Cauchy Theorem, Sylow Theorems, and Orbit-Stabilizer Theorem in Group Theory

Yaoshen Feng[1, †], Ziyue Song[2, *, †] and Baojie Xu[3, †]

[1]Mathematics Department, Stony Brook University, New York, United State

[2]School of math, Jilin University, Changchun, China

[3]Raffles American School, Johor, Malaysia

[†]These authors contributed equally.

*Corresponding author: songzy1021@mails.jlu.edu.cn

Abstract. With the rapid development of modern mathematics, math researchers have an increasing demand to take the advantage of group theory in the latest field. The group action is one of the essential parts of the group theory. In order to have a better understand of group action, this paper will describe the insight development and logic in it step by step. For this purpose, three essential theorems, which are Cauchy theorem, Sylow theorems, and orbit-stabilizer theorem, are chosen as representative examples. The proof and applications in some fields of modern science of these three theorems are discussed. In the proof, this paper emphasizes that group action can be used conveniently to solve the problem in group theory. In the application, this paper includes as many fields as possible to attach importance to group action. This paper is expected to give the opinion of how the field of group action is established and its far-reaching influence to the modern science.

Keywords: Cauchy theorem, Sylow theorems, Orbit-stabilizer theorem, Group theory.

1. Introduction

Group theory is a mathematical field that studies groups of various forms, and its history has been developed in different parallel threads. Group theory has three historical roots: algebraic equation theory, differential geometry, as well as number theory. In the field of group theory, the earliest researchers were Lagrange, Abel, and Galois [1]. The earliest studies of groups may be traced back to Lagrange's work in the end of 18th century [2]. However, this work was appreciably isolated, and the start of group theory is the publication of Cauchy and Galois in 1846. This theory wasn't developed without reason, and a few significant threads from its prehistory develop here.

A fundamental root of group theory is the method to solve the roots of polynomial equations with degree greater than four. Secondly, Felix Klein's 1872 Erlangen project initiated the systematic use of groups in geometry, mainly under the use of symmetry groups. The third root of group theory is number theory. In Euler's generalization of Fermat's little theorem, he considered algebraic computation on the residue modulo integers. Groups of the period 1870-1900 were named as Lie's finite groups, discontinuous/continuous groups, and finite groups of linear displacement. In the period 1880-1920, via the work of Schreier, von Dyck, Dehn, Nielsen, and Cayley, the group described by the presentation came into life of their own. During the period 1920-1940, Magnus and others initiated the area of combinatorial group theory. Between 1900 and 1940, an infinite group of "discontinuous" (now known as discrete) groups took on a life of their own [3]. In addition, the famous problem by Burnside caused the research of the subgroups of finite-dimensional linear groups under arbitrary groups. The development of Coxeter and Todd was promoted by fundamental and reflex groups. For example, in combinatorial group theory, the Todd-Coxeter algorithm. Group theory grew in depth, breadth, and influence. The field began to expand into fields such as representation theory and algebraic groups. Beginning in the 1950s, group theorists succeeded in classifying all finite simple groups in 1982 in a huge collaborative effort [4]. Proofs of complete and simplified classification are active areas of research. Some of the most fundamental and meaningful theorems are Cauchy theorem, Sylow theorems, and orbit-stabilizer theorem.

2. Cauchy Theorem

This theorem was first discovered in 1845 by Cauchy. It shows that a subgroup of *G* will have an order of *p* if *p* is a prime divisor of *G*. As a corollary, a finite group G will have an element of order p if the order of G is divided by the prime p [5].

2.1. Proof

To begin with, assume that group G is abelian and has a non-identification element a and a cyclic group H. Assume p no longer divides group $|H|$, afterwards the order $G:H]$ can be divided by the prime p which is consequently affected by the inductive hypothesis. If m is the order of the x in group G, then $x^m = e$ in G produces $(xH)^m = eH$ in G/H, which divides m. This element is a class of xH for a few x in G. This proof for abelian cases is completed since $x^{m/p}$ is once again an element of order p in G.

Interior the normal cases, Z is an abelian subgroup, and it is the middle of group G. After that, p, an element order in group Z, is also working for group G. Therefore, it is also possible to predict that p no longer divides the order of Z. Because p can divide $|G|$, Z has a disjoint union which is G. A non-central element a which cannot be divided by p is existed as a conjugacy class. However, given that centralizer $C_G(a)$ is divided by p in G, then this equation shows that size is $[G: C_G(a)]$, that could be a suitable subgroup given that the truth a isn't precious. This subgroup includes the element of order p through the inductive speculation.

The Cauchy theorem can also be proved from the orbit-stabilizer theorem which shall be introduced later. For a cyclic group within any action of prime order p, the likely orbit sizes could be 1 and p. This can be used to prove Cauchy theorem.

The cyclic set to be proved is

$$X = \{(x_1, \dots, x_p) \in G\ x^p : x_1\ x_2 \dots\ x_p = e\}. \tag{1}$$

This is a set of p-tuples of G's element, the product of which yields the identity. As the last element in the p-tuple have to be the inverse of what past elements produce, except for the last element, all components in the p-tuple can individually determine the p-tuple itself. Then, p-1 element is able to be selected. Therefore, $|G|^{p-1}$ elements that can be divided by p are in the group X.

Since it is known that in a group of $ab = e$, then $ba = e$, any cyclic permutation of an element of X's constituent parts results in another instance of that element. As a result, cyclic permutations of components can be used to show an action of the cyclic group C_p of order p on X:

$$(x_1, x_2, \dots, x_p) \mapsto (x_2, \dots, x_p, x_1). \tag{2}$$

Back to what has been discussed in literatures, X's orbit underneath this action will only have a size 1 or size p. The first happen just for tuples $(x, x, \dots, x)$ when $x^p = e$. One may see that the set of factors satisfying $x^p = e$ can be divided by p through modulo p is decreasing. However, since $x = e$ is one of these elements, there needs to be a minimum $p - 1$ alternative solutions to the problem of x, and all of which are elements of order p.

2.2. Application

Cauchy theorem is widely used in shade technology. The theory is originally defined in a completely unique situation that turned out to be appropriate for color [6]. The idea's utility is determined by identifying the situation is illuminant invariant. The application that discovers community disorders inside the color spectrum of subtractive and complex-subtractive colorant structures is described at the conclusion. All programs ought to be beneficial for the format of coloration. A helpful characterization of finite *p*-groups where *p* is a prime is another very immediate result of the Cauchy theorem. Moreover, people can use Cauchy's Theorem (abelian) in inductive proof of one of the Sylow theorems which will be in the next section.

3. Sylow Theorems

In mathematics, especially in the area of finite group theory, the Sylow theorems are three theorems proved by Sylow who is a Norwegian mathematician. They are significant and useful theorems in finite group theory because they demonstrate the relations between two things, which are the subgroup of a finite group G and its cardinality [7].

3.1. Sylow's First Theorem

Given a finite group G, if $p^n \parallel |G|$ where p is a prime, then there exists a Sylow p-subgroup of G, such that its order is p^n.

Proof. Let $|G| = p^k m = p^{k+r} u$ such that $p \nmid u$, and the set of subsets of G with size p^k is Ω. G acts on Ω under the rule: $g \cdot \omega = \{gx: x \in \omega\}$, where $g \in G$ and $\omega \in \Omega$. For $\omega \in \Omega$, let $G_\omega = \{g \in G: g \cdot \omega = \omega\}$, its stabilizer subgroup, and $G\omega$=$\{g \cdot \omega: g \in G\}$, its orbit, in Ω.

The following is to prove the existence of $\omega \in \Omega$ such that $|G_\omega| = p^k$, given the target subgroup. Since for any $\alpha \in \omega \subseteq G$, $G_\omega \alpha \subseteq \omega$, this is the maximal possible size of a stabilizer subgroup G_ω. Therefore, $|G_\omega| = |G_\omega \alpha| \leq |\omega| = p^k$. Therefore $|G\omega|\ |G\omega| = |G|$ for each $\omega \in \Omega$, by the orbit-stabilizer theorem, and therefore, using the additive p-adic valuation vp, which counts the number of factors p, one has the relation $v_p(|G\omega|) + v_p(|G\omega|) = v_p(|G|) = k + r$. This means that for those ω with $|G\omega| = pk$, the ones looked for, one has $v_p(|G\omega|) = r$, but for any other ω, $v_p(|G\omega|) > r$ (as $0 < |G\omega| < pk$ can deduce that $v_p(|G\omega|) < k$). Since $|\Omega|$ is the sum of $|G\omega|$ over all distinct orbits $G\omega$, by proving that $v_p(|\Omega|) = r$ (if none existed, that valuation would exceed r), one can prove the existence of ω of the former type. This is an example of Kummer's theorem and can also be illustrated by the following equation:

$$|\Omega| = C_{p^k m}^{p^k} = \prod_{j=0}^{p^k-1} \frac{p^k m - j}{p^k - j} = m \prod_{j=1}^{p^k-1} \frac{p^{k-v_p(j)} m - j/p^{v_p(j)}}{p^{k-v_p(j)} - j/p^{v_p(j)}}. \tag{3}$$

Now, any power of p does not appear in any factors of the product on the right side. Therefore, $v_p(|\Omega|) = v_p(m) = r$, and the proof is done.

3.2. Sylow's Second Theorem

Considering a finite group G, if p is a prime factor of $|G|$, then all Sylow p-subgroups of G are conjugate to each other. Moreover, for any two Sylow p-subgroups of G, H and K, there exists an element $g \in G$ such that $g^{-1}Hg = K$.

Proof. There is a Lemma that is useful in proving this theorem. Given a finite p-group H, H acts on a finite set Ω, and the set of points of Ω that are fixed under the action of H is Ω_0. Then $|\Omega| \equiv |\Omega_0| \pmod p$.

Let Ω denote the collection of left cosets of P in G and let H act on Ω by left multiplication. One can show that $|\Omega_0| \equiv |\Omega| \equiv [G:P] \pmod p$ using the above Lemma to H on Ω,. Now $p \nmid [G:P]$ by definition so $p \nmid |\Omega_0|$, so in particular $|\Omega_0| \neq 0$. This means there must exists some $gP \in \Omega_0$. Consider this gP, one has $hgP = gP$ for all $h \in H$. This implies $g^{-1}HgP = P$ and, on the other hand, $g^{-1}Hg \leq P$. Moreover, if H is a Sylow p-subgroup, then $|g^{-1}Hg| = |H| = |P|$. That is to say $g^{-1}Hg = P$.

3.3. Sylow's Third Theorem

Given a finite group G, if $p^n \parallel |G|$ where p is a prime and n is a positive integer. Let n_p be the number of Sylow p-subgroups of G. Then the following statements are true [8]:

- $n_p \left| \frac{|G|}{p^n} \right.$, where $\frac{|G|}{p^n}$ is called the index of the Sylow p-subgroup in G.
- $n_p \equiv 1 (mod\ p)$.

- if P is a Sylow p-subgroup of G and its normalizer is N_G, then $n_p = |G: N_G(P)|$.

Proof. Let Ω denote the collection of the Sylow p-subgroups of G and can be acted on by G under conjugation. If $P \in \Omega$, then, by the Sylow's second theorem, $|orb(P)| = np$. Moreover, $np = [G: G_P]$, by the orbit-stabilizer theorem. Under this group action, the stabilizer $G_P = \{g \in G \mid gPg^{-1} = P\} = N_G(P)$, which is the normalizer of P in G. Therefore, $np = [G: N_G(P)]$, and it means that this number divides $[G: P] = \frac{|G|}{q}$.

Let P act on Ω by conjugation, and the set of fixed points under this action is Ω_0. If $Q \in \Omega_0$, then, for all $x \in P$, $Q = xQx^{-1}$ so that $P \leq N_G(Q)$. By Sylow's second theorem, P and Q are conjugate in $N_G(Q)$ and Q is normal in $N_G(Q)$. That is to say $P = Q$. It means that $\Omega_0 = P$, so $|\Omega| \equiv |\Omega_0| = 1 (\mathrm{mod}\, p)$, by the Lemma in Sec. 3.2.

4. Orbit-Stabilizer Theorem

Orbit-stabilizer theorem is one of the core theorems of group action. It is just like a bridge between the group and the group theory, which is of great importance both in deeper research of group action and other fields of math. When people try to know the structure of group action, the orbit and stabilizer in group action are introduced. The orbit means the set of places where the point can be moved by group action and the stabilizer means the set of group elements that fix the point. This theorem states that for any group action $f: G \to Perm(s)$, and any $s \in S$, $|orb(s)|$ and $|stab(s)|$ satisfy the relation [9]

$$|orb(s)| * |stab(s)| = |G|. \tag{4}$$

4.1. Proof

Now that $stab(s)$ is a subgroup of G, one can easily obtain the identity $|G: stab(s)| * |stab(s)| = |G|$ by virtue of the Lagrange theorem. Then one only need to prove that $|G: stab(s)| = |orb(s)|$. Notice that $s * f(g) = s * f(k)$ if g and k are in the same right coset of $stab(s)$, it is straightforwardly to find that

$$sf(g) = sf(k) \leftrightarrow sf(g)f(k)^{-1} = s \leftrightarrow sf(g)f(k^{-1}) = s \leftrightarrow sf(gk^{-1}) = s. \tag{5}$$

It is revealed that $gk^{-1} \in stab(s)$ such that $Hgk^{-1} = H$ or $Hg = Hk$. This finishes the proof that two elements change s to the same one if and only if they are in the same coset, so a bijection is founded and the proof is done.

The proof shows the bijection between the coset of $stab(s)$ and the $orbit(s)$. This theorem gives a deep insight into the structure of group action, and inform people the close relationship between the $|G: stab(s)|$ and the $|orb(s)|$. What's more, one gets an easy way to know the size of some groups through this theorem. In addition, nearly all applications of group action to group theory will flow from the relations between orbits and stabilizer.

The following Lemma is important. Suppose that G is a finite group and also H and J belongs to G, then

$$|HJ| * |H \cap J| = |H| * |J|. \tag{6}$$

Proof. Define $X = \{Hg | g \in G\}$ and make the subgroup acts on X by right multiplication $Hg * j = Hgj$. It is not difficult to prove there should be a group action and $|HJ| = |H| * |Orb(h)|$. Further, $stab(h) = H \cap G$. Hence, using these equations, one can derive from the orbit-stabilizer theorem that

$$\frac{|HJ|}{|H|} = |J: stab(h)| = \frac{|J|}{|H \cap J|}, \tag{7}$$

which is exactly Eq. (6) after a simplification.

4.2. Application

The theorem has plenty of applications in group theory [10]. For the simplest example, it can be used to count the rotation symmetric group G of a cub, though people do not know what exactly it is. Since every rotation in G as a permutation has 6 faces, then the size of G is $|orb(s)| * |stab(s)| = 6 \times 4 = 24$. Without the orbit-stabilizer theorem, one may have to know what exactly the group is by counting the symmetric structure in the cub one by one before knowing its size. On the other hand, Cauchy theorem on finite groups is also its application. Finally, this theorem is essential in proving Sylow theorems to analyze the existence and properties of maximal p-subgroups.

5. Conclusion

To conclude, this paper has introduced three different kinds of theorems in group theory, which are Cauchy theorem, Sylow theorems, and orbit-stabilizer theorem. Cauchy theorem is mainly about a prime divisor in a group that is the order of its subgroup. Sylow theorem is most likely a relationship between finite group and its subgroup. Orbit-stabilizer theorem is about the relationship between the orbit and stabilizer. Notably, they are connected to each other as well. For example, Sylow theorem can be proved by using of Cauchy theorem. The methods of proving these three theorems are included. These theorems are significant not only in group theory, but also have applications on other related fields such as color science as mentioned early. In future studies, people are looking forward to discovering more applications that they can have.

References

[1] Massey W. S. Algebraic topology: An introduction. Harcourt, Brace & World, Inc., New York, 1967.

[2] Nganoi Jean. Converse of Lagrange's theorem (CLT) numbers under 1000. Int. J. Group Theory, 2017, 6(2): 37-42.

[3] Dummit David, Foote Richard. Abstract Algebra, Wiley, Vermont, 2004.

[4] Fein B., Kantor W. M., Schacher M. Relative Brauer groups II. J. Reine Angew. Math., 1981, 328: 39-57.

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

[6] Brill Michael H. Color science applications of the Binet Cauchy Theorem. Color Research and Application, 2002, 27(5): 310-315.

[7] Zhang Liangcai, Nie Wenmin, Zhang Miao. On Applications of Sylow's Theorem. Journal of Southwest China Normal University (Natural Science Edition), 2014, 39(08): 137-140.

[8] Huang Baoqin, Linghu Rongtao. On Sylow's Theorem of Remark and Application. Journal of Anshun University, 2009, 11(4): 89-91.

[9] https://ysharifi.wordpress.com/2021/01/12/group-actions-the-orbit-stabilizer-theorem/.

[10] Pyone Aye. Orbit-stabilizer theorem and consequences. J. Myanmar Acad. Art Sci., 2018, 16(3): 1-19.