23. Sylow theorems

We prove the Sylow theorems.

To warm up we will first prove that the only simple p-groups have prime power order. We will need:

Theorem 23.1 (Class equation)**.** *Let G be a finite group. Let $C_1, C_2, \ldots, C_k$ be the conjugacy classes with more than one element. Pick representatives $c_1, c_2, \ldots, c_k$ of each conjugacy class, so that $c_i \in C_i$.*

Then

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_{c_i}].$$

Proof. Let G act on itself by conjugation. The orbits are the conjugacy classes and these give a partition of G. In particular the sum of the cardinalities of the conjugacy classes is the cardinality of G.

Let O be an orbit of G, so that $O = C$ is a conjugacy class. Suppose that $c \in O$. The stabiliser H of c is the set of elements $g \in G$ such that

$$\begin{aligned} c &= g \cdot c \\ &= gcg^{-1}. \end{aligned}$$

But then $cg = gc$ so that the stabiliser of c is precisely the centraliser of c,

$$H = C_c = \{\, g \in G \,|\, gc = cg \,\}.$$

The cardinality of O is then precisely the index of H. In particular O has one element c if and only if $G = C_c$ if and only if c commutes with everything if and only if c belongs to the centre Z of G.

Thus if we group together the one element conjugacy classes we get the centre Z. □

Lemma 23.2. *Every subgroup of the centre Z of a group G is normal in G.*

Proof. Suppose that $H \subset Z(G)$ is a subgroup. Pick $g \in G$. Then g commutes with every element of H, so that

$$gHg^{-1} = H.$$ □

Proof of (21.8). We first prove (1). Suppose that $q = |G| = p^d$.

Consider the class equation

$$|G| = |Z| + \sum_{i=1}^{k} [G : C_{c_i}].$$

Every term in the sum has cardinality at least two and divides q. Thus every term in the sum is divisible by p. The LHS is also divisible by

p. It follows that the order of the centre is divisible by p. But then $|Z| > 1$.

We now turn to (2). By the classification of finitely generated abelian groups the centre contains a subgroup H of order p. But then H is normal in G, by (23.2). Let

$$G' = G/H$$

be the quotient group. Then G' is a p-group and its order is less than the order of G. By induction G' contains a nested sequence of normal subgroups of every order dividing the order of G',

$$\{e\} = K_1 \subset K_2 \subset \cdots \subset K_d = G'.$$

Now take the inverse image of these subgroups

$$G_i = \gamma^{-1}(K_i)$$

under the natural homomorphism

$$\gamma\colon G \longrightarrow G',$$

to get

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_k = G. \qquad \square$$

As the Sylow theorem is so fundamental, we give three different proofs of (21.3). Perhaps the most important step is to establish the existence of a single Sylow p-subgroup.

To give the first proof, we start with an easy:

Lemma 23.3. *Let p be a prime, let m be a positive integer coprime to p and let $n = p^k m$.*

Then

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

is coprime to p.

Proof. Expanding top and bottom of the binomial, the only terms on the top divisible by p are of the form $n - ap^i = p^i(p^{k-i}m - a)$, where a is coprime to p, in which case the corresponding term $p^k - ap^i = p^i(p^{k-i} - a)$ on the bottom, exactly cancels the factor of p^i. $\square$

First proof of existence. Let S be the set of all subsets of G of order p^k, and let G act on S by left translation,

$$G \times S \longrightarrow S \qquad \text{given by} \qquad g \cdot A = gA.$$

By (23.3) the order of S is coprime to p. It follows that there must be an orbit T whose cardinality is coprime to p. Pick an element A of T. If $a \in A$ then $e \in a^{-1}A$ belongs to T.

Hence we may assume that $e \in A$. Let H be the stabiliser of A. Then

$$\begin{aligned} h &= he \\ &= h \cdot e \in hA = A. \end{aligned}$$

It follows that $H \subset A$. As the cardinality of the orbit T is equal to the index of H, p^k must divide the order of H. The only possiblity is that $H = A$, in which case H is a Sylow p-subgroup. □

The following might explain the proof above and it is also a useful observation:

Lemma 23.4. *The Sylow p-subgroups are all stabilisers of elements of S.*

Proof. Let P be a Sylow p-subgroup. Then $P \in S$. Let H be the stabiliser of P. Then $P \subset H$ as P is a subgroup and $H \subset P$ as $e \in P$. Thus $P = H$ is a stabiliser. □

First proof of (21.31.1-2). It suffices to prove that given any p-subgroup H and we may find $g \in G$ such that $H \subset gPg^{-1}$. Consider an orbit T of the action of G on the subsets of cardinality p^k, whose cardinality is coprime to p.

Consider the action of H on T by left translation

$$H \times T \longrightarrow T \qquad \text{given by} \qquad h \cdot A = hA.$$

Consider the orbits of this action. Since any such orbit has cardinality a power of p, it follows that there must be an orbit of cardinality one. Let A be the corresponding subset of cardinality p^k. Let Q be the stabiliser of A under the action of G. Clearly $H \subset Q$. But any two stabilisers are conjugate and P is a stabiliser by (23.4), so that $Q = gPg^{-1}$, for some $g \in G$. □

First proof of (21.3.3). Let S be the set of Sylow p-subgroups. Then G acts on S by conjugation

$$G \times S \longrightarrow S \qquad \text{given by} \qquad g \cdot Q = gQg^{-1}.$$

By (21.3.2), this is action is transitive. In particular the cardinality of S divides n.

Pick a Sylow p-subgroup P and let P act on S by conjugation

$$P \times S \longrightarrow S \qquad \text{given by} \qquad g \cdot Q = gQg^{-1}.$$

Suppose that Q is its own orbit. Then

$$\begin{aligned} Q &= g \cdot Q \\ &= gQg^{-1}, \end{aligned}$$

for all $g \in P$. Thus $P \subset N = N_G(Q)$. But Q is normal in N, and any two Sylow p-subgroups of N are conjugate in N. Thus $P = Q$ and there is only one orbit of size one. But the other orbits have cardinality divisible by p. □

We now turn to the second proof:

Second proof of existence. We may assume by induction on the order of G, that for every subgroup K of G, p^k does not divide the order of K. In other words the index of any subgroup is divisible by p.

We consider the class equation for G:

$$|G| = |Z(G)| + \sum_i [G : C_{c_i}].$$

C_{c_i} is a subgroup of G and so every term in the sum is divisible by p. It follows that the order of the centre is divisible by p.

By the classification of finitely generated abelian groups the centre contains a subgroup K of order p. But then K is normal in G, by (23.2). Consider G/K. By induction this contains a Sylow p-subgroup K', and the inverse image under the quotient map is a Sylow p-subgroup. □

The rest of the proof proceeds as in the first proof.

The third proof of existence is quite novel. We include its proof for completeness but it will not be presented in class.

The idea is to embed G into a much larger group M, show that M contains Sylow p-subgroups and from there deduce that G also contains Sylow p-subgroups. The larger group will be S_{p^l}, for some large positive integer l. So we first need to determine the order of a Sylow p-subgroup of S_{p^l}.

Lemma 23.5. *Let $x = n(l)$ denote the index of the largest power of p dividing $(p^l)!$.*

Then

$$n(l) = 1 + p + \cdots + p^{l-1}.$$

Proof. The proof proceeds by induction on l. The case $l = 1$ is easy.

Now the terms of the expansion of $(p^l)!$ divisible by p are precisely p, $2p$, $\ldots$, $p^{l-1}p$. In other words $n(l)$ is the exponent of

$$p(2p)(3p)\ldots(p^{l-1}p) = p^{p^{l-1}}(p^{l-1})!,$$

so that

$$n(l) = p^{l-1} + n(l-1). \qquad \square$$

Lemma 23.6. *Let G be a group, and let $H_1, H_2, \ldots, H_k$ be a sequence of pairwise commuting subgroups. Let M_i be the subgroup generated by $H_1, H_2, \ldots, H_{i-1}$ and let $H = M_{k+1}$.*

If M_i and H_i have trivial intersection then

$$H = H_1 H_2 \ldots H_k \simeq H_1 \times H_2 \times \cdots \times H_k.$$

In particular

$$|H| = \prod_{i=1}^{k} |H_i|.$$

Proof. We proceed by induction on k. Let $K = M_k$. Note that H_k commutes with K, that

$$K = H_1 H_2 \ldots H_{k-1}$$

by induction on k and that by assumption $K \cap H_k = \{e\}$. Therefore we may assume that $k = 2$ in which case this is a homework problem. $\square$

Remark 23.7. *It is not enough for the subgroups $H_1, H_2, \ldots, H_k$ to be pairwise disjoint as Herstein seems to suggest in the book "Topics in Algebra".*

For example, let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then the three subgroups of order 2 are pairwise disjoint and commute but the group they generate is G, which has order 4 and not 8.

Lemma 23.8. *The symmetric group of order p^l contains a Sylow p-subgroup.*

Proof. By induction on l. If $l = 1$, then take P to be any subgroup generated by the p-cycle $(1, 2, \ldots, p)$.

Now suppose that $l > 1$. Let

$$H = \{\, \tau \in S_{p^l} \mid \tau(i) = i, \forall i > p^{l-1} \,\}.$$

Then H is a subgroup which is clearly isomorphic to $S_{p^{l-1}}$. By induction H contains a Sylow p-subgroup P_1.

Let

$$\sigma_i = (i, i + p^{l-1}, i + 2p^{l-1}, i + (p-1)p^{l-1}) \qquad \text{for} \qquad 1 \leq i \leq p^{l-1}$$

and let σ be the product of the σ_i. Then σ is a product of p^{l-1} disjoint p-cycles. Let

$$P_i = \sigma^j P \sigma^{-j} \qquad \text{where} \qquad j = i - 1.$$

Note that $P_i \subset H_i = \sigma^j H \sigma^{-j}$, which is the subgroup of permutations that fix everything outside the interval $[jp^k + 1, (j+1)p^k]$.

Note that the subgroups $P_1, P_2, \ldots, P_p$ commute and if T_i is the group generated by $P_1, P_2, \ldots, P_{i-1}$ then T_i commutes with P_i. Therefore

$$|T| = \prod_{i=1}^{p} |P_i| = |P_i|^p = p^{pn(l-1)},$$

where T is the group generated by $P_1, P_2, \ldots, P_p$. Finally let P be the group generated by σ and T. Note that T is invariant under conjugation by σ, so P is a disjoint union of $\sigma^i T$. In particular the order of T is $p^{p(n(l-1))+1} = p^{n(l)}$. But then P is a Sylow p-subgroup. □

Example 23.9. *Take $p = l = 2$, so that we are looking at S_4.*

We take $P_1 = \langle (1,2) \rangle$ and $\sigma = (1,3)(2,4)$. In this case $P_2 = \langle (3,4) \rangle$. Then $T = \langle (1,2), (3,4) \rangle$ and

$$\begin{aligned} P &= \langle (1,2,3,4), (1,2), (3,4) \rangle \\ &= \{e, (3,4), (1,3)(2,4), (1,3,2,4), (1,2), (1,2)(3,4), (1,4,2,3), (1,4)(2,3)\} \\ &\simeq D_4. \end{aligned}$$

is the group generated by T and σ.

Definition-Lemma 23.10. *Let G be a group and let A and B be two subgroups of G. Define a relation $\sim$ by the rule,*

$$x \sim y \qquad \text{if and only if} \qquad y = axb \qquad \text{for some} \qquad a \in A, b \in B.$$

Then $\sim$ is an equivalence relation and the equivalence classes are of the form AxB, for $x \in G$, known as ***double cosets***

Proof. Exercise for the reader. □

Lemma 23.11. *Let A and B be two subgroups of a group G.*
Then

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Proof. Define a map

$$f \colon A \times B \longrightarrow AB \qquad \text{by sending} \qquad (a,b) \longrightarrow ab.$$

This map is clearly surjective. Suppose that $z \in A \cap B$. Then $f(az, z^{-1}b) = f(a,b)$. Conversely, if $ab = cd$ then

$$z = a^{-1}c = bd^{-1} \in A \cap B.$$

Then $c = az$ and $d = z^{-1}b$. Thus the inverse images of f all have cardinality $A \cap B$. □

Lemma 23.12. *Let G be a group and let A and B be two subgroups of G.*

Then

$$|AxB| = \frac{|A||B|}{|A \cap xBx^{-1}|}.$$

Proof. Let $C = xBx^{-1}$. Note

$$AxBx^{-1} = AC.$$

Define a function

$$f\colon AxB \longrightarrow AC \qquad \text{by the rule} \qquad g \longrightarrow gx^{-1}.$$

Then f is clearly a bijection. Then

$$\begin{aligned} |AxB| &= |AC| \\ &= \frac{|A||C|}{|A \cap C|} \\ &= \frac{|A||B|}{|A \cap xBx^{-1}|}. \end{aligned}$$

□

Lemma 23.13. *Let $G \subset M$ be a subgroup of the finite group M.*

If M has a Sylow p-subgroup Q then G has a Sylow p-subgroup P, of the form $G \cap xQx^{-1}$, for some $x \in M$.

Proof. Suppose that $|G| = p^a m$ and $|M| = p^b m'$, where m and m' are coprime to p. Consider the decomposition of M into the double cosets of Q and G. Now

$$|GxQ| = \frac{p^{a+b}m}{|P_x|},$$

where $P_x = G \cap xQx^{-1}$. Since $P_x \subset xQx^{-1}$, it follows that P_x is a p-group. Suppose that $|P_x| = p^{m_x} < p^a$, for every x. Then every orbit is divisible by p^{b+1}. This is not possible, as the order of M is not divisible by p^{b+1}.

Thus $P = P_x$ is a Sylow p-subgroup for some x. □

Third proof of (1) of (2.13). Let G be a finite group. By Cayley's Theorem, we may embed G inside S_n. Since S_n embeds in S_{p^l} for l large enough, it follows that we may embed G into S_{p^l}, for l sufficiently large. Now apply (23.13) and (23.8). □

Third proof of (2) of (21.3). Let P and Q be two Sylow p-subgroups of order p. Consider the decomposition of G into the double cosets of P and Q. Then the order of an orbit is

$$|PxQ| = \frac{p^{2k}}{|P \cap xQx^{-1}|} = p^{m_x},$$

for some integer m_x. But for some $x \in G$, we must have $m_x < k+1$, so that $|P \cap xQx^{-1}| \geq p^k$. The only way that this can happen is if $P = xQx^{-1}$. □

Third proof of (3) of (21.3). As in the first proof, it suffices to prove that the number of Sylow p-subgroups is congruent to one modulo p. Consider the action of G on its Sylow p-subgroups. By (2) this action is transitive. Let P be a Sylow p-subgroup. Then the number of Sylow p-subgroups is equal to the index of the stabiliser of P. Thus it suffices to prove that the index of the normaliser $N = N_G(P)$ is congruent to one modulo p.

Consider the double cosets PxP. We have

$$|PxP| = \frac{p^{2k}}{|P \cap xPx^{-1}|}.$$

Thus $|PxP| \geq p^k$ with equality if and only if $P = xPx^{-1}$, so that $x \in N$. Thus

$$|G| = \sum_{x \in N} |PxP| + \sum_{x \notin N} |PxP|,$$

where the sum ranges over a representative of each double coset and second sum is divisible by p^{k+1}. Now if $x \in N$, then

$$PxP = xP$$

Thus the sum ranges over the set of left cosets of P in N, and it follows that the first sum is precisely $|N|$. Dividing both sides by $|N|$, we get

$$[G : N] = 1 + x,$$

where x is an integer, which is divisible by p. □