Sylow Theorems

Looking at the Structure of Arbitrary Groups

Andrew Clarey

Occidental College

Mentor: Professor Nalsey Tinberg

December 3, 2015

All material comes from Saracino, *Abstract Algebra* unless otherwise stated.

Overview

Definitions/Theorems

- A set G is called a **group** [denoted $(G, *)$] if:
  i) G has a binary operator $*$. We write $a * b$ as ab.
  ii) $*$ is associative
  iii) there is an element $e \in G$ such that $x * e = e * x = x$, $\forall x \in G$
  iv) for each $x \in G$, $\exists\, y \in G$ such that $x * y = y * x = e$. We write $y = x^{-1}$.
- A group G is called **cyclic** if $\exists\, x \in G$ such that $G = \{x^n | n \in \mathbb{Z}\} = \langle x \rangle$. Then x is called a **generator**. Example cyclic groups are $\mathbb{Z}, \mathbb{Z}_n$.
- The **order** of a group G, denoted $|G|$, is the number of elements in the group.

Definitions/Theorems

- A subset H of a group $(G, *)$ is called a **subgroup** of G if all $h \in H$ form a group under $*$.

- **Theorem**: Let H be a nonempty subset of a group G. Then H is a subgroup iff:
  i) $\forall a, b \in H,\ ab \in H$
  ii) $\forall a \in H,\ a^{-1} \in H$

  We write $H \leq G$.
- If $H \leqslant G$, then a **Left/Right coset** of H in G is a subset of the form aH/Ha where $a \in G$ and $aH/Ha = \{ah/ha | h \in H\}$.
- Two elements $x, y \in G$ are **conjugate** if $\exists g \in G$ such that $y = g^{-1}xg$.
- If $H \leqslant G$, then $gHg^{-1} \leqslant G$ is a **conjugate** subgroup of G, $\forall g \in G$.

Definitions/Theorems

- **Lagrange's Theorem**: Let G be a finite group and let $H \leqslant G$. Then $|H| \mid |G|$, as $|G| = |H|[G : H]$ where $[G : H]$ is the number of Left/Right cosets.
- Let $H \leqslant G$. Then the number of Left/Right Cosets of H in G is $[G : H]$, called the **index**.
- Let $H \leqslant G$. Then we say H is a **normal** subgroup if $\forall h \in H,\ g \in G,\ ghg^{-1} \in H$. We write $H \trianglelefteq G$.
- **Theorem**: Let $H \leqslant G$. Then the following are equivalent:

  i) $H \trianglelefteq G$
  ii) $gHg^{-1} = H,\ \forall g \in G$
  iii) $gH = Hg,\ \forall g \in G$

Definitions/Theorems

- If H is the only subgroup in G of order $|H|$ then $H \trianglelefteq G$.
- If $H \trianglelefteq G$ then G/H is a group called the **quotient group** whose elements are of the form $gH, \forall g \in G$, and whose operation is $*$ such that $aH * bH = (a * b)H$.
- If G, H are groups, then we can define a function ϕ: $G \rightarrow H$ as a **homomorphism** if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.
- Define a **surjection** ϕ from $G \rightarrow G/H$ where $g \rightarrow gH$.
- The **kernel** of ϕ is given by $Ker(\phi) = \{g \in G | \phi(g) = e_H\}$, where e_H is the identity in H and it is a normal subgroup.
- The **Normalizer** of $H \leqslant G$ is the subset $N(H) = \{g \in G | gHg^{-1} = H\}$.
- The **Center** of a group G is the set of elements $Z(G) = \{a \in G | ag = ga, \ \forall g \in G\}$.

Definitions/Theorems

- The **Centralizer** of a $g \in G$ is the set of elements $Z(g) = \{a \in G | ag = ga\}$
- **Theorem**: The **Class Equation** of a group G states: $|G| = |Z(G)| + [G : Z(g_1)] + \cdots + [G : Z(g_k)]$, $g_1, \ldots, g_k \notin Z(G)$, where each g_i is a representative of a **conjugacy class** which contains at least 2 elements.
- **Cauchy's Theorem**: Let G be an abelian group, and let p be a prime such that $p \mid |G|$. Then G contains an element of order p. That is, $\exists x \in G$ so that p is the lowest non-zero number such that $x^p = e$.

First Sylow Theorem

- A subgroup of a group G is called a p-**Sylow subgroup** if its order is p^n, p a prime and $n \in \mathbb{Z}^+$, such that $p^n \mid |G|$ and $p^{n+1} \nmid |G|$.
- **First Sylow Theorem:** Let G be a finite group, p a prime, $k \in \mathbb{Z}^+$.
  - i) If $p^k \mid |G|$, then G has a subgroup of order p^k. In particular, G has a p-Sylow subgroup.
  - ii) Let H be any p-Sylow subgroup of G. If $K \leqslant G$, $|K| = p^k$, then for some $g \in G$ we have $K \subseteq gHg^{-1}$. In particular, K is contained in some p-Sylow subgroup of G.

Examples

Say $|G| = 2^2 \cdot 3^4 \cdot 5^2 \cdot 7^2$. Then we know there will be at least one of each:
2-Sylow subgroup of order 4,
3-Sylow subgroup of order 81,
5-Sylow subgroup of order __,
7-Sylow subgroup of order __.
We also know there will be subgroups of order 2, 3, 9, 27, 5, and 7.

Examples

Let $G = A_4$, a group of order $12 = 2^2 \cdot 3$

$$A_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,2,4), (1,3,4), (1,3,2), (1,4,3), (1,4,2), (2,3,4), (2,4,3)\}$$

So, a 2-Sylow subgroup of G would be a subgroup of order 4, an example is:

$$H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

In fact this is the only one and therefore is normal, and all subgroups of order 2 and 4 are contained within it.

Examples

Say $G = SL_2(\mathbb{Z}_3)$.[1] Then $|G| = 24 = 2^3 \cdot 3$ and $-1 \equiv 2 \bmod 3$. The only 2-Sylow subgroup is:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix},$$
$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$$

and there are 4 3-Sylow subgroups:

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle, \left\langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle, \left\langle \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle, \left\langle \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \right\rangle$$

Proof

We now prove that if $p^k \mid |G|$, then G has a subgroup of order p^k. In particular, G has a p-Sylow subgroup, part i of the First Sylow Theorem.

Let G be a group, p a prime, $k \in \mathbb{Z}^+$ such that $p^k \mid |G|$. We will proceed with induction on $|G|$. If $|G| = 2$ the result is trivial, and we are done. So, let's assume the theorem is true for all groups of order less than $|G|$ and show it is true for $|G|$.

Case 1: Assume $\exists H < G$ such that $p \nmid [G : H]$.
$|G| = [G : H]|H|$ so p^k must divide $|H|$.
By the inductive hypothesis, Since $|H| < |G|$, H has a subgroup of order p^k, therefore G does as well.

Proof

Case 2: Assume $\nexists H < G$ such that $p \nmid [G : H]$.
So, $\forall H < G,\ p \mid [G : H]$.

By the Class Equation: $|G| = |Z(G)| + \sum [G : Z(g_i)]$.
Since $p \mid |G|$ and $p \mid [G : Z(g_i)]\ \ \forall i$, then $p \mid |Z(G)|$.

$\Rightarrow$ By Cauchy's Theorem $Z(G)$ has a subgroup of order p, say A. Then $A \trianglelefteq G$.

So, $|G/A| = |G|/p \Rightarrow p^{k-1} \mid |G/A|$. But $|G/A| < |G|$.

$\Rightarrow$ The inductive hypothesis applies to G/A. So, G/A has a subgroup of order p^{k-1}, say J.

Proof

Define $\phi : G \to G/A$

Let $H = \{g \in G | \phi(gA) \in J\}$. $H \neq \emptyset$, $e_H = A$. Then $H \leq G$.

Show that $g_1, g_2 \in H \Rightarrow g_1 g_2^{-1} \in H$, i.e. Show $g_1 g_2^{-1} A \in J$

But, $g_1 g_2^{-1} A = g_1 A (g_2 A)^{-1} \in J$ as $J < G/A$, and $A < H$ as $A \in J$.

So, map $\phi : H \to J$ by $h \to hA$ which is onto by definition.

Then $Ker(\phi) : H \cap A = A$, and therefore $H/A \cong J$.

So, J has the form H/A for some $H < G$, where $p^{k-1} = |H/A| = |H|/|A| = |H|/p$. So, $|H| = p^k$ as required.

additional proof 1

We proceed by induction on $|G|$. If$|G| = 2$, the result is trivially true. Now assume the statement is true for all groups of order less than $|G|$.

Case 1: If G has a proper subgroup H such that p^k divides $|H|$, then, by our inductive assumption, H has a subgroup of order p^k and we are done.

additional proof 1

Case 2: We may assume that p^k does not divide the order of any proper subgroup of G. Next, consider the class equation for G:

$$|G| = |Z(G)| + \sum [G : Z(g_i)]$$

where we sum over a representative of each conjugacy class. Since p^k divides $|G| = [G : Z(g_i)]|Z(g_i)|$ and p^k does not divide $|Z(g_i)|$, we know p must divide $[G : Z(g_i)]$, $\forall g_i \notin Z(G)$. Thus, from Cauchy's Theorem, we see that $Z(G)$ contains an element of order p, say x. Since x is in the center of G, $\langle x \rangle$ is a normal subgroup of G and we may form the factor group $G/\langle x \rangle$. Now observe that p^{k-1} divides $|G/\langle x \rangle|$. Thus, by the inductive hypothesis, $|G/\langle x \rangle|$ has a subgroup of order p^{k-1} and this subgroup has the form $H/\langle x \rangle$ where H is a subgroup of G. Finally, note that $|H/\langle x \rangle| = p^{k-1}$ and $|\langle x \rangle| = p$ imply that $|H| = p^k$ and this completes the proof.[2]

additional proof 2

We divide the proof into two cases.

Case 1: p divides the order of the center $Z(G)$ of G. By Cauchy's Theorem, $Z(G)$ must have an element of order p, say x. By induction, the quotient group $G/\langle x\rangle$ must have a subgroup P of order p^{k-1}. Then the pre-image of P in $Z(G)$ is the desired subgroup of order p^k.

Case 2: assume that p does not divide the order of the center of G. Again:

$$|G| = |Z(G)| + \sum [G : Z(g_i)],$$

where the sum is over all the distinct conjugacy classes of G; that is, conjugacy class with more than one element. Since p fails to divide the order of the center, $\exists i$ such that $p \nmid [G : Z(g_i)]$. Then p^k must divide the order of the subgroup $Z(g_i)$ as $|G| = [G : Z(g_i)]|Z(g_i)|$. Again, by induction, G will have a p-Sylow subgroup.[3]

Second Sylow Theorem

Second Sylow Theorem: All p-Sylow subgroups of G are conjugate to each other. Consequently, a p-Sylow subgroup is normal iff it is the only p-Sylow subgroup.

Proof:
Let K, H be p-Sylow subgroups of G. Then by the second part of the First Sylow Theorem $K \subseteq gHg^{-1}$. But K and H have the same order, so $K = gHg^{-1}$.

Next, if there is a p-Sylow subgroup $H \trianglelefteq G$ and K is any p-Sylow subgroup, then $K = gHg^{-1}$, so $K = H$. Therefore H is the only p-Sylow subgroup.

Finally, if H is the only p-Sylow subgroup, then $|gHg^{-1}| = |H| \Rightarrow H = gHg^{-1}$ and H is normal.

Third Sylow Theorem

We give the Third Sylow Theorem without proof:

Third Sylow Theorem: Let H be any p-Sylow subgroup of G. Then the number of p-Sylow subgroups in G is $[G : N(H)]$. This number divides $|G|$ and has the form $1 + jp$ for some $j \geq 0$ and this number divides $[G : H]$.

Note: $[G : H] = [G : N(H)][N(H) : H]$.

These theorems allow us to look at the structure of arbitrary groups in order to try and classify them.

Cyclic Theorem

Cyclic Theorem: Let G be a group of order pq, where p and q are primes and $p < q$. Then if $p \nmid q - 1$, G is cyclic.

Examples:

- Every group of order 15 is cyclic. $15 = 3 \cdot 5$ and $3 \nmid 5 - 1 = 4$. So by the theorem, all groups of order 15 are cyclic.
- Every group of order 35 is cyclic. $35 = 5 \cdot 7$ and $5 \nmid 7 - 1 = 6$. So by the theorem, all groups of order 35 are cyclic.
- Every group of order 119 is cyclic. $119 = 7 \cdot 17$ and $7 \nmid 17 - 1 = 16$. So by the theorem, all groups of order 119 are cyclic.

(It can be proven that when $p \mid q - 1$, $\exists$ a non-abelian group of order pq. Moreover, all non-abelian groups of order pq are isomorphic to each other.)

Simple Groups

A group G is called **simple** if its only normal subgroups are $\{e\}$ and G.

Examples:

- No group of order 200 is simple. $200 = 2^3 \cdot 5^2$.

  Consider the 5-Sylow subgroup H of 25 elements. The number of 5-Sylow subgroups is $[G : N(H)] = 1 + 5j \mid 8$. The only possibility is 1, so H is the only 5-Sylow subgroup and is normal by the Second Sylow Theorem, and therefore G cannot be simple.

Simple Groups

- No group of order 56 is simple. $56 = 2^3 \cdot 7$.

  The number of 2-Sylow subgroups is $1 + 2k$ and divides 7, therefore is 1 or 7. The number of 7-Sylow subgroups is $1 + 7j$ and divides 8, and therefore is 1 or 8. If either is 1, then we are done. So, let's say there are 8 7-Sylow subgroups. They have trivial intersection, which gives $8 \cdot 6 = 48$ elements. But, $56 - 48 = 8$ elements, which only allows for one 2-Sylow subgroup, and therefore this 2-Sylow subgroup is normal and the group is not simple.[4]

groups of order 30

Let's find all the groups of order $30 = 2 \cdot 3 \cdot 5$

So, we know there are Sylow subgroups A, B, and C of order 2, 3, and 5 respectively. The number of 5-Sylow subgroups is $[G : N(C)]$, so must divide 6. But it is also of the form $1 + 5j$, so either 1 or 6. Similarly, the 3-Sylow subgroups are $1 + 3k \mid 10$, either 1 or 10.

Suppose there are six 5-Sylow subgroups and 10 3-Sylow subgroups. Any two 5-Sylow subgroups must have trivial intersection since they are both order 5. All six 5-Sylow groups would give $6 \cdot 4 = 24$ elements of order 5 in G. Similarly, the 3-Sylow subgroups give 20 elements of order 3 in G. By our assumption, this would imply $|G| \geq 44$, which is impossible.

groups of order 30

So, we know the group is not simple, but let's continue to explore its structure.

So, either there is only one 5-Sylow or one 3-Sylow subgroup. Therefore, either B or C is normal, and BC is a subgroup of G, of order $|B| \cdot |C|/|B \cap C| = 15$. So BC is cyclic, say $BC = \langle x \rangle$.

Since $\langle x \rangle$ has index 2 (as $|G|/|BC| = 30/15 = 2$) it is normal in G. If we let $A = \langle y \rangle$, then $G = \langle x \rangle \langle y \rangle$ since $\langle x \rangle \langle y \rangle$ has order 30. We must have $yxy^{-1} = x^t$ for some integer t. If we knew the value of t, we could determine the structure of G.

groups of order 30

So yxy^{-1} must have order 15, because x does, and therefore $(t, 15) = 1$, so $t = 1, 2, 4, 7, 8, 11, 13, 14$. We also have

$$y(yxy^{-1})y^{-1} = yx^ty^{-1} = (yxy^{-1})^t = (x^t)^t = x^{t^2}.$$

So, $x = x^{t^2} \Rightarrow x^{t^2-1} = e$, and thus $15 \mid (t^2 - 1)$. This rules out $t = 2, 7, 8, 13$, so there are at most four possibilities for t, so at most four nonisomorphic groups of order 30.

In fact, there are four:

$$\mathbb{Z}_{30},\ S_3 \times \mathbb{Z}_5,\ \mathbb{Z}_3 \times D_5, \text{ and } D_{15}.$$

References

1. www.math.uconn.edu/∼kconrad/blurbs/grouptheory/sylowpf.pdf
2. Contemporary Abstract Algebra, Gallian
3. www.math.drexel.edu/∼rboyer/courses/math533_03/sylow_thm.pdf
4. http://turnbull.mcs.st-and.ac.uk/∼colva/topics/ch3.pdf
5. *Abstract Algebra: A First Course* Second Edition, Saracino