A jargon-minimal counting proof of Sylow's first theorem

Submissions October 2023 (Vol. 55, No. 5)

P. Mark Kayll (University of Montana, Missoula, MT, USA)

Abstract

We present a short proof of Sylow's famous 'First Theorem.' Stripped to its essentials, the proof—attributed to Wielandt (1959)—relies only on basic concepts (equivalence relations and divisibility). Whereas most textbook proofs invoke plenty of group-theoretic jargon (stabilizers, conjugacy classes, etc.), this one avoids all that, stands alone, and fits on a page.

A (binary) million years ago, Helmut Wielandt published an appealing counting proof [3] of Sylow's First Theorem. Stripped to its bare essentials, it requires surprisingly little group theory and ought to be better known. The version below lends itself to an hour or so in a classroom with second- or third-year university math enthusiasts.

Theorem ('Sylow's First') *If p is a prime, r is an integer coprime to p, and G is a group of order $p^\alpha r$, then G contains a(t least one) subgroup of order p^α.*

Proof. Let $\mathcal{S}$ denote the family of all sub***sets*** of G of size p^α, and write $\mathcal{S} = \{A_1, A_2, \ldots, A_n\}$. We shall argue that at least one member of $\mathcal{S}$ is a group—indeed, is a subgroup of G.

It's convenient to know that p and n are coprime, so we first establish this fact. We have

$$n = \binom{p^\alpha r}{p^\alpha} = \frac{p^\alpha r(p^\alpha r-1)(p^\alpha r-2)\cdots(p^\alpha r-(p^\alpha-1))}{p^\alpha\cdot 1\cdot 2\cdot\cdots\cdot(p^\alpha-1)} = r\prod_{k=1}^{p^\alpha-1}\frac{p^\alpha r-k}{k}.$$

Consider the factors $\frac{p^\alpha r-k}{k}$. If $p \nmid k$, then $p \nmid (p^\alpha r - k)$. On the other hand, if $p \mid k$, then $k = p^\beta s$ for some integer β with $1 \leq \beta < \alpha$ and $p \nmid s$. So here, we have

$$\frac{p^\alpha r-k}{k} = \frac{p^\beta(p^{\alpha-\beta}r-s)}{p^\beta s} = \frac{p^{\alpha-\beta}r-s}{s},$$

and $p \nmid p^{\alpha-\beta}r - s$ (for otherwise, $p \mid s$). In either case, p fails to divide each factor $\frac{p^\alpha r-k}{k}$, and thus we see that $p \nmid n$.

Now if $x \in G$ and $A_i \in \mathcal{S}$, then the set $A_i x$ also contains p^α elements (for the map $A_i \to A_i x$ given by $a \mapsto ax$ is injective). Hence, $A_i x = A_j$ for some $j \in \{1, \ldots, n\}$. Let us define a relation $\sim$ on $\mathcal{S}$ by

$$A_i \sim A_j \iff A_i x = A_j \text{ for some } x \in G.$$

Using the group axioms for G, it's easy to see that $\sim$ is an equivalence relation. Since $p \nmid n$, at least one equivalence class $\mathcal{C}$ of $\sim$ contains some q sets A_i with $p \nmid q$; say $\mathcal{C} = \{A_1, A_2, \ldots, A_q\}$ (relabelling the A_i's as necessary).

Let $H = \{x \in G\colon\ A_1 x = A_1\}$; one easily verifies that H is a subgroup of G—write h for its order. For $x, y \in G$, observe that

$$A_1 x = A_1 y \Leftrightarrow A_1 xy^{-1} = A_1 \Leftrightarrow xy^{-1} \in H \Leftrightarrow Hxy^{-1} = H \Leftrightarrow Hx = Hy;$$

therefore, $A_1 x \neq A_1 y$ if and only if $Hx \neq Hy$. It follows from this equivalence and the definition of $\mathcal{C}$ that $\mathcal{C}$'s order q coincides with the number of distinct (right) cosets of H in G; i.e., $q = p^\alpha r/h$, or $h = p^\alpha r/q$. But since $p \nmid q$, this implies that $q \mid r$, so that $h \geq p^\alpha$.

To see the reverse inequality, consider an element $a \in A_1$. The definition of H implies that the (left) coset aH is a subset of A_1; whence,

$$h = |H| = |aH| \leq |A_1| = p^\alpha,$$

and it now follows that $h = p^\alpha$. Therefore, the subgroup H of G is indeed a member of $\mathcal{S}$ □

.

Remark Other authors—e.g., [1, 2]—have presented Wielandt's proof; Professor Petrich (see below) distilled it particularly nicely on one chalkboard.

In memoriam

Submitted in honour of **Mario Petrich (1932–2021)**, who showed me (and the rest of the class) this proof at Simon Fraser University in 1986.

References

[1] I.N. Herstein, *Topics in Algebra*, Second edition, Xerox College Publishing, Lexington MA, 1975.

[2] I. Martin Isaacs, *Algebra. A Graduate Course*, Brooks/Cole, Pacific Grove CA, 1994.

[3] Helmut Wielandt, Ein Beweis für die Existenz der Sylowgruppen, *Arch. Math.* (Basel), **10** (1959), 401–402.

AMS (MOS) Subject Classifications: 20D20, 05A10, 00A05, 11-01