THE SYLOW THEOREMS AND THEIR APPLICATIONS

AMIN IDELHAJ

Abstract. This paper begins with an introduction into the concept of group actions, along with the associated notions of orbits and stabilizers, culminating in the proofs of Cayley's theorem and the orbit-stabilizer theorem. Then, we build up to the three Sylow theorems, and subsequently give some of their applications.

Contents

1. Introduction

One of the important results in the theory of finite groups is Lagrange's theorem, which states that the order of any subgroup of a group must divide the order of the group. One might suggest a possible converse to this theorem, that for any number dividing the order of a group, there exists a subgroup of that order. This is not true. For example, the group A_4 of even permutations on the set $\{1, 2, 3, 4\}$ has order 12, yet there does not exist a subgroup of order 6. The Sylow theorems do provide us with a sort of partial converse to Lagrange's theorem, by asserting the existence of certain subgroups (called Sylow p-subgroups) of any group with a given order, and gives some information about their properties. In this paper, we wish to build up to the proofs of the Sylow theorems by use of group actions and the orbit-stabilizer theorem.

Definition 1.1. Let G be a group and let X be a set. An action of G on X is a group homomorphism $\phi : G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ is the group of permutations of X.

Notation 1.2. When the action of G on X is unambiguous, we implicitly denote it by $G \curvearrowright X$. By abuse of notation, we will use g to denote both the group element and the permutation $\phi(g)$ it induces on X. If $x \in X$ is any point, we denote the action of g on it by gx. While this notation is also used for group multiplication, it is clear from context which one is intended.

Date: July 2016.

2. Group Actions, Orbits, and Stabilizers

In this section, we discuss two important concepts regarding group actions: orbits and stabilizers. Using these concepts, we prove Cayley's theorem and the orbit-stabilizer theorem. Throughout, we let the general action be that of G on X.

Definition 2.1. : The *orbit* of a point $x \in X$ is the set of points to which x is transported by the action of G: $\text{Orb}(x) = \{gx : g \in G\}$. The cardinality of the orbit is called its *length*.

Definition 2.2. The *stabilizer* of a point $x \in X$, denoted $\text{Stab}(x)$, is the set $\{g \in G : gx = x\} \subseteq G$.

Definition 2.3. The *transporter* from x to y is the set of elements that send x to y: $\text{Trans}(x, y) = \{g \in G : gx = y\} \subseteq G$.

Theorem 2.4. *The stabilizer of any element in X is a subgroup of G.*

Proof. If g and h are in $\text{Stab}(x)$, $(gh)x = g(hx) = gx = x$, implying that $\text{Stab}(x)$ is closed under multiplication. In addition, $x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, implying that the inverse of every element in $\text{Stab}(x)$ also lies in $\text{Stab}(x)$. The identity is in $\text{Stab}(x)$ as it is in the kernel of the associated homomorphism, and fixes every point in X. Thus, $\text{Stab}(x) \leq G$. □

Theorem 2.5. *The orbits of X form a partition.*

Proof. It is clear that every point in X is in its own orbit. Now, we wish to prove that if two orbits overlap, they coincide. Consider $x \in \text{Orb}(y) \cap \text{Orb}(z)$. Then $x = gy = hz$ for some $g, h \in G$. Thus, if $w = mz$ for some $m \in G$, then $w = mh^{-1}gy$. Thus, $\text{Orb}(z) \subset \text{Orb}(y)$. By an analogous argument, $\text{Orb}(y) \subset \text{Orb}(z)$, implying that they coincide. □

Definition 2.6. An action is:

(1) *Faithful* if the kernel of the associated homomorphism $\phi : G \to \text{Sym}(X)$ is trivial.
(2) *Transitive* if there is only one orbit.
(3) *Regular* if it is both faithful and transitive.

With this, we are now able to prove Cayley's theorem and the orbit-stabilizer theorem.

Theorem 2.7 (Cayley)**.** *Every group of order n is isomorphic to some subgroup of S_n.*

Proof. We consider the action of G on itself by left multiplication. Because this action is faithful, G embeds as a subgroup of $\text{Sym}(G)$, and because $\text{Sym}(G) \cong S_n$, G is isomorphic to a subgroup of S_n. □

Theorem 2.8 (Orbit-Stabilizer)**.** *When a group G acts on a set X, the length of the orbit of any point is equal to the index of its stabilizer in G:*

$$|Orb(x)| = [G : Stab(x)]$$

Proof. The first thing we wish to prove is that for any two group elements g and g', $gx = g'x$ if and only if g and g' are in the same left coset of $\text{Stab}(x)$. We know

this because if $gx = g'x$, then $g^{-1}g'$ fixes x. Thus, $g' \in g\text{Stab}(x)$, and since g' also lies in its own left coset of $\text{Stab}(x)$, $g\ \text{Stab}(x) = g'\ \text{Stab}(x)$.

Now define a mapping $\phi : G/\text{Stab}(x) \to \text{Orb}(x)$ by $\phi(g\text{Stab}(x)) = gx$. This map is surjective because for $y \in \text{Orb}(x)$, we can choose a $g \in \text{Trans}(x, y)$, for which $g\ \text{Stab}(x)$ maps to y under ϕ. Our previous result proves that this map is injective, and thus, we have a bijection. $|\text{Orb}(x)| = |G/\text{Stab}(x)| = [G : \text{Stab}(x)]$. □

3. The Sylow Theorems

Definition 3.1. Let G be a finite group of order $p^n m$ where $p \nmid m$. A Sylow p-subgroup of G is one of order p^n. By Lagrange's theorem, such a subgroup would be a maximal p-subgroup of G.

Example 3.2. If we consider the group $\mathbb{Z}_{100}$ under addition, it has order $100 = 2^2 * 5^2$. Thus, a Sylow 2-subgroup is a subgroup of order 4, while a Sylow 5-subgroup is a subgroup of order 25.

We now state the three Sylow theorems, and dedicate the rest of this section to their proofs.

Theorem 3.3 (Sylow's first theorem)**.** *If p is a prime number and $p \mid |G|$, then there exists a Sylow p-subgroup of G.*

Theorem 3.4 (Sylow's second theorem)**.** *For a given prime p, all Sylow p-subgroups of G are conjugate to each other.*

Theorem 3.5 (Sylow's third theorem)**.** *We denote the number of Sylow p-subgroups of G by n_p. Then the following results hold:*

1. *$n_p \equiv_p 1$.*
2. *If $|G| = p^n m$ so that $p \nmid m$, then $n_p | m$.*
3. *If P is any Sylow p-subgroup of G, then $n_p = [G : N(P)]$, where $N(P)$ is the normalizer of P in G.*

We now wish to prove Sylow's first theorem, beginning with a combinatorial lemma that will be employed in this proof:

Lemma 3.6. *If $p \nmid m$, then $p \nmid \binom{p^r m}{p^r}$, where $\binom{n}{k}$ are the binomial coefficients.*

Proof. If we expand the binomial coefficient, we get:

$$\binom{p^r m}{p^r} = \frac{\prod_{k=0}^{p^r m - 1} (p^r m - k)}{\prod_{k=0}^{p^r - 1} (p^r - k)}$$

Now, we wish to prove that if p divides a term $p^n m - k$ in the numerator, then it divides the corresponding term $p^n - k$ in the denominator. If we take $k = p^l q$ where either $l < r$ and $p \nmid q$ or $l = r$, we have that $\frac{p^r m - k}{p^r - k} = \frac{p^{r-l} m - q}{p^{r-l} - q}$, which is not divisible by p. Thus, the whole product is not divisible by p. □

Proof of Sylow's first theorem. We denote the set of all subsets of G with order p^n by Ω. This consists of taking the set of combinations of p^n elements out of the $p^n m$ elements of G, and thus we have $|\Omega| = \binom{p^n m}{p^n}$. Now, we let G act on Ω by left

multiplication. Since Ω is partitioned by its orbits, the sum of the lengths of its orbits is equal to $|\Omega|$. By Lemma 3.6, we find that $p \nmid |\Omega|$, and as such, there must exist at least one orbit whose length is coprime to p. Choose $\omega \in \Omega$ to be a set for which $p \nmid |\mathrm{Orb}(\omega)|$.
Now, define $H := \mathrm{Stab}(\omega)$. We can consider its action on ω by left multiplication, since H permutes the elements of ω. The orbits of this action are, by definition, right cosets of H, and thus, the length of each orbit is $[G : H]$. Thus, $|H| \mid |\omega| = p^n$, and thus, H is a p-group. By the orbit-stabilizer theorem, $|\mathrm{Orb}(\omega)||H| = |G| = p^n m$. Since H is a p-group and $p \nmid |\mathrm{Orb}(\omega)$, we have that $|H| = p^n$, implying that H is a Sylow p-subgroup of G. □

Example 3.7. Consider a group with order 72, and look at its prime factorization: $72 = 2^3 3^2$. By Sylow I, we know that there exists a subgroup of order 8 as well as a subgroup of order 9, without further information on the group structure.

In order to prove Sylow II and III, we will need the following lemma, regarding the actions of p-groups on finite sets.

Lemma 3.8. *If G is a p-group and X is finite, then $|X| \equiv_p |X^G|$, where X^G is the set of points $x \in X$ that are fixed by every $g \in G$.*

Proof. Consider a set of representatives $x_1, ..., x_n \in X$ for the G-orbits of X. We have that $|X| = \sum_{i=1}^{n} |\mathrm{Orb}(x_i)| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$. If x_i is not a fixed point, then $[G : \mathrm{Stab}(x_i)] = p^r$ for some $r > 0$. If x_i is a fixed point, then its orbit is the singleton $\{x_i\}$, and thus, $|\mathrm{Orb}(x_i)| = 1$. Thus in modulo p, each fixed point contributes 1 to the above sum, and every other term contributes 0, thereby giving the desired result. □

Proof of Sylow's second theorem. Consider two Sylow p-subgroups of G, call them R and S. We shall have R act on G/S by left multiplication. By Lemma 3.6, we have that the number of fixed points of G/S under the action of R is congruent to $[G : S]$ mod p. Suppose $|G| = p^n m$ where $p \nmid m$. Since S is a Sylow p-subgroup, $[G : S] = m \neq 0 \bmod p$, and thus, there must be some non-zero number of fixed points in the action. Denote one of the fixed points by gS. We have $rgS = gS$ for any $r \in R$. Thus, $g^{-1}rgS = S$ which implies $g^{-1}Rg \subset S$. Since $g^{-1}Rg$ and S are finite sets of the same size, the inclusion is an equality and we have that the two subgroups are conjugate. □

The following fact, which is used extensively in the next section, is an immediate consequence of Sylow's second theorem.

Corollary 3.9. *A Sylow p-subgroup of G is unique if and only if it is normal in G. In particular, it is unique if the group is abelian.*

Proof. If a Sylow p-subgroup is unique, then it is equal to all its conjugations and thus normal. If there are multiple Sylow p-subgroups, they must be conjugate to each other, so none of them can be closed under conjugation, prohibiting normality. Since any subgroup of an abelian group is normal, a Sylow p-subgroup must be unique. □

Finally, we turn our attention the third Sylow theorem.

Proof of part 1 of Sylow's third theorem. We consider $S := \mathrm{Syl}_p(G)$ to be the set of all Sylow p-subgroups of G. Fix a particular subgroup P, and have it act on S by conjugation. Note that S is finite since G has only finitely many subsets. Thus, Lemma 3.8 applies and we find that $|S| = n_p(G) \equiv_p |S^P|$. Because P is closed under conjugation by one of its elements, it is a fixed point, so now we consider any other fixed point, call it Q. Because $pQ = Qp$ for every $p \in P$, we know that $P \subset N(Q)$. In addition, $Q \subset N(Q)$, and thus, P and Q are subgroups of $N(Q)$. In particular, by Langrange's theorem, $p^n \mid |N(Q)|$, and since $p^{n+1} \nmid |G|$, it follows that $p^{n+1} \nmid |N(Q)|$. Therefore, P and Q are Sylow p-subgroups of $N(Q)$, and by Sylow's second theorem, they are conjugate in $N(Q)$. But since $Q \trianglelefteq N(Q)$, this can only be achieved if $P = Q$. This shows that there is only one fixed point in S, whereby we now have that $n_p = |S| \equiv_p |S^P| = 1$ □

Proof of part 2 of Sylow's third theorem. We now consider the action of the entire group G, on $\mathrm{Syl}_p(G)$. Because Sylow p-subgroups of G are conjugate, there is only one orbit, whose length is n_p. Using the orbit-stabilizer theorem, it follows that $n_p \mid |G| = p^n m$. Since $n_p \equiv 1 \bmod p$, p and n_p must be relatively prime. Thus, $n_p \mid p^n m$ can occur only if $n_p \mid m$. □

Proof of part 3 of Sylow's third theorem. We again look at the action of G on $\mathrm{Syl}_p(G)$. By orbit-stabilizer, $n_p = [G : \mathrm{Stab}(P)]$. Under the conjugation action, $\mathrm{Stab}(P) = N(P)$, giving us our desired result. □

We conclude this section with a theorem whose proof is similar in form to that of the third Sylow theorem.

Theorem 3.10. *Every p-subgroup of G is contained in some Sylow p-subgroup of G*

Proof. We consider H to be a p-subgroup of G, and let it act on $\mathrm{Syl}_p(G)$ by conjugation. There must be at least one fixed point under the action since $|\mathrm{Syl}_p(G)| \equiv_p 1$. We denote a fixed point by Q and note that H is a subgroup of $N(Q)$. $H \times Q$ is a subgroup of $N(Q)$ since Q is normal in $N(Q)$. $H \times Q$ is a p-subgroup of G since its order is $|H \times Q| = \frac{|H| \cdot |Q|}{|H \cap Q|}$. Because Q is not contained properly in any other p-subgroup of G, we now have that $Q = H \times Q$, implying that $H \leq Q$. □

4. Applications of the Sylow Theorems

In this section, we wish to explore some applications of the Sylow theorems to combinatorics, arithmetic, and finite group theory, in order to demonstrate their significance. We begin with a lemma that does not invoke any of the Sylow theorems, but will be useful throughout this section.

Lemma 4.1. *Every group of prime order is cyclic.*

Proof. By Lagrange's theorem, we know that for any element of G, we have $|\langle g \rangle| \mid |G|$. However, if G has prime order and g is not the identity, then this can only be satisfied if $\langle g \rangle = G$, making G cyclic. □

Now, we begin the applications.

Theorem 4.2 (**Wilson**). *A natural number p is prime if and only if* $(p-1)! \equiv_p 1$

Proof. We will only prove the "only if" part of this statement, since it uses the Sylow theorems. Consider the symmetric group S_p for p prime. Since $p \mid p!$ and $p^2 \nmid p!$, we have that the Sylow p-subgroups are cyclic groups of order p. There are $(p-1)!$ many p-cycles in S_p, and every Sylow p-subgroup contains precisely $(p-1)$ such cycles, while sharing none. Thus it follows that there are precisely $(p-2)!$ distinct Sylow p-subgroups. By the third Sylow theorem, we have that $n_p = (p-2)! \equiv_p 1$, thus implying that $(p-1)! \equiv_p p-1 \equiv_p -1$. □

Theorem 4.3. *Every group of order 15 is cyclic.*

Proof. A group of order 15 has a subgroup of order 3 and a subgroup of order 5. By Sylow III, we have that $n_3 \equiv_3 1$ and $n_3 \mid 5$, meaning there is only 1 Sylow 3-subgroup $\langle a \rangle$. By an analogous argument, there is only 1 Sylow 5-subgroup $\langle b \rangle$, which is also cyclic. By Sylow II, these two subgroups must be normal. We know that their intersection must be trivial, since any element in their intersection has an element whose order divides both 3 and 5. We know that $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 15 = |G|$. Thus, every element in G is of the form $a^i b^j$. It follows that $G = H \times K$ and therefore cyclic by the Chinese Remainder Theorem. □

Theorem 4.4. *Every finite p-group is isomorphic to some subgroup of the upper unitriangular group.*

Proof. The order of $GL(n,p)$ is $\prod_{k=0}^{n-1}(p^n - p^k) = p^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}(p^{n-k} - 1)$. Since $p \nmid p^{n-k} - 1$, a Sylow p-subgroup of $GL(n,p)$ has order $p^{\frac{n(n-1)}{2}}$.
We know that the unitriangular group is a subgroup of the general linear group, since it is closed under multiplication and all of its matrices have determinant 1. We note that a unitriangular matrix can take any value in its superdiagonal entries, thus it has $\frac{n(n-1)}{2}$ entries that are not fixed to be 0 or 1. Since they are allowed to take any value in $\mathbb{F}_p$, there are $p^{\frac{n(n-1)}{2}}$ such matrices. Thus, over a prime field, the unitriangular group is a Sylow p-subgroup of the general linear group.
If $|G| = p^k = n$, we can embed G in S_n, which is in turn embeded $GL(n,p)$ via the permutation matrices. Thus, G is a p-subgroup of $GL(n,p)$. By Theorem 3.10, G is contained in some Sylow p-subgroup H of $GL(n,p)$. By Sylow's second theorem, H is conjugate to the unitriangular group, which implies that the latter has a subgroup isomorphic to G. □

We now move to one of the more substantial theorems in this section. There exists a theorem which says that except for a particular set of 26 groups, called the sporadic groups, all finite simple groups are isomorphic to a cyclic group of prime order, an alternating group of degree at least 5, or a simple group of the Lie type (the definition of which is a bit too complicated to go into here). While the proof of this theorem is thousands of pages long, we will prove a simpler result that demonstrates the power of the Sylow theorems, which are very important in the full proof of the classification theorem. To begin, we prove the following lemma.

Lemma 4.5. *The order of a non-abelian simple group divides the factorial of the index of every proper subgroup.*

Proof. G acts on G/H by left multiplication. This action is clearly transitive, and thus, the homomorphism $\phi : G \to \mathrm{Sym}(G/H)$ has a kernel that is not all of G. However, since the kernel must be a normal subgroup, it must be trivial. Thus, the

homomorphism is injective, and G is isomorphic to a subgroup of $\mathrm{Sym}(G/H)$, and thus, $|G| \mid |\mathrm{Sym}(G/H)| = [G:H]!$. □

Theorem 4.6. *The smallest non-abelian simple group is A_5, and is unique up to isomorphism.*

Proof. In order to prove this theorem, we first eliminate all possibilities of simple non-abelian groups with order less than 60.

- Lemma 4.1 eliminates groups of prime order, for they are cyclic and thus abelian.
- Any group of order $p^k m$ where $m < p$ and $k \neq 0$ will have a single Sylow p-subgroup, since $n_p \equiv_p 1$ and $n_p \mid m$ is only satisfied by $n_p = 1$. Uniqueness of a Sylow p-subgroup implies normality by the second Sylow theorem, eliminating groups of order 6, 10, 14, 15, 18, 20, 21, 22, 26, 28, 33, 34, 35, 38, 39, 42, 44, 46, 50, 51, 52, 54, 55, 57, and 58.
- If p is a prime such that $q = 2^p - 1$ is a Mersenne prime, we claim that a group of order $2^p q$ also cannot be simple and non-abelian. We know that $n_q \equiv_q 1$ and $n_q \mid 2^p$. Either $n_q = 1$, in which case the q-Sylow subgroup is normal, or $n_q = 2^p$. In the latter case, assume $H_1, ..., H_{2^p}$ are the Sylow q-subgroups. Since they are all of prime order, the intersection of any two of them is trivial. Thus, the total number of non-identity elements of order q is $2^p(q-1) = |G| - 2^p$. The Sylow 2-subgroups of G must be contained entirely within the remaining 2^p elements, which means that this subgroup is unique and normal. This fact disqualifies groups of order 12 and 56.
- We know that $45 = 5 * 3^2$, so $n_5 \mid 9$ and $n_5 \equiv_5 1$, only satisfied by $n = 5$. Similarly, $40 = 5 * 2^3$, so $n_5 \mid 8$ and $n_5 \equiv_5 1$, implying that $n_5 = 1$. Thus, groups of those orders have normal subgroups and are thus disqualified.
- If G is simple and non-abelian, its order must divide the factorial of any Sylow number n_p. Let P be a Sylow p-subgroup of G. By Sylow III, $[G : N(P)] = n_p$. Note that $P \neq G$ because it is a p-group and has a non-trivial center. Since P is not the trivial group, it cannot be normal in G. In particular $N(P)$ is a proper subgroup of G. By lemma 4.5, $|G| \mid [G : N(P)]! = n_p!$. Groups of order 24, 36, and 48 fail to meet this condition, and are thus disqualified.
- If $|G| = 30$, we have that $n_3 = 1$ or 10, and $n_5 = 1$ or 6. If G is simple, then it has 10 subgroups of order 3 and 6 subgroups of order 5. However, since these groups are all cyclic of prime order, any non-trivial element of G is contained in at most one of these groups. However, that would require that $|G| \geq 10(3-1) + 6(5-1) = 44$, which is false. Thus, G is not simple.

We now wish to prove that A_5 is simple, and then that any simple group of order 60 is isomorphic to it. We note that the conjugacy classes of A_5 have sizes 1, 12, 12, 15, and 20. A non-trivial normal subgroup would contain the identity and at least one other conjugacy class, with its order being some sum of one and at least one of the other above numbers. However, the only such sum which divides 60 (required by Lagrange) is to sum all of them up. Thus, the two normal subgroups have order 1 (identity) and 60 (whole group), making A_5 simple.

If a simple group of order 60 has a subgroup H of index 5, then we could consider the 5 distinct left cosets of H. Now G acts on them transitively by left multiplication, we see that there is a non-trivial homomorphism $\phi : G \to S_5$. Clearly,

$\phi(G) \neq S_5$ since the latter is not simple, and if $|\phi(G)| < 60$, the homomorphism's kernel would be non-trivial, violating simplicity of G. Thus, $|\phi(G)| = 60$. Now, we apply the signature homomorphism $\text{sgn}|_{\phi(G)} : \phi(G) \to \{1, -1\}$. Since $\phi(G)$ is simple and the homomorphism is non-injective, it is trivial and $\phi(G) \subset A_5$. We now know that $\phi(G) = A_5$ since both have order 60.

Now, it remains to be shown that every simple group of order 60 has a subgroup of index 5. The four possibilities for n_2 are 1, 3, 5, and 15. Clearly, $n_2 \neq 1$ by simplicity, and we also know that $n_2 \neq 3$ since $60 \nmid 3!$. We know that $n_5 = 6$, since the only other possibility by Sylow III would be $n_5 = 1$, violating simplicity of G. Similarly, $n_3 = 10$, because $n_3 \neq 1$ by simplicity again, and $n_3 \neq 4$ because $60 \nmid 4!$. Thus, there are 20 elements of order 3 and 24 elements of order 5 in G. Two distinct Sylow 2-subgroups of G would intersect in up to 2 elements, meaning that if $n_2 = 15$, the group would need to have at least 75 elements, which it does not. Thus, $n_2 = 5$, implying that the normalizer of a Sylow 2-subgroup would have index 5. By the previous discussion, G is isomorphic to A_5.

□

Acknowledgements

I would like to thank my mentors, Nir Gadish and Oishee Banerjee, for their guidance throughout the research process. It is with their support that I was able to write a paper on group theory, which I previously had no background in. I would also like to thank Peter May for organizing this program and giving me the opportunity to explore this topic. Finally, I would like to thank my professor, Laci Babai, for his guidance and inspiration.

References

[1] I. N. Herstein. Topics in Algebra. John Wiley & Sons. 1975
[2] Keith Conrad. Group Actions. http://www.math.uconn.edu/∼kconrad/blurbs/grouptheory/gpaction.pdf
[3] Keith Conrad. Consequences of the Sylow Theorems. http://www.math.uconn.edu/∼kconrad/blurbs/grouptheory/sylowapp.pdf
[4] Gabe Cunningham. Sylow Theorems and The General Linear Group. http://www-math.mit.edu/∼dav/sylow.pdf