Section VII.36. Sylow Theorems

Note. In this section and the next, we look more closely at results that will help us classify finite groups. For finite abelian groups, we have the Fundamental Theorem for Finitely Generated Abelian Groups (Theorem 11.12) and the classification is complete. For nonabelian groups there is not now (nor likely to be in the near future) a complete classification of finite nonabelian groups. However, the Sylow Theorems will give us some perspective on finite groups (especially on the order of subgroups) and help us in some small way to start to classify simple groups in the next section.

Note. We need to briefly review some material from Sections 16 and 17 before looking at the Sylow Theorems.

Note. Section III.16 addresses "Group Action on a Set." We have already encountered this idea when considering the symmetric group on n letters, S_n, and the group of symmetries of the regular n-gon, D_n (the nth dihedral group). In these settings, there is a set of elements (either $\{1, 2, 3, \ldots, n\}$ or the vertices of a regular n-gon) and a group containing "actions" which are performed on the set. This idea is generalized in the following definition.

Definition 16.1. Let X be a set and G a group. An *action of G on X* is a map $* : G \times X \to X$ such that

1. $ex = x$ for all $x \in X$, and
2. $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

In this case, X is called a *G-set*.

Note. Let X be G-set and $x \in X$. Define $G_x = \{g \in G \mid gx = x\}$. Theorem 16.12 shows that G_x is a subgroup of group G, called the *isotropy subgroup of x*. For $g \in G$, denote $X_g = \{x \in X \mid gx = x\}$.

Example 16.6. Let X be the set of vectors in $\mathbb{R}^n$ and let $G = \mathbb{R}^*$ (the multiplicative group of nonzero real numbers). Then for all $\vec{v} \in X$ and all $r, s \in G$ we have (1) $a\vec{v} = \vec{v}$, and (2) $(rs)\vec{v} = r(s\vec{v})$, so $X = \mathbb{R}^n$ is a $\mathbb{R}^*$-set.

Theorem 16.14. Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Note. Recall the importance of an equivalence relation $\sim$ on set X from Theorem 0.22: The equivalence classes of $\sim$ partition set X.

Definition 16.15. Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 16.14 is an *orbit in X under G*. If $x \in X$, the cell containing x is the *orbit of x*, denoted Gx.

Theorem 16.16. Let X be a G-set and let $x \in X$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$. Also, $|Gx| = (G : G_x)$.

Note. Section III.17 addresses "Applications of G-Sets to Counting." The Sylow Theorems relate to counting as well and we need the following result and its corollary. We denote the points fixed by $g \in G$ as X_g: $X_g = \{x \in X \mid gx = x\}$.

Theorem 17.1. Burnside's Formula.
Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G then

$$r \cdot |G| = \sum_{g \in G} |X_g|.$$

Corollary 17.2. If G is a finite group and X is a finite G-set, then

$$(\text{The number of orbits in } X \text{ under } G) = \frac{1}{|g|} \sum_{g \in G} |X_g|.$$

Note. Nothing is implied about the *sizes* of the orbits in Burnside's Formula, only something about the *number* of the orbits. This should not be confused with the idea of cosets from Section II.10 in which every coset is of the same size.

Note. It is surprising that Fraleigh does not include biographical information on William Burnside (1852–1927).

William Burnside (1852–1927) (from the MacTutor History of Mathematics Archive)

Burnside published his influential *The Theory of Groups of Finite Order* in 1897. The second edition was published in 1911 and included "character theory." The second edition was for many decades the standard work in the field. Copies can be found online at Project Gutenburg and at GoogleBooks (accessed 7/12/2022). The book is available from Dover Publications for about $10. This book is of historical interest, but the terminology is not modern. "Because of Burnside's emphasis on the abstract approach, many consider him to be the first pure group theorist" [Joseph Gallian, *Contemporary Abstract Algebra*, 8th Edition (2013), page 505]. "Burnside's Conjecture" states that a group G of odd order has a normal series $\{e\} = G_0 \leq G_1 \leq G_2 \cdots \leq G_n = G$ such that G_{i+1}/G_i is abelian for $i = 0, 2, \ldots, n-1$. Notice that this implies that every finite group of odd order is solvable. This was proved by Feit and Thompson in 1963. See the supplement on Finite Simple Groups for more details.

Note. Let X be a finite G-set. For $x \in X$, the orbit of x is $Gx = \{gx \mid g \in G\}$ and the orbits partition set X. Let $\{x_1, x_2, \ldots, x_r\}$ be a set containing exactly one element of X from each orbit in X under G (again, we denote the number of orbits as r). We then have

$$|X| = \sum_{i=1}^{r} |Gx_i|. \tag{1}$$

Some of the orbits may be of length 1 (that is, we may have $gx_i = x_i$ for all $g \in G$). Let X_G be the set of all elements in orbits of length 1 (so X_G contains the elements of set X fixed by all elements of group G):

$$X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}.$$

With $|X_G| = s$, denote the $x_i \in X_G$ as $x_1, x_2, \ldots, x_s$. Then equation (1) gives

$$|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|. \tag{2}$$

Note. Fraleigh now develops the Sylow Theorems using the techniques of Thomas Hungerford (see *Algebra*, NY: Springer-Verlag, 1974—see Section II.5, pages 92–96). Fraleigh describes the arguments as "extremely pretty and elegant."

Theorem 36.1. Let G be a group of order p^n and let X be finite G-set. Then $|X| \equiv |X_G| \pmod{p}$.

Definition 36.2. Let p be prime. A group G is a *p-group* if every element in G

has order a power of the prime p. A subgroup of a group G is a *p-subgroup of G* if the subgroup is itself a p-group.

Note. The First Sylow Theorem (Theorem 36.8) will show us that finite group G has a subgroup of every *prime-power* order which divides $|G|$. Contrast this with Lagrange's Theorem (Theorem 10.10) which implies that the order of a subgroup of a finite group is a divisor of the order of the group. We know the general converse of this is not true, as demonstrated in Example 15.6 in which it is shown that A_4 (of order $4!/2 = 12$) has no subgroup of order 6. What the First Theorem of Sylow implies is that there is something "special" about prime-power divisors of the group and the existence of subgroups of these prime power orders. As a first step in this direction, we have the following.

Theorem 36.3. Cauchy's Theorem.

Let p be a prime. Let G be a finite group an dlet p divide $|G|$. Then G has an element of order p and (consequently) a subgroup of order p.

Note. The subgroup $\langle a \rangle$ of G in the proof of Cauchy's Theorem (Theorem 36.3) is a p-subgroup of G. This follows because the elements of $\langle a \rangle$ are of the form $e = a^0$ and a^k for $1 \leq k < p$. If $(a^k)^m = a^{km} = e$ then, since the order of a is p, km must be a multiple of p. The smallest value of m for which this is the case is $m = p$. Hence a^k is of order p and all elements of $\langle a \rangle$ are of order p (except e, which is of order $p^0 = 1$ [also a power of p]).

Corollary 36.4. Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.

Note. The proof is to be given in Exercise 36.14. It appears in Hungerford's *Algebra* as the proof of Corollary II.5.3.

Note. For group G, let $\mathcal{S}$ denote the set of all subgroups of G. Then $\mathcal{S}$ is a G-set where G acts on $\mathcal{S}$ as follows. Define $* : G \times \mathcal{S} \to \mathcal{S}$ as $h * H = gHg^{-1}$ (the conjugation subgroup of H by g—by Exercise 13.29, gHg^{-1} is a homomorphism image of G and so is a subgroup of G under $i_g : G \to G$). Consider $G_H = \{g \in G \mid gHg^{-1} = H\}$. By Exercise 36.11, G_H is a subgroup of G and by Theorem 14.13(2), H is a normal subgroup of G_H. Since G_H consists of all elements of G that leave H invariant under conjugation (and by Theorem 14.13, $gHg^{-1} = H$ if and only if $gH = Hg$) then G_H is the largest subgroup of G having H as a normal subgroup.

Definition 36.5. Let G be a group and $H \leq G$. Define $G_H = \{g \in G \mid gHg^{-1} = H\}$. Then G_H is the *normalizer of H in G* (the largest subgroup of G having H as a normal subgroup) and is denoted $N[H]$.

Lemma. Let H be a finite subgroup of group G. If $ghg^{-1} \in H$ for all $h \in H$ then $g \in N[H]$.

Proof. Let $ghg^{-1} \in H$ for all $h \in H$. Then the conjugation map $i_g : H \to G$ defined by $i_g(H) = gHg^{-1}$ actually maps H into H; that is, $i_g : H \to H$. Next, if $gh_1g^{-1} = gh_2g^{-1}$ then by cancellation in G, $h_1 = h_2$. So $i_g : H \to H$ is one to one. Since H is finite and i_g is one to one from H to H then i_g must be onto. So $i_g[H] = gHg^{-1} = H$ and $g \in N[H]$. ∎

Lemma 36.6. Let H be a p-subgroup of of a finite group G. Then $(N[H] : H) = (G : H) \pmod p$.

Corollary 36.7. Let H be a p-subgroup of a finite group G. If p divides $(G : H)$, then $N[H] \neq H$.

Theorem 36.8. First Sylow Theorem.

Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and where p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$, and
2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.

Definition 36.9. A *Sylow p-subgroup* P of a group G is a maximal p-subgroup of G, that is a p-subgroup contained in no larger p-subgroup.

Note. By the First Sylow Theorem (Theorem 36.8), is $|g| = p^n m$, the Sylow p-subgroups of G are the subgroups of order p^n. These subgroups are not unique, but are related by conjugation as given in the Second Sylow Theorem.

Theorem 36.10. Second Sylow Theorem.

Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G. That is, for some $g \in G$ we have $P_2 = gP_1g^{-1}$.

Theorem 36.11. Third Sylow Theorem.

If G is a finite group and p divides $|G|$, then the number of Sylow p-subgroups is congruent to 1 modulo p and divides $|G|$.

Example 36.12. To illustrate the Sylow Theorem, consider S_3 of order $3! = 6$. The Sylow 2-subgroups (in the notation of Example 8.7) 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 i_x representing conjugation by element x, we can confirm that $i_{\rho_2}[\{\rho_0, \mu_1\}] = \{\rho_0, \mu_3\}$ and $i_{\rho_1}[\{\rho_0, \mu_1\}] = \{\rho_0, \mu_2\}$, thus illustrating the Second Sylow Theorem.

Note. We will use the Sylow Theorems in Section 37 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 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 36.8), G has at least one subgroup of order 5 and this is a Sylow p-subgroup (with $p = 5$). By the Third Sylow Theorem (Theorem 36.11), 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. For each $g \in G$, conjugation by g (that is, using the inner automorphism based on g), i_g, of G with $i_g(x) = gxg^{-1}$ maps P onto gPg^{-1} which must again be a subgroup of G. Since all elements of the Sylow 5-subgroup P are of order 5, then all elements of gPg^{-1} must be of order 5 (notice that gPg^{-1} is not the trivial subgroup), so gPg^{-1} is also a Sylow 5-subgroup. Since P is the only Sylow 5-subgroup, then $P = gPg^{-1}$ for all $g \in G$ and so P is a normal subgroup of G. Therefore, G is not simple.

Note. The argument of the previous example is summarized in Exercise 29.12: "Let G be a finite group and let p be prime. If p divides $|G|$, but $|G|$ is not a power of p, and if G has precisely one proper Sylow p-subgroup, then this subgroup is normal in G. Hence, G is not simple."

Example. Every group of order 483 is not simple. Notice that $483 = 3 \cdot 7 \cdot 23$. By the Frist Sylow Theorem (Theorem 36.8), this group G has a Sylow 23-subgroup. By the Third Sylow Theorem (Theorem 36.11), the number of Sylow 23-subgroups is 1 modulo 23 and divides $|G| = 243$. The divisors of 243 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 Exercise 36.12, this subgroup is normal and G is not simple.

Note. The following two results are closely related to the Sylow Theorems. Together, they allow us to classify (up to isomorphism) groups of order pq where p and q are both prime. The statements and proofs can be found in Hungerford's *Algebra* (pages 96 and 97).

Proposition II.6.1. (From Hungerford's *Algebra*.)
Let p and q be primes such that $p > q$. If $q \nmid p-1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. If $q \mid p-1$, then there are (up to isomorphism) exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a nonabelian group K generated by c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$ where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$. (Here, Hungerford uses $|c|$ to denote the order of element c.)

Corollary II.6.2. (From Hungerford's *Algebra*.)
If p is an odd prime, then every group of order $2p$ is isomorphic either to the cyclic group $\mathbb{Z}_{pq}$ or the dihedral group D_p.

Note. Hungerford uses the Sylow Theorems and the previous two results to classify all groups of order 15 or less. See "Supplement: Small Groups" from Introduction to Modern Algebra (MATH 4127/5127) notes for the results.

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) he prepared an edition of Abel's complete work. After proving Cauchy's theorem (Theorem 36.3) that a finite group of order 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 the MacTutor History of Mathematics Archive.

Revised: 8/26/2022