p-groups and the Sylow theorems!

Spencer Bagley

With many thanks to Matthew Macauley,
http://www.math.clemson.edu/~macaule/

23 Apr 2025

Recap!

Review: p-groups

Definition

A *p*-group is a group whose order is a power of a prime p. A p-group that is a subgroup of a group G is a *p*-subgroup of G.

Notational convention

Throughout, G will be a group of order $|G| = p^n \cdot m$, with $p \nmid m$.
That is, p^n is the *highest power* of p dividing $|G|$. (We are isolating all the p.)

Warmup: On the lattice of A_5 (handout), highlight all the p-subgroup towers.

Use different colors for different ps.

Note: $|A_5| = \dfrac{5!}{2}$; which primes divide $|A_5|$?

Label as much other stuff as possible. Order? Index? What else?

Lemmas about p-groups

p-group Lemma

If a p-group G acts on a set S via $\phi\colon G \to \mathbf{Perm}(S)$, then

$$|\mathsf{Fix}(\phi)| \equiv_p |S|.$$

"The number of fixed points is congruent mod p to the size of the set."

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

$$[N_G(H)\colon H] \equiv_p [G\colon H].$$

"The index of H in its normalizer is congruent mod p to the index of H in the whole group."

Normalizer lemma, Part 2

Suppose $|G| = p^n m$, and $H \leq G$ with $|H| = p^i < p^n$. Then $H \lneq N_G(H)$, and the index $[N_G(H) : H]$ is a multiple of p.

"Non-maximal p-subgroups aren't fully unnormal."

The Sylow theorems!

The Sylow theorems

Here is sort of a driving question that we've been thinking about throughout the course:

Open-ended question

What group structural properties are possible, what are impossible, and how does this depend on $|G|$?

One approach is to decompose large groups into "building block subgroups." For example:

> *given a group of order* $72 = 2^3 \cdot 3^2$, *what can we say about its* 2*-subgroups and* 3*-subgroups?.*

This is the idea behind the Sylow theorems, developed by Norwegian mathematician Peter Sylow (1832–1918).

The Sylow theorems address the following questions of a finite group G:

1. How big are its p-subgroups?
2. How are the p-subgroups related?
3. How many p-subgroups are there?
4. Are any of them normal?

The Sylow theorems

Notational convention

Througout, G will be a group of order $|G| = p^n \cdot m$, with $p \nmid m$.

That is, p^n is the *highest power* of p dividing $|G|$.

A subgroup of order p^n is called a Sylow p-subgroup.

Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups, and $n_p := \big|\mathrm{Syl}_p(G)\big|$.

There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

1. **Existence**: In every group, p-subgroups of all possible sizes exist, and they're "*nested*".
2. **Relationship**: All maximal p-subgroups are conjugate.
3. **Number**: There are strong restrictions on n_p, the number of Sylow p-subgroups.

Together, these place strong restrictions on the structure of a group G with a fixed order.

The Sylow theorems

First Sylow theorem

G has a subgroup of order p^k, for each p^k dividing $|G|$.

Also, every non-Sylow p-subgroup sits inside a larger p-subgroup.

Second Sylow theorem

Any two Sylow p-subgroups are conjugate (and hence isomorphic).

Third Sylow theorem

Let n_p be the number of Sylow p-subgroups of G. Then

$$n_p \text{ divides } |G| \qquad \text{and} \qquad n_p \equiv_p 1\,.$$

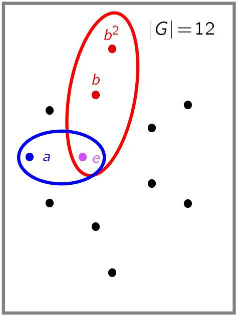
(Note that together, these imply that $n_p \mid m$, where $|G| = p^n \cdot m$.)

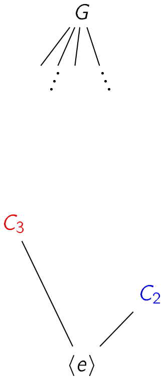
Our unknown group of order 12

Throughout, we will have a running example, a "mystery group" G of order $12 = 2^2 \cdot 3$.

We already know a little bit about G. By Cauchy's theorem, it must have:

- an element a of order 2, and
- an element b of order 3.





Using *only* the fact that $|G| = 12 = 2^2 \cdot 3$, we will unconver as much about its structure as we can.

The first Sylow theorem!

The first Sylow theorem: existence of p-subgroups

First Sylow theorem

G has a subgroup of order p^k, for each p^k dividing $|G|$.

Also, every non-Sylow p-subgroup sits inside a larger p-subgroup.

Proof

Induction! We'll prove this is true for every $k \geq 0$.

Base case: $k = 0$. Claim: G has a subgroup of order $p^0 = 1$.

(Sure: $\langle e \rangle$.)

Claim 2: This is a non-Sylow p-subgroup, so it must sit inside a larger p-subgroup.

(Sure: Cauchy's theorem says there is an element x of order p, so there's a cyclic subgroup $\langle x \rangle$ of order p, and $\langle e \rangle \leq \langle x \rangle$.)

The first Sylow theorem: existence of p-subgroups

First Sylow theorem

G has a subgroup of order p^k, for each p^k dividing $|G|$.

Also, every non-Sylow p-subgroup sits inside a larger p-subgroup.

Proof (inductive step)

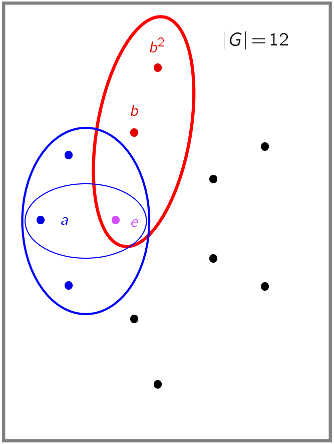
Take any $H \leq G$ with $|H| = p^i < p^n$. We know $H \trianglelefteq N_G(H)$ and p divides $|N_G(H)/H|$.

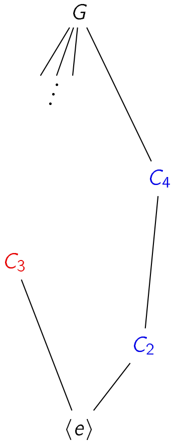
Find an element aH of order p. The union of cosets in $\langle aH \rangle$ is a subgroup of order p^{i+1}.

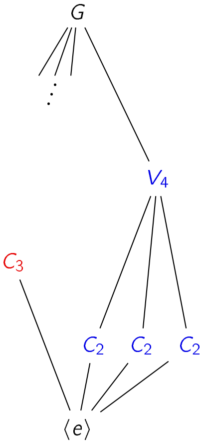
Order:			**Order**:
p^n	G		
$p^{i+j} \cdot r$	$N_G(H)$	$N_G(H)/H$	$p^j \cdot r$
	$\vdots$	$\vdots$	
p^{i+1}	H'	$\langle aH \rangle$	p
p^i	H	H/H	1
1	$\langle 1 \rangle$		

Our unknown group of order 12

By the first Sylow theorem, $\langle a \rangle$ is contained in a subgroup of order 4, which could be V_4 or C_4, or possibly both.







The second Sylow theorem!

The second Sylow theorem: relationship among p-subgroups

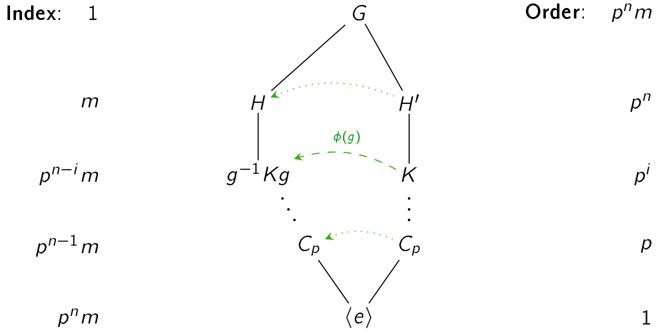
Second Sylow theorem

Any two Sylow p-subgroups are conjugate (and hence isomorphic).

We'll actually prove a stronger version, which easily implies the 2nd Sylow theorem.

Strong second Sylow theorem

Let $H \in \mathrm{Syl}(G)$, and $K \leq G$ any p-subgroup. Then K is conjugate to a subgroup of H.



The second Sylow theorem: All Sylow p-subgroups are conjugate

Strong second Sylow theorem

Let H be a Sylow p-subgroup, and $K \leq G$ any p-subgroup. Then K is conjugate to some subgroup of H.

Proof

Let $S = H\backslash G = \{Hg \mid g \in G\}$, the set of right cosets of H.

The group K acts on S by **right-multiplication**, via $\phi \colon K \to \mathrm{Perm}(S)$, where

$$\phi(k) = \text{the permutation sending each } Hg \text{ to } Hgk.$$

A fixed point of ϕ is a coset $Hg \in S$ such that

$$\begin{aligned} Hgk = Hg\,, \quad \forall k \in K \qquad &\Longleftrightarrow \qquad Hgkg^{-1} = H\,, \quad \forall k \in K \\ &\Longleftrightarrow \qquad gkg^{-1} \in H\,, \quad \forall k \in K \\ &\Longleftrightarrow \qquad gKg^{-1} \subseteq H\,. \end{aligned}$$

Thus, *if we can show that ϕ has a fixed point Hg, we're done!*

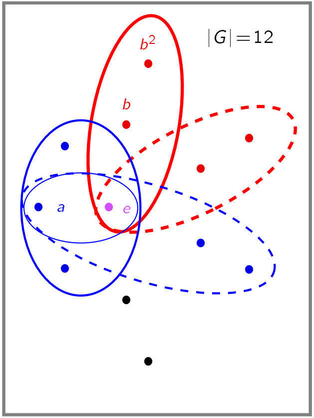
All we need to do is show that $|\mathrm{Fix}(\phi)| \not\equiv_p 0$. By the p-group Lemma,

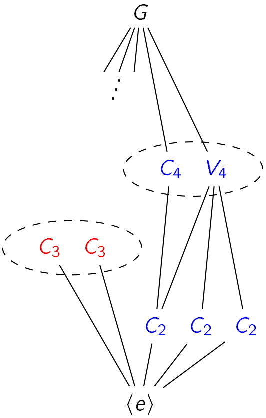
$$|\mathrm{Fix}(\phi)| \equiv_p |S| = [G : H] = m \not\equiv_p 0. \qquad \square$$

Our unknown group of order 12

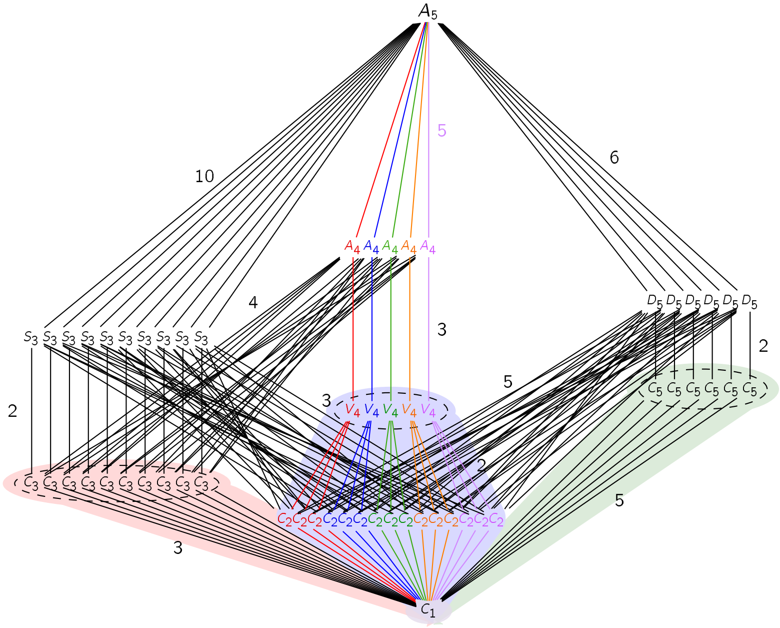
By the second Sylow theorem, all Sylow p-subgroups are conjugate, and hence isomorphic.

This eliminates the following subgroup lattice of a group of order 12.





Example: A_5 has no nontrival proper normal subgroups



(Side quest: The normalizer of the normalizer)

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
  (their normalizers are *bigger*)
- the normalizer of each Sylow p-subgroup is fully unnormal
  (their normalizers *aren't* bigger)

Proposition

Let P be a non-normal Sylow p-subgroup of G. Then its normalizer is fully unnormal.

Proof

We'll verify the equivalent statement of $N_G(N_G(P)) = N_G(P)$.

Note that P is a normal Sylow p-subgroup of $N_G(P)$.

By the 2nd Sylow theorem, P is the unique Sylow p-subgroup of $N_G(P)$.

Take an element x that normalizes $N_G(P)$ (i.e., $x \in N_G(N_G(P))$. We'll show that it also normalizes P. By definition, $xN_G(P)x^{-1} = N_G(P)$, and so

$$P \leq N_G(P) \qquad \Longrightarrow \qquad xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P).$$

But xPx^{-1} is also a Sylow p-subgroup of $N_G(P)$, and by uniqueness, $xPx^{-1} = P$. $\square$

The third Sylow theorem!

The third Sylow theorem: number of p-subgroups

Third Sylow theorem

Let n_p be the number of Sylow p-subgroups of G. Then

$$n_p \text{ divides } |G| \qquad \text{and} \qquad n_p \equiv_p 1\,.$$

(Note that together, these imply that $n_p \mid m$, where $|G| = p^n \cdot m$.)

Proof

Take $H \in \mathrm{Syl}_p(G)$. By the 2nd Sylow theorem, $n_p = |\mathrm{cl}_G(H)| = [G : N_G(H)] \,\big|\, |G|$. ✓

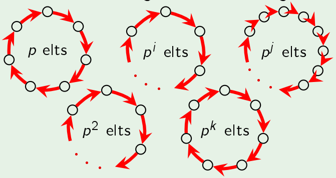
The subgroup H acts on $S = \mathrm{Syl}_p(G)$ by conjugation, via $\phi\colon G \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } K \text{ to } h^{-1}Kh.$$

Goal: *show that H is the unique fixed point.*

$|\mathrm{Fix}(\phi)| = 1$

other Sylow p-subgroups are in larger orbits



total # Sylow p-subgroups
$= n_p = |S| \equiv_p |\mathrm{Fix}(\phi)|$

The third Sylow theorem: number of p-subgroups

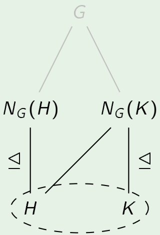
Proof (cont.)

Goal: *show that H is the unique fixed point.*

Let $K \in \mathrm{Fix}(\phi)$. Then $K \leq G$ is a Sylow p-subgroup satisfying

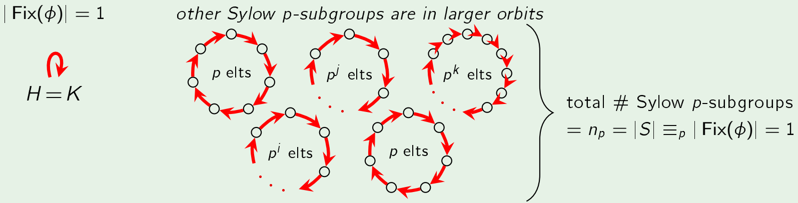
$$h^{-1}Kh = K\,, \quad \forall h \in H \quad \Longleftrightarrow \quad H \leq N_G(K) \leq G\,.$$

- H and K are p-Sylow in G, and in $N_G(K)$.
- H and K are conjugate in $N_G(K)$. (2nd Sylow thm.)
- $K \trianglelefteq N_G(K)$, thus is only conjugate to itself in $N_G(K)$.



Thus, $K = H$. That is, $\mathrm{Fix}(\phi) = \{H\}$.

By the p-group Lemma, $n_p := |S| \equiv_p |\mathrm{Fix}(\phi)| = 1$. $\square$



Summary of the proofs of the Sylow theorems

For the 1st Sylow theorem, we started with $H = \{e\}$, and inductively created larger subgroups of size $p, p^2, \dots, p^n$.

For the 2^{nd} and 3^{rd} Sylow theorems, we used a clever group action and then applied one or both of the following:

(i) *orbit-stabilizer theorem*. If G acts on S, then $|\mathbf{orb}(s)| \cdot |\mathbf{stab}(s)| = |G|$.

(ii) *p-group lemma*. If a p-group acts on S, then $|S| \equiv_p |\mathsf{Fix}(\phi)|$.

To summarize, we used:

S2 The action of $K \in \mathrm{Syl}_p(G)$ on $S = H \backslash G$ by right multiplication for some other $H \in \mathrm{Syl}_p(G)$.

S3a The action of G on $S = \mathrm{Syl}_p(G)$, by conjugation.

S3b The action of $H \in \mathrm{Syl}_p(G)$ on $S = \mathrm{Syl}_p(G)$, by conjugation.

Our mystery group order 12

By the 3rd Sylow theorem, every group G of order $12 = 2^2 \cdot 3$ must have:

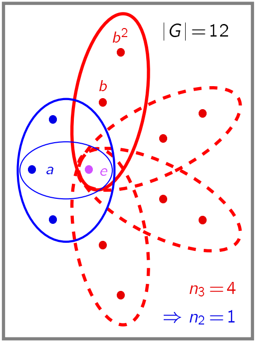
- n_3 Sylow 3-subgroups, each of order 3.

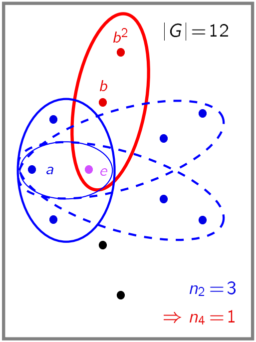
$$n_3 \mid 4, \qquad n_3 \equiv 1 \pmod 3 \qquad \Longrightarrow \qquad n_3 = 1 \text{ or } 4.$$

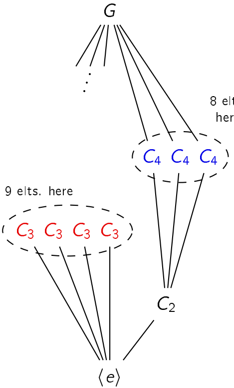
- n_2 Sylow 2-subgroups of order $2^2 = 4$.

$$n_2 \mid 3, \qquad n_2 \equiv 1 \pmod 2 \qquad \Longrightarrow \qquad n_2 = 1 \text{ or } 3.$$

But both are not possible! (There aren't enough elements.)





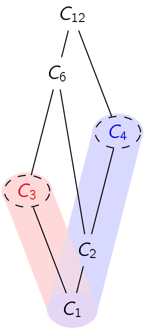


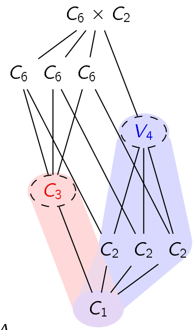
The five groups of order 12

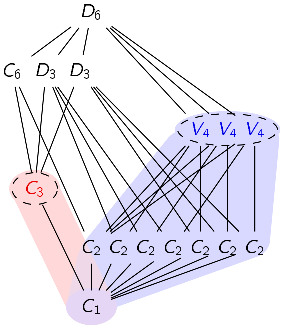
With a little work and the Sylow theorems, we can classify all groups of order 12.

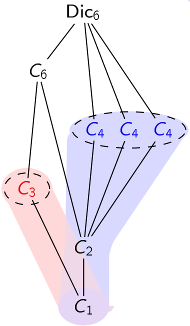
We've already seen them all. Here are their subgroup lattices.

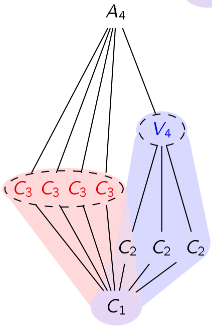
Note that *all* of these decompose as a direct or semidirect product of Sylow subgroups.











Simple groups and the Sylow theorems

Definition

A group G is simple if its only normal subgroups are G and $\langle e \rangle$.

Simple groups are to groups what primes are to integers, and are essential to understand.

The Sylow theorems are very useful for establishing statements like:

"There are no simple groups of order k (for some k)."

Since all Sylow p-subgroups are conjugate, the following result is immediate.

Remark

A Sylow p-subgroup is normal in G iff it's the unique Sylow p-subgroup (that is, if $n_p = 1$).

Thus, if we can show that $n_p = 1$ for some p dividing $|G|$, then G cannot be simple.

For some $|G|$, this is harder than for others, and sometimes it's not possible.

Tip

When trying to show that $n_p = 1$, it's usually helpful to analyze the largest primes first.

An easy example

We'll see three examples of showing that groups of a certain size cannot be simple, in successive order of difficulty.

Proposition

There are no simple groups of order 84.

Proof

Since $|G| = 84 = 2^2 \cdot 3 \cdot 7$, the third Sylow theorem tells us:

- n_7 divides $2^2 \cdot 3 = 12$ (so $n_7 \in \{1, 2, 3, 4, 6, 12\}$)
- $n_7 \equiv_7 1$.

The only possibility is that $n_7 = 1$, so the Sylow 7-subgroup must be normal. $\square$

Observe why it is beneficial to use the largest prime first:

- n_3 divides $2^2 \cdot 7 = 28$ and $n_3 \equiv_3 1$. Thus $n_3 \in \{1, \cancel{2}, 4, 7, \cancel{14}, 28\}$.
- n_2 divides $3 \cdot 7 = 21$ and $n_2 \equiv_2 1$. Thus $n_2 \in \{1, 3, 7, 21\}$.

A harder example

Proposition

There are no simple groups of order 351.

Proof

Since $|G| = 351 = 3^3 \cdot 13$, the third Sylow theorem tells us:

- n_{13} divides $3^3 = 27$ (so $n_{13} \in \{1, 3, 9, 27\}$)
- $n_{13} \equiv_{13} 1$.

The only possibilies are $n_{13} = 1$ or 27.

A Sylow 13-subgroup P has order 13, and a Sylow 3-subgroup Q has order $3^3 = 27$. Therefore, $P \cap Q = \{e\}$.

Suppose $n_{13} = 27$. Every Sylow 13-subgroup contains 12 non-identity elements, and so G must contain $27 \cdot 12 = 324$ elements of order 13.

This leaves $351 - 324 = 27$ elements in G not of order 13. Thus, G contains only one Sylow 3-subgroup (i.e., $n_3 = 1$) and so G cannot be simple. □

The hardest example

Proposition

There are no simple groups of order $24 = 2^3 \cdot 3$.

From the 3rd Sylow theorem, we can only conclude that $n_2 \in \{1, 3\}$ and $n_3 = \{1, 4\}$.

Let H be a Sylow 2-subgroup, which has relatively "small" index: $[G : H] = 3$.

Lemma

If G has a subgroup of index $[G : H] = n$, and $|G|$ does not divide $n!$, then G is not simple.

Proof

Let G act on the **right cosets** of H (i.e., $S = H \backslash G$) by **right-multiplication**:

$$\phi \colon G \longrightarrow \mathrm{Perm}(S) \cong S_n\,, \qquad \phi(g) = \text{the permutation that sends each } Hx \text{ to } Hxg.$$

Recall that $\mathrm{Ker}(\phi) \trianglelefteq G$, and is the intersection of all conjugate subgroups of H:

$$\langle e \rangle \leq \mathrm{Ker}(\phi) = \bigcap_{x \in G} x^{-1} H x \lneq G$$

If $\mathrm{Ker}(\phi) = \langle e \rangle$ then $\phi \colon G \hookrightarrow S_n$ is an embedding, which is impossible because $|G| \nmid n!$. $\square$