II.L. The Sylow theorems

Recall that a group of prime power order is called a *p-group*.

II.L.1. DEFINITION. Let G be a finite group with $|G| = p^k m$, p prime and $p \nmid m$. A **Sylow *p*-subgroup** of G is a subgroup of order p^k, the maximum possible power of p.

We already know that these *exist* when $k = 1$, by Cauchy's theorem (which in fact guarantees an element of order p in G if $k \geq 1$). To attack the general case, we briefly recall what we will need on group actions: if $\{x_i\}$ are representatives of the G-orbits in X with more than one element, and X^G denotes the fixed points (i.e. the union of 1-element orbits), then

$$\begin{aligned} |X| &= |X^G| + \sum_i |G(x_i)| \\ &= |X^G| + \sum_i [G{:}G_{x_i}] \end{aligned}$$

by the orbit-stabilizer theorem. Further, if $X = G$ and G acts on itself by conjugation, this becomes the *class equation*

$$|G| = |C(G)| + \sum_i [G{:}C_G(x_i)] \tag{II.L.2}$$

in which $\{x_i\}$ are representatives of ccl's with > 1 element.[26] The main points here are that

- $[G{:}C_G(x_i)] \big| |G|$, *and*
- $[G{:}C_G(x_i)] \neq 1$ (otherwise $x_i \in C(G)$).

We are now ready for

II.L.3. FIRST SYLOW THEOREM. *Every finite group has a Sylow p-subgroup for each prime p dividing its order:*

$$|G| = p^k m \implies \exists H \leq G \text{ with } |H| = p^k.$$

PROOF. Assume the theorem holds for all groups of order less than $|G|$. (The base case is just the one-element group $\{1\}$.) Here is the inductive step.

[26] So if G is abelian, there are no x_i's (and one is in case (2) in the next proof).

Clearly one of the following must be true: *either*

(1) $p^k \big| |C_G(x_i)|$ for some i; *or*
(2) p^k does not divide $|C_G(x_i)|$ for any i.

In case (1), $|C_G(x_i)| = p^k n$ is less than $|G|$. By the inductive hypothesis, there exists $H \leq C_G(x_i)$ with $|H| = p^k$. Since $C_G(x_i) \leq G$, $H \leq G$.

In case (2), since $|C_G(x_i)| \cdot [G{:}C_G(x_i)] = |G| = p^k m$, p divides $[G{:}C_G(x_i)]$ for every i. Hence, in the class equation (II.L.2), p divides everything but $|C(G)|$, and thus must *also* divide $|C(G)|$. By Cauchy's theorem, there is a subgroup $K \leq C(G)$ of order p. Since conjugation affects no element in $C(G)$, $K \trianglelefteq G$. We can thus speak of the quotient group G/K with order $p^{k-1}m$, which by the inductive hypothesis contains a subgroup H_0 of order p^{k-1}. Let

$$\varphi \colon G \twoheadrightarrow G/K$$

be the quotient map. Since this map is p-to-1,[27] the preimage $\varphi^{-1}(H_0) \leq G$ — which is a subgroup by II.I.25(iii) — has order p^k as desired. □

Recall that the normalizer of a subgroup $H \leq G$ is the largest subgroup of G in which H is normal:

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

If $K \leq N_G(H)$, then $KH = HK \implies KH$ is a group. We'll need a lemma for the proofs of the remaining Sylow theorems.

II.L.4. LEMMA. *Let $P_1, P_2 \leq G$ be Sylow p-subgroups, and suppose $P_1 \leq N_G(P_2)$. Then $P_1 = P_2$.*

PROOF. Write $|G| = p^k m$, so $|P_1| = |P_2| = p^k$ and (since the intersection of subgroups is a subgroup of each) $|P_1 \cap P_2| = p^s$ (for some $s \leq k$). Moreover,

$$P_1 \leq N_G(P_2) \implies P_1 P_2 \leq G \implies |P_1 P_2| \big| |G|$$

[27] The quotient (natural map) $\nu \colon G \twoheadrightarrow G/H$ by a normal subgroup $H \trianglelefteq G$ of order r is always an r-to-1 map: each coset of H has r elements, and you are collapsing each coset to a single element.

and since $P_2 \leq P_1P_2$,

$$p^k = |P_2| \big| |P_1P_2| \implies |P_1P_2| = p^k n$$

where $n \mid m$. Now use the product formula $|P_1P_2||P_1 \cap P_2| = |P_1||P_2|$ (from HW 4 #2), which gives $p^k n \cdot p^s = p^k \cdot p^k$. Since n was a factor of m which was relatively prime to p, this yields a contradiction unless $n = 1$. Conclude that $|P_1P_2| = p^k$. But now P_1 and P_2 are subgroups of P_1P_2 and all three have the same order; hence all three are equal. □

Let X **denote the set of all Sylow** p**-subgroups of** G, which is non- empty by Sylow I. Write $\mathrm{X} = \{P_1, P_2, \ldots, P_N\}$, so that $N = |\mathrm{X}|$.

II.L.5. SECOND SYLOW THEOREM. $N \underset{(p)}{\equiv} 1$.

PROOF. **We let** P_1 **act by conjugation on** X**.** This makes sense because the conjugate gP_ig^{-1} of a group of order p^k still has order p^k (because conjugation is an isomorphism). This group action decomposes X into orbits; taking a system of representatives $\{P_j\}$ of the orbits of order > 1, we have

$$N = |\mathrm{X}| = |\underbrace{\mathrm{X}^{P_1}}_{\substack{\text{fixed} \\ \text{pts.}}}| + \sum_j |\underbrace{P_1(P_j)}_{\substack{> 1 \text{ elt.} \\ \text{orbits}}}|. \tag{II.L.6}$$

By the orbit-stabilizer theorem, $1 < |P_1(P_j)| \big| |P_1| = p^k$. So p divides all the terms in the RHS of (II.L.6) except possibly $|\mathrm{X}^{P_1}|$.

Now consider the fixed points: to have $P_i \in \mathrm{X}^{P_1}$ means that $gP_ig^{-1} = P_i$ $(\forall g \in P_1)$; and so by the definition of the normalizer, $P_1 \leq N_G(P_i)$. Lemma II.L.4 then tells us that $P_1 = P_i$: that is, $i = 1$ and $P_1 \in \mathrm{X}$ is the *only* fixed point. So (II.L.6) reads $N = 1 + \{\text{multiple of } p\}$ and we are done. □

II.L.7. THIRD SYLOW THEOREM. *All Sylow p-subgroups are conjugate. (That is, if* $P_1, P_2 \leq G$ *are two such, then there exists* $g \in G$ *such that* $gP_1g^{-1} = P_2$.)

PROOF. **Let Γ denote the set of left cosets of P_2, and consider the action of P_1 on Γ by left-multiplication.** Suppose that the set of fixed "points" Γ^{P_1} is nonempty, and let gP_2 be one of them: that is, $hgP_2 = gP_2$ $(\forall h \in P_1)$. Then

$$g^{-1}hgP_2 = P_2 \implies g^{-1}hg \in P_2 \implies hg \in gP_2$$
$$\implies h \in gP_2g^{-1} \ (\forall h \in P_1) \implies P_1 \leq gP_2g^{-1}$$

$\implies P_1 = gP_2g^{-1}$, since P_1 and P_2 have the same order. So we just need to show $|\Gamma^{P_1}| \neq 0$.

As before, we have (by counting orbits)

$$|\Gamma| = |\Gamma^{P_1}| + \sum_j \{{}^{\text{size of}}_{j^{\text{th}}\text{ orbit}}\}$$

with the sum terms divisble by p (by the orbit-stabilizer theorem and the fact that a p-group is acting). So on the one hand, we have $|\Gamma^{P_1}| \underset{(p)}{\equiv} |\Gamma|$. On the other, by Lagrange we have

$$|\Gamma| = \#\text{ of cosets of } P_2 = [G{:}P_2] = \frac{|G|}{|P_2|} = \frac{p^k m}{p^k} = m \underset{(p)}{\not\equiv} 0.$$

Hence, $|\Gamma^{P_1}| \neq 0$. □

Here are two more important results on p-groups and p-subgroups (really, a refinement of Sylow I).

II.L.8. PROPOSITION. *Suppose $|G| = p^e$. Then for any $k \leq e$, there exists a normal subgroup $H \trianglelefteq G$ of order p^k.*

PROOF. (Assume true for p^{e-1}; this is the inductive step.) We know $C(G) \neq \{1\}$ by II.H.8; so $p \big| |C(G)|$ and by Cauchy, there exists a $\xi \in C(G)$ of order p. Since any subgroup of its center is normal in G, $\langle \xi \rangle \trianglelefteq G$; we may therefore consider $G/\langle \xi \rangle$ a group of order p^{e-1}. Applying the inductive hypothesis yields $K \trianglelefteq G/\langle \xi \rangle$ of order p^{k-1}. We claim that its preimage under $\eta \colon G \twoheadrightarrow G/\langle \xi \rangle$, namely $H := \eta^{-1}(K)$, is the desired subgroup of G: indeed, $H \trianglelefteq G$ by II.I.25(iv); and $|H| = p \cdot p^{e-1}$ since η is p-to-1. □

II.L.9. COROLLARY. *Suppose $|G| = p^e m$, where $p \nmid m$. Then for any $1 \leq k \leq e$, there exists a subgroup $H \leq G$ of order $|H| = p^k$.*

PROOF. By Sylow I, G has a Sylow p-subgroup $P \leq G$ (of order p^e). Applying II.L.8 to P yields $H \leq P$ of the correct order. □

How might one use Sylow III, with its characterization of set of Sylow p-subgroups of G as one big orbit under conjugation? The orbit-stabilizer theorem says that the size of any orbit must divide the order of G; so we get immediately that

(II.L.10) *the number N of Sylow p-subgroups divides the order $|G|$ of the group.*

Together with Sylow II this frequently gives enough information to determine N.

II.L.11. EXAMPLE. $\mathfrak{S}_5$ has six 5-Sylow subgroups.

PROOF. $N \big| |\mathfrak{S}_5| = 5!$ and $N \underset{(5)}{\equiv} 1 \implies N = 6$ or 1. But there's more than one, as $\langle(12345)\rangle$ and $\langle(12354)\rangle$ are distinct. □

In fact, we can use this to show that $\mathfrak{S}_6$ has an outer automorphism, thereby finishing off Theorem II.J.5:

PROOF. The action of $\mathfrak{S}_5$ (by conjugation) on its six 5-subgroups is transitive by Sylow III, hence gives a map

$$\varphi\colon \mathfrak{S}_5 \to \mathfrak{S}_6$$

with $|\varphi(\mathfrak{S}_5)| \geq 6 \implies |\ker(\varphi)| = \frac{|\mathfrak{S}_5|}{\varphi(\mathfrak{S}_5)} \leq 20$. But by HW 3, $\mathfrak{A}_5$ (of order 60) is the only nontrivial normal subgroup of $\mathfrak{S}_5$; hence $\ker(\varphi)$, being normal in $\mathfrak{S}_5$, must be trivial, and φ injective.

Now we claim that φ preserves parity (i.e. σ odd $\implies \varphi(\sigma)$ odd). Suppose first of all that $\varphi(\mathfrak{S}_5)$ was contained in $\mathfrak{A}_6$; then it has index 3 and the action of $\mathfrak{A}_6$ (by left translation) on its cosets maps $\mathfrak{A}_6 \to \mathfrak{S}_3$ nontrivially hence (since $\mathfrak{A}_6$ is simple and kernels are normal) injectively. But this contradicts $|\mathfrak{A}_6| > |\mathfrak{S}_3|$, and so $\varphi(\mathfrak{S}_5) \not\subset \mathfrak{A}_6$, making the composition $\mathfrak{S}_5 \xrightarrow{\varphi} \mathfrak{S}_6 \xrightarrow{\text{sgn}} \mathbb{Z}_2$ surjective. Again, $\mathfrak{A}_5$ is

the only nontrivial proper normal subgroup of $\mathfrak{S}_5$, so it must be the kernel of the composition. Thus the composition is $\operatorname{sgn}\colon \mathfrak{S}_5 \to \mathbb{Z}_2$, proving the claim.

Consider the homomorphism from $\mathfrak{S}_6$ to itself obtained by letting $\mathfrak{S}_6$ act on the six cosets of $\varphi(\mathfrak{S}_5)$ ($\cong \mathfrak{S}_5$) by left translation. This map

$$\alpha\colon \mathfrak{S}_6 \to \mathfrak{S}_6$$

has image of order ≥ 6, hence (by arguing as above) is injective, and thus an isomorphism. That is, $\alpha \in \operatorname{Aut}(\mathfrak{S}_6)$.

Recall that to prove α is *not inner*, we only have to show that it sends a transposition to a non-transposition.[28] Suppose $\alpha((12)) = (ab)$. Then $\alpha((12))$ is swapping two cosets of $\varphi(\mathfrak{S}_5)$ and fixing the other four. Let $x\varphi(\mathfrak{S}_5)$ be one of the fixed cosets, so that $(12)x\varphi(\mathfrak{S}_5) = x\varphi(\mathfrak{S}_5) \implies x^{-1}(12)x \in \varphi(\mathfrak{S}_5)$. Define $\sigma \in \mathfrak{S}_5$ by $\varphi(\sigma) = x^{-1}(12)x$. Since $x^{-1}(12)x$ is odd, and φ preserves parity, σ is *odd*; it is also of order 2 in $\mathfrak{S}_5$, and hence *must be a transposition*.

Since $\varphi(\sigma)$ is a transposition, σ's action on the 5-Sylow subgroups of $\mathfrak{S}_5$ swaps two and normalizes four. Let $P = \langle(12345)\rangle$ be one of the latter (relabeling if needed). We may assume $\sigma(1) = 1$, and so

$$\begin{aligned}\sigma(12345)\sigma^{-1} &= (1\,\sigma(2)\,\sigma(3)\,\sigma(4)\,\sigma(5)) \\ &\in P = \{(12345),\,(13524),\,(14253),\,(15432),\,1_{\mathfrak{S}_5}\},\end{aligned}$$

which is visibly *impossible* if σ is a transposition. (No element of P results from swapping two numbers in (12345).)

So $\alpha((12))$ *cannot* be a transposition and we are done. □

[28] In fact, this "non-transposition" had to be a product of three disjoint transpositions: in the notation of the proof of II.J.5(ii), a non-inner α (assuming it exists) must exchange C_1 and C_3. Notice that its square will then fix C_1 and is thus inner. In fact, its composition with any β exchanging C_1 and C_3 also fixes C_1, which shows that $\operatorname{Out}(\mathfrak{S}_6) \cong \mathbb{Z}_2$.