Groups - Extra Stuff

Abigail Tan

December 2020

I have left some proofs here in the form of exercises to be worked through.

Contents

1 Semidirect Products

(Notes taken roughly from brilliant.org, with a few additional own comments).

Recall that the direct product expresses a group as a product of subgroups (e.g. $G \times H$). We can generalise the idea of expressing a group in terms of its subgroups using the semidirect product.

1.1 Inner Semidirect Product

Let G be a group with $H \leq G$ and $N \trianglelefteq G$. If certain conditions are satisfied, then we can write G as the *inner semidirect product* of N and H, written $G = N \rtimes H$.

Theorem 1 (Inner Semidirect Product)**.** Let G be a group with $H \leq G$ and $N \trianglelefteq G$. Then the following statements are equivalent:

1. $NH = G$ and $N \cap H = \{e\}$.
2. Every $g \in G$ can be uniquely written in the form $g = nh$ for $n \in N$, $h \in H$.
3. Define $\psi : H \to G/N$ by $\psi(h) = hN$. Then ψ is an isomorphism.

(If these all hold, then we write $G = N \rtimes H$).

Proof. Left as an exercise. Show equivalence by showing that 1 $\implies$ 2, 2 $\implies$ 3 and 3 $\implies$ 1. □

Examples.

1. $G = S_3$: without loss of generality, choose $N = \langle(123)\rangle$ and $H = \langle(12)\rangle$. Then $G = N \rtimes H$.
2. $G = S_n, N = A_n, H \cong C_2$ gives $S_n = A_n \rtimes H$.
3. Let $D_{2n} = \langle r, s \,|\, r^n = e, s^2 = e, rs = sr^{-1}\rangle$. Then $D_{2n} = \langle r\rangle \rtimes \langle s\rangle$.

Proposition 1. If $|N||H| = |G|$ then $NH = G \iff N \cap H = \{e\}$.

Proof. Left as an exercise. Use the Second Isomorphism Theorem, which states that

$$H \leq G, N \trianglelefteq G \implies H \cap N \trianglelefteq H \text{ and } H/(H \cap N) \cong HN/N.$$

□

So if this condition holds then we only have to check one of the two conditions in statement 1 of Theorem 1. We can also check that if $|N||H| = |G|$ and $\text{hcf}(|N|, |H|) = 1$ then $N \cap H = \{e\}$, by Lagrange's theorem.

1.2 Outer Semidirect Product

We can take the opposite approach and consider two abstract groups, together with a relationship given by some homomorphism. Then we can construct a new group using certain properties.

Definition 1 (Automorphism)**.** An automorphism of a group G is an isomorphism $\phi : G \to G$, i.e. an isomorphism from the group to itself. The group consisting of automorphisms of G is denoted $\text{Aut}(G)$.

Definition 2 (Outer Semidirect Product)**.** Let N and H be groups. Let $\phi : H \to \text{Aut}(N)$ be a homomorphism sending elements $h \in H$ to automorphisms ϕ_h of N. Then the *outer semidirect product* $G = N \rtimes_\phi H$ is the set of ordered pairs (n, h) with $n \in N, h \in H$ related by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2). \tag{1.2.1}$$

Exercise. Verify that G in Definition 2 is a group.

Notice also that the outer semidirect product is a generalisation of the direct product. If $\phi : H \to \text{Aut}(N)$ is chosen to be the trivial automorphism, sending every element to itself, then $n_1\phi_{h_1}(n_2) = n_1n_2$ and equation 1.2.1 defines the *direct product* $N \times H$.

An outer semidirect product can be written as an inner semidirect product. Given groups N, H and a homomorphism $\phi : H \to \text{Aut}(N)$, the group $G = N \rtimes_\phi H$ has a normal subgroup $\tilde{N} = \{(n, e) : n \in N\}$ and a subgroup $\tilde{H} = \{(e, h) : h \in H\}$ such that $G = \tilde{N} \rtimes \tilde{H}$. (We can check that $\tilde{N}$ is a normal subgroup of G).

In addition, an inner semidirect product can also be written as an outer semidirect product. Let G be a group with subgroups N, H satisfying $G = N \rtimes H$. Then we can define a homomorphism $\phi : H \to \text{Aut}(N)$ such that $G \cong N \rtimes_\phi H$. Here we define it.
For $h \in H$, define $\phi_h(n) = hnh^{-1}$ (notice this is in N as it's normal - also note ϕ_h is bijective). Then we have

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = (n_1\phi_{h_1}(n_2))(h_1h_2)$$

which resembles the group law for the outer semidirect product. Note that this shows that the bijection $G \to N \rtimes_\phi H$ defined by $nh \mapsto (n, h)$ is also a homomorphism.

Example. Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\}$$

with multiplication as the operation. Let H be the subgroup of G consisting of diagonal matrices $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ and let N be the subgroup of G consisting of matrices of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then $N \trianglelefteq G$, $NH = G$ and $N \cap H = \{e\}$, so we have $G = N \rtimes H$ (inner semidirect product).

Now notice also that $N \cong \mathbb{R}$ and $H \cong \mathbb{R}^*$, so we can find some homomorphism ϕ such that $G \cong \mathbb{R} \rtimes_\phi \mathbb{R}^*$. We choose ϕ such that it sends a nonzero real number h to the automorphism of $(\mathbb{R}, +)$ given by multiplication by h.

Note that G can be written as a group of affine transformations $x \mapsto ax + b$. (Affine transformations behave like linear transformations, but do not necessarily have to fix the origin). Then matrix multiplication in G corresponds to their composition.

Problem. Let $N = C_2 \times C_2$ and $H = C_2$. Consider the automorphism $\phi : H \to \mathrm{Aut}(N)$ which sends the nontrivial element of H to the homomorphism $(a, b) \mapsto (b, a)$. What standard group is $N \rtimes_\phi H$ isomorphic to?

2 Abelian Groups

2.1 The 5/8 Theorem

This is an interesting result about abelian groups.

Theorem 2 (5/8 Theorem)**.** Let G be a group. If the probability that two (not necessarily distinct) elements randomly selected from G commute is greater than $5/8$, then G is abelian.

Proof. A more illustrative way is to reframe the problem as the following question: "Given that a group is non-abelian, what is the maximum probability that two randomly chosen elements commute?". If we can show that this is $5/8$, then we will be done.

We start by considering a non-abelian group and trying to make it "as commutative as possible" without being abelian. Let G be a non-abelian group and consider the centre Z of G. We know $Z \trianglelefteq G$, so by Lagrange, $|G|/|Z|$ is an integer m. We can try to maximise $|Z|/|G|$, which takes the form $1/m$.

If $m = 1$, then $|Z| = |G|$, making G abelian (contradiction). If $m = 2$ then $G/Z = \{Z, aZ\} \cong C_2$ for some $a \notin Z$ which commutes with everything in Z. So G is generated by Z and a (which commutes with everything in Z) and hence G is abelian (contradiction). Similarly, m cannot be 3 (in this case $G/Z \cong C_3$ and the same argument applies).

Now, what if $m = 4$? If $G/Z \cong C_4$ then we have the same problem as before, but it may also be possible that $G/Z \cong C_2 \times C_2$. In this case, G is generated by Z and *two* elements not in Z, and these two elements do not necessarily commute. We can hence say that $m \geq 4$ so $|Z|/|G| \leq 1/4$.

We can also consider the maximum possible size of the centraliser C_G of $g \in G$ (non-abelian), where g is not in the centre. This a proper subgroup of G so $|G|/|C_G(g)|$ is an integer at least 2. We hence have $|C_G(g)|/|G| \leq 1/2$.

Now, given a random element g chosen from G, we can choose a (not necessarily distinct) second element h from G. If $g \in Z(G)$, then they must commute. If not, then they only commute if $h \in C_G(g)$. Hence

$$\mathrm{P}(gh = hg) = \frac{|Z(G)|}{|G|} + \left(1 - \frac{|Z(G)|}{|G|}\right) \frac{|C_G(g)|}{|G|}$$

which is maximised when $|Z(G)|/|G|$ and $|C_G(g)|/|G|$ are both maximised. Hence

$$\mathrm{P}(gh = hg) \leq \frac{1}{4} + \frac{3}{4} \times \frac{1}{2} = \frac{5}{8}.$$

Therefore if the probability that they commute is greater than $5/8$, then the group is necessarily abelian. □

Remark. The bound 5/8 is actually a tight bound: the non-abelian quaternion group Q_8 has centre of size 2 (1/4 of the size of the group) and each non-central element commutes with exactly half of the elements.

Remark. We showed that $|Z|/|G|$ is at most 1/4 for a non-abelian group. If we had instead used the bounds 1/2 or 1/3, then instead of 5/8 we would have got the bounds 3/4 and 2/3, which also work, but a better one 5/8 can be found (which turns out to be the best possible bound).

2.2 Commutator Subgroups

2.2.1 Definitions

The commutator indicates to what extent a certain binary operation fails to be commutative.

Definition 3 (Commutator)**.** Let G be a group and let $g, h \in G$. The commutator $[g, h]$ of g and h is defined by

$$[g, h] = ghg^{-1}h^{-1}.$$

Notice that $[g, h] = e$ if and only if g and h commute. Here are some other important properties (which can be verified elementarily).

1. Inversion: $[g, h] = [h, g]^{-1}$
2. Conjugation: $x[g, h]x^{-1} = [xgx^{-1}, xhx^{-1}]$
3. For a homomorphism $f : G \to H$, have $f([g, h]) = [f(g), f(h)]$

In general, the set of all commutators in a group G does not form a subgroup (it is not closed under the group operation). However, we can generate a subgroup using commutators. This commutator subgroup is important because it is the smallest normal subgroup N such that G/N is abelian. The larger the commutator subgroup, the "less abelian" the group can be said to be.

Definition 4 (Commutator subgroup)**.** The commutator (or derived) subgroup, written $[G, G]$, $G^{(1)}$ or G', of a group G is the subgroup generated by all its commutators.

By closure, every element of $[G, G]$ takes the form $[g_1, h_1][g_2, h_2]...[g_n, h_n]$ with $g_i, h_i \in G$. By the conjugation property, for all $x \in G$ we have

$$x[g_1, h_1][g_2, h_2]...[g_n, h_n]x^{-1} = [xg_1x^{-1}, xh_1x^{-1}][xg_2x^{-1}, xh_2x^{-1}]...[xg_nx^{-1}, xh_nx^{-1}]$$

and hence $[G, G]$ is a normal subgroup of G.

2.2.2 Derived Series

The standard commutator subgroup of G is denoted $G^{(1)}$. The same construction can be iterated to form a series of subgroups. We define

$$G^{(0)} := G$$
$$\text{and } G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$$

(i.e. $G^{(n)}$, the nth derived subgroup, is the subgroup generated by the commutators of $G^{(n-1)}$).

This way we can obtain a "descending series" of sorts, made up of normal subgroups of G.

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

If G is finite, then this series will terminate in a perfect group, which may or may not be trivial. If G is infinite, then it may not terminate at a finite stage.

Definition 5 (Perfect group)**.** A perfect group is a group G such that $G = G^{(1)}$, i.e. it is equal to its own commutator subgroup.

Notice that all non-abelian simple groups are perfect groups. (Why?)

2.2.3 Examples

Definition 6 (Abelianisation)**.** Given a group G, its abelianisation is defined as the quotient $G^{\text{ab}} = G/[G,G]$.

Here are some examples/properties.

- A group G is *abelian* if and only if $[G,G]$ is trivial (or equivalently $G = G^{\text{ab}}$).
- A group G is *perfect* if and only if $G = [G,G]$ (or equivalently $G^{\text{ab}} = \{e\}$). This can be thought of as being the "opposite" to an abelian group.
- A group G is *solvable* if there exists $n \in \mathbb{N}$ with $G^{(n)} = \{e\}$ (and otherwise *non-solvable*). The special case $n = 1$ occurs when G is abelian (so solvable is a weaker property).

2.3 Classification of Finite Abelian Groups

2.3.1 Kronecker's Theorem

Definition 7 (Direct sum)**.** Let G be a group and let H_1 and H_2 be subgroups of G. We say G is the direct sum of H_1 and H_2 (written $G = H_1 \oplus H_2$) if all of the following hold:

- $H_1 \trianglelefteq G$ and $H_2 \trianglelefteq G$
- $H_1 \cap H_2 = \{e\}$
- $G = \langle H_1, H_2 \rangle$ (i.e. G is generated by H_1 and H_2).

It follows that $C_{mn} \cong C_m \oplus C_n$ if and only if m and n are coprime.

Exercise. Let G be a finite abelian group. Let n be the maximal order of an element of G. Show that $\text{ord}(g)$ divides n for all $g \in G$.
[Hint: first show that if $\text{hcf}(a,b) = 1$ then $\text{ord}(a)\,\text{ord}(b) = \text{ord}(ab)$, then consider powers of a prime factor and derive a contradiction.]

There are several formulations of a theorem called "Kronecker's theorem" which are related. Here I have given one version that I could find a proof for.

Theorem 3 (Kronecker's Theorem)**.** Let G be a finite abelian group. Then

$$G = A_1 \times A_2 \times \cdots \times A_s$$

where $A_1, A_2, \ldots$ are cyclic groups of orders $n_1, n_2, \ldots$ and each n_{i+1} divides n_i.

Proof. Let n_1 denote the maximal order among all the elements of G. Using the result in the above exercise, we have $a^{n_1} = e$ for all $a \in G$.
If $a_1 \in G$ has order n_1, then we call elements a' and a'' *equivalent relative* to a_1 if

$$a' a_1^k = a''$$

for some k. We can check that this is an equivalence relation, and the equivalence classes form a finite abelian group $G/\langle a_1 \rangle$. In particular, there is an equivalence class with maximal order n_2, so for any representative a^* of the class, we have that $(a^*)^{n_2}$ is the least of its powers equivalent to e. Since $(a^*)^{n_1} = e$ (so is equivalent to it), we must have $n_2 | n_1$.
Now if $(a^*)^{n_2} = a_1^k$ and we raise both sides to n_1/n_2, then we get

$$e = (a^*)^{n_1} = a_1^{kn_1/n_2}$$

so when k/n_2 is set equal to m, we have $a_1^{nm_1} = e$ from which it follows that m is an integer.

The equation

$$a_2 a_1^m = a^*$$

then defines an element a_2 equivalent to a^* whose nth power is not only equivalent to e, but also equal to it. We now call elements a', a'' *equivalent relative* to a_1, a_2 if

$$a' a_1^j a_2^k = a''$$

for some h, k and similarly obtain a group of equivalence classes whose maximal order n_3 divides n_2, and a representative a_3 of the class of maximal order such that $a_3^{n_3} = e$.
This procedure terminates when we have a set of elements $a_1, a_2, \ldots, a_s$ such that any a is equivalent to e relative to $a_1, a_2, \ldots, a_s$; that is, when any a is expressible as

$$a = a_1^{h_1} a_2^{h_2} \ldots a_s^{h_s}.$$

It also follows that this expression is unique, since the equivalence classes relative to $a_1, \ldots, a_{s-1}$ must constitute a cyclic group with a_s as a representative generator. An element a is therefore uniquely determined by the integers $h_1, \ldots, h_{s-1}$, which determine it relative to an equivalence class representative, and the integer h_s which determines the equivalence class representative itself, $a_s^{h_s}$.
Hence G is the direct product $A_1 \times A_2 \times \cdots \times A_s$ where A_i is the cyclic group generated by a_i and the order n_i of A_i is such that n_{i+1} divides n_i. □

Another related theorem is Kronecker's decomposition theorem, which allows us to classify finite abelian groups as direct sums of cyclic groups.

Theorem 4 (Kronecker's decomposition theorem)**.** An abelian group of order n can be written in the form

$$\mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_m}$$

where the k_i are powers of primes and the k_i multiply to n. This representation is unique up to permutations of the summands.

For instance, an abelian group of order 15 can be written only as $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ (which is the same as $C_3 \times C_5 \cong C_{15}$) so all abelian groups of order 15 are isomorphic. It is worth noting these two special cases:

- An abelian group of order p (p prime) must be isomorphic to C_p
- An abelian group of order p^2 (p prime) is isomorphic to either C_{p^2} or $C_p \times C_p$.

It follows from Kronecker's decomposition theorem that the number of non-isomorphic abelian groups of order $n = \prod_i p_i^{e_i}$ is

$$a(n) = \prod_i P(e_i)$$

where $P(n)$ is the function giving the number of partitions of n. Hence $a(n)$ is the product of the number of partitions of each exponent in the prime factorisation of n.

Exercise. It follows from the above result that if an abelian group has order n with $n = p_1 p_2 \ldots p_k$ for distinct primes p_i, then the group is cyclic. Verify this. Can you find another method by which to prove this result, which does not rely on Kronecker's decomposition theorem?

2.3.2 Using Sylow Subgroups

The Sylow theorems can be used to find out about the structure of abelian groups. Every subgroup of an abelian group is normal, so $n_p = 1$ for all primes p dividing $|G|$. So there is a unique Sylow p-subgroup for every such prime p.

Proposition 2. Let H and K be subgroups of an abelian group G, and suppose $H \cap K = \{e\}$. Then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G, which is isomorphic to $H \times K$.

Proof. We can quite quickly check that HK is a subgroup. Since G is abelian, we can see that it is closed under the operation:

$$(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2) \in HK.$$

There is a natural homomorphism $H \times K \to (h, k) \mapsto hk$. It is certainly surjective, and we can also check that it is injective. If $(h, k) \mapsto e$, then $hk = e \implies h = k^{-1} \in K$. But $H \cap K = \{e\}$ so $h = k = e$ and hence the kernel is trivial, as required. We therefore have an isomorphism. □

Note that if H and K are finite with coprime orders, then their intersection is trivial by Lagrange's theorem (order of intersection divides both orders), so this proposition applies to them.

Consider repeatedly applying the proposition to the Sylow p-subgroups of an abelian group G. Suppose $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Let H_i be the unique Sylow p_i-subgroup. Then the proposition shows that $H_1H_2 \cong H_1 \times H_2$. We can continue in this way (technically, inductively) to give

$$G \cong H_1 \times H_2 \times \cdots \times H_k.$$

Hence we have that a finite abelian group G is isomorphic to the direct product of its Sylow subgroups.

2.4 Fundamental Theorem of Finite Abelian Groups

Theorem 5 (Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group is an internal direct product of cyclic groups whose orders are prime powers. This product is unique up to reordering.

Proof. Let G be a finite abelian group. Every finite abelian group can be expressed uniquely as the product of prime-power order groups (as seen in subsection 2.3.2). We also know that an abelian group of prime-power order is a direct product of cyclic groups, so we apply this to each factor. Hence G must be a product of prime-power order cyclic groups. We then only have to show that the secondary factorisation is unique.
Suppose that $|G| = p^k$ with p prime. Suppose that G can be factorised in two ways:

$$G = H_1 \times H_2 \times \cdots \times H_m = K_1 \times K_2 \times \cdots \times K_n$$

where H_i and K_i are all nontrivial cyclic subgroups with

$$|H_1| \geq |H_2| \geq \cdots \geq |H_m|$$

and

$$|K_1| \geq |K_2| \geq \cdots \geq |K_n|.$$

We proceed by (strong) induction on k. For $k = 1$, the factorisation is unique, as groups of prime order are cyclic.
Now assume it is true for all abelian groups of order p^l, where $l < k$. Since G is abelian, we have that $G^p = \{x^p : x \in G\}$ is a proper subgroup of G (can check). Hence

$$G^p = H_1^p \times \cdots \times H_{m'}^p = K_1^p \times \cdots \times K_{n'}^p$$

where m' is the largest integer i with $|H_i| > p$ and n' is the largest integer j with $|K_j| > p$. This ensures that the above direct products do not have trivial factors. By Cauchy's theorem, we have $|G^p| < G$ (as there must exist an element of order p). Then we can apply the induction hypothesis. It follows that

$$m' = n'$$

and $|H_i^p| = |K_i^p|$ for $i = 1, 2, \ldots, m'$.
We know that $|H_i| = p|H_i^p|$ and $|K_i| = p|K_i^p|$. It then follows that

$$|H_1||H_2|\ldots|H_{m'}|p^{m-m'} = |G| = |K_1||K_2|\ldots|K_{n'}|p^{n-n'}$$

and therefore $m - m' = n - n'$. Since $m' = n'$, we have $m = n$ and the factorisation is unique.

□

3 Sylow Theorems

The Sylow theorems are important for analysis of particular subgroups of finite groups, called Sylow subgroups.

Definition 8 (p-group)**.** A p-group is a group whose order is a power of p, where p is prime. If it is a subgroup of another group, then it is called a p-subgroup.

Definition 9 (Sylow p-subgroup)**.** Let G be a group and p be a prime dividing the order of G. A Sylow p-subgroup is a subgroup with order a power of p and with index coprime to p. (Note: this means that the order of the Sylow p-subgroup is the *maximal* power of p dividing $|G|$, not just any power).

The first Sylow theorem guarantees the existence of a Sylow subgroup of a group G for any prime dividing its order. The second Sylow theorem states that all Sylow subgroups with a given order are conjugate. The third Sylow theorem gives information about the number of Sylow subgroups.

3.1 Theorems and Proofs

Let G be a finite group and let p be a prime dividing $|G|$. We write $|G| = kp^n$ with $n \geq 1$ and $p \nmid k$.

Theorem 6 (First Sylow Theorem)**.** There exists a Sylow p-subgroup of G. That is, there is a subgroup $H \leq G$ of order p^n.

Proof. Let T be the set of all subsets of G containing exactly p^n elements; that is $T = \{S \subseteq G : |S| = p^n\}$.
Let $N = |T|$.
Now N is the number of ways p^n can be chosen from a set of $p^n k$ elements. We hence have

$$N = \binom{p^n k}{p^n}.$$

We use the following result (see footnote[1] for proof):

$$\binom{p^n k}{p^n} \equiv k \pmod{p}$$

and hence

$$N \equiv k \pmod{p}.$$

We now let G act on T by the rule

$$\forall S \in T : g(S) = gS$$

(i.e. the left coset action, except S is not necessarily a subgroup - can check it's an action).
Let T have r orbits under this action. The orbits, represented by $\{S_1, S_2, \ldots, S_r\}$, partition T, so we have

$$T = \mathrm{Orb}(S_1) \cup \mathrm{Orb}(S_2) \cup \cdots \cup \mathrm{Orb}(S_r)$$

[1]Start by proving $(a+b)^p \equiv a^p + b^p \pmod{p}$ and then $(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} \pmod{p}$ by induction. Then compare the coefficients of b^{p^n} in the expansion of $(a+b)^{p^n k} \pmod{p}$ in two different ways.

and

$$|T| = |\operatorname{Orb}(S_1)| + |\operatorname{Orb}(S_2)| + \cdots + |\operatorname{Orb}(S_r)|.$$

If every orbit has size divisible by p, then $p|N$. But this cannot be true since $N \equiv k \pmod{p}$ with $p \nmid k$. So at least one orbit has size not divisible by p.
Without loss of generality, suppose that $\operatorname{Orb}(S_1)$ has size not divisible by p. Let $s \in S_1$. We claim that $\operatorname{Stab}(S_1)s = S_1$.

To show this, observe that by Orbit-Stabiliser, since p^n divides G but p does not divide $|\operatorname{Orb}(S_1)|$, we must have that p^n divides $|\operatorname{Stab}(S_1)|$ so $|\operatorname{Stab}(S_1)| \geq p^n$.
Notice also that $\operatorname{Stab}(S_1) = \{g \in G : gS_1 = S_1\}$ and hence for all $s \in S_1, g \in \operatorname{Stab}(S_1)$ we have $gs \in S_1$ and therefore $\operatorname{Stab}(S_1)s \subseteq S_1$. Hence $|\operatorname{Stab}(S_1)| = |\operatorname{Stab}(S_1)s| \leq |S_1| = p^n$.

Therefore $|\operatorname{Stab}(S_1)| = p^n$. But $\operatorname{Stab}(S_1) \leq G$ so $\operatorname{Stab}(S_1)$ is a subgroup of G containing p^n elements, so is a Sylow p-subgroup as required. □

Definition 10 (Normaliser)**.** Let G be a group and let S be a subset of G. Then the normaliser of S in G is the set $N_G(S)$ defined by

$$N_G(S) = \{g \in G : gSg^{-1} = S\}.$$

We can check that $N_G(S)$ is a subgroup of G. It also holds that if $H \leq G$ then $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup (not proved at this time).

Lemma 1 (Normaliser of Sylow p-subgroup)**.** Let P be a Sylow p-subgroup of a finite group G. Let $N_G(P)$ be the normaliser of P. Then any p-subgroup of $N_G(P)$ is contained in P, and in particular, P is the unique Sylow p-subgroup of $N_G(P)$.

Proof. Will do later. □

Lemma 2. Let P be a Sylow p-subgroup of the finite group G and let Q be any p-subgroup of G. Then Q is a subset of a conjugate of P.

Proof. Define $T = \{gPg^{-1} : g \in G\}$, which is the set of all distinct G-conjugates of P.

We claim that $|T| \equiv 1 \pmod{p}$.

To show this, consider the action $h(S) = hSh^{-1}$ with $h \in P$ and $S \in T$. (We can check that this is an action). We have $S \in T \implies \exists\, g \in G : S = gPg^{-1} \implies h(S) = h(gPg^{-1})h^{-1} = (hg)P(hg)^{-1} \implies h(S) \in T$, so the action is also closed for $S \in T$. We now consider the orbits and stabilisers of T under this action.
Notice that $hPh^{-1} = p$ so $\operatorname{Orb}(P) = \{P\}$. We will show that P is the only element of T with a singleton orbit.
If gPg^{-1} has one element in its orbit, then $xgPg^{-1}x^{-1} = gPg^{-1}$ for all $x \in P$. Hence $g^{-1}(xgPg^{-1}x^{-1})g = g^{-1}(gPg^{-1})g = P$ so $g^{-1}xg \in N_G(P)$. We have $|g^{-1}xg| = |x|$ (conjugate, so same order) and hence $P_1 = g^{-1}Pg$ is a p-subgroup of $N_G(P)$ (all orders powers of p). Since $|P| = |P_1|$, we have that P_1 is a Sylow p-subgroup of $N_G(P)$. By Lemma 1, $P_1 = P$ so $gPg^{-1} = P$. Hence only P has an orbit of size 1.

Therefore for any $g \notin P$, we have $|\operatorname{Orb}(gPg^{-1})| > 1$. Since $\operatorname{Stab}(S) \leq P$ for all $S \in T$, we have that $|\operatorname{Stab}(S)|$ divides $|P| = p^n$, so by Orbit-Stabiliser each orbit size is also a power of p. Hence each orbit size is 1 mod p if the size is 1 and 0 mod p otherwise. The orbits partition the set, so $|T| \equiv 1 \pmod{p}$ as required.

We now consider orbits of T under conjugation by elements of Q. Since Q is a p-subgroup, by the same argument as above, every orbit has size a power of p. Since $|T| \equiv 1 \pmod{p}$, there is at least one orbit of size 1. So there is an element g with $x(gPg^{-1})x^{-1} = gPg^{-1}$ for all $x \in Q$. As previously, we have $g^{-1}Qg \subseteq N_G(P)$. So by Lemma 1 we have $g^{-1}Qg \subseteq P$. Thus $Q \subseteq gPg^{-1}$ as required. □

Theorem 7 (Second Sylow Theorem)**.** All the Sylow p-subgroups of a finite group are conjugate.

Proof. Suppose P and Q are Sylow p-subgroups of G. By Lemma 2, Q is a subset of a conjugate of P. But $|P| = |Q|$, so Q must equal a conjugate of P. □

Lemma 3. Let G be a finite group with $|G| = kp^n$ with $p \nmid k$ and $n > 0$. Let $T = \{S \subseteq G : |S| = p^n\}$ and let G act on T by $g(S) = gS$. Then there are exactly as many Sylow p-subgroups as there are orbits whose length is not divisible by p. Each such orbit contains exactly one Sylow p-subgroup.

Proof. Will do later. □

Theorem 8 (Third Sylow Theorem)**.** Let G be a finite group with $|G| = p^n k, n \geq 1, p \nmid k$ (as before). Let r be the number of Sylow p-subgroups. Then

- $r \equiv 1 \pmod{p}$
- $r|k$
- $r = |G|/|N_G(H)|$ where H is any Sylow p-subgroup.

Proof. First, we will show that $r \equiv 1 \pmod{p}$. We start similarly to the proof of the first Sylow theorem. Let $T = \{S \subseteq G : |S| = p^n\}$, the set of all subsets of G with exactly p^n elements. Then

$$|T| = \binom{p^n k}{p^n}.$$

Let G act on T by $g(S) = gS = \{x \in G : x = gs : s \in S\}$.
We write out the partition equation

$$|T| = |\operatorname{Orb}(S_1)| + |\operatorname{Orb}(S_2)| + \cdots + |\operatorname{Orb}(S_r)| + |\operatorname{Orb}(S_{r+1})| + \cdots + |\operatorname{Orb}(S_s)|$$

noting that by Lemma 3 we have that each of $\operatorname{Orb}(S_i)$ for $i = 1, 2, \ldots, r$ contains exactly one Sylow p-subgroup. In addition, k divides the size of every orbit (as $\operatorname{Stab}(S)$ is a p-subgroup for all S so by Orbit-Stabiliser, k must divide $\operatorname{Orb}(S)$ not $\operatorname{Stab}(S)$). For $i = 1, 2, \ldots, r$, we have

$$|G| = |\operatorname{Orb}(S_i) \times |\operatorname{Stab}(S_i)| = p^n |\operatorname{Orb}(S_i)| \implies |\operatorname{Orb}(S_i)| = k.$$

As we have seen, each of the rest of the orbits are divisible by both k and p (again by Lemma 3). Hence for some $m \in \mathbb{Z}$ we have

$$|T| = \binom{p^n k}{p^n} = kr + mpk.$$

But notice that this applies to the special case where $G = C_{p^n k}$. Here, there is exactly one subgroup for each divisor of $p^n k$, and in particular, exactly one subgroup of order p^n. Hence $r = 1$ in this case. So there exists $m' \in \mathbb{Z}$ with

$$\binom{p^n k}{p^n} = k + m' pk$$

so we can equate these expressions:

$$kr + mpk = k + m'pk \implies r + mp = 1 + m'p \implies r - 1 = p(m' - m) \implies r \equiv 1 \pmod{p}.$$

We now prove the next two results.
By Orbit-Stabiliser, the number of conjugates of a Sylow p-subgroup P is equal to the index of $N_G(P)$. It then follows that $r = |G|/|N_G(H)|$ as required. Then by Lagrange's theorem, the number of Sylow p-subgroups r divides $|G|$. We know that $r \equiv 1 \pmod{p}$ so we have $r \nmid p$ and hence $r \nmid p^n$. Therefore $r|k$ as required. □

3.2 Examples

Example. Identify the Sylow subgroups of S_4.
We have $|S_4| = 24 = 2^3 \times 3$, so the Sylow 2-subgroups have order 8. By the third Sylow theorem, the number of Sylow 2-subgroups n_2 divides 3 and is congruent to 1 mod 2. We observe that $D_8 \leq S_4$ (as it permutes the vertices of a square). Three such copies of D_8 can be generated: either from (12)(34) and (1324), or (13)(24) and (1234), or (14)(23) and (1243). As $n_2|3$, these are all the Sylow 2-subgroups.
The Sylow 3-subgroups are generated by 3-cycles such as (123) and there are 8 such 3-cycles, so four subgroups (each contains two). So $n_3 = 4$. This agrees with $n_3|8$ and $n_3 \equiv 1 \pmod 3$. The third Sylow theorem also predicts that $N_{S_4}(H)$ is a subgroup of order $|S_4|/n_3 = 24/4 = 6$. Let $H = \langle(123)\rangle$ be one of the Sylow 3-subgroups. Then $N_G(H)$ is a copy of S_3 inside S_4 (interpreted as all the permutations fixing 4).

Note that any conjugate of a Sylow p-subgroup is also one, so if $n_p = 1$ then it must be normal.

Example. Show that there is no simple group G of order 30.
We have $30 = 2 \times 3 \times 5$, so the Sylow subgroups are isomorphic to C_2, C_3 and C_5 respectively. The group is simple so we have $n_2, n_3, n_5 \neq 1$. Consider $n_3|10$ and $n_3 \equiv 1 \pmod 3$ which implies $n_3 = 10$. They are distinct, so intersect only in the identity. Therefore there are 20 elements of order 3 in G.
Now consider n_5. We have $n_5|6$ and $n_5 \equiv 1 \pmod 5$, so $n_5 = 6$. Any pair intersects only trivially, so there are $4 \times 6 = 24$ elements of order 5 in G. So there are at least $1 + 20 + 24 = 45$ elements in G, a contradiction since $|G| = 30$. Hence no simple group has order 30. □