Lagrange's Theorem in Group Theory

Can Cui[1], Chenqin Gan[2], Changwang Ren[3, *], and Zhangying Mo[4]

[1]Ulink, Shanghai, Shanghai, 201615, China

[2]Ulink, Shanghai, Shanghai, 201615, China

[3]Taiyuan Xinlihuizhong School, Tai Yuan, Shan Xi, 030000, China

[4]Abbey College Cambridge, Cambridge, Cambridgeshire, CB2 8EB, United Kingdom

These authors contributed equally.

[*]1117410622@st.usst.edu.cn

Abstract. The structure and behavior of molecules and crystals depend on their different symmetries. Thus, group theory is an essential technique in some fields of chemistry. Within mathematics itself, group theory is very closely linked to symmetry in geometry. Lagrange's theorem is a statement in group theory that can be viewed as an extension of the number theoretical result of Euler's theorem. It is seen as a significant lemma for proving more complicated results in group theory. The main intention of this dissertation is to prove Lagrange's theorem which illustrates that every quadratic irrationality has a periodic continued fraction. Conversely, every periodic continued fraction is a quadratic irrationality. The first part of this paper is the research of so-called Dirichlet groups, which are subgroups of preserving certain pairs of lines. These groups are closely related to the periodicity of sails. The structure of a Dirichlet group is induced by the structure of the group of units in order. Taking n-th roots of two-dimensional matrices using Gauss's reduction theory will also be shown. Finally, the solutions of Pell's equation and Lagrange's theorem will be proved.

1. Introduction

The research object of this paper is group theory and the Lagrange theorem. It is undeniable that the research on them is very meaningful because they are often applied in life or scientific experiments.

Group theory is a significant branch of mathematics, which has various applications in many disciplines. In the application of physics, group theory is the basis of quantum mechanics [1-3]. Group theory was initially mainly used in the study of robot kinematics, with further study, robot assembly, calibration, and control used in group theory [4]. In 1984, Vage and Margrick proposed the first method of constructing a public-key cryptographic system using combinatorial group theory. With the joint efforts of cryptographers, a variety of public key cryptography systems and key exchange protocols have been proposed using combinatorial group theory [5]. In the network, group theory is mainly used to study the network theory of the double port network set, double port converter set, and 2n port converter set. Using the group theory method to find out the connection between them is an effective way [6]. With the application of group theory in atomic materials, human's understanding of the basic "units" that constitute the material world is gradually deepened. In 1869, Mendeleev formulated the periodic table of elements. It is the first time to understand the basic "unit" laws of the material world at the atomic level [7]. Lagrange's theorem proves the order of a subgroup must be an approximate value of the order of a finite group using cosets. It is established between the function and the derivative value of quantitative analysis, so it can be used to study function. Lagrange's theorem is the main function of theory analysis and proof [8]. The outcome showed that simple Lie algebras have been chosen to meet the requirements of unified model builders who researched Yang-Mills theories ground on brief, local-symmetry groups. The central topic includes reviewing its unification and standard model into a simple group; the application of Dynkin charts which is used to find the configuration of the group generators and to track the weights (quantum numbers) of the representative vectors; an analysis of the subgroup structure of simple groups [9]. Lagrange Theorem for Moufang loops written by Gaola's proof that the order of any subloop of a finite Moufang loop is a factor of the order of the loop, thus obtaining an analog of Lagrange Theorem for finite Moufang loops [10]. The Lagrange proof of the Hom group, written by Hassanzadeh, interprets that the Hom group is pointing to an idempotent quasigroup (Pique). It uses the Cayley table of quasi-groups to introduce some examples of the Hom group. By introducing the concepts of Hom subgroups and cosets, Lagrange's theorem for finite Hom groups is demonstrated. This suggests that the order of any Hom subgroup H of the finite Hom group A is divided by order of G. As a result of the application, the order of the Hom-hopf algebra of the finite-dimensional Home group of the Hob algebra BA divides the order of A by order of A [11]. The Lagrange theorem for polygroups written by Sedighi and Hosseini shows that the relations of polygroups properties with the introduction of a suitable equivalence relation are strongly regular. Their main purpose in the paper is to investigate the Lagrange theorem and other expressions of isomorphism theorems for polygroups [12].

In general, the Lagrange theorem is useful when some of the variables in the simplest description of a problem are made redundant by the constraint. It is one of the central theorems of abstract algebra which can be used in other fields in the future, such as physics, chemistry, and network application. This paper is organized as follows. In Section 2, several proofs of Lagrange's theorem are scattered. In section 3, some applications of Lagrange's theorem will be presented. Section 4 is devoted to giving the conclusion of this paper.

2. Lagrange's theorem

Theorem 1: Let B be a subgroup of a finite group A, then $|A| = |B|(A{:}B)$.

Proof: Let (A: B) =s. The left coset decomposition of A concerning B is

$$a_2h_i \in B \Rightarrow a_2h_i = h_j(i \neq j) \Rightarrow a_2 = h_i^{-1}h_j \in B \Rightarrow a_2 \in B. \tag{1}$$

Since $\phi{:}\, a_ih \to a_jh\ (h \in B)$ is a bijection of the left coset a_iB and a_jB, so

$$|a_iB| = |a_jB|. \tag{2}$$

So

$$|a_1B| = \cdots |a_sB| = |B|. \tag{3}$$

Since

$$G = a_1B \cup a_2B \cdots \cup a_sB. \tag{4}$$

We get

$$|A| = |B|s, \tag{5}$$

i.e.

$$|A| = |B|(A{:}B) \tag{6}$$

Theorem 2: Let G is a finite group that $K \leq B \leq G$, then

$$(A{:}B)(B{:}K) = (A{:}K). \tag{7}$$

Proof: Based on Lagrange's theorem, we know that

$$|A| = |B| \cdot (A{:}B) = |K| \cdot (A{:}B). \tag{8}$$

And

$$|B| = |K| \cdot (B{:}K). \tag{9}$$

Substituting into the previous equation to cancel out $|H|$, we get

$$(A{:}B)(B{:}K) = (A{:}K). \tag{10}$$

Theorem 3 (Sylowp theorem) Let p be a prime number, A is a finite group. Then

1) let $p^k|A|$, then the number modulus of subgroups of the group that the order of A is p^k congruent to 1.

2) Sylowp subgroups are conjugated.

3) any order subgroup of A that is p^k must be contained in a Sylow subgroup of A.

4) group that satisfies all the rules from 1)-3) are called Sylowp subgroups.

3. Application of Lagrange's Theorem

Example 3.1. Suppose that p and q are two prime numbers and p<q, then the group B and K of order pq have at most one subgroup of order q.

Proof: H and K are q-order subgroups belonging to A, then we can know from the above theorem,

$$|BK| = \frac{|q^2|}{|B \cap K|} \tag{11}$$

But $|H \cap K|$ is divisible, and q is a prime number, so $|H \cap K| = 1 \; or \; q;$ If $|B \cap K| = 1$, then

$$|BK| = q^2 > pq = |A| \tag{12}$$

isn't true. So $|B \cap K| = q,$ then B=K.

Example 3.2. Suppose that a and b are two elements of a group A, and ab=ba, and let the order of a be m, the order of b be n, and (m, n) =1. Prove the order of an is mn.

Proof: Let the order of ab be k, given by

$$\text{ab=ba.} \tag{13}$$

We know that

$$a^{-1} = b, b^{-1} = a. \tag{14}$$

Then we can get

$$(ab)^{mn} = a^{mn}b^{mn} = e. \tag{15}$$

By Lagrange's theorem,

$$k|mn. \tag{16}$$

Now prove it the other way that

$$mn|k. \tag{17}$$

From

$$e = (ab)^{k^n} = a^{k^n}b^{k^n} = a^{k^n}. \tag{18}$$

Given the order of a is m, we get $m|kn.$

Given (m, n)=1, we get $m|k.$

From

$$e = (ab)^{k^n} = a^{k^n}b^{k^n} = b^{k^n}, \tag{19}$$

and the order of b is n, we get $n|km.$

Given (m, n)=1, we get $n|k.$

From the discussion above, we can know that the order of ab is mn.

Example 3.3. Suppose that H and K are two m- and n-order subgroups of group A, respectively. Prove if (m, n)=1, then $B \cap K = \{e\}$.

Proof: Since

$$B \cap K \leq B, B \cap K \leq K. \tag{20}$$

By Lagrange's theorem, we can know that

$$B \cap K|m, B \cap K|n. \tag{21}$$

So $|B \cap K|$divides (m, n).

But (m, n)=1, then $B \cap K = \{e\}$

Example 3.4. Suppose that A is a finite abelian group of order 2n, where n is an odd number, and prove that group A has and only has one second-order subgroup.

Proof: It is only necessary to prove that A has and only has one element of order 2. Since elements of order greater than 2 appear in pairs in A, and the order of identity element e is 1, and

$$|A| = 2n. \tag{22}$$

Therefore, there must be second-order elements in A and an odd number of elements. If a is a second-order element of A, then B = {e, a} is a second-order subgroup of A.

If A has another element ba of order 2, then K= {e, b} is a subgroup of A which is different from B. Since A is an abelian group, it is easy to know that BK= {e, a, b, ab} is a fourth-order subgroup of A.

By Lagrange's theorem,

$$|BK|\big||A| \Rightarrow 4\big|2n. \tag{23}$$

This contradicts the fact that n is an odd number, so A can have only one second-order element, that is only one second-order subgroup.

Example 3.5 Suppose A is a group, where $|A| = p^t m,\ p$ is a prime number, p/m, and B and K is $p^t\ and\ p^s$ −ordered subgroups of A, respectively; $(0 \leq s \leq t)$ and K ∉ B. To prove that the product of BK is not the subgroup of group G.

Proof: Because

$$|B| = p^t, |K| = p^s, |A| = p^t m. \tag{24}$$

And

$$|BK| = \frac{}{\{|B|\cdot|K|\}\{|B\cap K|\}} = \frac{}{\{p^{s+t}\}\{|B\cap K|\}}, \tag{25}$$

So

$$|BK| \cdot |B \cap K| = p^{s+t}. \tag{26}$$

As p is a prime number, then $|HK|$ must be to the power of p. Suppose

$$|BK| = p^r, 0 < r \leq s + t. \tag{27}$$

If the product of $BK \leq G,$ then according to Lagrange's theorem

$$|BK||p^t m. \tag{28}$$

However, p/m, as $|A| = p^t m,$ where $r \leq t$, according to (27), we can get:

$$p^s = |B| \geq |B \cap K| = p^{(t-r)+s}. \tag{29}$$

And then we can get t=r, and

$$|B \cap K| = p^s = |K| \tag{30}$$

But $|B \cap K| \leq K$. We can get

$$|B \cap K| = K, K \subseteq B. \tag{31}$$

This contradicts to $K \subset H,$ so HK is not a subgroup of group A.

Example 3.6: $S_3 = (1), (12), (13), (23), (123), (132)$. Try to find all subgroups of the symmetric group with Lagrange's theorem.

Proof: We know that S_3 has six subsets which are: $B_1 = \{(1)\},\ B_2 = \{(1), (12)\},\ B_3 = \{(1), (13)\},\ B_4 = \{(1), (23)\},\ B_5 = \{(1), (123), (132)\},\ B_6 = B_3$.

The multiplications of permutations are closed, and therefore they are subgroups of S_3.

Prove that when $|B| = 2,$ there are only six subgroups.

Suppose that B is any nontrivial subgroup of S_3, because $|B|$ is a factor of $|S_3| = 6,$ therefore, only $|B| = 2{,}3$.

When $|B| = 2,$ except for the identity element 1, another element in B can only be a second-order element. There are only three second-order elements in S_3 which are (12), (13), and (23).

Therefore, B can only be B_2, B_3, B_4.

When $|B| = 3,$ according to Lagrange Theorem, the order of the element in B must be the factor of 3, so only 1 or 3 are available. Thus, except for the identity element 1, the other elements must be the factor of 3.

However, there are only two third-order elements in S_3, which are (12) and (13), Therefore, only true for $B = B_5$.

In conclusion, S_3 has and only has the above 6 subgroups.

Example 3.7: Abelian groups of order 15 must be cyclic groups.

Proof: let A be an abelian group of order 15, except for the identity e, the order of the element in A must not be 3, because if not, suppose:

$$|a| = |b| = 3, \tag{32}$$

And

$$b \notin \langle a \rangle, a, b \in G. \tag{33}$$

Then

$$B = \langle a \rangle, K = \langle b \rangle \tag{34}$$

are two third-order subgroups of A, whose intersection is e. As A is substitutable, so $BK \leq A$ and

$$|BK| = |B| \cdot |K| = 9. \tag{35}$$

According to Lagrange's Theorem, 9|15 is a contradiction,

Similarly, A cannot be 5th order except for e, Therefore, third-order and 5th order must exist in A. As A is substitutable, A must have 15th elements, so A is a cyclic group.

Example 3.8: Suppose that P is a Sylowp subgroup of a finite group A, B is a subgroup of A, $p||H|$. Then there exists $a \in A$, so $aPa^{-1} \cap B$ is a Sylowp subgroup of B.

Proof: As $p||B|$, therefore, the Sylowp subgroup Q of N can be obtained, according to the Sylowp theorem, we know that Q is inside some Sylowp subgroup of aPa^{-1} of A.

Then

$$Q \in aPa^{-1} \cap B \tag{36}$$

is a subgroup of B to the power of P, then

$$|aPa^{-1} \cap B| \leq |Q| \tag{37}$$

So

$$Q = aPa^{-1} \cap B. \tag{38}$$

then $aPa^{-1} \cap B$ is a Sylowp subgroup of B.

Example 3.8 Let G be a finite group and $K \leq B \leq A$. Then we have $(A\colon B)(B\colon K) = (A\colon K)$.

Prove: From Lagrange's theorem, we know that $|A| = |B|(A\colon B) = |K|(A\colon B)$ and $|B| = |K|(B\colon K)$. Then $(A\colon B)(B\colon K) = (A\colon K)$.

Example 3.9 Let B and K are finite subgroups of group A, then $|BK| = |BK|/|B \cap K|$.

Prove:

Let $|B|\backslash\, |B \cap K| = m\ and\ B = h1(B \cap K)\ \cup h2(B \cap K)\ \cup \ldots \cup hm(B \cap K), hi \in B, hi - 1hj \notin K, i \neq j$. Then $BK = h1K \cup h2K \cup \ldots \cup hm\, K, hiK \cap\ hjK = \emptyset, i \neq j$. We have |BK|=m |K|, which is the same as |BK|=|B||K|\|B∩K|.

4. Conclusion

To sum up this paper, the theme of the article is Lagrange's theorem. The author clearly shows what is Lagrange's theorem through the proof of Lagrange's theorem and the application of group theory knowledge. The following is a summary of this article. First of all, in abstract algebra, groups are of fundamental importance. Many algebraic structures, including rings, fields, and modules, can be seen as being formed by adding new operations and axioms to groups. The concept of the group appears in many parts of mathematics, and the research technique of group theory also has valuable effects on other branches of abstract algebra. In this paper, the author illustrates the proof process of the Lagrange theorem, elaborates on the meaning of the Lagrange theorem, studies the application of the Lagrange theorem, then expresses the importance of the Lagrange theorem. In general, the author uses the characteristics of cosets and subsets in group theory combing with the knowledge of group action and orbit. The characteristics and effects of Lagrange's theorem are also shown. Lagrange's theorem is not only a part of group theory but also a milestone in the history of mathematics. Lagrange's theorem will be applied to more aspects in the future and will be combined with more new knowledge to create more possible applications for people. Classical theorem about integer solutions for Pell's equation, which is proof of Lagrange theorem, shows a strong connection between quadratic irrationalities and periodic fractions.

References

[1] Zeng Y 1998 Application of group theory to the central field problem of quantum mechanics [J]. Guangxi Physics, vol.2.pp.4

[2]Waerden B 1974 Group theory and quantum mechanics [M]. McGraw-Hall Book Company. New York.

[3] He Y 1989 Application of group theory in modern physics [J]. Journal of Wuhan Institute of Technology, vol.3. pp.40-46.

[4] Wei W Ye C and Yuan Y 2016 Research on motion space of hexapod robot based on group theory. Robot, vol.38.pp.10.

[5] Lu Z 2018 Constant round Group Key Agreement Protocol and its application Research [D]. University of Electronic Science and Technology of China.

[6] Chen K Xiao F and Li Z et al. 2007 Research on Synthesis method of reversible logic circuits based on group theory [C]. Proceedings of the 13th National Conference on Optical Fiber Communication and 14th Integrated Optics.

[7]Thomas W and Liu K 2016 Application of group theory to the theory of atoms, molecules and solids [J]. Review of Foreign Science and Technology New Books, vol.7.pp.1.

[8] He D and Li Y 2019 Generalization and application of Lagrange's theorem in group theory [J]. Journal of Ningde Normal University: Natural Science Edition, vol.31.pp.3.

[9] Slansky R 1981 Group theory for unified model building[J]. Physics Reports, vol.79.pp.1-128.

[10] Gagola S M I and Hall J I 2005 Lagrange's theorem for Moufang loops[J]. Mathematical Proceedings of the Cambridge Philosophical Society, vol.139.pp.41-57.

[11] Hassanzadeh M 2018 Lagrange's Theorem For Hom-Groups[J]. https://arXiv.1803.07678

[12] Sedighi A and Hosseini M H 2015 Lagrange Theorem for polygroups[J]. New Trends in Mathematical Sciences. Vol.3. pp.29-34