SYLOW'S THEOREMS

December 18, 2020

Mariam Mousa
ID: 900183871
Instructor: Dr. Daoud Siniora
The American University in Cairo

1 Introduction

Sylow Theorems are of the most fundamental theorems in the field of finite group theory. They are named after the Norweign mathematician Peter Ludwig Sylow. In this paper, we prove the three Sylow theorems.

2 Sylow's First Theorem

Before we delve into the statement and the proof of the first theorem, we need to illustrate some concepts.

2.1 Preparation

Definition. Conjugacy Class Let a be an element of a group G. The conjugacy class of a, cl(a) $= \{xax^{-1} | x \in G\}$.
Theorem. *Conjugacy is an equivalence relation on G*

Proof. Let ϕ be a relation on G, such that, $\phi(a) = xax^{-1}$. Notice that:

- ϕ is reflexive: $\phi(x) = xax^{-1} = xxx^{-1} = x$.
- ϕ is symmetric: Let $a, b \in G$, then if $\phi(a) = \phi(b)$, then $\phi(b) = \phi(a)$.
- ϕ is transitive: Let $a, b, c \in G$, then if $\phi(a) = \phi(b)$ and $\phi(b) = \phi(c)$, then $\phi(a) = \phi(c)$.

Hence, ϕ is an equivalence relation on G, that is conjugacy classes partition the group. ■

Theorem. *Let G be a finite group and let a be an element of G. Then,* $|cl(a)| = |G : C(a)|$.

Proof. Let T be a function from $G/C(a)$ to $cl(a)$, such that, $T(xC(a)) = xax^{-1}$. We need to show that T is:

- **well defined**
  Let $xC(a) = yC(a)$. We need to show $T(xC(a)) = T(yC(a))$, that is $xax^{-1} = yay^{-1}$.
  Since $xC(a) = yC(a), y^{-1}xC(a) = C(a)$, therefore $y^{-1}x \in C(a)$. This gives us:
  $(y^{-1}x)a = a(y^{-1}x)$
  $y^{-1}xax^{-1} = ay^{-1}$
  $xax^{-1} = yay^{-1}$
  Hence, T is well defined.
- **injective**
  Let $T(xC(a)) = T(yC(a))$, we need to show $xC(a) = yC(a)$. We have that:
  $T(xC(a)) = T(yC(a))$
  $xax^{-1} = yay^{-1}$

$xax^{-1}y = ya$
$ax^{-1}y = x^{-1}ya$
Hence, $x^{-1}y \in C(a)$, so, $x^{-1}yC(a) = C(a)$. Multiply by x from the right on both sides to get $yC(a) = xC(a)$.

- **surjective**
  Let $y \in cl(a)$, then $y = xax^{-1}$ for some $x \in G$. Hence, $T^{-1}(y) = xC(a) \in G/C(a)$.

Hence, T is a bijection from $G/C(a)$ to $cl(a)$, that is $|cl(a)| = |G : C(a)|$. [3] ■

Now, that we know conjugacy classes partition groups and $|cl(a)| = |G : C(a)|$, it is clear that the following equation holds:

$$|G| = \sum |G : C(a)|,$$

where the summation runs over the conjugacy class of every element a in G. Also, notice that if $a \in Z(G)$, then $xax^{-1} = xx^{-1}a = a$, for any $x \in G$, hence, $cl(a) = \{a\}$. Therefore, the class equation can be written as:

$$|G| = \sum |Z(G)| + \sum |G : C(a)|.$$

Also, we need the following Lemma to prove the first Sylow theorem:
H/N Lemma. Let N be a normal subgroup of a group G. Then, every subgroup of G/N has the form H/N, where H is a subgroup of G.

Proof. Let ϕ be the natural homomorphism from G to G/N and let H' be a subgroup of G/N, then, by the properties of homomorphisms, $\phi^{-1}(H') = \{g \in G \mid gN \in H'\}$ is subgroup of G, call it H. Hence, $H' = H/N$. [6] ■

2.2 The Theorem

Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

Proof. We will proceed by induction on $|G|$. The base case is when $|G| = 1$, hence, the theorem is clearly true.
Now, assume the theorem is true for any group of order less than $|G|$. We need to prove the theorem for groups of order $|G|$. Let $|G| = p^k m$, such that p doesn't divide m. For contradiction, assume there are no subgroups of G of order p^k and let H be a proper subgroup of G. We have the following class equation:

$$|G| = |Z(G)| + \sum |G : C(a)|.$$

If p^k divides $|C(a)|$, then, by the induction hypothesis, $C(a)$ has a subgroup of order p^k and this subgroup is also a subgroup of G and we will be done. So, assume p^k doesn't divide $|C(a)|$. Now, since $|G| = |G : C(a)||C(a)|$ and p^k divides $|G|$ and also, p^k doesn't divide $|C(A)|$, p^k must divide $|G : C(a)|$. Hence, from the class equation, we know that p^k divide $|Z(G)|$. Now, from the Fundamental Theorem of Finite Abelian Groups, $Z(G)$ has an element x of order p. x generates a subgroup $\langle x \rangle$, also of order p. Notice that since $x \in Z(G)$, $\langle x \rangle$ is Abelian and hence, it is normal in G, so, we can construct the factor group $G/\langle x \rangle$. Notice that, by the induction hypothesis, there is a subgroup of $G/\langle x \rangle$ of order p^{k-1}. Also, we know from H/N Lemma, that this subgroup has the form $H/\langle x \rangle$. Hence, $|H| = |\langle x \rangle|.p^{k-1} = p^k$. Hence, H is a subgroup of G of order p^k, which contradicts our assumption that there is no such group. This proves the Sylow's first theorem. [1] ■

3 Sylow's Second Theorem

3.1 Preparation

First, we need to know what a Sylow p-subgroup is.

Definition. Let p be a prime and G be a group. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, any subgroup of order p^k is called a *Sylow p-subgroup.*

Also, before diving into the second and the third Sylow theorems, we need to introduce the concept of a group action.

Definition. a ***group action*** of a group G on a set X is a function $f : G \times X \to X$, such that:

$f(e_G, x) = x$, for all $x \in X$.

$f(gh, x) = f(g, f(h, x))$.

Now, let f be a group action of G on a set X. There are 3 concepts related to an action:

1. A **fixed point** of an element $g \in G$ is an element $x \in X$ such that $f(g, x) = x$
2. The **orbit** of an element $x \in X$ is the set of all elements $y \in X$ such that $f(g, x) = y$.
3. The **stabilizer** of an element $x \in X$ is the set of all elements $g \in G$ such that x is a fixed point of g.

Notice that the stabilizer of an element x in X is a subgroup of G. To show this, let $g, h \in Stab(x)$ and * be the group action, then:

$$(gh) * x = g * (h * x) = g * x = x.$$

Hence, $gh \in Stab(x)$ and $Stab(x)$ is closed under the group operation. Also:

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = 1 * x = x.$$

Hence, $Stab(x)$ is closed under the inverses. Therefore, $Stab(x)$ is a subgroup of G for any $x \in X$. [5]

Now, we prove the Orbit-Stabilizer theorem, which describes the relationship between the orbit and the stabilizer.

The Orbit-Stabilizer Theorem

There is a bijection from $Orb(x)$ to $G/Stab(x)$, i.e. $|Orb(x)|.|Stab(x)| = |G|$.

Proof. Let ϕ be a function from $Orb(x)$ to $G/Stab(x)$, such that:
$\phi(g * x) = gStab(x)$, where * is the group action.
First, we need to show that ϕ is well-defined, i.e. if there are two representatives of the same coset, ϕ sends both of them to this coset. To prove that, let $g * x = h * x$, such that $g, h \in G$, then:
$h^{-1}g * x = h^{-1}h * x$,
$h^{-1}g * x = x$,
Hence, $h^{-1}g \in Stab(x)$, which means $g, h \in Stab(x)$, so, $gStab(x) = hStab(x)$.
Now, we need to show ϕ is injective and surjective:

- injectivity:
  Let $\phi(g * x) = \phi(h * x)$, for some $g, h \in G$, then:
  $gStab(x) = hStab(x)$,
  $h^{-1}gStab(x) = Stab(x)$,
  hence, $h^{-1}g \in Stab(x)$. By the definition of $Stab(x)$,
  $h^{-1}g * x = x$,
  $g * x = h * x$.
  Hence, ϕ is injective.

- surjectivity:
  By definition of ϕ, that is $\phi(g * x) = gStab(x)$, ϕ is surjective.

Hence, ϕ is a bijection from $Orb(x)$ to $G/Stab(x)$. [4] ■

p-group Lemma. Let G be a p-group that acts on a set S via the action $\phi : G \to Perm(S)$, then the number of fixed points of ϕ is congruent mod p to the order of S.

Proof. Let $|G| = p^n$, then by the Orbit-Stabilizer theorem, the only possible sizes of the orbits are $1, p^1, p^2, ...p^n$. Notice that orbits of sizes 1 are the fixed points. Now, observe that:

$$|S| = \sum |Orb(x)| + |Fix(\phi)|,$$

such that, $\sum |Orb(x)|$ sums over the order of the orbits of prime-power order and $|Fix(\phi)|$ is the number of fixed points. Hence, $|S| \equiv_p |Fix(\phi)|$. [8] ■

3.2 The Theorem

Any two Sylow p-subgroups of G are conjugate.

Proof. Let H be a proper subgroup of G with $|H| = p^n$ and $G = p^n m$, and let $S = G/H$. Let K be another subgroup of order p^n. Let ϕ be the group action from K on the set of permutations of S, $Perm(S)$, such that, $\phi(k) = kgH$. Now, notice that a fixed point of ϕ is a coset $gH \in S$, such that:
$kgH = gH$,
$\iff g^{-1}kgH = H$,
$\iff g^{-1}kg \in H$, for all $k \in K$,
$\iff g^{-1}Kg \subset H$,
but since $|H| = |K| = p^n$, $g^{-1}Kg = H$. Now, we only need to show that there is a number of fixed points of ϕ to prove H and K are conjugate.
By the p-group lemma, $|Fix(\phi)| \equiv_p |S|$, but we know that $|S| = |G|/|H| = m$ and m is not divisible by p. Hence, $|Fix(\phi)| \equiv_p |S| \not\equiv_p 0$. Therefore, a number of fixed points exists, hence, H and K are conjugate. [7] ■

4 Sylow's Third Theorem

Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to 1 modulo p and divides m.

Proof. Let S be the set of all Sylow p-subgroups and let ϕ be the group action from G to the permutations of S, such that:

$$\phi(g) = \text{the permutation sending } H \text{ to } g^{-1}Hg.$$

We know from Sylow's second theorem that all Sylow subgroups are conjnugate. Hence, $|orb(H)| = |S| = n$. By the Orbit-Stabilizer Theorem, $|G| = |orb(H)|.|stab(H)| = k|orb(H)| = kn$, hence, n divides $|G|$. Now, let $H \in S$ and let θ be an action from H onto S, such that:

$$\theta(h) = \text{the permutation sending } K \text{ to } h^{-1}Kh.$$

So, the action $\theta(h)$ is the permutation $\phi(h) = h^{-1}Kh$. Let K be a fixed point of the action θ, then:

$$h^{-1}Kh = K, \quad \text{for all } h \in H.$$

Hence, H is a subgroup of $N_G(K)$. Also, since we know that H and K are Sylow p-subgroups of G and $N_G(K)$ is of order that divides G, say $p^n m'$, H and K are also Sylow p-subgroups of $N_G(H)$. By Sylow's second theorem, H and K are conjugate. Now, since K is normal

in its normalizer, $N_G(K)$, and the only conjugate of K in $N_G(K)$ is itself, then $K = H$. Therefore, $Fix(\theta) = \{H\}$. By the p-group lemma, $|S| = n \equiv_p |Fix(\theta)| = 1$. [7] ■

References

[1] J. A. Gallian. *Contemporary Abstract Algebra*. 9th ed. Boston, MA: Cengage Learning, 2015. Accessed on: Dec. 17, 2020.

[2] *Group Actions*. URL: https://brilliant.org/wiki/group-actions/. Accessed on: Dec. 15, 2020.

[3] *Let G be a finite group and let a be an element of G. Then,* $|cl(a)| = |G : C(a)|$. Sept. 2014. URL: https://math.stackexchange.com/questions/907214/let-g-be-a-finite-group-and-let-a-be-an-element-of-g-then-cl-a. Accessed on: Dec. 17, 2020.

[4] *Orbit-Stabilizer Theorem*. URL: https://proofwiki.org/wiki/Orbit-Stabilizer_Theorem#Proof_2. Accessed on: Dec. 15, 2020.

[5] *Proving the stabilizer is a subgroup of the group to prove the Orbit-Stabiliser theorem*. Jan. 2013. URL: https://math.stackexchange.com/questions/265963/proving-the-stabilizer-is-a-subgroup-of-the-group-to-prove-the-orbit-stabiliser. Accessed on: Dec. 17, 2020.

[6] *Showing that every subgroup of a factor group G/N has the form H/N*. July 2017. URL: https://math.stackexchange.com/questions/2355740/showing-that-every-subgroup-of-a-factor-group-g-n-has-the-form-h-n. Accessed on: Dec. 17, 2020.

[7] *Visual Group Theory, Lecture 5.6: The Sylow theorems*. Apr. 2016. URL: https://www.youtube.com/watch?v=MVojEjXdVgA&t=1538s&ab_channel=ProfessorMacauley. Accessed on: Dec. 9, 2020.

[8] *Visual Group Thoery, Lecture 5.5: p-groups*. Apr. 2016. URL: https://www.youtube.com/watch?v=0VvsNCPZRR8&t=323s&ab_channel=ProfessorMacauley. Accessed on: Dec. 15, 2020.