Section VII.37. Applications of the Sylow Theory

Note. We now get some mileage out of the Sylow Theorems. We prove a few general results, and then further explore properties of finite groups of certain orders.

Theorem 37.1. Every group of prime-power (that is, every finite p-group) is solvable.

Note. We have followed Hungerford's proofs of the Sylow Theorems. Older proofs use the "class equation" which we now discuss.

Note. Let X be a finite G-set where G is a finite group. With $X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}$ and $Gx_i = \{gx_i \mid g \in G\}$, we have from Equation (2) on page 322

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

where $x_1, x_2, \ldots, x_r$ are the fixed points under the action of G (so they are in X_G—they represent the orbits of length 1) there are r orbits of elements, and x_i is chosen from the ith orbit.

Note. Now let set X be the group G and define the action as conjugation: for $x \in X = G$ and $g \in G$, define the action on x as gxg^{-1}. then

$$\begin{aligned} X_G &= \{x \in G \mid gxg^{-1} = x \text{ for all } g \in G\} \\ &= \{x \in G \mid gx = xg \text{ for all } g \in G\} \\ &= Z(G) \end{aligned}$$

where $Z(G)$ is the *center* of G (see page 58). Let $c = |Z(G)|$ and $n_i = |Gx_i|$. Then Equation (1) becomes

$$|G| = c + n_{c+1} + n_{c+2} + \cdots + n_r \tag{2}$$

where n_i is the number of elements in the ith orbit of G:

$$n_i = |Gx_i| = \{gxg^{-1} \mid g \in G\}.$$

By Theorem 16.16 $|Gx_i| = (G : G_{x_i})$ (the number of left cosets of G_{x_i} in G) and (also by Theorem 16.16) this is a divisor of $|G|$.

Definition. Equation (2) is the *class equation* of G. Each orbit in G under conjugation by G is a *conjugate class* in G.

Example 37.3. Recall that if G is abelian, then $Z(G) = G$ and so the class equation is $|G| = c$ (and the number of orbits is $r = 1$). So for a nontrivial example, consider $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$. Then $A(G) = \{\rho_0\}$ and $c = 1$. Now we compute conjugate classes using the multiplication table for S_3 (see page 79):

$$\begin{aligned}
\rho_1 : \quad & \rho_0\rho_1\rho_0^{-1} = \rho_0\rho_1\rho_0 = \rho_0\rho_1 = \rho_1 \\
& \rho_1\rho_1\rho_1^{-1} = \rho_1\rho_1\rho_2 = \rho_1\rho_0 = \rho_1 \\
& \rho_2\rho_1\rho_2^{-1} = \rho_2\rho_1\rho_1 = \rho_2\rho_2 = \rho_1 \\
& \mu_1\rho_1\mu_1^{-1} = \mu_1\rho_1\mu_1 = \mu_1\mu_3 = \rho_2 \\
& \mu_2\rho_1\mu_2^{-1} = \mu_2\rho_1\mu_2 = \mu_2\mu_1 = \rho_2 \\
& \mu_3\rho_1\mu_3^{-1} = \mu_3\rho_1\mu_3 = \mu_3\mu_2 = \rho_2.
\end{aligned}$$

So the orbit of ρ_1 (and ρ_2) is $\{\rho_1, \rho_2\}$. Next:

$$\begin{aligned}
\mu_1 : \quad & \rho_0\mu_1\rho_0^{-1} = \rho_0\mu_1\rho_0 = \rho_0\mu_1 = \mu_1 \\
& \rho_1\mu_1\rho_1^{-1} = \rho_1\mu_1\rho_2 = \rho_1\mu_3 = \mu_2 \\
& \rho_2\mu_1\rho_2^{-1} = \rho_2\mu_1\rho_1 = \rho_2\mu_2 = \mu_3 \\
& \mu_1\mu_1\mu_1^{-1} = \mu_1\mu_1\mu_1 = \mu_1\rho_0 = \mu_1 \\
& \mu_2\mu_1\mu_2^{-1} = \mu_2\mu_1\mu_2 = \mu_2\rho_1 = \mu_3 \\
& \mu_3\mu_1\mu_3^{-1} = \mu_3\mu_1\mu_3 = \mu_3\rho_2 = \mu_2.
\end{aligned}$$

So the orbit of μ_1 (and μ_2 and μ_3) is $\{\mu_1, \mu_2, \mu_3\}$. So $n_2 = |G\rho_1| = 2$ and $n_2 = |G\mu_1| = 3$. The class equation of S_3 is then $|S_3| = 6 = c + n_2 + n_3 = 1 + 2 + 3$. Notice that the conjugate classes are *not* of the same sizes.

Theorem 37.4. The center of a finite nontrivial p-group of G is nontrivial.

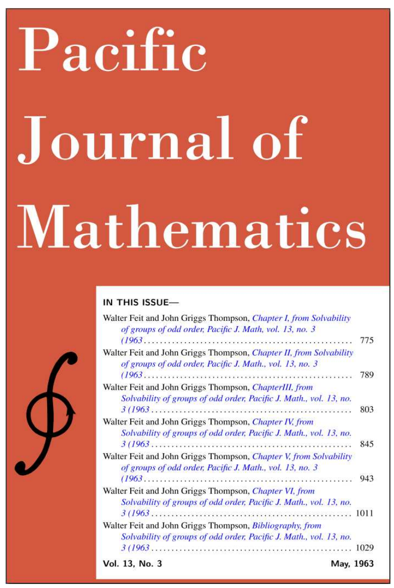
Lemma 37.5. Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$.

Note. For a prime number p, every group of order p^2 is abelian.

Theorem 37.6. For a prime number p, every group of order p^2 is abelian.

Note. Combining Theorem 37.6 with the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), we see that a group of order p^2, p prime, is either isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Note. We further illustrate the power of the Sylow Theorems by exploring finite simple groups. As mentioned in the supplement to Introduction to Modern Algebra (MATH 4127/5127), "Finite Simple Groups," simple groups are the building blocks of finite groups, as revealed in the Jordan-Hölder Theorem (Theorem 35.15). William Burnside conjectured that every finite simple group of non-prime order must be of even order. This was proved by Walter Feit and John Thompson in an issue of the *Pacific Journal of Mathematics* entirely devoted to their result: "Solvability of Groups of Odd Order" [*Pacific Journal of Mathematics*, **13**(3), 775–1029 (1963)].



Pacific Journal of Mathematics, **13**(3), 775-1029 (1963) [from `http://msp.org/pjm/1963/13-3/pjm-v13-n3-s.pdf`]

Theorem 37.7. If p and q are prime with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence G is not simple. If q is not congruent to 1 modulo p, then G is abelian and cyclic.

Note. We can restate Theorem 37.3 as: If group G is of order pq where p and q are distinct primes then G is not simple. If, in addition, $p < q$ and $q \not\equiv 1 \pmod{p}$, then $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Note. Notice that the proof of the first part of Theorem 37.7 implies the following (not stated explicitly in the text):

Corollary 37.7′. If a group G of finite order has only one proper nontrivial subgroup of a given order, then that subgroup is normal and G is not simple.

Lemma 37.8. If H and K are finite subgroups of a group G, then

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Note 1. We now use Sylow theory to draw some conclusions about abelian and simple groups. We will also use the fact established in Exercise 15.34 that a subgroup H of index 2 (i.e. H has two cosets) in a finite group G is normal and hence G is not simple.

Example 37.9. No group of order p^r for $r > 1$ is simple, where p is prime. By the First Sylow Theorem (Theorem 36.8), G contains a subgroup of order p^{r-1} which is normal in G. So G is not simple.

Example 37.10. Theorem 37.7 allows us to classify many finite groups as cyclic:

p	q	$q \pmod{p}$	The Groups of order pq
2	$q > 2$	1	?
3	5	2	$\mathbb{Z}_{15}$
3	7	1	?
3	11	2	$\mathbb{Z}_{33}$
3	13	1	?
3	17	2	$\mathbb{Z}_{51}$
5	7	2	$\mathbb{Z}_{35}$
5	11	1	?
5	13	3	$\mathbb{Z}_{65}$
5	17	2	$\mathbb{Z}_{85}$
5	19	4	$\mathbb{Z}_{95}$
7	11	4	$\mathbb{Z}_{77}$
7	13	6	$\mathbb{Z}_{91}$
7	17	3	$\mathbb{Z}_{119}$
7	19	5	$\mathbb{Z}_{133}$

Example 37.11. No group G of order 20 is simple. By the First Sylow Theorem (Theorem 36.8), G has a Sylow 5-subgroup. By the Third Sylow Theorem (Theorem 36.11) the number of such Sylow 5-subgroups of G is 1 (mod 5) and is a divisor of $|G| = 20$. So this number must be 1. By Corollary 37.7$'$, this Sylow 5-subgroup is a normal subgroup and G is not simple.

Note. Notice that an argument similar to that of Example 37.11 shows that no group of order 40 is simple (again, the only number which is both 1 (mod 5) and a divisor of 40 is 1). However, this argument fails for 80 (since 16 is both 1 (mod 5) and a divisor of 80).

Example 37.12. No group G of order 30 is simple. This argument is a bit more involved than the previous one. We again show that there is a unique Sylow p-subgroup, but we are unclear on what p is (well, it is either 3 or 5). By the Third Sylow Theorem (Theorem 36.11), the number of Sylow 5-subgroups is either 1 or 6, and the number of Sylow 3-subgroups is either 1 or 10. But is G has 6 distinct Sylow 5-subgroups, then the intersection of any two such subgroups is again a subgroup (Theorem 7.4) and so must have an order that is a divisor of 5 (Theorem of Lagrange, Theorem 10.10). Since the groups are distinct, it must be that the intersection is $\{e\}$. So each of the 6 Sylow 5-subgroups contain 4 elements of order 5, and hence G contains 24 elements of order 5. Similarly, if G has 10 Sylow 3-subgroups, each of the 10 Sylow 3-subgroups contains 2 elements of order 3, and hence G contains 20 elements of order 3. But then G must contain at least 45 elements (24 of order 5, 20 of order 3, and e). So G cannot have both 6 Sylow 5-subgroups and 10 Sylow 3-subgroups. So G had either a unique Sylow 5-subgroup or a unique Sylow 3-subgroup. By Corollary 37.7′ the unique Sylow p-subgroups is normal and G is not simple.

Example 37.13. No group G of order 48 is simple. By the Third Sylow Theorem (Theorem 36.11) G has either 1 or 3 Sylow 2-subgroups of order $2^4 = 16$ (recall that a Sylow p-subgroup is a maximal subgroup of order p^n for some $n \in \mathbb{N}$). (1) If there is only 1 such subgroup, then as above Corollary 37.7′ implies that G is not simple. (2) I there are 3, we now construct a normal subgroup of G of order 8. Let H and K be two such distinct Sylow 2-subgroups. Then $H \cap K$ is a subgroup of H (Theorem 7.4) and has order 1, 2, 4, or 8 by the Theorem of Lagrange (Theorem 10.10). But if $|H \cap K| \leq 4$ then by Lemma 37.8, $|HK| \geq 16 \times 16/4 = 64$, contradicting the facts that $HK \subseteq G$ and $|G| = 48$. So $H \cap K$ must be of order 8. So $H \cap K$ is a subgroup of both H and K (Theorem 7.4) of order half the order of H and K. So by Note 1 above, $H \cap K$ is a normal subgroup of both H and K. The normalizer of $H \cap K$ is (by definition) $N[H \cap K] = \{g \in G \mid g(H \cap K)g^{-1} = H \cap K\}$ and so includes both H and K since $H \cap K$ is normal in both H and K. Since $|H| = |K| = 16$ and $|H \cap K| = 8$, then $|N[H \cap K]| \geq 24$. Since $H < N[H \cap K]$ (and $N[H \cap K]$ is itself a group by Exercise 36.11) then by the Theorem of Lagrange (Theorem 10.10) $|N[H \cap K]|$ is a multiple of 16 and a divisor of 48. Hence $|N[H \cap K]| = 48$ and so $H \cap K = G$. So $H \cap K$ is normal in G (by Theorem 14.13(2), say) and G is not simple.

Example 37.14. No group G of order 36 is simple. By the Third Sylow Theorem (Theorem 36.11), G has either 1 or 4 Sylow 9-subgroups. If there is only 1 such subgroup, then by Corollary 37.7′ it is a normal subgroup of G and G is not simple. If there are 4 such distinct subgroups of order 9, then let H and K be two of them. Now, $|H \cap K| \geq 3$, since $|H \cap K| \leq 2$ implies by Lemma 37.8 that $36 \geq |HK| = (|H|\,|K|)/|H \cap K| \geq 9 \times 9/2 > 40$. As in the previous example, $N[H \cap K]$ includes H and K. Since $|H| = |K| = 9$, then $|N[H \cap K]|$ is a multiple of 9 by Lagrange's Theorem and since $H \neq K$, then this is at least 18 and since $N[H \cap K] < G$ it is a divisor of 36. So $|N[H \cap K]|$ is either 18 or 36. If $|N[H \cap K]| = 18 = 36/2$, then by Note 1 above $N[H \cap K]$ is a normal subgroup of G and G is not simple. If $|N[H \cap K]| = 36$ then $N[H \cap K] = G$ and $H \cap K$ is a normal subgroup of G and G is not simple.

Example 37.15. Every group G of order $255 = (3)(5)(17)$ is abelian. By the Third Sylow Theorem (Theorem 36.11), G has a Sylow 17-subgroup, and the number of such subgroups is 1 (mod 17) and a divisor of 255. Hence there is one such subgroup and by Corollary 37.7′ this subgroup, say H, is normal. Then G/H has order 15. Since $|G/H| = 15$, by Example 37.10 G/H is abelian. By Theorem 15.20, since G/H is abelian, the commutator subgroup C of G is a subgroup of H: $C \leq H$. Since $|H| = 17$, then

$$\text{either } |C| = 1 \text{ or } |C| = 17. \qquad (*)$$

As argued several times above, the Third Sylow Theorem (Theorem 36.11) shows that G has either 1 or 85 Sylow 3-subgroups and either 1 or 51 Sylow 5-subgroups.

As argued in Example 37.12, by Theorem 7.4 and the Theorem of Lagrange, the intersection of two distinct Sylow 3-subgroups (or two distinct Sylow 5-subgroups) must consist only of e. So if there are both 85 Sylow 3-subgroups and 51 Sylow 5-subgroups, then there are $85 \times 2 = 170$ elements of order 2 in G and $51 \times 4 = 204$ elements of order 5 in G. But $170 + 204 = 374 > 255 = |G|$, so there is either only 1 Sylow 3-subgroup of G or only 1 Sylow 5-subgroup of G. By Corollary 37.7$'$, G then has either a normal subgroup of order 3 or a normal subgroup of order 5. Denote this normal subgroup as K. Then $|G/K| = (G : K) = |G|/|K|$ is either (5)(17) or (3)(17). We now apply Theorem 37.7 with either $p = 3$ and $q = 17$ of $p = 5$ and $q = 17$. In either case, $q \equiv 2 \pmod{p}$ (and $q \not\equiv 1 \pmod{p}$) and so Theorem 37.7 implies that G/K is abelian. Now, by Theorem 15.20 again, $C \leq K$ and so the possible values of $|C|$ are 1, 3, 5. Combining this with $(*)$, gives that $|C| = 1$ and so $C = \{e\}$. by Theorem 15.20, G/N is abelian if and only if $C \leq N$. With $N = C = \{e\}$, we then have that $G/N = G/C = G/\{e\} \cong G$ is abelian. Notice that $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \cong \mathbb{Z}_{255}$ (by the Fundamental Theorem of Finitely Generated Abelian Groups—Theorem 11.12).

Revised: 8/15/2022