Corollary 20. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$
(2) P is normal in G
(3) P is characteristic in G
(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Proof: If (1) holds, then $gPg^{-1} = P$ for all $g \in G$ since $gPg^{-1} \in Syl_p(G)$, i.e., P is normal in G. Hence (1) implies (2). Conversely, if $P \trianglelefteq G$ and $Q \in Syl_p(G)$, then by Sylow's Theorem there exists $g \in G$ such that $Q = gPg^{-1} = P$. Thus $Syl_p(G) = \{P\}$ and (2) implies (1).

Since characteristic subgroups are normal, (3) implies (2). Conversely, if $P \trianglelefteq G$, we just proved P is the unique subgroup of G of order p^α, hence P char G. Thus (2) and (3) are equivalent.

Finally, assume (1) holds and suppose X is a subset of G such that $|x|$ is a power of p for all $x \in X$. By the conjugacy part of Sylow's Theorem, for each $x \in X$ there is some $g \in G$ such that $x \in gPg^{-1} = P$. Thus $X \subseteq P$, and so $\langle X \rangle \leq P$, and $\langle X \rangle$ is a p-group. Conversely, if (4) holds, let X be the union of all Sylow p-subgroups of G. If P is any Sylow p-subgroup, P is a subgroup of the p-group $\langle X \rangle$. Since P is a p-subgroup of G of maximal order, we must have $P = \langle X \rangle$, so (1) holds.

Examples

Let G be a finite group and let p be a prime.

(1) If p does not divide the order of G, the Sylow p-subgroup of G is the trivial group (and all parts of Sylow's Theorem hold trivially). If $|G| = p^\alpha$, G is the unique Sylow p-subgroup of G.
(2) A finite abelian group has a unique Sylow p-subgroup for each prime p. This subgroup consists of all elements x whose order is a power of p. This is sometimes called the *p-primary component* of the abelian group.
(3) S_3 has three Sylow 2-subgroups: $\langle (1\,2) \rangle$, $\langle (2\,3) \rangle$ and $\langle (1\,3) \rangle$. It has a unique (hence normal) Sylow 3-subgroup: $\langle (1\,2\,3) \rangle = A_3$. Note that $3 \equiv 1 \pmod 2$.
(4) A_4 has a unique Sylow 2-subgroup: $\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle \cong V_4$. It has four Sylow 3-subgroups: $\langle (1\,2\,3) \rangle$, $\langle (1\,2\,4) \rangle$, $\langle (1\,3\,4) \rangle$ and $\langle (2\,3\,4) \rangle$. Note that $4 \equiv 1 \pmod 3$.
(5) S_4 has $n_2 = 3$ and $n_3 = 4$. Since S_4 contains a subgroup isomorphic to D_8, every Sylow 2-subgroup of S_4 is isomorphic to D_8.

Applications of Sylow's Theorem

We now give some applications of Sylow's Theorem. Most of the examples use Sylow's Theorem to prove that a group of a particular order is not simple. After discussing methods of constructing larger groups from smaller ones (for example, the formation of semidirect products) we shall be able to use these results to classify groups of some specific orders n (as we already did for $n = 15$).

Since Sylow's Theorem ensures the existence of p-subgroups of a finite group, it is worthwhile to study groups of prime power order more closely. This will be done in Chapter 6 and many more applications of Sylow's Theorem will be discussed there.

For groups of small order, the congruence condition of Sylow's Theorem alone is often sufficient to force the existence of a *normal* subgroup. The first step in any numerical application of Sylow's Theorem is to factor the group order into prime powers. The largest prime divisors of the group order tend to give the fewest possible values for n_p (for example, the congruence condition on n_2 gives no restriction whatsoever), which limits the structure of the group G. In the following examples we shall see situations where Sylow's Theorem alone does not force the existence of a normal subgroup, however some additional argument (often involving studying the elements of order p for a number of different primes p) proves the existence of a normal Sylow subgroup.

Example: (Groups of order pq, p and q primes with $p < q$)

Suppose $|G| = pq$ for primes p and q with $p < q$. Let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$. We show that Q is normal in G and if P is also normal in G, then G is cyclic.

Now the three conditions: $n_q = 1 + kq$ for some $k \geq 0$, n_q divides p and $p < q$, together force $k = 0$. Since $n_q = 1$, $Q \trianglelefteq G$.

Since n_p divides the prime q, the only possibilities are $n_p = 1$ or q. In particular, if $p \nmid q - 1$, (that is, if $q \not\equiv 1 \pmod{p}$), then n_p cannot equal q, so $P \trianglelefteq G$.

Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. If $P \trianglelefteq G$, then since $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(Z_p)$ and the latter group has order $p - 1$, Lagrange's Theorem together with the observation that neither p nor q can divide $p - 1$ implies that $G = C_G(P)$. In this case $x \in P \leq Z(G)$ so x and y commute. (Alternatively, this follows immediately from Exercise 42 of Section 3.1.) This means $|xy| = pq$ (cf. the exercises in Section 2.3), hence in this case G is cyclic: $G \cong Z_{pq}$.

If $p \mid q - 1$, we shall see in Chapter 5 that there is a unique non-abelian group of order pq (in which, necessarily, $n_p = q$). We can prove the existence of this group now. Let Q be a Sylow q-subgroup of the symmetric group of degree q, S_q. By Exercise 34 in Section 3, $|N_{S_q}(Q)| = q(q - 1)$. By assumption, $p \mid q - 1$ so by Cauchy's Theorem $N_{S_q}(Q)$ has a subgroup, P, of order p. By Corollary 15 in Section 3.2, PQ is a group of order pq. Since $C_{S_q}(Q) = Q$ (Example 2, Section 3), PQ is a non-abelian group. The essential ingredient in the uniqueness proof of PQ is Theorem 17 on the cyclicity of $\text{Aut}(Z_q)$.

Example: (Groups of order 30)

Let G be a group of order 30. We show that G has a normal subgroup isomorphic to Z_{15}. We shall use this information to classify groups of order 30 in the next chapter. Note that any subgroup of order 15 is necessarily normal (since it is of index 2) and cyclic (by the preceding result) so it is only necessary to show there exists a subgroup of order 15. The quickest way of doing this is to quote Exercise 13 in Section 2. We give an alternate argument which illustrates how Sylow's Theorem can be used in conjunction with a counting of elements of prime order to produce a normal subgroup.

Let $P \in Syl_5(G)$ and let $Q \in Syl_3(G)$. If either P or Q is normal in G, by Corollary 15, Chapter 3, PQ is a group of order 15. Note also that if either P or Q is normal, then both P and Q are characteristic subgroups of PQ, and since $PQ \trianglelefteq G$, *both* P and Q are normal in G (Exercise 8(a), Section 4). Assume therefore that neither Sylow subgroup is normal. The only possibilities by Part 3 of Sylow's Theorem are $n_5 = 6$ and $n_3 = 10$. Each element of order 5 lies in a Sylow 5-subgroup, each Sylow 5-subgroup contains 4 nonidentity elements and, by Lagrange's Theorem, distinct Sylow 5-subgroups intersect in the identity. Thus the number of elements of order 5 in G is the number of nonidentity elements in one Sylow 5-subgroup times the number of Sylow 5-subgroups. This would be $4 \cdot 6 = 24$ elements of order 5. By similar reasoning, the number of elements of order 3 would be $2 \cdot 10 = 20$. This is absurd since a group of order 30 cannot contain $24 + 20 = 44$ distinct elements. One of P or Q (hence both) must be normal in G.

This sort of counting technique is frequently useful (cf. also Section 6.2) and works particularly well when the Sylow p-subgroups have order p (as in this example), since then the intersection of two distinct Sylow p-subgroups must be the identity. If the order of the Sylow p-subgroup is p^α with $\alpha \geq 2$, greater care is required in counting elements, since in this case distinct Sylow p-subgroups may have many more elements in common, i.e., the intersection may be nontrivial.

Example: (Groups of order 12)

Let G be a group of order 12. We show that either G has a normal Sylow 3-subgroup or $G \cong A_4$ (in the latter case G has a normal Sylow 2-subgroup). We shall use this information to classify groups of order 12 in the next chapter.

Suppose $n_3 \neq 1$ and let $P \in Syl_3(G)$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$, it follows that $n_3 = 4$. Since distinct Sylow 3-subgroups intersect in the identity and each contains two elements of order 3, G contains $2 \cdot 4 = 8$ elements of order 3. Since $|G : N_G(P)| = n_3 = 4$, $N_G(P) = P$. Now G acts by conjugation on its four Sylow 3-subgroups, so this action affords a permutation representation

$$\varphi : G \to S_4$$

(note that we could also act by left multiplication on the left cosets of P and use Theorem 3). The kernel K of this action is the subgroup of G which normalizes all Sylow 3-subgroups of G. In particular, $K \leq N_G(P) = P$. Since P is not normal in G by assumption, $K = 1$, i.e., φ is injective and

$$G \cong \varphi(G) \leq S_4.$$

Since G contains 8 elements of order 3 and there are precisely 8 elements of order 3 in S_4, all contained in A_4, it follows that $\varphi(G)$ intersects A_4 in a subgroup of order at least 8. Since both groups have order 12 it follows that $\varphi(G) = A_4$, so that $G \cong A_4$.

Note that A_4 does indeed have 4 Sylow 3-subgroups (see Example 4 following Corollary 20), so that such a group G does exist. Also, let V be a Sylow 2-subgroup of A_4. Since $|V| = 4$, it contains all of the remaining elements of A_4. In particular, there cannot be another Sylow 2-subgroup. Thus $n_2(A_4) = 1$, i.e., $V \trianglelefteq A_4$ (which one can also see directly because V is the identity together with the three elements of S_4 which are products of two disjoint transpositions, that is, V is a union of conjugacy classes).

Example: (Groups of order p^2q, p and q distinct primes)

Let G be a group of order p^2q. We show that G has a normal Sylow subgroup (for either p or q). We shall use this information to classify some groups of this order in the next chapter (cf. Exercises 8 to 12 of Section 5.5). Let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$.

Consider first when $p > q$. Since $n_p \mid q$ and $n_p = 1 + kp$, we must have $n_p = 1$. Thus $P \trianglelefteq G$.

Consider now the case $p < q$. If $n_q = 1$, Q is normal in G. Assume therefore that $n_q > 1$, i.e., $n_q = 1 + tq$, for some $t > 0$. Now n_q divides p^2 so $n_q = p$ or p^2. Since $q > p$ we cannot have $n_q = p$, hence $n_q = p^2$. Thus

$$tq = p^2 - 1 = (p-1)(p+1).$$