21. Sylow Theorems and applications

In general the problem of classifying groups of every order is completely intractable. Given any group G, the first thing to do to understand G is to look for subgroups H. In particular if H is normal in G, then one can take the quotient G/H and one can think of G as being built up from the two smaller groups H and G/H.

In turn, one can then consider H, or G/H, and try to break it up into pieces.

Definition 21.1. *Let G be a group.*

*We say that G is **simple** if it contains no proper normal subgroups.*

In the sense outlined above, we can think of simple groups as being the building blocks of creating an arbitrary group. (In fact even this approach is ridiculously optimistic; even the problem of finding all groups with a normal subgroup isomorphic to a cyclic group of order a power of a prime, whose quotient is cyclic of order the same prime, seems too hard to solve.) Thus we would like to classify all finite simple groups.

Turning this problem onto its head, we would like to find ways of producing normal subgroups of a group G.

If one thinks about Lagrange's Theorem, and its implications, two things are obvious.

First of all, the key part of the proof of Lagrange's Theorem, is to use the decomposition of G into the left cosets of H in G and to prove that each coset has the same size (namely the cardinality of H).

Secondly, in terms of applications, the problem of classifying subgroups of a group G turns into a problem of counting and considering the divisors of the order of the group.

As the problem of finding normal subgroups is so much harder than the problem of finding subgroups, the plan is to pick a prime p dividing the order of G and look for normal subgroups of order a power of p.

Definition 21.2. *Let G be a finite group of order $n = p^k m$, where p is a prime dividing n, not dividing m.*

*A subgroup H of order p^k is called a **Sylow p-subgroup** of G.*

Theorem 21.3 (Sylow's Theorems)**.** *Let G be a finite group of order $n = p^k m$ where p is a prime dividing n, not dividing m.*

1. *Every p-subgroup is contained in a Sylow p-subgroup.*
2. *Any two Sylow p-subgroups of G are conjugate.*
3. *The number of Sylow p-subgroups is congruent to 1 modulo p and divides n.*

With the Sylow Theorem in hand, let us prove one of the basic facts about simple groups.

Proposition 21.4. *Let G be a simple group of order less than sixty. Then the order of G is prime.*

To prove (21.4), it clearly suffices to assume that we have a simple group G of composite order n, less than sixty and derive a contradiction.

First an easy, but useful Lemma.

Lemma 21.5. *Let G be a group of finite order and let p be a prime dividing the order of G.*

(1) G has at least one Sylow p-subgroup P.

(2) If P is the only Sylow p-subgroup then P is normal in G (in fact, characteristically normal).

Proof. (1) follows from (3) of (21.3), as zero is not congruent to 1.

Suppose that P is the unique Sylow p subgroup of G. Let $g \in G$ and let $Q = gPg^{-1}$. Then Q is a subgroup of G, of the same order as P. Thus Q is another Sylow p-subgroup of G. By uniqueness $Q = P$ and so P is normal in G. □

To give a flavour of the method of attack, and to illustrate the strength of (21.3), suppose first that $n = 15$. Let $p = 5$.

We count the number of Sylow 5-subgroups of G. Suppose there are x. What do we know about x? Well x is supposed to be congruent to one modulo 5. Thus

$$x = 1, 6, 11, 16 \ldots$$

On the other hand x is supposed to divide 15. Since x does not divide 5, x must divide 3. But then $x = 1$ and there is one Sylow 5-subgroup, which is automatically normal in G. Thus G has a normal subgroup of order 5 and index 3.

Proposition 21.6. *Let G be a group of order pq the product of two primes, where $p < q$.*

Then G has a normal subgroup of order q. In particular G is not simple.

Proof. Let x be the number of Sylow q-subgroups. Then x is congruent to 1 modulo q. In particular x does not divide q. As x divides pq, it must divide p. If $x > 1$ then $x \geq q + 1 > q > p$. Thus $x = 1$ and there is exactly one subgroup P of order q. But then P is normal in G. □

We will also need the following Proposition, whose proof we defer to later.

Definition 21.7. *G is called a p-group if its cardinality is a power of a prime p.*

Note that a Sylow p-subgroup is automatically a p-group.

Proposition 21.8. *If G is a p-group then*

(1) The centre of G is non-trivial.
(2) There is a nested sequence of normal subgroups of G of every order dividing G,

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_d = G.$$

Now consider the numbers from 1 to 60. Eliminating those that are prime, a power of a prime or the product of two primes, leaves the following cases. $n = 12$, 18, 20, 24, 28, 30, 34, 36, 40, 42, 45, 48, 50, 52, 54, 56, 58.

We do some illustrative cases; the rest are left as an exercise for the reader.

Pick $n = 30 = 2 \cdot 3 \cdot 5$. Let $p = 5$. How many Sylow 5-groups are there? Suppose that there are x. Then x is congruent to 1 modulo 5. In this case,

$$x = 1, 6, \ldots.$$

On the other hand, x must divide 30, so that $x = 1$ or $x = 6$. If G is simple, then $x \neq 1$ and so $x = 6$. Let H and K be two Sylow 5-subgroups. Then $|H| = |K| = 5$. On the other hand $H \cap K$ is a subgroup of H and so by Lagrange, $|H \cap K| = 1$. Since there are 6 Sylow 5-subgroups and each such group contains 4 elements of order 5 that are not contained in any other subgroup, it follows that there are 24 elements of order 5.

Let y be the number of Sylow 3-subgroups. Then y is congruent to 1 modulo 3, so that

$$y = 1, 4, 7, 10 \ldots$$

As y divides 30 and $y \neq 1$, it follows that $y = 10$. As before there must therefore be 20 elements of order 3. But $24 + 20 > 30$, impossible.

Let us deal with one of the most tricky cases. Suppose that $n = 48 = 2^4 \cdot 3$. We count the number of Sylow 2-subgroups. Anyone of these must have order 16. Suppose that there are x such groups. Then x is congruent to one modulo two. The possibilities are then

$$x = 1, 3, 5, \ldots.$$

On the other hand x is supposed to divide 48, so that the only possibilities are 1 and 3. If G is simple, then there must be 3 subgroups

of order sixteen. Let S be the set of Sylow 2-subgroups. Define a homomorphism

$$\phi\colon G \longrightarrow A(S) \simeq S_3$$

by sending $g \in G$ to the permutation $\sigma = \phi(g)$,

$$\sigma\colon S \longrightarrow S,$$

where $\sigma(H) = gHg^{-1}$. It is not hard, as in the proof of Cayley's Theorem, to prove that ϕ is a homomorphism. As G has order 48 and $A(S)$ has order six, ϕ cannot be injective. Thus the kernel is a non-trivial normal subgroup.

In fact all finite simple groups have been classified. Finite simple groups come into two classes. There are those that belong to an infinite series of well-understood examples. There are 15 of these series, two of which are the cyclic groups of prime order and the alternating groups A_n, $n \geq 5$. Then there are the sporadic groups. There are 26 sporadic groups.

The monster group is the largest sporadic group; it has order

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

The prime factorisation of this number is

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

It is a subgoup of the group of linear symmetries of a real vector space of dimension $196883 = 47 \cdot 59 \cdot 71$,

$$\mathbb{R}^{196883},$$

in other words it is a subgroup of

$$\mathrm{GL}(196883, \mathbb{R}),$$

the group of 196883×196883 invertible matrices.

All finite groups appear as subgroups of a finite permutation group. The smallest n such that the monster is a subgroup of S_n is

$$2^4 \cdot 3^7 \cdot 5^3 \cdot 7^4 \cdot 11 \cdot 13^2 \cdot 29 \cdot 41 \cdot 59 \cdot 71.$$