13. Sylow Theorems and applications

In general the problem of classifying groups of every order is completely intractable. Let's imagine though that this is not the case. 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, and try to break it up into pieces.

Definition 13.1. *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 an arbitrary group. (In fact this 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 considering the prime factorisation of the order.

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 13.2. *A group of order a power of a prime p is called a* ***p-group****.*

Let G be a finite group of order $n = p^k m$, where p is prime and p does not divide m. A subgroup H of order p^k is called a **Sylow p-subgroup** *of G.*

Theorem 13.3. *Let G be a finite group of order $n = p^k m$, where p is prime and p does not divide m.*

1. *The number of Sylow p-subgroups is conqruent to 1 modulo p and divides n.*
2. *Any two Sylow p-subgroups are conjugate.*

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

Proposition 13.4. *If G is a simple group of order less than sixty then the order of G is prime.*

To prove (13.4), we assume that we have a group G of composite order n, less than sixty and show that it has a proper normal subgroup.

First an easy, but useful Lemma.

Lemma 13.5. *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 (1) of (13.3), 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 (13.4), suppose first that $n = 15$. Let $p = 5$.

We count the number n_5 of Sylow 5-subgroups of G. What do we know about n_5? Well n_5 is supposed to congruent to one modulo 5. Thus

$$n_5 = 1, 5, 11, 16 \dots$$

On the other hand n_5 is supposed to divide 15. Since n_5 does not divide 5, n_5 must divide 3. But then $n_5 = 1$ 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 13.6. *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 n_q be the number of Sylow q-subgroups. Then n_q is congruent to 1 modulo q. In particular n_q does not divide q. As n_q divides pq, it must divide p. If $n_q > 1$ then $n_q > q > p$, a contradiction. Thus $n_q = 1$ and there is exactly one subgroup Q of order q. But then Q is normal in G. □

We will also need the following Proposition, whose proof we omit.

Proposition 13.7. *If G is a p-group then the centre of G has order greater than one.*

In particular, ever simple p-group has prime order.

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 n_5. Then n_5 is congruent to 1 modulo 5. In this case,

$$n_5 = 1, 6, \ldots.$$

On the other hand, n_5 must divide 30, so that $n_5 = 1$ or $n_5 = 6$. If G is simple, then $n_5 \neq 1$ and so $n_5 = 6$. 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 n_3 be the number of Sylow 3-subgroups. Then n_3 is congruent to 1 modulo 3, so that

$$n_3 = 1, 4, 7, 10 \ldots$$

As n_3 divides 30 and $n_3 \neq 1$, it follows that $n_3 = 10$. Arguing as above, there must therefore be 20 elements of order 3. But $24 + 20 > 30$, impossible.

Definition 13.8. *Let G be a group and let S be a set.*

*An **action** of G on S is a function*

$$G \times S \longrightarrow S \qquad \text{denoted by} \qquad (g, s) \longrightarrow g \cdot s,$$

such that

$$e \cdot s = s \qquad \text{and} \qquad (gh) \cdot s = g \cdot (h \cdot s)$$

We have already seen lots of examples of actions. D_n acts on the vertices of a regular n-gon. S_n acts on the integers from 1 to n. S_n acts on the polynomials of degree n. G acts on itself by left multiplication. G acts on itself by conjugation, and so on.

In fact, an action of G on a set S is equivalent to a group homomorphism (invariably called a **representation**)

$$\rho \colon G \longrightarrow A(S).$$

Given an action $G \times S \longrightarrow S$, define a group homomorphism

$$\rho\colon G \longrightarrow A(S) \qquad \text{by the rule} \qquad \rho(g) = \sigma\colon S \longrightarrow S,$$

where $\sigma(s) = g \cdot s$. Vice-versa, given a representation (that is, a group homomorphism)

$$\rho\colon G \longrightarrow A(S),$$

define an action

$$G \cdot S \longrightarrow S \qquad \text{by the rule} \qquad g \cdot s = \rho(g)(s).$$

It is left as an exercise for the reader to check all of the details.

If G acts on itself by left multiplication the corresponding representation is precisely the group homomorphism which appears in Cayley's theorem. In fact if H is any subgroup of G then G acts on the left cosets of H in G by left multiplication (exercise for the reader).

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 8. Suppose that there are n_2 such groups. Then n_2 is congruent to one modulo two. The possibilities are then

$$n_2 = 1, 3, 5, \ldots.$$

On the other hand n_2 is supposed to divide 48, so that the only possibilities are 1 and 3. If $n_2 = 1$ then we are done. Otherwise there must be 3 subgroups of order sixteen. Let S be the set of Sylow 2-subgroups. Define an action

$$G \times S \longrightarrow S,$$

by the rule

$$g \cdot P = gPg^{-1}.$$

By (13.3) given two elements of S, P_1 and P_2, we can always find $g \in G$ such that $g \cdot P_1 = gP_1g^{-1} = P_2$. Let

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

be the corresponding representation. Thus we send $g \in G$ to the permutation $\sigma = \phi(g)$,

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

where $\sigma(P) = gPg^{-1}$. Consider the kernel of ϕ. By what we aleady observed, the kernel is not the whole of G. On the other hand, 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 in two classes. There are those that belong to 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. One such sporadic group is the monster group, which has order

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

which is

$$808017424794512875886459904961710757005754368000000000.$$

It is a subset of the group of rotations in a space of dimension

$$196,883.$$