$, assume the two costs are not disjoint. This means one can find elements $h_1, h_2 \in H$ satisfying $g_1h_1 = g_2h_2$.The author rewrites this as $g_1 = g_2h_2h^{-1}$. Now take any element $g \in g_1H$. It is supposed to show that g is also in g_2H. g Can be written as $g = g_1\, h$ for some $h \in H$. Then

$$g = g_1h = g_2h_2h^{-1} \in h_2H \tag{5}$$

Since the assumption that H is a subgroup ensures that the product $h_2h_1h^{-1}$is in H. This shows that every element of g_1H is in g_2H, and a similar argument shows the reverse inclusion. Alternatively, the fact from (b) that g_1H and g_2H have the same number of elements can be used, so if one is a subset of the other, they must be equal.

Example 1. Let H be a subgroup of G, and let L_H be the set of all left cosets of H. There is a map $f: G \times L_H \to L_H$, $(g, xH) \to (gx)H$. for any two elements $x, y \in G$, if $xH = yH$, then $y = xh$ for some $h \in H$. So, $g(yH) = g(xh)H = (gx)(hH) = (gx)H = g(xH)$, thus f is well defined. For any $xH \in L_H$, $g1, g2 \in G$, $f(1G, xH) = xH$, and also $f(g1g2, xH) = ((g1g2)x)H = (g1(g2x))H = f(g1, f(g2, xH))$. So f is a group G action on L_H.

Example 2. There is a finite group G, define a map $f: G \times G \to G, (g, h) \to ghg^{-1}$. since $f(1G, x) = x$, then $f(g_1g_2, x) = (g_1g_2)x({g_2}^{-1}{g_1}^{-1}) = f(g_1, f(g_2, x))$. G is group acts on itself, f is called the conjugation action of G on itself.

3. Lagrange's Theorem

3.1 Definition of Lagrange's Theorem

If There is a finite group G and H is a subgroup of G, then the order of H divides the order of G (i.e.,$|H|\big||G|\big)$ and the number of left cosets of H in G equals $\frac{|G|}{|H|}$ [8].

Proof. Let $|H| = n$ and let the number of left cosets of H in G equal k. The set of left cosets of H in G partition G. By definition of a left coset the map: $H \to gH$ defined by $h| \to gh$. It is a surjection from H to the left coset $g\,H$. The left cancellation law implies this map is injective since $gh_1 = gh_2$ implies $h_1 = h_2$. This proves that H and gH have the same order

$$|gH| = |H| = n. \tag{6}$$

Since G is partitioned into k disjoint subsets each of which has cardinality n,$|G| = kn$. thus $k = (|G|)/n = (|G|)/(|H|)$, completing the proof.

3.2 Applications of Lagrange's Theorem

Example 3.1: Assume that there are two numbers p and q, which are prime, and $p < q$, getting the group B and K with the orders of $p\ q$ at most have one subgroup with the order of q.

Proof: H and K are q-order subgroups which belong to$A$, according to the theorem above, it can be learnt that $|BK| = \frac{|q^2|}{|B \cap K|}$. Here, q is prime, but $|H \cap K|$is divisible, so $|H \cap K|$=1 or q. When $|B \cap K|$ =1, the author can get $|BK| = q^2 > pq = |A|$ is incorrect. So $|B \cap K| = q$, then $B = K$.

Example 3.2: Assume that a and b are two elements in group A, there exists $ab = ba$, and assume that the order of a is m, the order of b is n, and $(m, n) = 1$. Solve the order of ab and prove it is mn.

Proof: Assume the order of ab is k, there exists $ab = ba$. the author knows that $a^{-1} = b\ , b^{-1} = a$. Then the author can get $(ab)^{mn} = a^{mn}b^{\,mn} = e$. According to Lagrange's theorem, $k|mn$. Now prove it the other way that $mn|k$. Since $e = (ab)^{k^n} = a^{k^n}b^{k^n} = a^{k^n}$, given the order of a i s m, the author gets $m|kn$. Also, given $(m, n) = 1$, the author gets $m|k$.

From the fact that $e = (ab)^{k^n} = a^{\mathrm{k^n}}b^{\,\mathrm{k^n}}$ and the order of b is n, the author gets $n|km$. Given $(m, n) = 1$, it can be learnt that $n|k$. From the proof above, it can be learnt that the order of ab is mn.

Example 3.3: Assume that there exist H and K that are two m- and n-order are group A's subgroups. Show that when $(m, n) = 1$, and $B \cap K = \{\mathrm{e}\}$

Proof: There exists $B \cap K \leq B, B \cap K \leq K$. According to Lagrange's Theorem, the author can know that $B \cap K|m, B \cap K|n$. so $|B \cap K|$divides(m, n). But$(m, n) = 1$, then $B \cap K = \{e\}$.

Example 3.4: Assume that A is a group, there is $|A| = p^t m, p$ is prime, p/m and B and K is $p^{\,\mathrm{t}}$ and p^{s}–ordered subgroups of A, respectively $(0 \leq s \leq t)$ $K \notin B$. Prove that the product of BK does not belong to group G.

Proof: Since $|B| = p^t, |K| = p^s, |A| = p^t m$. There is

$$|BK| = \frac{}{\{|B| \cdot |K|\}\{|B \cap K|\}} = \frac{}{\{p^{s+t}\}\{|B \cap K|\}}. \tag{7}$$

So $|BK| \cdot |B \cap K| = p^{s+t}$ as p is prime, then $|HK|$ must be the power of p. Suppose $|BK| = p^r, 0 < r \leq s + t$. If there exists $BK \leq G$, then according to Lagrange's theorem $|BK||p^t m$. However, p/m as $|A| = p^t m$, where $r \leq t$, the author gets

$$p^s = |B| \geq |B \cap K| = p^{(t-r)+s}. \tag{8}$$

Then the author can get $t = r$, there exists $|B \cap K| = p^s = |K|$. However, $|B \cap K| \leq K$.Then the author gets $|B \cap K| = K, K \subseteq B$. it does not fit the condition that $K \subset H$, so HK does not belong to group A.

Example 3.5: Let B and K are finite subgroups of group A, then $|BK| = |BK|/|B \cap K|$.

Proof. Let $|B||B \cap K| = m\ and\ B = h1(B \cap K) \cup h2(B \cap K) \cup ... \cup hm(B \cap K)$, $hi \in B$ $hi - 1hj \notin K$ $i \neq j$. Then $B\ K = h1K \cup h2K \cup ... \cup hmK, hiK \cap hjK = \emptyset\ i \neq j$ .The author has$|BK| = m|K|$, whichis the same as $|BK| = |B||K||B \cap K|$.

Example 3.6. Let G be a group that acts on a set X, define a relation $\sim$on X by the following rule $x \sim y$ if x and y are in the same orbit. Then $\sim$ is an equivalence relation and equivalance class of x is the orbit of x, thus X can be written as a disjoint union$\bigcup_{x \in X} Gx$

Proof. (i) Since $1Gx = x$ by the definition of group acting on sets, $\sim$ is reflexive.

(ii) If $x \sim y$, then $g \in G$ such that $gx = y$, thus $g^{-1}y = g^{-1}gx = (g^{-1}g)x = x$. it can be proved that $y \sim x$, $\sim$ is symmetric.

(iii) If $x \sim y$, $y \sim z$, there exists g_1, $g_2 \in G$, $g_1 x = y$, $g_2 y = z$, thus $z = g_2 y = g_2 (g_1 x) = (g_2 g_1)x$. Then, $x \sim y$, $\sim$ is transitive.

4. Conclusion

In summary, this paper focuses on Lagrange's theorem and effectively explains its proof and application. These theorem sand effectively explains how Group Theory can be proved and applicated in other examples. Firstly, Groups play a fundamental role in abstract algebra, serving as the basis for many algebraic structures like rings, fields, and modules. They are widely used in various mathematical areas, and the method of Group Theory in this research has important implications for other fields in abstract algebra. The author demonstrates the process of proving Lagrange's theorem, explains its significance, explores its practical applications, and highlights its importance. This paper utilizes the properties of cosets and subgroups in group theory, as well as knowledge of group actions and group orbits, to showcase the implications and the importance of Lagrange's theorem. It's clear that Lagrange's theorem contributes to group theory, it holds historical significance in mathematics, too. It is anticipated that Lagrange's theorem will continue to find applications across different domains by integrating new knowledge to create more possibilities.

Reference

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

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

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

[4] 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.

[5] 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.

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

[7] 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.

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