Journal of Mathematics and System Science 11 (2021) 34-37
doi: 10.17265/2159-5291/2021.02.004

Some Applications of the First Sylow Theorem

Emmanuel Akweittey[1], Yarhands Dissou Arthur[1], Daniel Gyam[2], and Albert Adu-Sackey[3]

1. Department of Mathematics Education, Akenten Appiah-Menka University of Skills Training & Entrepreneurial Development, Ghana

2. Department of Mathematics & Statistics, University of Energy & Natural Resources, Ghana

3 Department of Applied Mathematics, Koforidua Technical University, Ghana

Abstract: In this research, numerical examples of the first Sylow theorem are discussed. Groups, subgroups, cyclic groups, *p*-group, Sylow *p*-subgroup and, Cauchy's theorem were used to illustrate the results.

Key words: Groups, subgroups, cyclic group, Sylow's theorem.

1. Introduction

Sylow theorems form a primal part of finite group theory and have very significant applications in the classification of finite simple groups. Sylow's theorems give significantly more information about the subgroups of a finite group. The reverse of Lagrange's theorem is not true. Thus if G is a group of order p and q divides p, then G does not necessarily possess a subgroup of order q. The Sylow theorem however, does provide a converse for Lagrange's theorem; in certain cases it ensures subgroups of specific orders. This theorem yields a powerful set of tools for the classification of all finite nonabelian groups. Sylow's and Lagrange's theorem are the two most substantial results in finite group theory. The first gives a sufficient condition for the existence of subgroups and the second gives a necessary condition [1].

2. Preliminaries

In this section, supporting definitions, corollary, theorems and lemma are presented.

Lemma 2.1. If p is prime that divides ab, then p divides a or p divides b.

Proof. Suppose p is a prime that divides ab but does not divide a. We must show that p divides b. Since p does not divide a, there are integers s and t such that $1 = as+pt$. Then $b = abs+ptb$, and since p divides the right-hand side of this equation, p also divides b.

2.1 Binaary Operation

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

2.2 Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a group under this operation if the following three properties are satisfied.

1) Associative. The operation is associative; that is, $abc = a(bc)$ for all $a, b, c \in G$.
2) Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all $a \in G$.
3) Inverse. For each element $a \in G$, there is an element $b \in G$ (called inverse of a) such that $ab = ba = e$.

If a group has the property that $ab = ba$ for every pair of elements a and b, we say the group is Abelian.

Corresponding author: Emmanuel Akweittey, E-mail: eakweittey@aamusted.edu.gh.

Theorem 2.2. In a group G, there is only one identity element.

Proof. Suppose both e and e' are identities of G. Then,

1) $ae = a$ for every $a \in G$, and
2) $ea = a$ for every $a \in G$.

The choices of $a = e'$ in (part 1) and $a = e$ in (part 2) yields $e'e = e$. Thus e and e_0 are both equal to $e'e$ and so are equal to each other.

Theorem 2.3. For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$.

Proof. Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so that $ab = ac$.

Canceling the a on both side gives $b = c$, as desired.

2.3 Order of a Group

The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of G.

Thus, the group Z of integers under addition has infinite order, whereas the group $U(10) = \{1; 3; 7; 9\}$ g under multiplication modulo 10 has order 4.

2.4 Order of an Element

The order of an element g in a group G is the smallest positive n such that $g^n = e$. (In addition notation, this would be $ng = 0$). If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

2.5 Subgroup

If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

The notation $H \leq G$ is used to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write H < G. Such a group is called a proper subgroup.

2.6 Cyclic Group

A group G is called cyclic if there is an element $a \in G$ such that $G = \{a^n | n \in \mathbb{Z}\}$. Such an element a is called a generator of G. The cyclic group G generated by G is denoted by $G = < a >$.

Theorem 2.4. Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the order of the cyclic groups are uniquely determined by the group [2].

Theorem 2.5. Every cyclic group is Abelian.

Proof. The elements of cyclic groups are of the form ai. Commutativity amounts to proving that

$a^i a^j = a^j a^i$.

$a^i a^j = a^{i+j}$

$= a^{j+i}$ addition of integers is commutative

$= a^j a^i$ [3].

3. Main Result

3.1 p-Group

Let p be a prime number. A p group is any finite group whose order is a power of p.

3.2 Example and Non-example

1) The dihedral group $D_4 = < a, b | a^4 = b^2 = e; ab = ba^{-1} >$ has order $8 = 2^3$ and therefore is a 2-group.

2) The symmetric group S^3 has order $6 \neq p^n$ for any prime p and therefore not a p-group.

3.3 Sylow p-Subgroup

Let G be a finite group and let p be prime such that p^k divides G and p^{k+1} does not divide G, then any subgroup of G of order p^k is called a Sylow p-subgroup of G.

3.4 Examples

1) Let G be a group of order $315000 = 2^3.3^2.5^4.7$. We call any subgroup of order $8 = 2^3$, a Sylow 2-subgroup of G. Similarly, any subgroup of order $625 = 5^4$ is a Sylow 5-subgroup of G and so on.
2) Consider the symmetric group $S_3 = \{e; (12); (13); (23); (231); (312)\}$ with order $|S_3| = 6 =$

$2^1.3^1$. This group has three Sylow 2-subgroups, namely

(a) $H_1 = \{e; (12)\}$ such that $H_1 = 2^1$

(b) $H_2 = \{e; (13)\}$ such that $H_2 = 2^1$

(c) $H_3 = \{e; (23)\}$ such that $H_3 = 2^1$

3) The dihedral group D_4 has five Sylow 2-groups, each generated respectively by s; γ^2; γ^s; $\gamma^2 s$; $\gamma^3 s$.

Lemma 3.1. Let A be a finite abelian group and p be prime. If $p||A|$, then A has an element of order p [4].

3.5 Examples

1) Let p be prime. Then the group $(\mathbb{Z}_n, +)$ is cyclic and therefore abelian if $n = p$. Thus $(\mathbb{Z}_p, +)$ is an abelian group of order p and the order of every element a in $(\mathbb{Z}_p, +)$ is $p/gcd(a, p)$. Thus, every $a \in \mathbb{Z}_p$ which is relatively prime to p has order p.

2) The prime number 5 divides the order of the abelian group $\mathbb{Z}_5$ and every element in $\mathbb{Z}_5$, except 0, has order five.

Theorem 3.2. Let G be a finite group and p be prime. If $p^k||G|$, then G has a subgroup of order p^k.

3.6 Illustration

Suppose we have a group G such that $|G| = 360 = 2^3.3^2.5^1$. Then the Sylow's First Theorem says that G must have at least one subgroup of each of the following orders: 8, 9, and 5. In contrast, this theorem tells us nothing about the existence of subgroups of orders 6, 10, 12, or any other divisors of $|G| = 360$ that has two or more distinct prime factors.

Corollary 3.3. Let G be a finite group and let p be a prime that divided the order of G.

Then G has an element of order p [5].

3.7 Examples

1) The Dihedral group D_8 has order 8 and

$D_8 = < x, a: a^4 = x^2 = e; xax^{-1} = G^{-1} >$

Hence the prime 2 divides $|D_8|$ and is also the order of the elements

a^2, x, $ax = xa^3$, a^2x, $a^3x = xa \in D_8$

2) The Klein 4-group $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ has order 4. The prime $2||(\mathbb{Z}/8\mathbb{Z})^*|$ and it's also the order of the non identity elements 3, 6, $7 \in (\mathbb{Z}/8\mathbb{Z})^*$

Theorem 3.4. Let G be a p-group. Then the order of G is a power of p.

Proof. If $q \neq p$ is a prime which divides $|G|$, then G would have an element of order q by Cauchy's Theorem. This contradicts the definition of a p-group, so we must have $|G| = p^n$ for some $n \in \mathrm{N}$ [6].

3.8 Example

Consider the group $(\mathbb{Z}_{36}, +)$. The order of the group is $36 = 2^2 3^2$ and therefore a Sylow 2-subgroup has order 4, and a Sylow 3-subgroup has order 9.

Theorem 3.5. Let p be a prime. Then every group of order p^2 is abelian.

Proof. If G is not cyclic, then every element for e must have order p because the only option are 1 (the identity), p, and p^2 (not possible since G is not cyclic).

We fix $a \in G$. So $< a >$ is a subgroup of order p, and is a proper subgroup of G. Now fix $b \in G$, with $b \notin < a >$. We have $< a > \cap < b > = \{e\}$, since, if there exist $c \neq e$ with $c \in < a > \cap < b >$, then c generates both $< a >$ and $< b >$. We would then have $< a > = < b >$ which is a contradiction.

By the First Sylow Theorem, the subgroup $< a >$ is normal in some subgroup of G with order p^2, and so $< a >$ is normal in G. Now $< a > \upsilon < b >$ is a subgroup of G, and its order must divide p^2. Therefore $< a > \upsilon < b > = G$. This implies we have $G \cong < a > \times < b >$. Since $< a >$ and $< b >$ are abelian, then G is also abelian. We have $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ [6].

3.9 Examples

1) The Klein four-group has a representation as a 2×2 real matrices with the matrix multiplication operation:

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, c = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, d = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

This group has order $2^2 = 4$. Though a matrix group, it is abelian.

Since $ab = ba = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$, $ac = ca = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$,

$ad = da = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$, $bc = cb = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $cd = dc =$

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $bd = db = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

2) For every prime p, there are (up to isomorphism) exactly two groups of order p^2, namely, $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}p$. Specifically, we can say $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order $2^2 = 4$ and is abelian.

Theorem 3.6. Let G be a finite group, and H any subgroup of G. The order of G is a multiple of the order of H. Thus the order of H divides the order of G.

Proof. Suppose that G has order n and that H has order m. We prove that m divides n. Since the cosets of H partition G, each element of G lies in exactly one coset. Let the number of distinct cosets be k. Each coset has exactly m elements, the same number as H. Thus, as each of the k cosets has m elements, there are km elements in all. Therefore, $n = km$, and m divides n [7].

3.10 Example

The symmetric group

$\{S_3 = e, (12), (13), (23), (231), (312)\}$

with order $|S_3| = 6$ has subgroups

$H_1 = e$; (12) with $H_1 = 2$

$H_2 = e$; (13) with $H_2 = 2$

$H_3 = e$; (23) with $H_3 = 2$

We see that the order of each subgroup H_i divides the order of S_3.

4. Conclusion

In this paper, a numerical illustration of some applications of the first Sylow theorem was given. These numerical applications shows that if p is prime and p^k divides the order of a finite group G, then G has a subgroup of order p^k.

References

[1] Joseph A. Gallian (2015). "*Contemporary Abstract Algebra* (9th ed.)". Printed in the United States of America.

[2] Kaplansky, I. (1972). "*Fields and Rings"*. University of Chicago Press, Chicago.

[3] Kwasi Baah Gyam (2021). "Abraham Aidoo, and Emmanuel Akweittey: Some Applications of Lagranges Theorem in Group Theory Using Numerical Examples". *World Wide Journal of Multidisciplinary Research and Development* 7: 32-34.

[4] Walker, E. A. (1987). "*Introduction to Abstract Algebra*". Random House, New York.

[5] Pollard, H., and Diamond, H. G. (2010). "*Theory of Algebraic Numbers*". Dover, Mineola, NY.

[6] Fraleigh, J. B. (2003). "*A First Course in Abstract Algebra. Pearson*". Upper Saddle River, NJ.

[7] Dean, R. A. (1966). "*Elements of Abstract Algebra*." Wiley, New York.