Academic Voices
A Multidisciplinary Journal
Volume 8, No. 1, 2018
ISSN: 2091-1106

AN ANALYTICAL STUDY OF P-GROUP, P-SUBGROUP AND DIFFERENT CASES OF SYLOW'S THEOREMS

Binod Prasad

Dept. of Mathematics, TU, Thakur Ram Multiple Campus, Birgunj,Nepal

Email: bp97251@gmail.com

Abstract

This paper deals with the series of Sylow's theorems and their applications. Actually First Sylow's theorem provides the idea that whether a group has a sylow subgroup or not. The second Sylow's theorem deals with conjugate subgroups of a Group and the third Sylow's theorem provides the information about the number of Sylow's subgroups.

Keywords

p-group; Sylow's theorems; conjugate subgroups; p-sylow subgroups; double coset

Introduction

In the universal subject mathematics, especially in the case of finite group theory, the Sylow's theorems are a collection of theorems named after the Norwegian mathematician Peter Ludwing Sylow (1872), which give detailed information about the number of subgroups of fixed order that a given finite group contains.

Definition

i. p-Group: A group G is said to be a p-group if each element of G is of order a power of some fixed prime number p.

ii. p-Subgroup: A subgroup H of a group G is called p-subgroup if order of each element of H is a power of p, where p is a prime number.

iii. p-Sylow's subgroup of a group: Let G be a finite group and p a prime number such that $p^m | o(G)$ and $p^{m+1} \nmid o(G)$. Then any subgroup of G of order p^m is called p-Sylow's subgroup of G.

iv. Double coset: Let A and B be subgroups of a group G. Let $x, y \in G$ We define a relation "~" on G such that

$x \sim y$ if y=axb for some $a \in A, b \in B$.

AxB = $\{axb: a \in A, b \in B\}$. The set AxB is called the double coset of A & B in G.

v. Conjugate subgroup: Let A, B be two subgroup of G then B is said to be a conjugate subgroup of A if there exists an element $x \in G$ such that B = x Ax^{-1} and we write $A \sim B \ if \ B = xAx^{-1}$.

Sylow's First Theorem

Statement: If p is a prime number, $p^m | o(G)$, then G has a subgroup of order p^m.

Proof: We will prove the theorem by induction on o(G). we assume that the theorem is true for all groups having order less than o(G). We shall show that it is also true for G. We also note that the result is true for o(G)=1.

Suppose that $p^m | o(G)$, $m \geq 1$, and p is a prime number. If H is any subgroup of G, $H \neq G$, and if $p^m | o(H)$,then by our induction hypothesis, there exists a subgroup T of H such that $o(T) = p^m$. But $T \leq H \Rightarrow T \leq G$ ($\because H \leq G$). Therefore the theorem holds in this case.

So we suppose that $p^m \nmid o(H)$, where H is any proper subgroup of G. Consider the class equation,

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

if $a \notin z(G) \Rightarrow N(a) \neq G$

$\Rightarrow p^m \nmid o(N(a))$

$p^m | o(G) \Rightarrow p^m \mid \frac{o(G)}{o(N(a))} . o(N(a))$

$\Rightarrow p^m \mid \frac{o(G)}{o(N(a))} \left[\because p^m \nmid o(N(a)) \right]$

$p^m | o(G)$, $p^m \mid \frac{o(G)}{o(N(a))}$ for all $a \notin Z(G)$.

$\Rightarrow p \mid \frac{o(G)}{o(N(a))}$ for all $a \notin Z(G)$

$$\Rightarrow p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

Also $p^m|o(G) \Rightarrow p|o(G)$.

$$\therefore p|o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$\Rightarrow p|o(Z(G))$.

$\Rightarrow$There exits an element $b \in Z(G)$, $b \neq e$, such that $b^p = e$ i.e $o(b) = p$.

Let B = <b> where B is a subgroup of Z(G) generated by b. Since $B \subset Z(G)$ and $Z(G) \Delta G$ therefore $B \Delta G$ i.e. B is normal in G. Hence we can form the quotient group $\overline{G} = {}^{G}/_{B}$. Now

$$o(\overline{G}) = o\left({}^{G}/_{B}\right) = \frac{o(G)}{o(B)} = \frac{p^m.r}{p}$$

$\therefore o(\overline{G}) = p^{m-1}.r$

$\Rightarrow p^{m-1}/o(\overline{G})$.

Thus $p^{m-1}/o(\overline{G})$ and certainly $o(\overline{G}) < o(G)$. So by our induction hypothesis $\overline{G}$has a subgroup $\overline{P}$of order p^{m-1}. We know that the natural mapping $\phi: G \to \overline{G}$ defined by $\phi(x)=xB$ for all $x \in G$ is a homomorphism of G onto ${}^{G}/_{B}$ with kernel B.

Let $P = \{x \in G |\ \phi(x) \in \overline{P}\}$

$\quad = \{x \in G |\ xB \in \overline{P}\}$

Then P is a subgroup of G and $\overline{P} \approx {}^{P}/_{B} \overline{P} \approx {}^{P}/_{B}$.

$\therefore o(\overline{P}) = o\left({}^{P}/_{B}\right) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}$

$\therefore o(P) = o(\overline{P}).\ p = p^{m-1}.\ p = p^m$.

Thus P is a subgroup of G of order p^m. This completes the proof of the theorem.

Corollary: If p is a prime number such that $p^m|o(G)$, $p^{m+1} \nmid o(G)$, then there exists a p-Sylow's subgroup of G.

i) Lemma: If A, B are finite subgroups of G then $o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$

ii) Lemma : Let G be a subgroup of a finite group M. Suppose further that M has a p-Sylow's subgroup Q. Then G has a p-Sylow's subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in G$.

Sylow's Second Theorem

Statement:- If Gis a finite group, p a prime number and $p^n/o(G)$ but $P^{n+1}\nmid o(G)$ then any two subgroups of G of order p^n are conjugate.

Proof:- Let A and B be any two subgroups of G such that o (A) = p^n and o(B)= p^n. We want to show that A = gBg^{-1} for some $g \in G$.We have

$$G = U\,AxB$$

$$o(AxB) = \frac{O(A)O(B)}{O(A \cap xBx-1)}$$

If $A \neq xBx^{-1}$ $for\ every\ x \in G$ then

$$o(A \cap xBx^{-1}) = p^m \quad where\ m < n.$$

Thus $o(AxB) = \frac{O(A)O(B)}{O(A \cap xBx-1)}$

$$= \frac{p^n p^n}{p^m} = p^{2n-m}$$

Since $2n - m \geq n + 1, \quad \therefore\ p^{n+1}/o(AxB)$

$$\Rightarrow p^{n+1}/\sum o(AxB)$$

$$\Rightarrow p^{n+1}/o(G) \qquad [\because o(G) = \sum o(AxB)$$

Which is a contradiction that $p^{n+1} \nmid o(G)$.

A = gBg^{-1} for some $g \in G$.This completes the proof of the theorem.

Sylow's Third Theorem

Statement:- The number of p-Sylow's subgroups in G, for a given prime is of the form 1 + kp.

Where 1 + kp/o(G), k is a non-negative integer.

Proof:- Let P be a p-Sylow's subgroup of G, and let o(P)=p^n. We decompose G into double cosets of P andP then$G = \bigcup_x PxP$

$$= \bigcup_{x \in N(P)} PxP \quad U_{x \notin N(P)} PxP$$

$$\therefore o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$If\ x \in N(P) then\ x \in N(P) \Rightarrow xPx^{-1} = p$

$$\Rightarrow xP = Px$$

$$\Rightarrow PxP = PPx$$

$$\Rightarrow PxP = Px$$

$\therefore\ \bigcup_{x\in N(P)} PxP = \bigcup_{x\in N(p)} Px = N(P).$

$\therefore\ \sum_{x\in N(P)} o(PxP) = o(N(P))$

Again if $x \notin N(P)$

$\Rightarrow P\cap xPx^{-1} \neq P.$

Let $o(P\cap xPx^{-1}) = p^m \quad where\, m < n.$
$[\therefore\ P\cap xPx^{-1} \leq P\ and\ o(P) = p^n]$

Now $o(PxP) = \frac{o(P)O(xPx^{-1})}{O(P\cap xPx^{-1})}$

$= \frac{o(P)o(P)}{O(P\cap xPx^{-1})} = \frac{p^n p^n}{p^m} = p^{2n-m}$

$\therefore\ p^{n+1}/o(PxP) \qquad \because\ 2n-m > n+1 \quad \therefore m < n$

So $p^{n+1}/ \sum_{x\notin N(P)} o(PxP)$

Therefore, we can write

$$\sum_{x\notin N(P)} o(PxP) = p^{n+1}.r$$

Thus we have,

$o(G) = o(N(P)) + p^{n+1}.r \qquad [From\ (1)]$

$or, \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}.r}{o(N(P))}$

Since $N(P) \leq G, therefore \frac{o(N(P))}{o(G)}$

i.e$\frac{O(G)}{O(N(P))}$ is an integer.

Hence$\frac{p^{n+1}.r}{o(N(P))}$ must be an integer.

Also $p^{n+1} \nmid o(G) \Rightarrow p^{n+1} \nmid o(N(P))$

Let $o\big(N(P)\big) = p^t,\ t \leq n.$

$$\therefore \frac{p^{n+1}.r}{o(N(P))} = \frac{p^{n+1}.r}{p^t} = p^{n+1-t}.r = kp \quad [\because n+1 > t].$$

$$\frac{o(G)}{O(N(P))} = 1 + kp$$

i.e. The number of p-Sylow's subgroups in G = 1 + kp.This completes the proof of the theorem.

Conclusion:

The Sylow's theorems form a fundamental part of finite group theory and have very import applications in the classification of finite simple groups. The Sylow's theorems assert a partial converse to Lagrange's theorem. Lagrange's theorem states that for any finite group G, the order of every subgroup of G divides the order of G. The Sylow's theorm give the best attempt at a converse, showing that if p^n is a prime power that divide o(G), then G has subgroup of order p^n. For example, a group of order 100 = $2^2 . 5^2$ must contain subgroups of order 1, 2, 3, 4, 5 and 25, the subgroups of order 4 are conjugate to each other, and subgroups of order 25 are conjugate to each other. Also the number of p-Sylow's subgroups is equal to $\frac{O(G)}{O(N(P))}$.

Acknowledgement

I am very grateful to Prof. Dr. Shanti Bajracharya Central Department of Mathematics, T.U.

References

Herstein, I.N. (1993). Topics in Algebra, Wiley Eastern Limited, New Delhi.

Dimmit D. & Foote R.(2004) Abstract Algebra.John Wiley and sons.

Jack Schmidth "Sylow's structure of finite groups" International Mathematical Forum Vol.09291-295, Sep-2-2002.

Vasishtha, A.R.(1996). Modern Algebra, Krishna Prakashan Mandir Meerut, India.