Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Peter Cameron's 2010 Revision Notes, Sections 4 and 5, slightly updated by LHS, 2014

---

4 Sylow's Theorem

Sylow's Theorem is arguably the most important theorem about finite groups, so I am going to include a proof.

To begin, let's ask the question: is the converse of Lagrange's Theorem true? In other words, if G is a group of order n, and m is a divisor of n, does G necessarily contain a subgroup of order m? We note that this statement is true for cyclic groups. As an exercise, verify it for abelian groups (using the Fundamental Theorem of Abelian Groups).

In fact it is not true in general. Let G be the alternating group A_4. Then G is a group of order 12, containing the identity, three elements with cycle structure $[2,2]$, and eight elements with cycle structure $[3,1]$. We claim that G has no subgroup of order 6. Such a subgroup must contain an element of order 3, since there are only four elements not of order 3; also it must contain an element of order 2, since elements of order 3 come in inverse pairs, both or neither of which lie in any subgroup, so there are an even number of elements not of order 3, one of which is the identity. But it is not hard to show that, if you choose any element of order 2 and any element of order 3, together they generate the whole group.

4.1 Statement

Cauchy proved the first partial converse to Lagrange's Theorem:

Theorem 4.1 (Cauchy's Theorem) *Suppose that the prime p divides the order of the finite group G. Then G contains an element of order p.*

Sylow's Theorem is a far-reaching extension of Cauchy's. It is often stated as three separate theorems; but I will roll it into one here.

Theorem 4.2 (Sylow's Theorem) *Let G be a group of order $p^a \cdot m$, where p is a prime not dividing m. Then*

(a) G contains subgroups of order p^a, any two of which are conjugate;

(b) any subgroup of G of p-power order is contained in a subgroup of order p^a;

(c) the number of subgroups of order p^a is congruent to 1 mod p and divides m.

Subgroups of order p^a of G, that is, subgroups whose order is the largest power of p dividing $|G|$, are called *Sylow p-subgroups* of G.

The smallest positive integer which has a proper divisor whose order is not a prime power is 12; and we have seen that the group A_4 of order 12 has no subgroup of order 6. So Sylow's theorem cannot be improved in general!

4.2 Proof

This is quite a substantial proof; you may skip it at first reading. You can find different proofs discussed in some of the references. The crucial tool is the Orbit-Stabiliser Theorem, which is used many times, sometimes without explicit mention.

The proof uses two different actions of G. First, we consider the action on the set Ω consisting of all subsets of G of cardinality p^a, by right multiplication: $\mu(X,g) = Xg = \{xg : x \in X\}$. Each orbit consists of sets covering all elements of G. (For, if $x \in X$, and y is any element, then $y \in X(x^{-1}y)$.) So there are two kinds of orbits:

(A) orbits of size m, forming a partition of G;

(B) orbits of size greater than m.

Now by the Orbit-Stabiliser Theorem, the size of any orbit divides $|G|$; so an orbit of type (B) must have size divisible by p. But $|\Omega| = \binom{p^a m}{p^a}$ is not a multiple of p (this is a number-theoretic exercise); so there must be orbits of type (A). Again by the Orbit-Stabiliser Theorem, the stabiliser of a set in an orbit of type (A) is a subgroup of order p^a (and the orbit consists of the right cosets of one such stabilizer). This shows that subgroups of order p^a exist.

Now consider a different action of G, on the set Δ of all Sylow subgroups of G by conjugation (that is, $\mu(P,g) = g^{-1}Pg$).

We first observe that, if Q is a subgroup of G of p-power order which stabilises a Sylow subgroup P in this action, then $Q \leq P$; for otherwise PQ is a subgroup of order $|P| \cdot |Q|/|P \cap Q|$, a power of p strictly greater than p^a, which is not possible. (Further discussion of this point is at the end of this section.)

Take $P \in \Delta$. Then P stabilises itself, but no other Sylow subgroup (by the preceding remark), so all other orbits of P have size divisible by p. We conclude that $|\Delta|$, the number of Sylow p-subgroups, is congruent to 1 mod p.

Now G-orbits are unions of P-orbits, so the G-orbit containing P has size congruent to 1 mod p, and every other G-orbit has size congruent to 0 mod p. But P was arbitrary; so there is only a single orbit, whence all the Sylow p-subgroups are conjugate. The number of them is $|G:N|$, where $N = \mathrm{Stab}_G(P)$; since $P \leq N$, this number divides $|G:P| = m$.

Finally, if Q is any subgroup of p-power order, then the orbits of Q on Δ all have p-power size; since $|\Delta|$ is congruent to 1 mod p, there must be an orbit $\{P\}$ of size 1, and so $Q \leq P$ by our earlier remark.

All parts of the theorem are now proved.

Here is a two-part lemma which we made use of in the above proof. The proof is an exercise. If H is a subgroup of G, we say that the element $g \in G$ *normalises* H if $g^{-1}Hg = H$; and we say that the subgroup K *normalises* H if all its elements normalise H. Thus H is a normal subgroup of G if and only if G normalises H. By HK we mean the *subset* $\{hk : h \in H, k \in K\}$ of G (not in general a subgroup).

Lemma 4.3 *Let H and K be finite subgroups of G. Then*

(a) $|HK| = |H| \cdot |K| / |H \cap K|$;

(b) if K normalises H, then HK is a subgroup of G.

4.3 Applications

There are many applications of Sylow's Theorem to the structure of groups. Here is one, the determination of all groups whose order is the product of two distinct primes.

Theorem 4.4 *Let G be a group of order pq, where p and q are primes with $p > q$.*

(a) If q does not divide $p-1$, then G is cyclic.

(b) If q divides $p-1$, then there is one type of non-cyclic group, with presentation

$$G = \langle a, b \mid a^p = 1, b^q = 1, b^{-1}ab = a^k \rangle$$

for some k satisfying $k^q \equiv 1$ mod p, $k \not\equiv 1$ mod p.

Proof Let P be a Sylow p-subgroup and Q a Sylow q-subgroup. Then P and Q are cyclic groups of prime orders p and q respectively. The number of Sylow p-subgroups is congruent to 1 mod p and divides q; since $q < p$, there is just one, so $P \lhd G$.

Similarly, the number of Sylow q-subgroups is 1 or p, the latter being possible only if $p \equiv 1 \bmod q$.

Suppose there is a unique Sylow q-subgroup. Let P and Q be generated by elements a and b respectively. Then $b^{-1}ab = a^k$ and $a^{-1}ba = b^\ell$ for some k, ℓ. So $a^{k-1} = a^{-1}b^{-1}ab = b^{-\ell+1}$. This element must be the identity, since otherwise its order would be both p and q, which is impossible. So $ab = ba$. Then we see that the order of ab is pq, so that G is the cyclic group generated by ab.

In the other case, q divides $p-1$, and we have $b^{-1}ab = a^k$ for some k. Then an easy induction shows that $b^{-s}ab^s = a^{k^s}$. Since $b^q = 1$ we see that $k^q \equiv 1 \bmod p$. There are exactly q solutions to this equation; if k is one of them, the others are powers of k, and replacing b by a power of itself will have the effect of raising k to the appropriate power. So all these different solutions are realised within the same group.

In particular, the only non-cyclic group of order $2p$, where p is an odd prime, is the dihedral group $\langle a, b \mid a^p = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$.

There are two groups of order 21, the cyclic group and the group

$$\langle a, b \mid a^7 = 1, b^3 = 1, b^{-1}ab = a^2 \rangle;$$

in this group, if we replace b by b^2, we replace the exponent 2 by 4 in the last relation.

5 Composition series

A non-trivial group G always has at least two normal subgroups: the whole group G, and the identity subgroup $\{1\}$. We call G *simple* if it has no other normal subgroups. Note that the trivial group is not considered to be simple. A cyclic group of prime order is simple, and we will see that there are other simple groups.

In this section we will discuss the Jordan–Hölder Theorem. This theorem shows that, in a certain sense, simple groups are the "building blocks" of arbitrary finite groups. In order to describe any finite group, we have to give a list of its "composition factors" (which are simple groups), and describe how these blocks are glued together to form the group.

5.1 The Jordan–Hölder Theorem

Suppose that G is a finite, non-trivial, and non-simple group: then it has a normal subgroup N which is neither $\{1\}$ nor G, so the two groups N and G/N are smaller than G. If either or both of these is not simple, we can repeat the procedure. We will end up with a list of simple groups. These are called the *composition factors* of G.

More precisely, a *composition series* for a group G is a sequence of subgroups

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G,$$

so that each subgroup is normal in the next (as shown), and the quotient group G_{i+1}/G_i is simple for $i = 0, 1, \ldots, r-1$.

We can produce a composition series for a (non-trivial) finite group G by starting from the series $\{1\} \lhd G$ and refining it as follows. If we have $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is not simple, let it have a normal subgroup N, with $\{G_i\} \neq N \neq G_{i+1}/G_i$. Then there is a subgroup N^* of G_{i+1} containing G_i by the Correspondence Theorem, with $G_i \lhd N^* \lhd G_{i+1}$, and we may insert another term in the sequence.

(The *Correspondence Theorem*, sometimes called the *Second Isomorphism Theorem*, asserts that, if A is a normal subgroup of a group B, then there is a bijection between subgroups of B/A and subgroups of B containing A, under which normal subgroups correspond to normal subgroups. The bijection works in the obvious way: if $C \leq B/A$, then elements of C are cosets of A, and the union of all these cosets gives the corresponding subgroup C^* of B containing A.)

Now, given a composition series for G, say

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G,$$

we have r simple groups G_{i+1}/G_i. We are interested in them up to isomorphism; the *composition factors* of G are the isomorphism types. (We think of them as forming a list, since the same composition factor can occur more than once.)

For a simple example, let $G = C_{12}$. Here are three composition series:

$$\{1\} \lhd C_2 \lhd C_4 \lhd C_{12}$$
$$\{1\} \lhd C_2 \lhd C_6 \lhd C_{12}$$
$$\{1\} \lhd C_3 \lhd C_6 \lhd C_{12}$$

The composition factors are C_2 (twice) and C_3, but the order differs between series.

Theorem 5.1 (Jordan–Hölder Theorem) *Any two composition series for a finite group G give rise to the same list of composition factors.*

Note that the product of the orders of the composition factors of G is equal to the order of G.

We will prove this theorem in an Appendix to this chapter.

5.2 Groups of prime power order

In this section, we will see that a group has order a power of the prime p if and only if all of its composition factors are the cyclic group of order p.

One way round this is clear, since the order of G is the product of the orders of its composition factors. The other depends on the following definition and theorem. The *centre* of a group G, denoted by $Z(G)$, is the set of elements of G which commute with everything in G:

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

It is clearly a normal subgroup of G.

Theorem 5.2 *Let G be a group of order p^n, where p is prime and $n > 0$. Then*

(a) $Z(G) \neq \{1\}$;

(b) G has a normal subgroup of order p.

To prove this, we let G act on itself by conjugation. By the Orbit-Stabiliser Theorem, each orbit has size a power of p, and the orbit sizes sum to p^n. Now by definition, $Z(G)$ consists of all the elements which lie in orbits of size 1. So the number of elements not in $Z(G)$ is divisible by p, whence the number in $Z(G)$ is also. But there is at least one element in $Z(G)$, namely the identity; so there are at least p such elements.

Now, if g is an element of order p in $Z(G)$, then $\langle g \rangle$ is a normal subgroup of G of order p.

This proves the theorem, and also finds the start of a composition series: we take G_1 to be the subgroup given by part (b) of the theorem. Now we apply induction to

G/G_1 to produce the entire composition series $\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$. We see that all the composition factors have order p, and that G_i is a subgroup of G of order p^i.

We note in passing the following result:

Proposition 5.3 *Let p be prime.*

(a) Every group of order p^2 is abelian.

(b) There are just two such groups, up to isomorphism

For let $|G| = p^2$. If $|Z(G)| = p^2$, then certainly G is abelian, so suppose that $|Z(G)| = p$. Then $G/Z(G)$ is a cyclic group of order p, generated say by the coset $Z(G)a$; then every element of G has the form za^i, where $z \in Z(G)$ and $i = 0, 1, \ldots, p-1$. By inspection, these elements commute.

Finally, the Fundamental Theorem of Abelian Groups shows that there are just two abelian groups of order p^2, namely C_{p^2} and $C_p \times C_p$.

This theorem shows that the list of composition factors of a group does not determine the group completely, since each of these two groups has two composition factors C_p. So the "glueing" process is important too. In fact, worse is to come. The number of groups of order p^n grows very rapidly as a function of n. For example, it is known that the number of groups of order $1024 = 2^{10}$ is more than fifty billion; all of these groups have the same composition factors (namely C_2 ten times)!

Remark At this point, we have determined the structure of all groups whose order has at most two prime factors (equal or different); so we know all the groups of order less than 16 except for the orders 8 and 12.

5.3 Soluble groups

A finite group G is called *soluble* if all its composition factors are cyclic of prime order.

Historically, soluble groups arose in the work of Galois, who was considering the problem of solubility of polynomial equations by radicals (that is, the existence of formulae for the roots like the formula $(-b \pm \sqrt{b^2 - 4ac})/2a$ for the roots of a quadratic. It had already been proved by Ruffini and Abel that no such formula exists in general for polynomials of degree 5. Galois associated with each polynomial a group, now called the *Galois group* of the polynomial, and showed that the polynomial is soluble by radicals if and only if its Galois group is a soluble group. The result on degree 5 comes about because the smallest simple group which is not cyclic of prime

order (and, hence, the smallest insoluble group) is the alternating group A_5, as we shall see.

I will not discuss soluble groups in detail here, but note just one theorem.

Theorem 5.4 *A finite group G is soluble if and only if it has a series of subgroups*

$$\{1\} < H_1 < H_2 < \cdots < H_s = G$$

such that each H_i is a normal subgroup of G, and each quotient H_{i+1}/H_i is abelian for $i = 0, 1, \ldots, s-1$.

(Note that in the definition of a composition series, each subgroup is only required to be normal in the next, not in the whole group.)

This theorem is important because the definition we gave of a soluble group makes no sense in the infinite case. So instead, we use the condition of the theorem as the *definition* of solubility in the case of infinite groups.

5.4 Simple groups

In the course, we will spend some time discussing simple groups other than cyclic groups of prime order. Here, for a starter, is the argument showing that they exist.

Theorem 5.5 *The alternating group A_5 is simple.*

The group $G = A_5$ consists of the even permutations of $\{1, \ldots, 5\}$. (Recall that even permutations are those for which the number of cycles is congruent to the degree mod 2.) Their cycle types and numbers are given in the following table.

Cycle type	Number
$[1,1,1,1,1]$	1
$[1,2,2]$	15
$[1,1,3]$	20
$[5]$	24

Since a normal subgroup must be made up of entire conjugacy classes, our next task is to determine these.

It is easy to see that all the elements of order 2 are conjugate, as are all those of order 3. The elements of order 5 are not all conjugate, but the subgroups of order 5 are (by Sylow's Theorem), and a potential normal subgroup must therefore either contain all or none of them.

So if N is a normal subgroup of A_5, then $|N|$ is the sum of some of the numbers 1, 15, 20, 24, certainly including 1 (since it must contain the identity), and must divide 60 (by Lagrange's Theorem).

It is straightforward to see that the only possibilities are $|N| = 1$ and $|N| = 60$. So A_5 is simple.

Exercise Show that there is no simple group of non-prime order less than 60.

In perhaps the greatest mathematical achievement of all time, all the finite simple groups have been determined. We will say more about this in the course. But, by way of introduction, they fall into four types:

(a) cyclic groups of prime order;

(b) alternating groups A_n (these are simple for all $n \geq 5$);

(c) the so-called *groups of Lie type*, which are closely related to certain matrix groups over finite fields — for example, if $G = \mathrm{SL}(n,q)$, then $G/Z(G)$ is simple for all $n \geq 2$ and all prime powers q except for $n = 2$ and $q = 2$ or $q = 3$;

(d) twenty-six so-called *sporadic groups*, most of which are defined as symmetry groups of various algebraic or combinatorial configurations.

The proof of this simply-stated theorem is estimated to run to about 10000 pages!

This theorem means that, if we regard the Jordan–Hölder theorem as reducing the description of finite groups to finding their composition factors and glueing them together, then the first part of the problem is solved, and only the second part remains open.

5.5 Appendix: Proof of the Jordan–Hölder Theorem

Recall that we are proving that any two composition series for a finite group G have the same length and give rise to the same list of composition factors.

The proof is by induction on the order of G. If $G = \{1\}$ then its only composition series is $G = G_0 = \{1\}$, and the list of commposition factors is empty. We now assume $|G| > 1$ and that the theorem is true for groups smaller than G. Let

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{1\}$$

and

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_s = \{1\}$$

be two composition series for G.

Case 1: $G_1 = H_1$. Then the parts of the series below this term are composition series for G_1 and so have the same length and composition factors. Adding in the composition factor G/G_1 gives the result for G.

Case 2: $G_1 \neq H_1$. Let $K_2 = G_1 \cap H_1$, a normal subgroup of G, and take a composition series

$$K_2 \rhd K_3 \rhd \cdots \rhd K_t = \{1\}$$

for K_2.

We claim that $G_1/K_2 \cong G/H_1$ and $H_1/K_2 \cong G/G_1$. If we can prove this, then the two composition series

$$G_1 \rhd G_2 \rhd \cdots \rhd \{1\}$$

and

$$G_1 \rhd K_2 \rhd K_3 \rhd \cdots \rhd \{1\}$$

for G_1 have the same length and composition factors; the composition factors of G using the first series are these together with G/G_1. A similar remark holds for H_1. So each of the given composition series for G has the composition factors in the series for K_2 together with G/G_1 and G/H_1, and the theorem is proved. So it only remains to establish the claim.

Now G_1H_1 is a normal subgroup of G properly containing G_1; so $G_1H_1 = G$. Thus, by the Third Isomorphism Theorem,

$$G/G_1 = G_1H_1/G_1 \cong H_1/(G_1 \cap H_1) = H_1/K_2,$$

and similarly $G/H_1 \cong G_1/K_2$. Thus the claim is proved.