Section II.5. The Sylow Theorems

Note. Finite abelian groups are classified in the "Fundamental Theorem" (Theorem II.2.6). So we now turn our attention to finite nonabelian groups. We won't completely classify finite nonabelian groups (nor is this likely to ever be done) but we make some initial steps with the First, Second, and Third Sylow Theorems.

Note. Peter Ludvig Sylow (1832–1918) published the three "Sylow Theorems" of this section in "Théorèmes sur les groupes de substitutions," *Mathematische Annalen* **5** (1872), 584–594. He, like Abel, was from Norway.

In 1862 Sylow lectured at the University of Christiania (Oslo, Norway). In his lectures Sylow explained Abel's and Galois's work on algebraic equations. Between 1873 and 1881 Sylow (with Sophus Lie) prepared an edition of Abel's complete work. After proving Cauchy's theorem (Theorem II.5.2) that a finite group of an order which is divisible by a prime p, has a subgroup of order p, Sylow asked whether it can be generalized to powers of p. The answer and the results on which

Sylow's fame rests are in his 10 page paper published in 1872; almost all work on finite groups uses Sylow's theorems. He spent most of his career as a high school teacher in Halden, Norway. Sylow was awarded an honorary doctorate from the University of Copenhagen and taught at Christiania University starting in 1898. (This information is from MacTutor History of Mathematics Archive biography of Sylow.)

Note. Fraleigh mimics Hungerford's presentation of this material. When we present the results we will also give a reference to Fraleigh's corresponding result. Most of the results concern prime power order groups and subgroups.

Lemma II.5.1. Fraleigh, Theorem 36.1.
If a group H of order p^n (p prime) acts on a finite set S and if $S_0 = \{x \in S \mid h \star x = x \text{ for all } h \in H\}$ then $|S| \equiv |S_0| \pmod{p}$.

Theorem II.5.2. Fraleigh, Theorem 36.3. Cauchy's Theorem.
If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Note. The abstract to M. Meo's "The Mathematical Life of Cauchy's Group Theorem" (*Historia Mathematica* **31** (2004), 196–221) reads:

> "Cauchy's theorem on the order of finite groups is a fixture of elementary course work in abstract algebra today: its proof is a straightforward exercise in the application of general mathematical tools. The initial proof by Cauchy, however, was unprecedented in its complex computations involving permutational group theory and contained an egregious error. A direct inspiration to Sylow's theorem, Cauchy's theorem was reworked by R. Dedekind, G.F. Frobenius, C. Jordan, and J.H. McKay in ever more natural, concise terms. Its most succinct form employs just the structure lacking in Cauchys original proof—the wreath product."

On the second page of this paper, Meo comments: "Cauchy's theorem in permutation groups, which constituted the major conclusion of the 101 pages of *Mémoire sur les arrangements que l'on peut former avec des lettres données* [Cauchy, 1845]. . . It appeared just before the posthumous publication of Galois [1846]. . . and the two publications together [i.e., that of Cauchy and Galois] have recently been characterized as 'the two sources that introduced group theory to mathematics' [Neumann, 1989, 293]." Meo's paper is online: "The Mathematical Life of Cauchy's Group Theorem" (accessed 11/14/2019). As a side note, the "J.H. McKay" (that's "James Harold") mentioned in the abstract had the same Ph.D. adviser (William Richard Ball) as my graduate algebra professor (Paul Daniel Hill).

Definition. A group in which every element has order a power (≥ 0) of some fixed prime p is a *p-group*. If H is a subgroup of group G and H is a p-group, then H is a *p-subgroup* of G.

Note. The subgroup $\langle e \rangle$ of a group G is a p-subgroup since $e^1 = e^{p^0} = e$.

Corollary II.5.3. Fraleigh Corollary 36.4.
A finite group G is a p-group if and only if $|G|$ is a power of p.

Corollary II.5.4. The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Lemma II.5.5. If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Corollary II.5.6. Fraleigh Corollary 36.7.
If H is a p-subgroup of a finite group G such that p divides $[G : H]$, then $N_G(H) \neq H$.

Note. Now for the First Sylow Theorem. Notice that it deals with subgroups which are of order a power of a prime and also makes a normality claim for certain subgroups.

Theorem II.5.7. Fraleigh Theorem 36.8. First Sylow Theorem. Let G be a group of order $p^n m$ with $n \geq 1$, p prime, and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G (that is, $P < H < G$ with H a p-group implies $P = H$).

Note. By the first Sylow Theorem (Theorem II.5.7), every finite group G, say $|G| = p^n m$ where $n \geq 1$, p is prime, and $(p, m) = 1$, has a nontrivial Sylow p-subgroup (namely, a subgroup of order p^n).

Corollary II.5.8. Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $(p, m) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of G if and only if $|H| = p^n$.

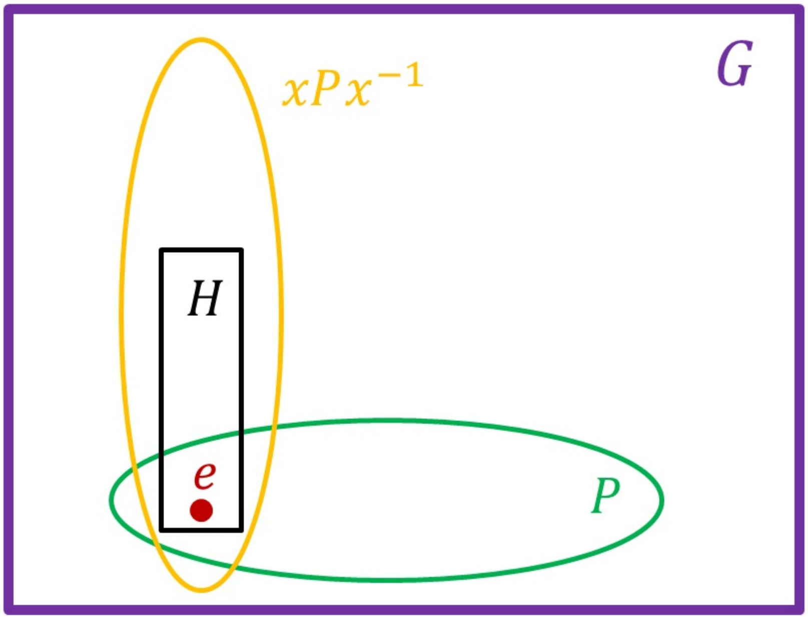
(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Theorem II.5.9. Fraleigh Theorem 36.10. Second Sylow Theorem.

If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $x \in G$ such that $H < xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Note. We can illustrate the Second Sylow Theorem as:



Theorem II.5.10. Fraleigh 36.11. Third Sylow Theorem.

If G is a finite group and p a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Theorem II.5.11. If P is a Sylow p-subgroup of a finite group G, then $N_G(N_G(P)) = N_G(P)$.

Example. Fraleigh, Example 36.12.

To illustrate the Sylow Theorems, consider S_3 of order $3! = 6$. S_3 consists of the permutations

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The multiplication table for S_3 is then:

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

The Sylow 2-subgroups are $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$. With $p = 2$, we see that there are $3 \equiv 1 \pmod{2}$ such subgroups and 3 divides $|S_3| = 6$, thus illustrating the Third Sylow Theorem. With the group action as conjugation, we have $\rho_2\{\rho_0, \mu_1\}\rho_2^{-1} = \{\rho_0, \mu_3\}$, $\rho_1\{\rho_0, \mu_1\}\rho_1^{-1} = \{\rho_0, \mu_2\}$, and $\rho_1\{\rho_0, \mu_2\}\rho_1^{-1} = \{\rho_0, \mu_3\}$, thus illustrating the Second Sylow Theorem.

Note. We will use the Sylow Theorems in Section II.6 to help classify certain finite order groups. In particular, the Second Sylow Theorem can be used to deal with showing that groups are *not* simple by allowing us (under certain conditions) to show that a Sylow p-subgroup is a normal subgroup. We now give two such examples.

Example. Fraleigh, Example 36.13.

We claim that no group of order 15 is simple. Suppose group G is of order 15, $|G| = 15$. We will show that G has a normal subgroup of order 5. By the First Sylow Theorem (Theorem II.5.7), G has at least one subgroup of order 5 and this is a Sylow p-subgroup (with $p = 5$) by Corollary II.5.8(i). By the Third Sylow Theorem (Theorem II.5.10), the number of such subgroups is congruent to 1 modulo 5 and divides 15. Now 1 is the only such number, and so G has exactly one subgroup of order 5, say P. By Corollary II.5.8(iii), subgroup P is a normal subgroup of G, and so G is not simple.

Example. Every group G of order 483 is not simple. Notice that $483 = 3 \cdot 7 \cdot 23$. By the First Sylow Theorem (Theorem II.5.7), this group G has a Sylow 23-subgroup. By the Third Sylow Theorem (Theorem II.5.10), the number of Sylow 23-subgroups is 1 modulo 23 and divides $|G| = 483$. The divisors of 483 which are not multiples of 23 are 1, 3, 7, and 21. The only one of these which is 1 modulo 23 is 1. So G has 1 Sylow 23-subgroup. By Corollary II.5.8(iii) this Sylow 23-subgroup is a normal subgroup of G, and so G is not simple.

Revised: 4/12/2021