Cauchy and Sylow

Notation: In this handout G denotes a finite group of order n and p is a prime.

The Sylow theorems give us partial converses of Lagrange's theorem. In particular, they give us information about subgroups of prime power orders. There are many variant statements of the Sylow theorems and quite a variety of proofs. Our route to proving (our versions of) the Sylow theorems starts with establishing a special case of the first Sylow theorem called Cauchy's theorem.

Theorem: (Cauchy's Theorem) Suppose p divides the order of G. Then G has an element of order p.

Proof: This rather ingenious proof is due to James McKay.

Consider the following set: $X = \{(g_1, g_2, \ldots, g_p) \mid g_1, \ldots, g_p \in G \text{ and } g_1 g_2 \cdots g_p = 1\}$. Notice that we can freely choose $g_1, \ldots, g_{p-1} \in G$ and then must have $g_p = (g_1 \cdots g_{p-1})^{-1}$ to get $(g_1, \ldots, g_p) \in X$. Therefore, $|X| = |G|^{p-1}$.

In general, we can permute p-tuples of elements of G using permutations in S_p. Observe that $g_1 g_2 \cdots g_p = 1$ implies $g_1^{-1}(g_1 \cdots g_p)g_1 = g_1^{-1}1g_1$ so $g_2 \cdots g_p g_1 = 1$. This means we can cyclicly permute the p-tuples in X. Thus the group $C = \langle (123\cdots p) \rangle$ acts on X. For example: $(123\cdots p) \bullet (g_1, g_2, \ldots, g_{p-1}, g_p) = (g_2, g_3, \ldots, g_p, g_1)$.

Now $|C| = p$ and thus by the orbit-stabilizer theorem, orbits of this action must have cardinality 1 or p. Notice that $(1, 1, \ldots, 1) \in X$ since $1 \cdots 1 = 1$ and $\{(1, 1, \cdots, 1)\}$ is this element's orbit. Suppose this was the only singleton orbit. Then we would have $|X| = 1 + p + p + \cdots + p \equiv 1 \pmod{p}$. However, $|X| = |G|^{p-1} \equiv 0 \pmod{p}$ since $|G|$ is divisible by p. Therefore, X must have at least one more singleton orbit, say $\{(g_1, \ldots, g_p)\}$ where $(g_1, \ldots, g_p) \neq (1, \ldots, 1)$. Now if this p-tuple is by itself in an orbit, we must have that $(123\cdots p) \bullet (g_1, \ldots, g_{p-1}, g_p) = (g_2, \ldots, g_p, g_1)$ equals $(g_1, \ldots, g_{p-1}, g_p)$. Therefore, $g_1 = g_2 = \cdots = g_p$. In other words, $g_1 \neq 1$ and $(g_1)^p = g_1 \cdots g_p = 1$. Thus g_1 is an element of order p. ■

What makes this proof rather ingenious is that McKay builds the set X from the group G and then acts on it with a totally different group (i.e., C). His published proof is significantly shorter (less detailed) than mine above.

Definition: We say H is a **p-group** if the order of every element of H is a power of p. In particular, by Cauchy's theorem, H is a finite p-group if and only if $|H| = p^k$ for some $k \geq 0$.

We need the following theorem and technical lemma to aid with our proofs of the Sylow theorems. First, suppose G acts on a set X. For any subgroup H, let $X_H = \{x \in X \mid h \bullet x = x \text{ for all } h \in H\}$ (i.e., X_H are the elements of X that are fixed by elements of H).

Theorem: Let H be a finite p-group and suppose H acts on a finite set X. Then $|X| \equiv |X_H| \pmod{p}$.

Proof: We restrict from the action of G on X to the action of H on X. Then X_H is the union of the singleton orbits in X (since $x \in X_H$ implies $h \bullet x = x$ for all $h \in H$). Notice that since $|H| = p^k$ for some $k \geq 0$, we must have that the size of each orbit is a power of p. Therefore, since orbits partition X, $|X|$ is the sum of 1's (from singleton orbits) and multiples of p. Thus $|X|$ mod p is equivalent to the number of singleton orbits (i.e., $|X| \equiv |X_H| \pmod{p}$). ■

Let S be a subset of G and recall $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$ is the **normalizer** of S in G. When G is finite, we just need $gSg^{-1} \subseteq S$ to get $g \in N_G(S)$ (since considering sizes guarantees equality). When the ambient group is understood, we just write $N(S)$.

Normalizers are an important tool in studying groups. For example, if H and K are subgroups of G, then $H \triangleleft K$ if and only if $K \subseteq N_G(H)$. In other words, $N_G(H)$ is the largest subgroup of G in which H is a normal subgroup. In particular, $H \triangleleft G$ if and only if $N_G(H) = G$.

We can let G act on its powerset $\mathcal{P}(G)$ (i.e., the set of all subsets of G) via conjugation: $g \bullet S = gSg^{-1} = \{gsg^{-1} \mid s \in S\}$. Notice that $N_G(S)$ is exactly the stabilizer of S under this conjugation action. We can also let G act on its powerset via left multiplication. This action lets us establish the following lemma:

Lemma: Let H be p-subgroup of G (i.e., a subgroup and a p-group), then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof: Let H act on G/H via left multiplication: $h \bullet gH = (hg)H$ where $h \in H$ and $gH \in G/H$. Then

$$\left(G/H\right)_H = \{gH \mid hgH = gH \text{ for all } h \in H\} = \left\{gH \mid g^{-1}hg \in H \text{ for all } h \in H\right\} = \left\{gH \mid g^{-1}Hg \subseteq H\right\}$$
$$= \left\{gH \mid g^{-1} \in N_G(H)\right\} = \{gH \mid g \in N_G(H)\} = N_G(H)/H$$

where we used the fact that $g^{-1} \in N_G(H)$ if and only if $g \in N_G(H)$ (since normalizers are subgroups). Therefore, using the above theorem we have $[G : H] = |G/H| \equiv |(G/H)_H| \pmod{p}$ and our above calculation implies $|(G/H)_H| = |N_G(H)/H| = [N_G(H) : H]$. ■

Notation: Let $|G| = n = p^k m$ where $k \geq 0$ and p does not divide m.

Definition: Let H be a subgroup of G. We say H is a **Sylow p-subgroup** if $|H| = p^k$ (i.e., the order of H is the largest prime power dividing $|G|$).

The above definition is fine for finite groups. However, the general definition states that Sylow p-subgroups of G are the maximal p-subgroups of G. In other words, H is a Sylow p-subgroup of G if given any p-subgroup of G, say K, such that $H \subseteq K$, we have $H = K$. This means H is not contained in any bigger p-subgroup. It turns out that once the Sylow theorems are established, when considering finite groups, our above definition matches this more general definition.

The first Sylow theorem addresses a very reasonable question: Do Sylow p-subgroups even exist? The answer is Yes!

Theorem: (Sylow I) Let G be a group of order $p^k m$ where p is prime and does not divide m.

1. For each $0 \leq \ell \leq k$, there exists a subgroup H of G of order p^ℓ.
2. Suppose H is a subgroup of G of order p^ℓ where $0 \leq \ell < k$. Then there exists a subgroup K of G of order $p^{\ell+1}$ such that $H \triangleleft K$.

In other words, p-subgroups for every prime power divisor of our group's order exist and every p-subgroup is contained in a Sylow p-subgroup.

Proof: We proceed via induction. The trivial subgroup $\{1\}$ has order $p^0 = 1$ (this is our base case). Suppose we have a subgroup H of order p^ℓ where $0 \leq \ell < k$. Then $[G : H] = p^{k-\ell} m$ is divisible by p. Using our lemma above, we have $[N_G(H) : H] \equiv [G : H] = 0 \pmod{p}$. Therefore, the order of $N_G(H)/H$ is divisible by p. Since $H \triangleleft N_G(H)$ (subgroups are normal in their normalizers), we have a quotient group whose order is divisible by a prime p. Therefore, by Cauchy's theorem there exists some $xH \in N_G(H)/H$ of order p. By the lattice isomorphism theorem, the cyclic subgroup $\langle xH \rangle$ must be of the form $\langle xH \rangle = K/H$ for some subgroup K of $N_G(H)$. Thus $[K : H] = |\langle xH \rangle| = p$. Therefore, $|K| = [K : H] \cdot |H| = p \cdot p^\ell = p^{\ell+1}$. Thus K is a subgroup of G of order $p^{\ell+1}$. Moreover, $K \subseteq N_G(H)$ so $H \triangleleft K$. The theorem now follows by induction on ℓ. ■

We note that when p does not divide the order of the group (i.e., $|G| = p^0 m$), our Sylow p-subgroup is just the trivial subgroup $\{1\}$. So Sylow p-subgroups exist for all primes, but they are only interesting when p is a divisor of the group's order.

Now that we know Sylow p-subgroups exist we establish some more notation.

Notation: Let $\mathcal{S}\text{yl}_p$ be the set of and $n_p = |\mathcal{S}\text{yl}_p|$ the number of Sylow p-subgroups of G.

The first Sylow theorem tells us that $n_p > 0$. The second Sylow theorem tells us that for a fixed prime p all the Sylow p-subgroups have the same structure.

Theorem: (Sylow II) Let $P, Q \in \mathcal{S}\text{yl}_p$. Then there exists $x \in G$ such that $Q = xPx^{-1}$.

In other words, any two Sylow p-subgroups are conjugate.

Proof: Let $P, Q \in \mathcal{S}\text{yl}_p$. We let Q act on G/P (the left cosets of P in G) by left multiplication: $g \bullet xP = (gx)P$. Since Q is a p-group, the preliminary theorem says $\left|\left(G/P\right)_Q\right| \equiv \left|G/P\right| = [G : P] = m \pmod{p}$. Recall that p does not divide m, so the cardinality of $\left(G/P\right)_Q$ must be non-zero. Let $xP \in \left(G/P\right)_Q$. This means that $qxP = xP$ for all $q \in Q$. Thus $x^{-1}qx \in P$ for all $q \in Q$. In other words, $x^{-1}Qx \subseteq P$. But $|x^{-1}Qx| = |Q| = |P| = p^k$ (since conjugation is an automorphism and thus preserves cardinalities). Therefore, $x^{-1}Qx = P$. ■

Consequently, any Sylow p-subgroup is carried to any other Sylow p-subgroup via some inner automorphism. This means that every subgroup in $\mathcal{S}\text{yl}_p$ must have the same group structure (i.e., they are all isomorphic).

We note that Sylow II is commonly stated as "Given any p-subgroup H and Sylow p-subgroup K, there exists some $x \in G$ such that $xHx^{-1} \subseteq K$." This version of the second Sylow theroem follows from our Sylow I and II.

The final Sylow theorem allows us to get a handle on exactly how many Sylow p-subgroups exist. This often puts enough of a restriction on what a group of a particular order can look like that we can classify all groups of that order.

Theorem: (Sylow III) Recall that n_p is the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \pmod{p}$ and $n_p = [G : N_G(P)]$ for any $P \in \mathcal{S}\text{yl}_p$. In particular, n_p must divide $\frac{n}{p^k} = m$.

Proof: Let $P \in \mathcal{S}\text{yl}_p$ and we let P act on $\mathcal{S}\text{yl}_p$ via conjugation: $x \bullet Q = xQx^{-1}$ for any $x \in P$ and $Q \in \mathcal{S}\text{yl}_p$. Then since P is a p-group, we can apply our preliminary thereom and get $n_p = |\mathcal{S}\text{yl}_p| \equiv \left|\left(\mathcal{S}\text{yl}_p\right)_P\right| \pmod{p}$. Note that

$$\begin{aligned}\left(\mathcal{S}\text{yl}_p\right)_P &= \{Q \in \mathcal{S}\text{yl}_p \mid x \bullet Q = Q \text{ for all } x \in P\} = \{Q \in \mathcal{S}\text{yl}_p \mid xQx^{-1} = Q \text{ for all } x \in P\} \\ &= \{Q \in \mathcal{S}\text{yl}_p \mid x \in N_G(Q) \text{ for all } x \in P\} = \{Q \in \mathcal{S}\text{yl}_p \mid P \subseteq N_G(Q)\}\end{aligned}$$

We note that if Q is a Sylow p-subgroup of G and $Q \subseteq K \subseteq G$ for some subgroup K, then Q is a Sylow p-subgroup of K since if a larger power of p than $|Q| = p^k$ divided $|K|$, then by Lagrange's theorem this power would also divide $|G|$ contradicting p^k being the largest such power.

We now know that if $Q \in \left(\mathcal{S}\text{yl}_p\right)_P$, then $P \subseteq N_G(Q)$ and so both P and Q are Sylow p-subgroups of $N_G(Q)$. By the second Sylow theorem $P = xQx^{-1}$ for some $x \in N_G(Q)$. But $Q \triangleleft N_G(Q)$ and so $P = xQx^{-1} = Q$. Therefore, we have that $\left(\mathcal{S}\text{yl}_p\right)_P = \{P\}$. Thus $n_p \equiv \left|\left(\mathcal{S}\text{yl}_p\right)_P\right| = 1 \pmod{p}$.

For our second fact about n_p we note that G acts on $\mathcal{S}\text{yl}_p$ via conjugation as well. By the second Sylow thereom (i.e., all Sylow p-subgroups are conjugate), we have that $\mathcal{S}\text{yl}_p$ is a single orbit under this action. Also, the stabilizer of some $P \in \mathcal{S}\text{yl}_p$ is by definition

$$\text{stab}_G(P) = \{g \in G \mid g \bullet P = P\} = \{g \in G \mid gPg^{-1} = P\} = \{g \in G \mid g \in N_G(P)\} = N_G(P)$$

Thus by the orbit-stablizer theorem, $|n_p| = |\mathcal{S}\text{yl}_p| = |\text{orbit}(P)| = [G : \text{stab}(P)] = [G : N_G(P)]$. Since $|G| = [G : N_G(P)] \cdot |N_G(P)|$ and $P \subseteq N_G(P)$, we have p^k divides $|N_G(P)|$ and so $n_p = [G : N_G(P)]$ must divide $n/p^k = m$. ■

Example: Suppose G is a group of order 15. Then $n_3 \equiv 1 \pmod{3}$ and n_3 must divide $15/3 = 5$. Therefore, $n_3 = 1$. Likewise, $n_5 \equiv 1 \pmod{5}$ and n_5 must divide $15/5 = 3$. Therefore, $n_5 = 1$ as well. Notice that any element of order 3 must live in a Sylow 3-subgroup (in fact, since Sylow 3-subgroups have order 3 here, such an element must generate a Sylow 3-subgroup). Since there is only $n_3 = 1$ Sylow 3-subgroup, we must have exactly $3 - 1 = 2$ elements of order 3. Likewise, we have exactly $5 - 1 = 4$ elements of order 5. Therefore, we have a total of $1 + 2 + 4 = 7$ elements of orders 1, 3, and 5. The remaining $15 - 7 = 8$ elements must have order 15 (this is the only possibility left by Lagrange's theorem). Since G has elements of order 15, it is cyclic (i.e., $|G| = 15$ implies $G \cong \mathbb{Z}_{15}$).

We record the following useful fact:

Proposition: If $\mathcal{S}\text{yl}_p = \{P\}$ (i.e., there is a unique Sylow p-subgroup so $n_p = 1$), then $P \triangleleft G$.

Proof: Let $x \in G$, then xPx^{-1} is a subgroup of G. Since conjugation preserves cardinalities, $|xPx^{-1}| = |P| = p^k$. Thus we have that xPx^{-1} is a Sylow p-subgroup of G. By the assumed uniqueness, $xPx^{-1} = P$ and so $P \triangleleft G$. ■

Proposition: If G is a simple p-group, then G is cyclic of prime order. In other words, there are no non-Abelian simple p-groups.

Proof: Suppose G is a simple group of order p^k for some $k \geq 0$. The trivial group (order $p^0 = 1$) is not simple by definition so $k > 0$. If $k = 1$, $|G| = p$ is prime and thus G is cyclic of prime order. Therefore, let $k > 1$.

[Proof #1:] Notice G itself is its Sylow p-subgroup. By Sylow I part (2), we have a normal subgroup of order p^{k-1}. Since $k > 1$ this is a non-trivial proper normal subgroup (i.e., G is not simple). [Proof #2:] From the class equation, we know that p-groups must have a non-trivial center. Therefore, since the center, $Z(G)$, is a normal subgroup and G is simple, we must conclude that $Z(G)$ is not a proper subgroup (i.e., $G = Z(G)$). Therefore, G is Abelian. But Cauchy's theorem implies that we have an element of order p. This generates a cyclic subgroup of order p. Since $p < p^k$ and all subgroups of Abelian groups are normal, G has a proper non-trivial subgroup. Thus it is not simple – contradiction. ■

Corollary: Let p and q be primes. There are no simple groups of order pq.

Proof: Suppose G is a simple group of order pq. The above proposition rules out $p = q$ (i.e., $pq = p^2$), so $p \neq q$.

We know that $n_p = 1$ or $n_q = 1$ imply we have a normal Sylow p-subgroup or q-subgroup. Sylow's third theorem tells us that n_p must divide $pq/p = q$ so we must have $n_p = q$. Likewise, we must conclude $n_q = p$. Recall that groups of prime order are generated by any of their non-identity elements. Thus distinct subgroups of prime orders can only overlap at the identity. Therefore, $n_p = q$ subgroups of order p imply that G has $q(p-1)$ elements of order p. Likewise, G must have $p(q-1)$ elements of order q. Adding in the identity, this accounts for $q(p-1) + p(q-1) + 1 = pq + (pq - p - q) + 1$ elements of G. If $p < q$, then $pq - p - q > pq - q - q \geq 2q - 2q = 0$ similarly if $q < p$. In other words, G has at least $pq + 1$ elements – contradiction. ■

Corollary: Let p and q be primes. There are no simple groups of order p^2q.

Proof: Suppose G is a simple group of order p^2q. Again, if $p = q$, then $|G| = p^3$ and by the above proposition G is not simple. Therefore, $p \neq q$.

We know that $n_p = 1$ or $n_q = 1$ imply we have a normal Sylow p-subgroup or q-subgroup. Sylow's third theorem tells us that n_p must divide q and n_q must divide p^2. Also, the theorem says that $n_p \equiv 1 \pmod{p}$ and $n_q \equiv 1 \pmod{q}$. Notice that $p > q$ implies $n_p = q \not\equiv 1 \pmod{p}$. Therefore, we must have that $p < q$. Thus we cannot have $n_q = p$ since $p \not\equiv 1 \pmod{q}$ if $p < q$. Thus we must have $n_q = p^2$.

We have p^2 subgroups of order q. As before, these can only overlap at the identity. Therefore, elements of order q account for $p^2(q-1) = p^2q - p^2$ elements of our group. This only leave room for one subgroup of order p^2 (i.e., $n_p = 1$) – contradiction. ■

In fact, one can prove that there are no simple groups of order p^kq^ℓ (given we don't have $k = 0$ and $\ell = 1$ or $k = 1$ and $\ell = 0$). This is called Burnside's theorem and is significantly more difficult to prove. The standard proof uses a significant amount of group representation theory and we shall not pursue that here. Thus a non-Abelian simple group must have an order involving at least 3 primes.

The celebrated and incredibly difficult Feit-Thompson odd order theorem says that every non-Abelian simple group must be of even order. Their proof occupied an entire issue of a journal (over 200 pages long). This very long, very technical proof has not been meaningfully simplified or shortened even now over 50 years later. Oddly, once one knows that a non-Abelian simple group must have even order, it is easy to show that in fact its order must be divisible by either 8 or 12.

Let us use the Sylow theorems to classify groups of order $2p$.

Theorem: Let p be a prime. Groups of order $2p$ are either cyclic or dihedral. In other words, if G is a group of order $2p$, then either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

Proof: We recall the generator and relation definition of the dihedral groups: $D_n = \langle x, y \mid x^n = 1, y^2 = 1, (xy)^2 = 1\rangle$.

Consider the case $p = 2$: If $|G| = 2p = 4$, then G is Abelian and so G is either cyclic or isomorphic with the Klein 4-group. Notice that $D_2 = \{1, x, y, xy\}$ is just the Klein 4-group since $x^2 = y^2 = (xy)^2 = 1$.

Now let p be an odd prime. We have that $n_p \equiv 1 \pmod{p}$ and n_2 divides $|G|/p = 2$. Therefore, $n_p = 1$ so we have a unique (normal) Sylow p-subgroup, say P. Now $|P| = p$ so that P is a group of prime order. Consequently P is cyclic. Let $x \in G$ such that $P = \langle x\rangle$. We note that any element of order p must be contained in a Sylow p-subgroup. Since P is the *only* Sylow p-subgroup, we have that G has exactly $p-1$ elements of order p (they are precisely: $x, x^2, \ldots, x^{p-1}$).

Next, $n_2 \equiv 1 \pmod{2}$ and n_2 must divide $|G|/2 = p$. Therefore, either $n_2 = 1$ or $n_2 = p$.

- Case 1: $n_2 = 1$. Then there is a unique (normal) Sylow 2-subgroup, say Q. Similar to P, Q contains the identity plus every element of order 2. Since $|Q| = 1$, there is exactly 1 element of order 2.

  Lagrange's theorem tells us that the elements of G must be of orders 1, 2, p, and $2p$. Since we have 1 element of order 1, 1 element of order 2, and $p-1$ elements of order p, we must have $2p - 1 - 1 - (p-1) = p - 1$ elements of order $2p$. Since G has elements of order $2p$, it is cyclic.

- Case 2: $n_2 = p$. Let $\mathcal{S}\text{yl}_2 = \{Q_1, \ldots, Q_p\}$. These Sylow 2-subgroups of G are of order 2. Such groups look like $Q_i = \langle y_i\rangle = \{1, y_i\}$ where $y_i^2 = 1$. Considering the identity plus the $p-1$ elements of order p account for p elements of our group, these elements of order 2 exhaust the rest of G. Thus $G = \{1, x, x^2, \ldots, x^{p-1}, y_1, y_2, \ldots, y_p\}$. Let $y = y_1$. Notice that $x^ky \neq x^\ell$ for any ℓ since otherwise, $y = x^{-k}x^\ell = x^{\ell-k}$ has order 1 or p contradicting $|y| = 2$. Therefore, x^ky must one of the y_i's. Also, $x^ky = x^\ell y$ imples $x^k = x^\ell$ and so $k \equiv \ell \pmod{p}$ since $|x| = p$. Thus $y, xy, \ldots, x^{p-1}y$ are exactly our elements of order 2. We have $G = \{1, x, \ldots, x^{p-1}, y, xy, \ldots, x^{p-1}y\}$ where $x^p = 1$, $y^2 = 1$, and $(xy)^2 = 1$ (since xy has order 2). Therefore, $G \cong D_p$ is dihedral. ■

We end with a somewhat unrelated but useful result generalizing the index 2 theorem: Index 2 implies normal.

Theorem: Let H be a subgroup of G such that $[G : H] = p$ is the smallest prime divisor of $|G|$. Then $H \triangleleft G$.

Proof: Let G act on G/H via left multiplication. Since $|G/H| = [G : H] = p$, this action yields a permutation representation $\varphi : G \to S_p$. Now $\varphi(G)$ is a subgroup of S_p so its order divides $p!$. But we also know $|G| = |\text{Ker}(\varphi)| \cdot |\varphi(G)|$. Thus $|\varphi(G)|$ divides both $|G|$ and $|S_p| = p!$. Therefore, any prime dividing $|\varphi(G)|$ must divide both $|G|$ and $p!$. The prime divisors of $p!$ are p and smaller with p dividing once. Since p is the smallest prime dividing $|G|$, we have that the only possible prime dividing $|\varphi(G)|$ is p itself (and at most once). Thus either $|\varphi(G)| = 1$ or p.

Note that $k \in \text{Ker}(\varphi)$ implies k acts as the identity on G/H (i.e., $kxH = xH$ for all $x \in G$). In particular, $kH = H$ so that $k \in H$. Therefore, $\text{Ker}(\varphi) \subseteq H$. Notice that $|\varphi(G)| = 1$ would imply $|\text{Ker}(\varphi)| = |G|/1 = |G|$ so that $G = \text{Ker}(\varphi) \subseteq H \neq G$ (impossible). Thus we must conclude that $|\varphi(G)| = p$. Therefore, $|\text{Ker}(\varphi)| = |G|/p = |H|$. Therefore, since $\text{Ker}(\varphi) \subseteq H$, we must conclude $H = \text{Ker}(\varphi) \triangleleft G$. ■