A Teacher's Contribution to Group Theory - Sylow's First Theorem

Christopher Burke Tomás Gillanders David Murphy

Introduction - A Converse to Lagrange's Theorem?

Lagrange's Theorem is ubiquitous in the study of finite groups, a consequence of the group axioms that places a strong constraint on which subsets of a group can be subgroups.

Theorem 1 *(Lagrange)*. Let G be a group and H be a subgroup of G. Then $|H| \mid |G|$.

Given Lagrange's Theorem, it is natural to ask whether the converse of Lagrange's Theorem is true; given a positive integer n, such that $n \mid |G|$, does a subgroup $H \leqslant G$ exist such that $n = |H|$? In general, this is in fact, not true. However, there are special cases in which it does hold.

In this project, we explore "Sylow's First Theorem", which provides a case for which the converse does hold; namely when p^k is the highest power of a prime p that divides $|G|$. The objective of this project to to outline the material that is required to prove this theorem, assuming only a basic understanding of group and set theory, and an inquisitive disposition.

Equivalence Relations

Definition 2 *(Equivalence Relation)*. Let S be a set and $\sim$ be a relation on S. We say that $\sim$ is an Equivalence Relation on S iff the following properties hold. Let $x, y, z \in S$, then,

- $x \sim x, \forall x \in S,$ *(Reflexivity)*
- If $x \sim y$, then $y \sim x$, *(Symmetry)*
- If $x \sim y$ and $y \sim z$, then $x \sim z$. *(Transitivity)*

Lemma 2. Let G be a group that acts on a set S. Let $\sim$ be the relation $x \sim y$ iff $x \in O_G(y)$. Then $\sim$ is an equivalence relation on S.

Proof. Let G and S be as stated above. We consider each of the conditions that $\sim$ must satisfy to be an equivalence relation:

- By definition of a group action, the permutation induced by $\mathrm{id} \in G$, π_{id}, is the identity permutation and thus, $\pi_{\mathrm{id}}(x) = x, \forall x \in S$. Thus $x \in O_G(x)$ and $x \sim x, \forall x \in S$.
- Suppose that $x \sim y$. Thus, $x \in O_G(y)$. Therefore, $x = \pi_g(y)$ for some $g \in G$. Then we have:

$$\begin{aligned} x = \pi_g(y) \Rightarrow \pi_{\mathrm{id}}(x) = \pi_g(y) \Rightarrow \pi_{g^{-1}}\pi_{\mathrm{id}}(x) = \pi_{g^{-1}}\pi_g(y) \\ \Rightarrow \pi_{g^{-1}\mathrm{id}}(x) = \pi_{g^{-1}g}(y) \Rightarrow \pi_{g^{-1}}(x) = \pi_{\mathrm{id}}(y) \Rightarrow y = \pi_{g^{-1}}(x) \end{aligned}$$

  Thus $y \in O_G(x)$ and $y \sim x$.
- Suppose $x \sim y$ and $y \sim x$. Then for some $g, h \in G$, we have $x = \pi_g(y)$ and $y = \pi_h(z)$. Substituting the latter into the prior expression, we get $x = \pi_g(\pi_h(x)) = \pi_g\pi_h(x) = \pi_{gh}(z)$. Thus $x \in O_G(z)$ and $x \sim z$.

Therefore, we have that the relation $\sim$ is reflexive, symmetric and transitive. Thus, $\sim$ is an equivalence relation on S. ■

Corollary 1. Since $\sim$ is an equivalence relation on S, $P = {}^{S}\!/\!\sim$ is a partition of S.

Group Actions

Definition 1 *(Group Action)*. A group G acts on a set S if every element $g \in G$ induces a permutation π_g of the set S, such that

- For $\mathrm{id} \in G$, π_{id} is the identity permutation on S.
- For all $g, h \in G$, $\pi_g\pi_h = \pi_{gh}$, where $\pi_g\pi_h = \pi_g \circ \pi_h$ is read "π_g after π_h".

Notation. Let G be a group that acts on a set S. We define the following notation:

- π_g is the permutation of S induced by $g \in G$.
- $O_G(x) = \{\pi_g(x) \mid g \in G\}$ is the orbit of $x \in S$ under the action of G.
- $Stab_G(x) = \{g \in G \mid \pi_g(x) = x\}$ is the stabilizer of $x \in S$ in G.

Lemma 1. Let G be a group that acts on a set S. Then for all $x \in S$, $Stab_G(x) \leqslant G$. ($Stab_G(x)$ is a subgroup of G)

The Orbit-Stabilizer Theorem & A Useful Lemma

Theorem 2 *(Orbit-Stabilizer Theorem)*. Let G be a group that acts on a set S, and let $x \in S$, then, $|O_G(x)| = [G : Stab_G(x)]$.

Lemma 3. Let p be prime and m, k be positive integers such that $p \nmid m$. Then

$$p \nmid \binom{p^k m}{p^k}$$

Proof. Let p, m and k be as above. Recall the definition of the binomial coefficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

Then we have

$$\begin{aligned} \binom{p^k m}{p^k} &= \frac{p^k m(p^k m - 1)\cdots(p^k m - p^k + 1)}{p^k(p^h - 1)\cdots(p^k - p^k + 1)} \\ &= m \prod_{j=1}^{p^k - 1} \frac{p^k m - j}{p^k - j} \end{aligned}$$

Note from above that for each term of the product, $\frac{p^k m - j}{p^k - j}$ with $0 < j \leq p^k - 1$, the largest integer power of p that divides $p^k m - j$ is equal to the largest integer power of p that divides j; and similarly the largest integer power of p that divides $p^k - j$ is equal to the largest integer power of p that divides j. [1] Therefore, the highest power of p that divides both $p^k m - j$ and $p^k - j$ is the same. Thus, after reduction of the quotients to lowest terms, no factor of p remains in the integer, $\prod_{j=1}^{p^k-1} \frac{p^k m - j}{p^k - j}$. Therefore, since $p \nmid m$ and $p \nmid \left(\prod_{j=1}^{p^k-1} \frac{p^k m - j}{p^k - j}\right)$, $p \nmid \binom{p^k m}{p^k}$. ■

Sylow's First Theorem

Theorem 3 (Sylow's First Theorem). Let G be a group such that $p^k m = |G|$, where p is a prime and $p \nmid m$. Then G has a subgroup of order p^k (A Sylow p-subgroup).

Proof. Let G, p and m be as described in the theorem. Now consider the set S of all p^k-element subsets of G. That is

$$\begin{aligned} S &= \{S_i \subseteq G \mid |S_i| = p^k\} \\ &= \{S_1, S_2, \dots, S_n\} \end{aligned}$$

We note that there are $\binom{p^k m}{p^k}$ ways to choose p^k-element subsets from a set of size $p^k m$, and thus, $n = |S| = \binom{p^k m}{p^k}$. Note that by Lemma 3, $p \nmid n$.

Now consider the following action of G on S. For $g \in G$ and $S_i \in S$,

$$\pi_g(S_i) = gS_i = \{gx \mid x \in S_i\}$$

Recall that by Corollary 1, $P = \{O_G(S_i) \mid S_i \in S\}$ is a partition of S, and thus,

$$|S| = \sum_P |O_G(S_i)|$$

Since $p \nmid n$, it follows that there must exist at least one $S^\star \in S$ such that $p \nmid |O_G(S^\star)|$. Let $O_G(S^\star) = \{x_1, \dots, x_r\}$. We then note that by Theorem 2,

$$|G| = [G : Stab_G(S^\star)] \cdot |Stab_G(S^\star)| = |O_G(S^\star)| \cdot |Stab_G(S^\star)|$$

However, we note that $p^k \mid |G|$ and $p^k \nmid |O_G(S^\star)|$, and therefore, $p^k \mid |Stab_G(S^\star)|$. Thus, $p^k \leq |Stab_G(S^\star)|$.

Now note $Stab_G(S^\star) = \{g \in G \mid \pi_g(S^\star) = gS^\star = S^\star\}$. Let $H = Stab_G(S^\star)$ for notational simplicity and note that we can consider the following action of H on $S^\star$ (since $S^\star$ is itself a set). For $h \in H$ and $x \in S^\star$,

$$\sigma_h(x) = hx = x$$

We now consider $Stab_H(x)$ for any $x \in S^\star$. We note that this set consists of all $h \in H$ such that $hx = x$. However, while $x \in S^\star$, by definition $x \in G$, and thus, by the group axioms, $\exists x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = \mathrm{id}$. Therefore,

$$hx = x \implies (hx)x^{-1} = xx^{-1} \implies h(xx^{-1}) = \mathrm{id} \implies h\,\mathrm{id} = \mathrm{id} \implies h = \mathrm{id} \in G$$

Thus, by definition of a group, $Stab_H(x) = \{\mathrm{id}\}$, and $|Stab_H(x)| = 1$. Once again applying Theorem 2, we find,

$$|H| = [H : Stab_H(x)] \cdot |Stab_H(x)| = |O_H(x)| \cdot |Stab_H(x)| = |O_H(x)|$$

But $O_H(x)$ is the set of all elements of $S^\star$ that can be reached by acting on x by the elements of H, and thus, since $|S^\star| = p^k$ we have $|H| = |Stab_G(S^\star)| = |O_H(x)| \leq p^k$.

Therefore, we have shown $p^k \leq |Stab_G(S^\star)| \leq p^k$, and thus, we deduce, $|Stab_G(S^\star)| = p^k$. We also note from Lemma 1 that $Stab_G(S^\star)$ is a subgroup of G. Therefore, we have identified a subgroup $H \leqslant G$ such that $|H| = p^k$; a Sylow p-subgroup. ■

A Note on Peter Sylow

Sylow's Theorems are attributed to the Norwegian mathematician Peter Ludvig Mejdell Sylow (1832-1918). From 1858 to 1898 he worked as a maths and science teacher in Halden Norway, and in 1898 he began lecturing in Christina University. Sylow published his theorems in a brief paper in 1872. Sylow proved the theorem in terms of permutations of groups as the abstract definition of a group had not yet been conceived. Georg Frobenius re-proved the theorems for abstract groups in 1887. [2, 6]

Conclusion

In this project we set out to investigate Peter Sylow and his contributions to group theory. We decided to focus on his first theorem, which identifies a case in which the converse of Lagrange's Theorem holds. Sylow's First Theorem states that for every prime factor p with multiplicity k of the order of a finite group G, there exists a Sylow p-subgroup of G, of order p^k. Sylow's First Theorem is a powerful statement which gives insight to the internal structure of a group.

References

The proof of Sylow's First Theorem was adapted from a proof presented in Durbin's "Modern Algebra" [1]. The proof and its notation were altered in order to improve its clarity and readability for a wider audience. The statement and proof of Lemma 3 was also adapted from this text for clarity. Further information on the topic of Sylow's First Theorem was obtained from Menini and Van Oystaeyen's "Abstract Algebra" [5], and Hall's "An Introduction to Abstract Algebra", [3]. We would also have liked to have presented a more 'complete' proof of Lemma 3. However, due to space restrictions, this unfortunately could not be done. The link to the image used is found in Reference [4].

[1] J. R. Durbin. *Modern Algebra.* John Wiley & Sons, 2000. ISBN: 0-471-32147-6.
[2] J. B. Fraleigh. *A First Course in Abstract Algebra.* Addison-Wesley Publishing Company, Inc., 1999. ISBN: 0-201-47436-0.
[3] F. M. Hall. *An Introduction to Abstract Algebra, Volume II.* Cambridge University Press, 1969. ISBN: 521-7055-4.
[4] School of Mathematics and Scotland Statistics University of St Andrews. July 2014. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Sylow/pictdisplay/.
[5] C. Menini and Van Oystaeyen. *Abstract Algebra, A Comprehensive Treatment.* Marcel Dekker, Inc., 2004. ISBN: 0-8247-0985-3.
[6] J. J. O'Connor and Robertson E. F. *Peter Ludwig Mejdell Sylow.* July 2014. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Sylow/.