10 Sylow's Theorems

Humanity is on the cusp of knowing all the symmetries of every possible shape (in this universe, or any other universe!). A fundamental tool for this are Sylow's Theorems. Peter Ludwig Sylow (1832–1918) was a Norwegian mathematician with a great sense of humour who liked the outdoors.

Motivation. Lagrange's Theorem allows us to say what orders of subgroups are impossible. For example, if $|G| = 7^2 \cdot 3$ then G has no subgroup of order 3. We already that the converse to Lagrange's Theorem doesn't hold: A_4 has no subgroup of order 6, even though $|A_4| = 12$.

Sylow's Theorems are a partial converse to Lagrange's Theorem. They tell us for example, that if $|G| = 7^2 \cdot 3$ then G has a subgroup of order 7^2.

10.1 The Sylow Theorems

Definition 10.1.1. If p is a prime, and H is a group of order p^r, for some r, then we say that H is a *p group*. If H is a subgroup of another group G, then we say H is a *p-subgroup of G*.

Example 10.1.2. (i) The group C_9 is a 3 group because it's order is a power of 3. It is a 3-subgroup of S_9.

(ii) The group S_9 is not a p group for any prime p, since its order is not a prime power.

(iii) The Klein 4-group K_4 is a 2-group, because its order is a power of 2. It is a 2-subgroup of S_4.

Definition 10.1.3. Let G be a finite group. For any prime number p that divides $|G|$, we can write

$$|G| = p^r t, \quad \text{with } p \nmid t \text{ (i.e. } p \text{ does not divide } t)$$

A *Sylow p-subgroup of G* is a subgroup $H \leq G$ such that $|H| = p^r$. We will also call these p-Sylow subgroup. [Note: a p-Sylow subgroup of G is the largest p-subgroup of G.]

Example 10.1.4. S_5 has order $|S_5| = 5! = 2^3 \cdot 3 \cdot 5$. Taking $p = 2$ we can write $|S_5| = 2^3 \cdot 15$, and we check that $2 \nmid 15$. Any subgroup of S_5 that has order $2^3 = 8$ is then a Sylow 2-subgroup of S_5.
Note that subgroups of S_5 of order 2 or 4 are 2-subgroups of S_5, but **not** 2-Sylow subgroups of S_5.

Theorem 10.1.5. (First Sylow Theorem) *Let G be a finite group. If prime p divides $|G|$, then G has at least one Sylow p-subgroup H.*

Theorem 10.1.6. (Second Sylow Theorem) *Let G be a finite group with p-Sylow subgroup H. If J is any p-subgroup of G* [Note: J is not necessarily a p-Sylow subgroup] *then $J \leq g^{-1}Hg$ for some $g \in G$.*

Theorem 10.1.7. (Third Sylow Theorem) *Let G be a finite group and let $a(p)$ be the number of p-Sylow subgroups of G. Then:*

(i) $a(p)$ divides t (where $|G| = p^r \cdot t$, with t and p coprime) and

(ii) $a(p) \equiv 1 \mod p$

What is the point?!. Why are these so important? Well the first theorem tells us that every finite group has a p-Sylow subgroup for each prime p dividing $|G|$, the second tells us how they are all related, and the third tells us how many there are. Using them, we can often determine all the groups of a given order. Amazing!

Remark 10.1.8. Sylow's First Theorem is a generalisation of Cauchy's Theorem, which states that if G is a finite group and p is a prime number dividing $|G|$, then G contains a subgroup of order p.

Question 10.1.9. Let G be a group of order 54. Use Sylow's Theorems to prove that G has a subgroup H of order 27 and a subgroup K of order 2.

> This is easy! Since $|G| = 3^3 \cdot 2$, any 3-Sylow subgroup of G has order $3^3 = 27$, and any 2-Sylow subgroup of G has order 2. By Sylow's First Theorem, G has a 3-Sylow subgroup and a 2-Sylow subgroup.

10.1.1 Handout for Section 10.1

Example 10.1.10. What are some Sylow subgroups of D_{10}? Well $|D_{10}| = 10 = 2^1 \cdot 5^1$. Hence D_{10} has 5-Sylow subgroups and 2-Sylow subgroups.
The 5-Sylow subgroups have order $5^1 = 5$. For example, $\langle (12345) \rangle$ is a 5-Sylow subgroup of D_{10}. It is isomorphic to C_5.
You should check yourself, but C_2 is a 2-Sylow subgroup of D_{10}. In fact, up to isomorphism, these are the only Sylow subgroups of D_{10}.

Example 10.1.11. What are some Sylow subgroups of S_6? Well $|S_6| = 6! = 2^4 \cdot 3^2 \cdot 5$. Therefore, the 3-Sylow subgroups of S_6 have order $3^2 = 9$, the 2-Sylow subgroups have order 2^4 and the 5-Sylow subgroups have order 5.

- C_5 is a 5-Sylow subgroup of S_6.
- $\langle (123) \rangle \times \langle (456) \rangle \cong C_3 \times C_3$ is a subgroup of S_6. Also $|C_3 \times C_3| = 3 \cdot 3 = 9$. Hence, $C_3 \times C_3$ is a 3-Sylow subgroup of S_6.
- $\langle (1\ 2) \rangle \cong C_2$ is **not** a 2-Sylow subgroup of S_6, because 2-Sylow subgroups of S_6 must have order 2^4.

10.2 Applying Sylow's Theorems

Example 10.2.1. We will now prove that every group of order 162 has a normal subgroup H of order 81.

Claim 1: There is a subgroup H of G with order 81. Proof: well $|G| = 3^4 \cdot 2$, so any 3-Sylow subgroup of G has order 3^4. By Sylow's First Theorem, there is a 3-Sylow subgroup H of G.

Claim 2: H is the only 3-Sylow subgroup of G. The number $a(3)$ of 3-Sylow subgroups in G satisfies $a(3)\big|2$ and $a(3) \equiv 1 \mod 3$ by Sylow's Third Theorem. Now $a(3)\big|2$ implies $a(3) = 1$ or 2, and $a(3) \equiv 1 \mod 3$ implies $a(3) \in \{1, 4, 7, 10, \ldots\}$. Hence $a(3) = 1$.

Claim 3: $H \trianglelefteq G$. Fix $g \in G$. We will show that $g^{-1}Hg = H$. First, note that $g^{-1}Hg$ is a subgroup of G by the Quick Subgroup Test [Identity: obvious. Closure: $(g^{-1}h_1g)(g^{-1}h_2g) = g^{-1}h_1h_2g \in g^{-1}Hg$. Inverse: $(g^{-1}hg)(g^{-1}h^{-1}g) = e$]. Also $|g^{-1}Hg| = |H|$. Therefore $g^{-1}Hg$ is a 3-Sylow subgroup of G. Since G has only one 3-Sylow subgroup (by Claim 2), we have $g^{-1}Hg = H$.

Example 10.2.2. We will now prove that every group of order 15 is cyclic using Sylow's theorems. Let G be a group with $|G| = 15$. Notice that $|G| = 15 = 3^1 \cdot 5^1$.

Claim 1: A subgroup of G can only have orders 1, 3, 5 and 15. Proof: by Lagrange's Theorem.

Claim 2: G has only one subgroup of order 1. Proof: obvious—it's $\langle e_G \rangle$ by Proposition 2.2.6.

Claim 3: G has only one subgroup of order 15. Proof: obvious—it's G by Proposition 2.2.6.

Claim 4: G has only one subgroup of order 3. Proof: By the First Sylow Theorem, we know that G has at least one 3-Sylow subgroup H, with $|H| = 3^1 = 3$. Notice that every 3-subgroup of G is a 3-Sylow subgroup, because $|G| = 3^1 \cdot 5^1$.

By the Third Sylow Theorem, $a(3) \mid 5$ **and** $a(p) \equiv 1 \mod 3$. First fact means $a(3) = 1, 5$ and second fact means $a(3) = 1$. So, there is only one 3-subgroup of G.

Claim 5: G has only one subgroup of order 5. Proof: As above, every 5-subgroup of G is a 5-Sylow subgroup, and $a(5) = 1$ or 3, with $a(5) \equiv 1 \mod 5$, so $a(5) = 1$.

Claim 6: G is cyclic. Proof: Let J be the unique 3-subgroup of G, and let K be the unique 5-subgroup. The only subgroups of G are thus $\langle e_G \rangle, J, K, G$. Note that (because $e_G \in J \cap K$) there are at most $1 + (3-1) + (5-1) = 7$ elements of G that lie in $\langle e_G \rangle$ or J or K. Choose some $g \in G$ that is not in any of them. Now $\langle g \rangle \leq G$, but it can't equal $\langle e_G \rangle, J$ or K because none of these contain g. Hence $\langle g \rangle = G$.

10.3 Handout: Proof of the First Sylow Theorem (not examinable)

It is important that you fully understand this proof, however you will not be required to repeat the entirety of this proof in an examination.

Let us first recall the theorem.

First Sylow Theorem. Let G be a finite group. If prime p divides $|G|$, then G has at least one Sylow p-subgroup H.

Proof of Sylow's First Theorem. Write $|G| = p^r t$, where p and t are coprime and $r \geq 1$. Idea: We will look at subsets of G that have size p^r, and we will see that the stabiliser of one of them is a subgroup of G and has size p^r. This will be the p-Sylow subgroup of G we are looking for.
Let $X := \{W \subseteq G : |W| = p^r\}$ be the set of all of these subsets. Now $|X|$ equals the number of ways of choosing p^r from $p^r t$, therefore:

$$|X| = \binom{p^r t}{p^r} = \frac{p^r t}{p^r} \cdot \frac{(p^r t - 1)}{(p^r - 1)} \cdots \frac{(p^r t - i)}{(p^r - i)} \cdots \frac{(p^r t - (p^r - 1))}{1}.$$

> **Claim:** $p \nmid |X|$. Proof: if p^h divides some term $(p^r t - i)$, then $p^h \mid i$. Hence p^h divides $(p^r - i)$. But this means that any p^h factor in a numerator is matched by a p^h factor in the denominator, so they cancel. Thus p does not divide $|X|$.

Now X is a G-set, with $\lambda(g)W = gW$ for all $g \in G$ and all $W \in X$. Let $W_1, \ldots, W_a$ be representatives of the orbits of G on X, so $X = GW_1 \cup \ldots \cup GW_a$. Therefore,

$$|X| = |GW_1| + \cdots |GW_a|.$$

Since $p \nmid |X|$, there is some orbit GW_i such that $p \nmid |GW_i|$. Let $S := \mathrm{Stab}_G(W_i)$. We will prove that S is a p-Sylow subgroup of G. Now $S \leq G$ by Proposition 9.1.0, so all we need to prove is that $|S| = p^r$.
By the Orbit-Stabiliser Theorem (Theorem 9.1.1), $|GW_i| = |G|/|S|$. Since $S \leq G$, we know that $|S|$ divides $|G|$ by Lagrange's Theorem. Since $|G| = p^r t$, we have $|S| = p^k s$ for some $k \leq r$ and $s \mid t$. However, p does not divide $|GW_i|$, so we must have

$$|S| = p^r s.$$

> **Claim:** $|S| \leq |W_i|$. Proof: fix any $w \in W_i$ and consider the orbit $Sw = \{gw : g \in S\}$. If $|S| > |Sw|$ then $gw = hw$ for distinct $g, h \in S$. However, since $w \in G$ we have $gww^{-1} = hww^{-1}$, so $g = h$. This is a contradiction. Hence $|S| \leq |Sw|$. Furthermore, $Sw \subseteq W_i$ because S is the stabiliser of W_i, so $|Sw| \leq |W_i|$. Therefore $|S| \leq |W_i|$ as claimed.

Using our claim, we have $p^r s = |S| \leq |W_i| = p^r$, so $s = 1$. Hence $|S| = p^r$. Thus S is a p-Sylow subgroup of G. □

[Advanced handout: You are NOT required to read this, it is here just in case you are interested] Proof of the Second and Third Sylow Theorems (not examinable)

First, a definition that we will need.

Definition 10.3.1. Let G be a group and $h \in G$. The *centraliser of h in G* is defined to be

$$C_G(h) = \{g \in G : g^{-1}hg = h\}.$$

For a subset $S \subseteq G$ a similar object $N_G(S)$ is called the *normaliser of S in G*, and is defined to be

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

(These objects will play a role in some 4th year courses.)
Notice that when a group acts on itself by conjugation, we have that $\lambda(g)x = gxg^{-1}$; hence the stabiliser of x under this action is $\{g \in G : gxg^{-1} = x\} = \{g \in G : x = g^{-1}xg\} = C_G(x)$. The orbits of this action are called the *conjugacy classes* of G.

Second Sylow Theorem. Let G be a finite group with p-Sylow subgroup H. If J is any p-subgroup of G [Note: J is not necessarily a p-Sylow subgroup] then $J \leq g^{-1}Hg$ for some $g \in G$.

Proof of Sylow's Second Theorem. Recall that G/H is the set of cosets of H in G, and G acts on $Y = G/H$ by left multiplication, so $\lambda(g)(g'H) = gg'H$ for all $g \in G$ and all $g'H \in Y$. Since $J \leq G$, this means λ is also an action of J on Y.
Since J acts on Y, this means Y can be partitioned into orbits. Let $\mathrm{Fix_Y(J)}$ be the set of points in Y that are fixed by every element in J. Points in Y lie in orbits of size one. Hence we can write

$$Y = \mathrm{Fix_Y(J)} \cup \mathrm{Orb_1} \cup \ldots \cup \mathrm{Orb_m},$$

where all the sets in the union are pairwise disjoint and all orbits have size at least 2. Now $|J|$ is a power of p, and the Orbit Stabiliser Theorem tells us that the size of each orbit divides $|J|$. Therefore,

$$|Y| = |\mathrm{Fix_Y(J)}| + \mathrm{p^{k_1}} + \ldots + \mathrm{p^{k_m}},$$

for some $k_1, \ldots, k_m \in \mathbb{N}$. Now $|Y| = [G : H]$, and $[G : H]$ is coprime to p because H is a p-Sylow subgroup of G. Hence we must have that $|\mathrm{Fix_Y(J)}| \geq 1$.
Since $|\mathrm{Fix_Y(J)}| \geq 1$, we can choose some $gH \in Y$ such that $\lambda(a)gH = gH$ for all $a \in J$. Hence $agH = gH$, and therefore $a \in gHg^{-1}$. Since this is true for all $a \in J$ we have that $J \subseteq g^{-1}Hg$. Since J and $g^{-1}Hg$ are groups, it then follows that $J \leq g^{-1}Hg$. □

Third Sylow Theorem. Let G be a finite group and let $a(p)$ be the number of p-Sylow subgroups of G. Then:

(i) $a(p)$ divides t (where $|G| = p^r \cdot t$, with t and p coprime) and

(ii) $a(p) \equiv 1 \mod p$

Proof of Sylow's Third Theorem. Let Y be the set of all p-Sylow subgroups of G. Then $|Y| = a(p)$. For all $g \in G$ and $H \in Y$ we have that gHg^{-1} is also a p-Sylow subgroup of G, and hence $gHg^{-1} \in Y$. It is easy to see that we have an action λ of G on Y given by

$$\lambda(g)H = gHg^{-1},$$

for all $g \in G$ and all $H \in Y$.
By Sylow's Second Theorem, we know that G has only one orbit on Y. Therefore $Y = Gy$ for all $y \in Y$. By the Orbit Stabiliser Theorem, $a(p) = |Y| = |Gy| = |G|/|\mathrm{Stab}_G(y)|$, and so in particular,

$$a(p) \text{ divides } |G|. \tag{3}$$

We now show that $a(p) \equiv 1 \mod p$. Fix $J \in Y$. Since $J \leq G$ this means that λ is also an action of J on Y. As we did in the proof of Sylow's Second Theorem, we can write Y as a union of orbits and use the Orbit Stabiliser Theorem to show that

$$|Y| = |\mathrm{Fix}_Y(J)| + p^{k_1} + \ldots + p^{k_m},$$

for some $k_1, \ldots, k_m \in \mathbb{N}$. Hence, since $|Y| = a(p)$,

$$a(p) \equiv |\mathrm{Fix}_Y(J)| \mod p.$$

Claim: $\mathrm{Fix}_Y(J) = \{J\}$**.** Proof: first note that it is obvious that $J \in \mathrm{Fix}_Y(J)$. Suppose $H \in Y$ is some element in $\mathrm{Fix}_Y(J)$. Then for all $a \in J$ we have $aHa^{-1} = H$. Of course we can also write this as $H = a^{-1}Ha$.

Recall (from Definition 10.3.1) that the normaliser of H in G is $N_G(H) = \{g \in G : g^{-1}Hg = H\}$. It is easy to see (using the Quick Subgroup Test) that $N_G(H) \leq G$. Now $H \leq N_G(H)$ and $J \leq N_G(H)$, so H and J are two p-Sylow subgroups of $N_G(H)$. We can apply Sylow's Second Theorem to $N_G(H)$ to deduce that H and J satisfy,

$$J \leq g^{-1}Hg,$$

for some $g \in N_G(H)$. However, by the definition of $N_G(H)$, we know that $g^{-1}Hg = H$. Therefore $J \leq H$. Since $|J| = |H|$ we therefore have that $J = H$. Hence $\mathrm{Fix}_Y(J) = \{J\}$ and our claim is true.

By our claim, we see that $|\mathrm{Fix}_Y(J)| = 1$, and therefore,

$$a(p) \equiv 1 \mod p. \tag{4}$$

By (3) above we have that $a(p)$ divides $|G| = p^r t$, and so $a(p) = p^k s$ for some $k \leq r$ and some s that divides t. On the other hand, by (4) above we have that $a(p)$ is coprime to p. Hence $a(p) = s$ and so $a(p)$ divides t. □