Sylow theorems

Shing Tak Lam

December 24, 2021

1 Motivation

Recall Lagrange's theorem in group theory.

Theorem (Lagrange's theorem)
Let G be a finite group, H be a subgroup of G. Then

$$|G| = |G : H||H|$$

where $|G : H|$ is the index of H in G.

What this tells us is that the size of any subgroup must divide the size of the group. This leads us to a natural question.

Question. Is the converse true? That is, if $n \mid |G|$, must we have a subgroup of size n?

As it turns out, this is false in general. A_4, the alternating group on 4 elements, has size 12, but it does not have any subgroups of order 6. However, there are special cases where this turns out to be true.

2 Cauchy's Theorem

The simplest case is known as Cauchy's theorem, where we take p to be a prime number. In this case, we do have a subgroup of size p.

Theorem (Cauchy's theorem)
Let p be a prime, and suppose $p \mid |G|$. Then there exists an element $g \in G$ such that g has order p.

There are multiple proofs of this, here we will only discuss McKay's proof involving group actions.

Proof. Let $S = \{(a_1, \dots, a_p) \in G^p : a_1 \dots a_p = e\}$. Then S has size $|G|^{p-1}$. In particular, p divides the size of S. Now let C_p act on S by cycling, that is, if $C_p = \langle h \rangle$, $h \cdot (a_1, \dots, a_p) = (a_2, \dots, a_p, a_1)$. By the orbit stabiliser theorem, the size of orbits must be 1 or p. As orbits partition, and $p \mid |S|$, we must have that the number of size 1 orbits is a multiple of p. $\mathrm{Orb}((e, \dots, e))$ has size 1, so we must have at least $p - 1$ more. Note that $(a_1, \dots, a_p)$ is in a size 1 orbit if and only if $a_1 = \cdots = a_p$, so $a_1^p = e$. □

In fact, this proof of Cauchy's theorem also gives us information about the number of subgroups of order p.

Proposition
Let p be a prime, and suppose $p \mid |G|$. Let N be the number of subgroups of G of order p. Then

$$N \equiv 1 \pmod{p}$$

Proof. First, we note that any nontrivial element in a subgroup of size p generates that subgroup, so any two must intersect trivially. Thus, this reduces to counting the number of elements of order p. Using the above proof, we note that the number of elements of order p must be $kp - 1$ for some k. Each subgroup of order p has $p - 1$ nontrivial elements, so the number of elements of order p must be $N(p - 1)$. Equating these, we get that

$$Np - N = kp - 1$$

reducing $\pmod p$, we get that $N \equiv 1 \pmod p$. □

3 Sylow I

We can now generalise Cauchy's theorem to higher powers of the prime p. What this gives us is known as Sylow's first theorem. But first, we will need to see some definitions.

Definition (p-Sylow subgroup)

Let p be a prime, and suppose $|G| = p^k m$, where $\gcd(m, p) = 1$. Then a subgroup P of order p^k is known as a p-Sylow subgroup.

In the case where p does not divide the size of G, the existence of such a subgroup shouldn't be surprising.

Example

If p does not divide $|G|$, then we have a p-Sylow subgroup, namely $\{e\}$.

On the other hand, Sylow's first theorem tells us that one exists even if p does divide G.

Theorem (Sylow I)

Let p be a prime, G be a finite group. Then there exists a p-Sylow subgroup of G.

First, we are going to use the following lemma to reduce this to an equivalent statement.

Lemma

Let G be a finite group, $|G| = p^k$. Then for $r \leq k$, there exists a normal subgroup of G of order p^r.

Proof. By induction on k and then induction on r. The case $k = 0$ is trivial. Now suppose it holds for all $m < k$.

r. $r = 0$ is the trivial subgroup, and $r = k$ is G. Now suppose we had N which is a normal subgroup of G, with $|N| = p^r$, where $0 < r < k$. Then we want to construct a subgroup of G with order p^{r+1}.

$$\left|\frac{G}{N}\right| = \frac{|G|}{|N|} = p^{k-r}$$

which means that p divides the order of G/N. By Cauchy's theorem and the induction hypothesis (on k), we have a normal subgroup H of G/N of size p. Let $\pi : G \to G/N$ be the quotient map, and $P = \pi^{-1}(H)$. Then P is a subgroup of G. Furthermore, N is a normal subgroup of P, as $\pi(N) = \{e\} \subseteq H$, and N is normal in G. Then

$$\frac{P}{N} \cong \pi(P) = \pi\left(\pi^{-1}(H)\right) = H$$

as the quotient map is surjective. This means that

$$|P| = |P/N| \cdot |N| = p \cdot p^r = p^{r+1}$$

As P is the preimage of a normal subgroup, it is a normal subgroup of G. □

Proposition

If p^k divides the order of G, then there exists a subgroup of order p^k.

Proof. The case $k = 0$ we have the trivial group. Thus, we may assume $k \geq 1$, which means that $p \mid |G|$. We then argue by induction on $|G|$.

If $|G| = p$, then we are done. For the inductive case, $|G| > p$. If G has a subgroup H where the index $|G : H|$ is coprime to p, then p^k divides the size of H, so by the induction hypothesis we have a subgroup of H order p^k, which is then a subgroup of G. Thus, we may now assume that there is no subgroup where the index is coprime to p.

Considering the orbits under the conjugation action, we have that

$$|G| = |Z(G)| + \sum_{\substack{C \text{ conjugacy class} \\ |C| \geq 2}} |C|$$

and by orbit-stabiliser, we have that

$$|\mathrm{ccl}(g)| = \frac{|G|}{|C(g)|} = [G : C(g)]$$

which means that p divides the size of $\mathrm{ccl}(g)$ if it is bigger than 1. Which then means that p divides the size of $Z(G)$. Thus we have a subgroup N of $Z(G)$ with size p, which is normal in G. Then,

$$\left|\frac{G}{N}\right| = \frac{|G|}{|N|} = \frac{|G|}{p}$$

So p^{k-1} divides the size of G/N. By the induction hypothesis, we have a subgroup H of G/N of size p^{k-1}. Let $\pi : G \to G/N$ be the quotient map, and $P = \pi^{-1}(H)$. As in the lemma above, we have that $|P| = |H| \cdot p = p^k$. □

Sylow's first theorem is then an immediate consequence of this proposition.

Proof of Sylow's first theorem. The above proposition implies Sylow's first theorem, and the converse holds by the lemma. □

4 Sylow II

Sylow's first theorem gives us an existence statement about p-Sylow subgroups, that is, we have subgroups of sizes p^k as large as Lagrange's theorem would allow. In fact, we can show even more about the p-subgroups.

Theorem (Sylow's second theorem)

Let G be a finite group, p be prime. Let P be a p-Sylow subgroup of G, and H be a p-subgroup of G. Then H is contained in a conjugate of P. That is, there exists $g \in G$ such that $H \subseteq gPg^{-1}$.

Proof. Let S be the set of left cosets of P. Then $|S| = |G : P|$ is coprime to p. Let H act on S by left multiplication. As orbits partition, we have that

$$|S| = |\{\text{size 1 orbits}\}| + \sum_{\substack{O \text{ orbit} \\ |O| \geq 2}} |O|$$

Since H is a p-group, the size of nontrivial orbits must be a multiple of p. Thus, the action must have a fixed point, say gP such that $hgP = gP$ for all $h \in H$. That is, $g^{-1}hg \in P$ for all $h \in H$, or $h \in gPg^{-1}$ for all $h \in H$. □

5 Sylow III

Recall that from the proof of Cauchy's theorem, we also derived an expression for the number of subgroups of size p. As it turns out, a similar statement holds for Sylow subrgoups as well.

Theorem (Sylow's third theorem)

Let G be a finite group, p be a prime number. Suppose $|G| = p^r m$, where $\gcd(p, m) = 1$. Let N_p be the number of p-Sylow subgroups. Then we have that $N_p \mid m$ and $N_p \equiv 1 \pmod{p}$.

Before we can prove this, we are going to need a new definition and a lemmas.

Definition (Normaliser)

Let G be a group, H be a subgroup of G. Then the normaliser $N(H)$ is the stabiliser under the conjugation action, that is,

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

We will not expand too much on this definition right now, since we only need the very basics to be able to prove Sylow's third theorem, and when we use it later on we will discuss it further.

Lemma

Let H be a p-subgroup of a finite group G. Then

$$|N(H) : H| \equiv |G : H| \pmod{p}$$

Proof. If H is trivial, then $N(H) = G$ and we are done. Otherwise, let S be the set of left cosets of H in G, and let H act on S by left multiplication. Now consider the fixed points under this action.

$$hgH = gH \iff g^{-1}Hg \subseteq H \iff g^{-1}Hg = H \iff g \in N(H)$$

So the set of fixed points has the same size as the normaliser of H. Now as

$$|G : H| = |S| = |\{\text{size 1 orbits}\}| + \sum_{\substack{O \text{ orbit} \\ |O| \geq 2}} |O|$$

and p divides the size of all orbits of size ≥ 2, we get the required result. □

With this, we can then prove Sylow's third theorem.

Proof of Sylow's third theorem. Sylow's second theorem tells us that all p-Sylow subgroups are conjugate. Let P be a p-Sylow subgroup. Then N_p is just the size of the orbit of P, under conjugation by G. By orbit stabiliser, this means that $N_p = |G : N(P)|$. This means that

$$m = |G : P| = |G : N(P)| \cdot |N(P) : P| = N_p \cdot |N(P) : P|$$

so N_p divides m. By the lemma, we have that

$$m = |G : P| \equiv |N(P) : P| \pmod{p}$$

multiplying by N_p, we get that $mN_p \equiv m \pmod{p}$, and as $m \not\equiv 0 \pmod{p}$, we get that $N_p \equiv 1 \pmod{p}$ □

6 Chains of p-subgroups

Another way of thinking about Sylow's first theorem is in terms of ascending chains of p-groups. This can be summarised in the following proposition.

Proposition

Let H be a p-subgroup of a finite group G, and suppose H is not a p-Sylow subgroup. Then there exists a p subgroup K of G containing H, such that $|K : H| = p$ and H is normal in K.

Proof. Since H is not a p-Sylow subgroup, then we have that p divides $|G : H|$, which means p divides $|N(H) : H|$. H is normal in $N(H)$, which means that we can consider the quotient group $N(H)/H$. $|N(H)/H| = |N(H) : H|$, so p divides the size of $N(H)/H$. By Cauchy's theorem, we have a subgroup M of $N(H)/H$ of order p. Let π be the quotient map, and $K = \pi^{-1}(M)$. Then $|K : H| = p$, and H is normal in K since K is a subgroup of $N(H)$. □

We can use this proposition to extend increasing chains of p-subgroups.

Proposition

Suppose we have a chain

$$H_0 = \{e\} \subseteq H_1 \subseteq \cdots \subseteq H_k$$

of p-subgroups of a finite group G, where $|H_i| = p^i$. Then we can extend the chain all the way to a p-Sylow subgroup of G, as

$$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k \subseteq H_{k+1} \subseteq \cdots \subseteq H_r$$

Furthermore, we can choose them such that H_k is normal in H_{k+1}, H_{k+1} is normal in H_{k+2} and so on.

Proof. Apply the previous proposition. □

This then gives us an alternative proof of the first Sylow theorem.

Alternative proof of Sylow's first theorem. By Cauchy's theorem, we have a subgroup of order p. Then use the above proposition to construct a chain of p-subgroups going up to a p-Sylow subgroup. □

7 Applications of the Sylow theorems

The Sylow theorems are useful when we want to classify finite groups of a certain size, or to determine whether a group is simple.

Theorem

Let G be a group of order mp^r, where p is prime and $\gcd(m, n) = 1$ and if $d \mid m$ and $d \equiv 1 \pmod{p}$, then $d = 1$. Then G is not simple.

Proof. By the third Sylow theorem, N_p divides m and is of the form $1 + kp$. This forces $N_p = 1$. So G has a normal subgroup of order p^r, as the p-Sylow subgroup must be normal, so it is not simple. □

Theorem

Suppose $p < q$ are primes, and $q \not\equiv 1 \pmod{p}$, and $|G| = pq$. Then G is cyclic.

Proof. By the third Sylow theorem, N_p divides q and is $1 \pmod{p}$. This means $N_p = 1$. Similarly, $N_q = 1$. So there is only one subgroup of size p, and one subgroup of size q. Then, there is 1 element of order 1, $p - 1$ elements of order p, $q - 1$ elements of order q, and

$$1 + (p - 1) + (q - 1) = p + q - 1 < 2q - 1 < 2q \leq pq$$

which means that we must have an element of order pq, which would generate G. □

A Miscellany

Here is a collection of results that I've used in tha above document, which might not be immediately obvious, but can be assumed without proof when first reading.

Lemma

Let G, H be groups, K be a subgroup of G, $\varphi : G \to H$ is a homomorphism. Then $\varphi(K)$ is a subgroup of H.

Proof. This follows by just checking the axioms for a subgroup.

- $e = \varphi(e) \in \varphi(K)$.
- If $x = \varphi(g)$ and $y = \varphi(h)$ are in $\varphi(K)$, then $xy = \varphi(g)\varphi(h) = \varphi(gh) \in \varphi(K)$.
- If $x = \varphi(g)$ is in $\varphi(K)$, then $x^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \varphi(K)$.

□

Lemma

Let G, H be groups, K be a subgroup of H, $\varphi : G \to H$ is a homomorphism. Then $\varphi^{-1}(K)$ is a subgroup of G.

Proof. This follows by just checking the axioms for a subgroup.

- $\varphi(e) = e \in K$, so $e \in \varphi^{-1}(K)$.
- For all $a, b \in \varphi^{-1}(K)$, $\varphi(ab) = \varphi(a)\varphi(b) \in K$.
- For all $a \in \varphi^{-1}(K)$, $\varphi(a^{-1}) = \varphi(a)^{-1} \in K$.

□

Lemma

Let G, H be groups, K be normal subgroup of H, $\varphi : G \to H$ is a homomorphism. Then $\varphi^{-1}(K)$ is a normal subgroup of G.

Proof. Let $a \in \varphi^{-1}(K)$, $g \in G$. Then $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1}$ is in K, as $\varphi(a) \in K$ and K is normal. □

Lemma

Let G be a group, K be a subgroup of $Z(G)$. Then K is normal in G.

Proof. For $g \in G, k \in K$, $gkg^{-1} = gg^{-1}k = k \in K$ □