Study on Cauchy Theorem as a Special Case of Sylow Theorem

Wenxian Zhao *

School of Mathematics, The University of Edinburgh, Edinburgh, United Kingdom

* Corresponding Author Email: s2156274@ed.ac.uk

Abstract. The Cauchy Group Theorem and the Sylow Theorem are foundations of the finite group theory. The Cauchy Group Theorem focuses on the existence of prime order elements in a finite group, whereas Sylow Theorems provide a more complete framework for the analysis of the structure and number of subgroups. A formal proof of the two theorems is given in this paper. The Cauchy Group Theorem is proved by proving the existence of an order p element in a finite group G, here p is a prime divisor of n, and n is the order of group G. The Sylow Theorem is proved by existence, conjugacy and amount of Sylow p-subgroups. In this process, the relation between two theorems is revealed. In other words, the Cauchy Group Theorem is a special case of Sylow Theorem, and the Cauchy Group Theorem is equivalent to the case $k = 1$ in which the order of group is $|G| = p^k m$. The Cauchy Group Theorem is used to classify finite simple groups and the Structure Theorem of finite abelian groups. The application of the Sylow Theorem is to classify and analyze the group structure.

Keywords: Group theory; Cauchy's Theorem; Sylow Theorem.

1. Introduction

One of the most significant and foundational branches within abstract mathematics is group theory. Moreover, the Cauchy Group Theorem and the Sylow Theorem are prominent in this field. These theorems provide insight into the existence and structure of subgroups in a finite group, and help mathematicians to understand the composition, classification and properties of groups. Cauchy Group Theorem is the foundation of finite group theory, and is indispensable to construction and analysis of its subgroups [1]. The relation between prime factorization of group order and existence of corresponding prime order elements is emphasized. The Cauchy Group Theorem helps to simplify the classification of groups. It is also the basis of other theorems in group theory, including the Sylow Theorems. The Sylow Theorems are an extension of Cauchy Group Theorem, it gives a detailed analysis of the existence, conjugacy, and number of subgroups of prime power order in a finite group. It provide a systematic method to understand the subgroup structure based on its order and provide critical information about the behavior of prime power order subgroups. They enable mathematicians to systematically study the distribution of prime power subgroups within a group, and provide a framework for studying normal subgroups, simple groups, and group actions [2].

The importance of the Cauchy Group Theorem stems from its ability to assure that elements with specific orders within a group exist. It provides a direct link between the prime factorization of group's order and the group's internal composition. Because of its direct application, it is a valuable tool in many fields of mathematics, from algebraic topology to number theory. The Sylow Theorems are important because they can break down a group into more manageable pieces. These theorems, by providing detailed information about the Sylow subgroups, allow mathematicians to analyze the structure of finite groups with much more accuracy. The applications of these two theorems go far beyond pure algebra, affecting areas like algebraic geometry, number theory, even combinatorics.

This paper will focus on the definitions of Cauchy Group Theorem and Sylow Theorem, and gives a formal proof, which will reveal the relationship of these two theorems. And attempt to apply these two theorems in various contexts.

2. Proof of Theorems

2.1. Cauchy Group Theorem

Group theory is a branch of abstract mathematics, and the Cauchy Group Theorem is a foundational theorem in group theory. Cauchy Group Theorem claims: group G contains an order p element if the group's order n is divisible by prime number p [3].

The proof is essentially same as demonstrating that a prime order p element of a finite group G exists, here p divides the group's order n. Define set X of all ordered p-tuples from G,

$$X = \{(g_1, g_2, \cdots, g_p) | g_i \in G \text{ for } i = 1, 2, \cdots, p\} \tag{1}$$

The amount of such p-tuples is $|X| = |G|^p = n^p$. Define a left multiplication action of G on X. For any element $h \in G$ and p-tuple $(g_1, g_2, \cdots, g_p) \in X$. The action is given by

$$h \cdot (g_1, g_2, \cdots, g_p) = (hg_1, hg_2, \cdots, hg_p) \tag{2}$$

This action is well-defined and the properties of group action are met. Specifically, the action by identity of G on all p-tuples is trivial, and the action is compatible with the group operation.

According to the Orbit-Stabilizer Theorem, the orbit size of a p-tuple $(g_1, g_2, \cdots, g_p)$ under this action is given by [4]

$$|\text{Orbit of } (g_1, g_2, \cdots, g_p)| = \frac{|G|}{|\text{Stabilizer of } (g_1, g_2, \cdots, g_p)|} \tag{3}$$

Since p divides $|G| = n$, the size of any orbit must either be 1 (when the stabilizer is the whole group G) or a multiple of p.

An orbit of size 1 occurs if and only if all element of G fix the p-tuple. This implies that all elements in the p-tuple must be identical, that is, $g_1 = g_2 = \cdots = g_p = g$ here g is in center of G. Thus, there are exactly $|G|$ such orbits.

Total elements number in X is n^p. Since there are n orbits of size 1, the remaining $n^p - n$ elements must be divided among orbits of size p or larger, specifically multiples of p. That can be written as:$n^p = n + kp$ here k is non-negative integer representing the amount of elements in orbits of size p or greater. Since n^p and n can be divided by p, kp must also can be divided by$p$, implying $k > 0$.

Thus, there is at least one orbit whose size is exactly p. This orbit corresponds to p-tuples where the elements are not all identical, indicating the existence of an order p element in G.

Therefore, conclusion is made, that G contains an order p element, thereby proving Cauchy Group Theorem.

2.2. Sylow Theorem

The Sylow Theorems give deeper understanding into the finite groups' subgroup structure, specifically concerning properties of prime power order subgroups within a finite group and whether those subgroups exist. A useful method to learn structure of finite groups is provided by detailing the number and types of subgroups associated with specific prime divisors of the group's order. There exist three theorems in the Sylow Theorem, the presence, conjugacy, and amount of Sylow p-subgroups.

First Theorem. For limited group G and a prime number p. If $|G| = p^k m$, here p cannot divide m (i.e., p^k is the greatest power of number p that can divide group's order), thus G contains an order p^k subgroup. This subgroup is refered to as Sylow p-subgroup of group G [5].

Proof. Consider a group G with $|G| = p^k m$, p is a prime and does not divide m. Now show that G has an order p^k subgroup. Counting argument and the class equation is used. Denote P as a Sylow p-subgroup of the group. The class equation of G is given by:

$$|G| = |Z(G)| + \sum [G : C_G(g_i)] \tag{4}$$

Where $Z(G)$ is the center of G and the sum is over representatives of conjugacy classes of elements outside $Z(G)$ each term $[G : C_G(g_i)]$, (the index of the centralizer of g_i) is divisible by p if g_i is outside $Z(G)$. This implies that there are enough elements in G of order that can be divided by p to cover all of G, suggesting the existence of a Sylow p-subgroup.

Second Theorem. Any Sylow p-subgroups of the finite group is conjugate to all others. That means, if N and M are Sylow p-subgroups of group G, then an element $g \in G$ such that $gNg^{-1} = M$ exists [6].

Proof. Denote N and M as two Sylow p-subgroups of the group. To show that N and M are conjugate, consider the amount of Sylow p-subgroups, denoted n_p. According to Third Theorem, n_p satisfies the remainder of n_p divided by n_p is 1, and m is divisible by n_p, here $|G| = p^k m$ and p cannot divide m. If N and M were not conjugate, they would be distinct Sylow p-subgroups. This would imply that $n_p > 1$, which would contradict the minimality of n_p and the constraints on divisibility and congruence. Thus, N and M must be conjugate.

Third Theorem. Let n_p denotes amount of Sylow p-subgroups of group. Then n_p meet the following, which are the remainder of n_p divided by n_p is 1, as well as m is divisible by n_p, here $|G| = p^k m$ and p cannot divide m [7].

Proof. The amount of Sylow p-subgroups n_p must have remainder 1 when divided by p and $n_p|m$. The argument for the congruence that the remainder of n_p divided by n_p is 1 is derived from the fact that the group action of G on the Sylow p-subgroups (via conjugation) partitions G into orbits of size p^k, and these orbits must cover G such that The remainder of n_p divided by n_p is 1. In addition, the divisibility of n_p by m follows from the constraint that the amount of Sylow p-subgroups must be consistent with the structure of the group.

2.3. Relation

Cauchy Group Theorem and Sylow Theorems are both foundations in finite groups. They both provide insights into the existence of subgroups with specific properties, and address different aspects of group structure.

Cauchy Theorem states that there exist at least one exactly prime order p element in finite group G, if the amount of elements of G can be divided by p. This element produces an order p cyclic subgroup. The theorem ensures that at least one order p element exists (hence a subgroup) whenever group's order is divisible by p [8].

The Sylow Theorems generalize this concept by considering not just prime order subgroups, but also subgroups with any power of prime order p. The first Sylow Theorem claims that G has an order p^k subgroup, a Sylow p-subgroup, if $|G| = p^k m$, here p is not divisible by$m$.

The connection between these theorems is due to the fact that the Cauchy Group Theorem is a extension of the first theorem of Sylow Theorems. Specifically, Cauchy Group Theorem corresponds to the case where $k = 1$ in Sylow Theorem. When $k = 1$, the Sylow p-subgroup is simply an order p subgroup, which is exactly what Cauchy Group Theorem guarantees.

Thus, the Cauchy Group Theorem can be regarded as a specific instance of the Sylow Theorems. While Cauchy Theorem is concerned with the existence of prime order subgroups, Sylow Theorems extend this idea to subgroups of any prime power order, providing a more comprehensive framework of the understanding of finite groups structure.

3. Applications

3.1. Applications of Cauchy Group Theorem

3.1.1. Applications in Classify Finite Simple Groups

Simple groups are that it do not have non-trivial subgroups, and only have trivial subgroup except itself. Simple groups are the cornerstones of finite groups, just as prime numbers serves as foundation of integers. Cauchy Theorem is crucial for the study of the structure of simple groups, ensuring the presence of prime order elements within a group. This helps in analyzing whether a given group can be simple, especially when combined with other results like Sylow Theorems.

To examining an order n finite group G, where n can be divided by a prime p. Cauchy Group Theorem guarantees that G contains an order p element g. This element g generates an order p cyclic subgroup $\langle g \rangle$. The existence of this subgroup is critical in several respects.

Analyzing Normal Subgroups: If G is a simple group, this cyclic subgroup of order p cannot be normal unless it is trivial or the entire group. Therefore, the existence of such a subgroup can help in ruling out the simplicity of certain groups or in comprehending the specific framework of G.

Eliminating Non-Simple Structures: If the group has a normal order p subgroup, then it cannot be simple, that is, does not have any non-trivial normal subgroups. This fact can be used in the classification process to systematically eliminate groups that cannot be simple due to the presence of non-trivial normal subgroups generated by elements of prime order [9].

Consider Cauchy Group Theorem is applied to analysis of structure of a group with 60 elements. The prime factorization of 60 is $2^2 \times 3 \times 5$ indicating that 60 is divisible by the primes 2 3, and 5. According to Cauchy Group Theorem, the group has elements of orders 5 3, and 2, and hence contains cyclic subgroups of these orders. The presence of these subgroups is crucial in analyzing whether the group can be simple.

If the group has any normal subgroup with these prime orders, it is not simple. If it has an order 5 normal subgroup, this subgroup would be normal, contradicting the definition of a simple group unless G is cyclic of order 5 (which is already simple and not of order 60). In the absence of normal subgroups of these orders, further analysis of the interactions between the different Sylow subgroups (using Sylow's Theorems) can be constructed, to determine if G can indeed be simple. This process might involve constructing non-abelian groups where none of the Sylow subgroups are normal, leading to possible candidates for simple groups.

3.1.2. Application for Finite Abelian Groups by Structure Theorem

The structure theorem for finite commutative groups is a pivotal result that states every finite commutative group are composition of prime power order cyclic groups. This theorem completely classified finite abelian groups, so any such group G can be written as

$$G \cong Z_{{p_1}^{k_1}} \times Z_{{p_2}^{k_2}} \times \cdots \times Z_{{p_m}^{k_m}} \tag{5}$$

Here p_i are prime numbers,k_i are positive integers.

Cauchy Theorem is important in the proof and apply of this structure theorem by guaranteeing whether elements of prime order exist, which correspond to the cyclic factors in the disintegration of the group.

Consider an order n abelian group G. The prime factorization of the order is given by $n = {p_1}^{a_1} \times {p_2}^{a_2} \times \cdots \times {p_m}^{a_m}$, here $p_1, p_2, \cdots, p_m$ are different prime numbers, and $a_1, a_2, \cdots, a_m$ are their respective powers. According to Cauchy Group Theorem, group G contains elements of order $p_1, p_2, \cdots, p_m$. The cyclic subgroups produced by these elements correspond to factors in the decomposition of the group. G Can be break down into a direct product of smaller cyclic groups because of the existence of prime order elements. For instance, if group's order is 60, with prime factorization $60 = 2^2 \times 3 \times 5$, Cauchy's Group Theorem guarantees that elements of orders 2 3, and 5 exist, which lead to subgroups isomorphic to Z_2, Z_3 and Z_5, respectively.

These cyclic subgroups can be combined into a direct product according to the Structure Theorem, depending on the group's specific structure. Possible decompositions include $G \cong Z_{60}$ $G \cong Z_{30} \times Z_2$ $G \cong Z_{15} \times Z_4$ $G \cong Z_{10} \times Z_6$ $G \cong Z_5 \times Z_3 \times Z_4$, and $G \cong Z_2 \times Z_2 \times Z_3 \times Z_5$.

3.2. Applications of Sylow Theorem

3.2.1. Application in Classify Finite Groups

One of the applications of the Sylow Theorems is to classify finite groups. The theorems give crucial understanding into the possible structures of finite groups based on their order, particularly for small orders or orders with a limited prime factor.

Consider an order n finite group G where n is a composite number. The prime factorization of n provides information about the possible Sylow subgroups of$G$. Sylow Theorems then are used in determination of number and structure of these subgroups, which in turn can help in classifying the group. For example, apply the Sylow Theorems in classifying the order 12 groups. The prime factorization of 12 is $2^2 \times 3$, so the possible Sylow subgroups correspond to the primes 2 and 3.

Sylow 2-Subgroups: By the first Sylow Theorems, at least one subgroup of order 4 exist (since $4 = 2^2$). The third Sylow Theorem states that $\frac{12}{4} = 3$ must be divisible by the n_2 of Sylow 2-subgroups and satisfy that the remainder of n_2 divided by 2 is 1. Hence, n_2 can be 1 or 3.

Sylow 3-Subgroups: Similarly, there is at least one subgroup of order 3. The number n_3 of Sylow 3-subgroups must divide $\frac{12}{3} = 4$ and satisfy that the remainder of n_3 divided by 3 is 1. Therefore, n_3 can be 1 or 4.

Possible structures for groups of order 12 can be explored by using these constraints. If $n_2 = 1$ and $n_3 = 1$, there exist unique Sylow 2-subgroup and unique Sylow 3-subgroup, and both are normal in the group. This indicates that the group can be a direct result of its Sylow subgroups, specifically $Z_4 \times Z_3$, which is isomorphic to Z_{12}. If $n_2 = 3$ and $n_3 = 1$, there are three Sylow 2-subgroups and one Sylow 3-subgroup. The group could be isomorphic to the dihedral group D_6. If $n_3 = 4$, the four Sylow 3-subgroups must be conjugate, implying more complex group structures, potentially involving non-abelian groups. Thus, Sylow Theorems can narrow down the possibilities and constructing explicit examples or classifications of groups of order 12.

3.2.2. Application in Analysis of Group Structure

Sylow Theorems are extensively used in analysis of a group's internal structure, particularly in determining whether the normal subgroups exist and in constructing specific types of groups. A common application of the Sylow Theorems is showing the existence of normal Sylow subgroups to show whether group is simple. Consider a group with 56 elements. The prime factorization of 56 is $2^3 \times 7$. Sylow 7-Subgroups: By the first Sylow Theorems, the group has at least one Sylow 7-subgroup of order 7. The third Sylow Theorem claims that 8 is divisible by the number n_7 of Sylow 7-subgroups and satisfy that the remainder of n_7 is 1 when divided by 7. The values for n_7 could be 1 or 8.

4. Conclusion

This paper discusses the Cauchy Group Theorem and the Sylow Theorems, which are prominent in finite group theory. Both theorems provide foundational understanding into the structure and properties of finite groups, giving a comprehensive understanding of subgroup existence and behavior. Cauchy Group Theorem asserts that finite group G contains order p element if the order of G is divisible by prime p. Proof of this theorem utilized combinatorial and group action arguments, showcasing that the divisibility of the group's order by that prime inherently decides whether an element of prime order exist. This result not only affirms the presence of specific subgroup structures but also complements the broader framework established by the Sylow Theorems. The Sylow Theorems are extension of the Cauchy Theorem, which concerns subgroups whose order is power of primes. The Sylow Theorems prove whether Sylow p-subgroups, their conjugacy, and their number in a group exist. The proofs for these theorems involve counting arguments, class equations, and group actions, highlighting their robust applicability in classifying and analyzing finite groups. The exploration reveals that the Cauchy Theorem is a specific instance of the more general Sylow Theorems, highlighting its role in broader context of the group theory.

Applications of these theorems are significant in various areas of abstract mathematics. The Cauchy Theorem helps to classify finite simple groups, which is helpful for the analysis of normal subgroups and simple groups. The Sylow Theorems can classify and analyze the finite groups structure, particularly determining number and types of Sylow subgroups and examining their normality. They also help in understanding the possible structures of groups based on their order and in ruling out non-simple groups. The application of both theorems is simplified in this paper. Future research could explore the application of these two theorems to other fields of mathematics, such as algebraic topology and combinatorics.

References

[1] Jordan, C., & Jordan, D. Groups-Modular Mathematics Series. Butterworth-Heinemann, 1994.

[2] Meo, M. The mathematical life of Cauchy's group theorem. Historia Mathematica, 2004, 31(2), 196–221.

[3] He Xuanli, et al. On SS-Supplemented Subgroups of Some Sylow Subgroups of Finite Groups. Journal of Algebra and Its Applications, 2023, 22(01): 2350027.

[4] Kammüller, F., & Paulson, L. C. A formal proof of sylow's theorem. Journal of Automated Reasoning, 1999, 23(3), 235–264.

[5] SHABEEB, A. L. M. A. Sylow Theorems and Its Applications in Mathematics-Algebra. Journal of Missan Researches, 2016, 12(24): 434-438.

[6] Yang, X., & He, Y. A proof of Cauchy theorem by action of group. In 2nd International Conference on Applied Mathematics, Modelling, and Intelligent Computing (CAMMIC 2022), 2022, 12259: 369-373.

[7] Feng, Y., Song, Z., & Xu, B. Cauchy Theorem, Sylow Theorems, and Orbit-Stabilizer Theorem in Group Theory. Highlights in Science, Engineering and Technology, 2023, 47, 58-62.

[8] Aschbacher, M. Finite group theory. Cambridge University Press, 2000.

[9] Mannan, M. A., Ullah, M. A., Dey, U. K., & Alauddin, M. A Study on Sylow Theorems for Finding out Possible Subgroups of a Group in Different Types of Order, 2022, 10(4): 851-960.