On the Proof of Sylow's Theorems in Group Theory

Han Chen*

Department of Mathematics, University of Arizona, Tucson, USA

*Corresponding author: hanchen@arizona.edu

Abstract. The Sylow's theorems are significant principles for analysis of special subgroups of a finite group, and they are significant theories in finite group research area. It is firmly established that every group G owns more than one Sylow group pertaining to every prime factor of $|G|$. The purpose of this article is to summarize and generalize the existing research progress of Sylow's theorems. A summary of them will help more people comprehend and apply group theory to analyze problems. In this paper, the basic information of three distinct Sylow's theorems are introduced, including their definitions and detailed proof procedures. After that, some examples and application that are related to the Sylow's theorems are shown one by one. After that, the relationship between the Sylow's theorems to that of the orbit-stabilizer theorem is discussed. This work will potentially stimulate more research efforts on the basis theorems in group theory.

Keywords: Sylow's theorems, p-subgroup, Group theory.

1. Introduction

Group theory is a significant branch of higher mathematics, first proposed by E. Galois in the 1830s. At first, the theory was only of modest value in the analysis of complex equations. However, with the advancement of time, more and more scientific fields need to use group theory to solve practical problems [1]. For example, group theory is widely used in quantum physics and computing. The Sylow's theorems introduced in this paper are exactly important principles in group theory. Norwegian mathematician Peter Ludwig Sylow shares the name Sylow's theorems because the academic community commemorates his contribution to formulating these theorems [2]. Their appearances provide very important theoretical basses for people to study finite groups. Notably, there is a very strong connection between Sylow's theorems and Lagrange's theorem. Therefore, Learning Sylow's theorems can help people better understand Lagrange's theorem.

The Sylow's theorems assume a partial converse of Lagrange's theorem. Given a finite group G and its subgroup H, the Lagrange's theorem claims that $|H|$ divides $|G|$. Sylow's theorems guarantee that, for some factors of the purpose of G, there are subgroups corresponding to these factors, and it will give relevant information about the number of such subgroups [3]. Sylow's theorems tell people that finite groups can be understood by examining the properties of subgroups of groups, thus leading to the study of finite groups which is also a very rich direction. Because the existing Sylow's theorems system is relatively complete, this article mainly focuses on the summary of the existing content. This article will briefly introduce some basic conclusions and applications of Sylow's theorems, and it can be considered an introductory article for scholars who are just learning Sylow's theorems or who wish to understand Sylow's theorems deeply.

2. Sylow's Theorems

2.1. Sylow's First Theorem

Theorem 1. If group G is finite, and $|G|$ can be divided by a prime power p^k, then there must be a group H whose order is p^k, and H is a subgroup of G [4].

Proof. Suppose that $|G| = p^k m = p^{k+r}u$, and u is not divisible by p. Then, assume the subsets of G of size p^k form a set named Ω. By left multiplication, G acts on Ω. Thus, with the action of G in mind, its equivalence classes can be written as the orbits $G_\omega = \{g\omega \mid g \in G\}$ of the $\omega \in \Omega$.

It is true that $G_\omega = \{g \in G \mid g\omega = \omega\}$ is the stabilizer subgroup for any $\omega \in \Omega$. As long as the element $\alpha \in \omega$, G_ω can be mapped to ω injectively by the function $[g \mapsto g\alpha]$. Therefore, if $g\alpha = h\alpha$ is true for any $g, h \in G_\omega$, it's certain that $g = h$ since cancellation on the right is possible as long as $\alpha \in \omega \subseteq G$. Thus, $p^k = |\omega| \geq |G_\omega|$.

Additionally,

$$|\Omega| = \binom{p^k m}{p^k} = m \prod_{j=1}^{p^k-1} \frac{p^k m - j}{p^k - j} = m \prod_{j=1}^{p^k-1} \frac{p^{k-v_p(j)} m - \frac{j}{p^{v_p(j)}}}{p^{k-v_p(j)} - \frac{j}{p^{v_p(j)}}}. \quad (1)$$

Here, the power of p is not preserved by any factors. Thus, $v_p(|\Omega|) = v_p(m) = r$. Assume that a complete representation of all the equivalence classes within the action of G is $R \subseteq \Omega$, then, $|\Omega| = \sum_{\omega \in R} |G_\omega|$.

Hence, $s := v_p(|G_\omega|) \leq V_p(|\Omega|) = r$ is true for some element $\omega \in R$. Therefore, $|G_\omega| = p^s v$ if v cannot be divided by p. Thus, $|G_\omega| = |G| / |G_\omega| = p^{k+r-s} u/v$ can be inferred by the orbit-stabilizer theorem. Therefore, in light of $p^k \mid |G_\omega|$, it is found that $p^k \leq |G_\omega|$ and G_ω is the subgroup as expected [5].

2.2. Sylow's Second Theorem

Lemma. Let G be a finite p-group and it acts on a finite set Ω. The set of points of Ω under the fixed action of G is written as Ω_0. Thus, $|\Omega| \equiv |\Omega_0| \bmod p$.

Proof. Assume a disjoint sum of orbits within G as Ω. Therefore, according to assumption the arbitrary element x belongs to Ω that is not restricted by G is a multiple of p. Consequently, it lies in an orbit of order $|G|/|G_x|$ (here, G_x represents stabilizer) and the result is obvious.

Theorem 2. Let H be a p-subgroup and P be a Sylow p-subgroup of G, then $g^{-1}Hg \leq P$ is true for an element g in G. Besides, all Sylow p-subgroups of G are mutually conjugate, so they are isomorphic. For instance, if G owns two Sylow p-subgroup H and K, then $g^{-1}Hg = K$ for an element g in G [6].

Proof. Two assumptions are useful. One is that the left cosets of P in G is Ω, while the other is that H works on Ω by left multiplication. Applying the *Lemma*, the condition $|\Omega_0| \equiv |\Omega| = [G: P] \pmod p$ holds. Noticing that $|\Omega_0|$ is nonzero, there should be $gP \in \Omega_0$. With this gP, one finds that $hgP = gP$ for any $h \in H$. Meanwhile, with $g^{-1}HgP = P$ in mind, $g^{-1}Hg \leq P$. Moreover, let H be a Sylow p-subgroup, hence $|g^{-1}Hg| = |H| = |P|$, $g^{-1}Hg = P$.

2.3. Sylow's Third Theorem

Theorem 3. Assume G is a finite group and q is the order of a Sylow p-subgroup of G. Then $n_p \mid |G|/q$ and $n_p \equiv 1 \bmod p$.

Proof. As what is proved in *Theorem* 2, $n_p = [G : N_G(P)]$, where such subgroup is P as well as the normalizer of P in group G is $N_G(P)$, thus, $|G|/q$ can divide this number. Let Ω be the set of Sylow p-subgroups in G and suppose that P act on Ω through conjugation. Assume $Q \in Q_0$, since for any $x \in P$ there is $Q = xQx^{-1}$, thus, $P \leq N_G(Q)$. By *Theorem* 2, P and Q are conjugate in $N_G(Q)$ especially, also, Q is normal in $N_G(Q)$, therefore, $P = Q$. Then, $\Omega_0 = \{P\}$, since the proved *Lemma*, $|\Omega| \equiv |\Omega_0| = 1 \bmod p$ [7].

3. Applications and Orbit-Stabilizer Theorem

3.1. Applications

To corroborate the Sylow's theorems, three examples are shown in this subsection [8]. For the first example, assume G is a group whose order is pq, both p and q are prime, additionally, $p < q$.

Then it only has a normal subgroup of order q. To explain it, let's work out n_q by Sylow's theorem. Firstly, $pq/q = p$ is true. Therefore, the only possible numbers of it are 1 or p. Secondly, $1 \bmod q$ must be congruent to it. It is clear from the above that 1 is less than p and q is greater than p, Thus, $q + 1$ is greater than it, therefore, the exactly one choice of n_q is 1. Thus, a Sylow q-subgroup of order q is unique and normal.

Regarding the second example, by using the Sylow's theorems, it can be determined that 2, 3, 4, and 5 are the orders of A_5's subgroup. For the Sylow p-subgroups of A_5, the Sylow's third theorem tells exactly the amount of Sylow p-subgroups A_5 has. Because the Sylow 5-subgroups' number must satisfy two conditions: first, it must divide 60; second, it must be congruent to 1 (mod 5), either one or six must be the number of conjugate Sylow 5-subgroups in A_5. If the number of Sylow 5-subgroup is one, self-conjugate is the only explanation. In other words, it would be considered as normal. However, this situation is not possible, and the reason is that there is no normal subgroups of A_5. Therefore, it is certain that the number of A_5's Sylow 5- subgroup is six. Meanwhile, the Sylow 2-subgroups of S_3 is also considered, which are {(1), (12)}, {(1), (13)} , and {(1), (23)}. Based on Sylow's third theorem, it is possible for one to using the conjugation to gain the latter two from the initial one. In fact, {(1), (13)} = {(1), (23)}, (23) {(1), (12)}$(23)^{-1}$ = (13){(1), (12)}$(13)^{-1}$. The amount of Sylow 3-sub-groups of G is equivalent to 1 (mod 3) which divides 8. Therefore, the amount is either 4 or 1. If it is 1, then it must be normal according to the corollary of Sylow's third theorem. Or assume H and H' be two different Sylow 3-subgroups. Since $|G| = 72$ and $|H \cap H'|$ is H's and H''s subgroup, then $|H \cap H'| = 3$. Therefore, $|N\ (H \cap H')|$ can divide 72, which is divisible by 9, and the elements number of it must no less than $|H\ H'|' = 27$. In this case, 36 or 72 are the only two choices for $|N\ (H \cap H')|$. In the first and second situations, respectively, it is found that either $N\ (H \cap H')$ or H and H' is normal in G [9].

3.2. Orbit-Stabilizer Theorem

Orbit-Stabilizer Theorem is a key result for group theory and is the crucial step in the proof of many important theorems, e.g., the Sylow's theorems for groups with finite orders. For orbit-stabilizer theorem, some preliminaries should be available before stating the theorem. Suppose that G acts on a set X, then the orbit of an element x that is in the set X, is the set of all elements with the behavior $g(x)$. Notice that an orbit has the natural structure of an equivalence class, with the equivalence relation x equivalent to y defined as $y = g(x)$ if g belongs to G. It is simple to prove that this is indeed an equality class. The orbits are disjoint, in the scene if two orbits share an element, then they are the same orbit. The proof is as follows. If it belongs to both $Orb(x)$ and $Orb(y)$, then it has the behavior of $g(x)$ for several g in G, and $h(y)$ for some h in G. Therefore, any element $s(x)$ in $Orb(x)$ is equal to $s(g^{-1}\ h(y))$. Note that any element in $Orb(x)$ is also in $Orb(y)$, thus $Orb(x)$ is in $Orb(y)$. This proof is symmetric, so $Orb(y)$ is also in $Orb(x)$.

Next, the stabilizer of x is known as a set in G. It is consisted of all elements in G that sends x back to itself. For example, when the group action is conjugation, and the set X is chosen to be G, the orbit of x is its conjugations in G, and the stabilizer is consisted by certain elements in G. In this situation, the stabilizer can be named the centralizer of x too.

Another significant notion is the normalizer of H. This is the subgroup of G consisting of all g in G that H is unchanged under conjugation by g [10]. Notice that H is normal in its normalizer. In particular, if the normalizer is the whole group G, then H can be called normal in G.

This is an interesting result, indicating that the stabilizer of x under conjugation of an element g, is the stabilizer of $g(x)$. This result could be proved in the sense that the left-hand and right-hand sides are within each other, but here a different way of proof is provided from their definitions. First, notice that the stabilizer of $g(x)$ is all elements h in G that $hg(x)$ equal $g(x)$. Then substitute h by gkg^{-1}, where k is equal to $g^{-1}hg$. This gives the set gkg^{-1} in G, with $gkg^{-1}g$(x) equals to $g(x)$. The g^{-1}, g cancels out, and left multiplicate g^{-1} on both sides gives gkg^{-1} in G, with k acting trivially on x. This is precisely stabilizer of x under conjugation by g.

Here comes the statement of orbit-stabilizer theorem. For a group G acting on a set X, and for any x in capital X, the orbit of x is bijective with the left-cosets of stabilizer of x. In particular, the size of $Orb(x)$ is the same as the number of stabilizers of x in G.

To prove the equation, it is necessary to define a bijective function f from the set of cosets of stabilizer of x, by sending $gStab(x)$ to $g(x)$. This is straightforward by a isomorphism theorem because the kernel of f is just stabilizer of x. Unfortunately, a stabilizer need not be a subgroup, and X need not be a group. To demonstrate it, one needs to show f is indeed a function. Suppose $gStab(x) = hStab(x)$, then $h^{-1}g$ is in $Stab(x)$, thus $g^{-1}e\ h(x)$ is equal to x, showing $g(x)$ is equal to $h(x)$. It is obvious since any element in $Orb(x)$ is of the form $g(x)$ for some g in group G. For injection, assume $g(x) = h(x)$, then $h^{-1}\ g$ is equal to x, showing $h^{-1}g$ belongs to stabilizer of x. Therefore, g is in the left coset of $Stab(x)$ by h, but also h is in $gStab(x)$ by symmetry. This gives $gStab(x)$ is within $hStab(x)$ times $Stab(x)$, which is just $hStab(x)$. Again, by symmetry, the other inclusion follows. Taken together, f is a well-defined bijection, which gives the result desired.

4. Conclusion

To sum up, the Sylow's theorems are not incomprehensible, and their proof processes are not very sophisticated to understand. The most natural proofs of Sylow's theorem are to use double cosets. The Sylow's theorems are typical settings that use the order of a group to determine their internal structure, and their proofs mainly use the effect of the group on itself. It can be said that the whole proof is the basic properties of double cosets plus the numerical analysis of p^r, such as some counts of groups. Sylow's theorems mainly include three distinct statements. If combining the orbit-stabilizer theorem and the group action theorem together, the Sylow's theorem looks much simpler. It is necessary to mention that it has been more than a hundred years since Sylow put forward these three theories, albeit the Sylow's theory has not made much progress recently. However, in terms of applications, Sylow's theorems are very helpful for people's understanding of subsets of group theory, and these theorems have massive applications in the field of quantum physics. In a word, it is urgent to extend the scope of Sylow's theory to more branches of group theory, and discovery more applications of these theorems in natural science.

References

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

[2] Sylow L. Théorèmes sur les groupes de substitutions (in French), 1872, Math. Ann. 5 (4): 584-594.

[3] 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.

[4] Ol'shanskiI A. Y. Geometry of defining relations in groups (Vol. 70). Springer Science & Business Media, 2012.

[5] Casadio G., Zappa G. History of the Sylow theorem and its proofs. Boll. Storia Sci. Mat, 1990, 10(1), 29-75.

[6] Li, D. Three Sylow theorems and their proofs. In 2nd International Conference on Applied Mathematics, Modelling, and Intelligent Computing (CAMMIC 2022) 2022, 12259: 457-465.

[7] Waterhouse William C. The early proofs of Sylow's theorem. Arch. Hist. Exact Sci. 1980, 21(3): 279-290.

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

[9] Escobar J. M., Nunez Valdes, J., Pérez-Fernández, P. Graded contractions of filiform Lie algebras. Mathematical Methods in the Applied Sciences, 2018, 41(17): 7195-7201.

[10] Lee John, M. Introduction to topological manifolds, in graduate texts in mathematics. Springer New York, NY, 2011.