Lecture 5.6: The Sylow theorems

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Overview

The Sylow theorems are about one question:

What finite groups are there?

Early on, we saw five families of groups: cyclic, dihedral, abelian, symmetric, alternating.

Later, we classified all (finitely generated) *abelian* groups.

But what *other* groups are there, and what do they look like? For example, for a fixed order $|G|$, we may ask the following questions about G:

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

There is no one general method to answer this for any given order.

However, the Sylow Theorems, developed by Norwegian mathematician Peter Sylow (1832–1918), are powerful tools that help us attack this question.

Recall from last time

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

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 $|G|$.

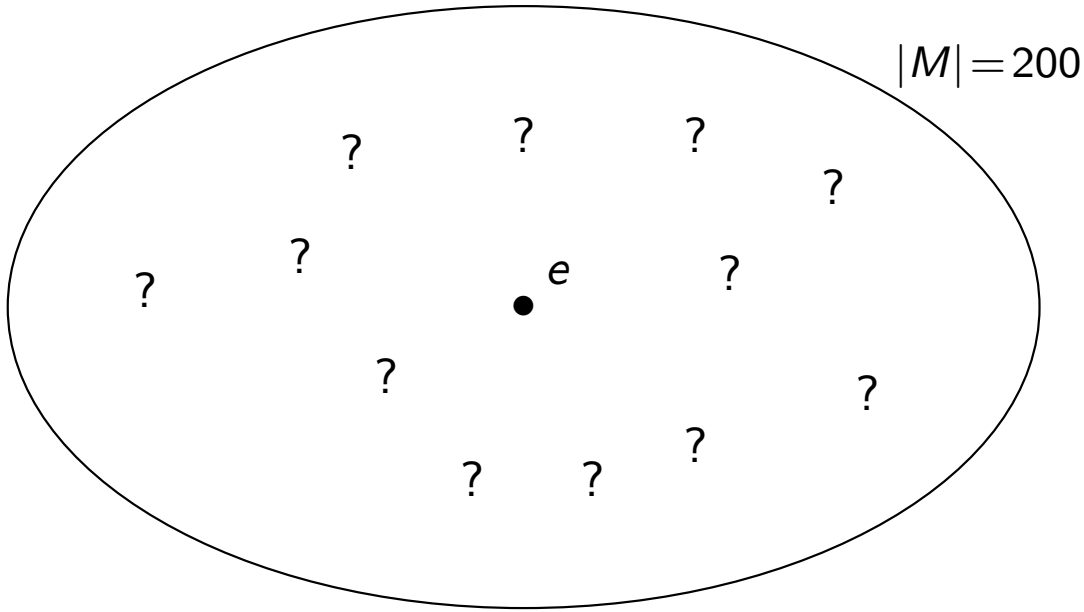
There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

1. **Existence**: In every group, p-subgroups of all possible sizes exist.
2. **Relationship**: All maximal p-subgroups are conjugate.
3. **Number**: There are strong restrictions on the number of p-subgroups a group can have.

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

Our unknown group of order 200

Throughout our two lectures on the Sylow theorems, we will have a running example, a "mystery group" M of order 200.



Using *only* the fact that $|M| = 200$, we will unconver as much about the structure of M as we can.

We actually already know a little bit. Recall Cauchy's theorem:

Cauchy's theorem

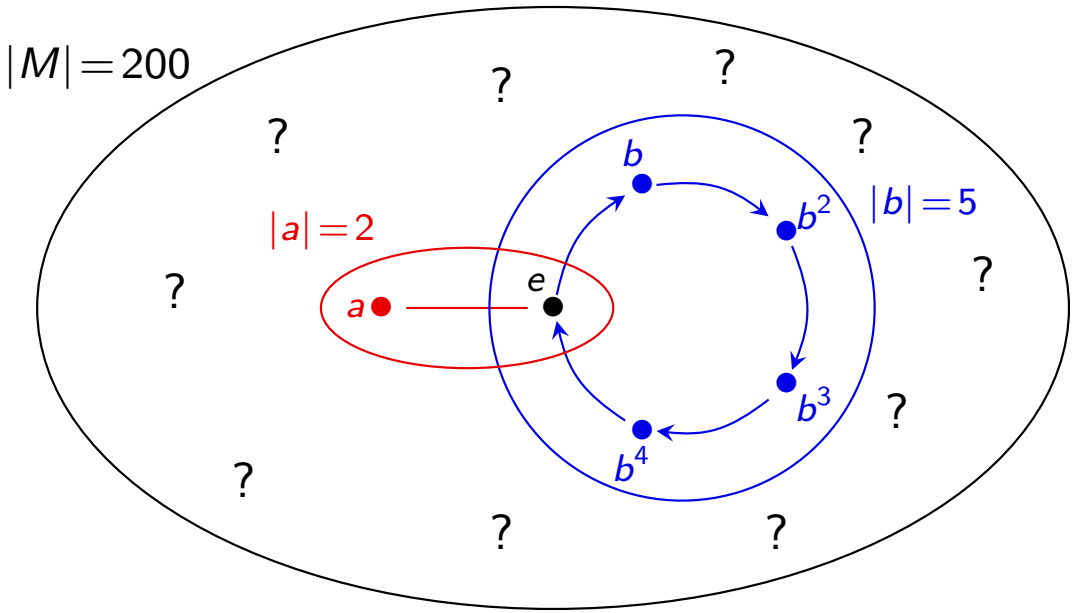
If p is a prime number dividing $|G|$, then G has an element g of order p.

Our mystery group of order 200

Since our mystery group M has order $|M| = 2^3 \cdot 5^2 = 200$, Cauchy's theorem tells us that:

- M has an element a of order 2;
- M has an element b of order 5;

Also, by Lagrange's theorem, $\langle a \rangle \cap \langle b \rangle = \{e\}$.



The 1st 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 p-subgroup with fewer than p^n elements sits inside one of the larger p-subgroups.

The First Sylow Theorem is in a sense, a generalization of Cauchy's theorem. Here is a comparison:

Cauchy's Theorem	First Sylow Theorem
If p divides $\|G\|$, then ...	*If p^k divides $\|G\|$, then ...*
There is a subgroup of order p	There is a subgroup of order p^k
which is cyclic and has no non-trivial proper subgroups.	which has subgroups of order $1, p, p^2 \ldots p^k$.
G contains an element of order p	G might not contain an element of order p^k.

The 1st Sylow Theorem: Existence of p-subgroups

Proof

The trivial subgroup $\{e\}$ has order $p^0 = 1$.

Big idea: Suppose we're given a subgroup $H < G$ of order $p^i < p^n$. We will construct a subgroup H' of order p^{i+1}.

By the normalizer lemma, $H \lneq N_G(H)$, and the order of the quotient group $N_G(H)/H$ is a multiple of p.

By Cauchy's Theorem, $N_G(H)/H$ contains an element (a coset!) of order p. Call this element aH. Note that $\langle aH \rangle$ is cyclic of order p.

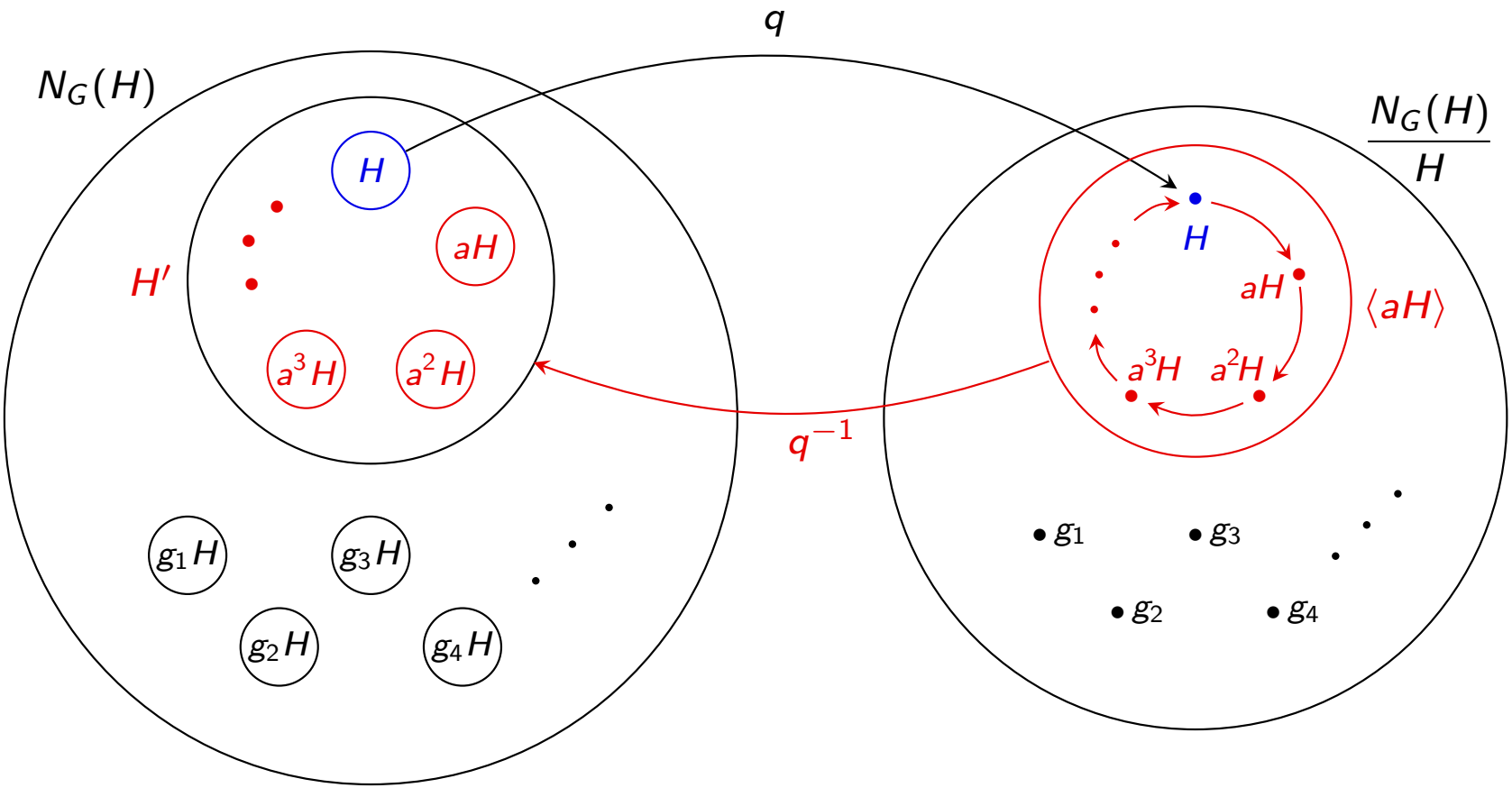
Claim: The preimage of $\langle aH \rangle$ under the quotient $q \colon N_G(H) \to N_G(H)/H$ is the subgroup H' we seek.

The preimages $q^{-1}(H)$, $q^{-1}(aH)$, $q^{-1}(a^2H)$, $\ldots$, $q^{-1}(a^{p-1}H)$ are all distinct cosets of H in $N_G(H)$, each of size p^i.

Thus, the preimage $H' = q^{-1}(\langle aH \rangle)$ contains $p \cdot |H| = p^{i+1}$ elements. $\square$

The 1st Sylow Theorem: Existence of p-subgroups

Here is a picture of how we found the group $H' = q^{-1}(\langle aH \rangle)$.

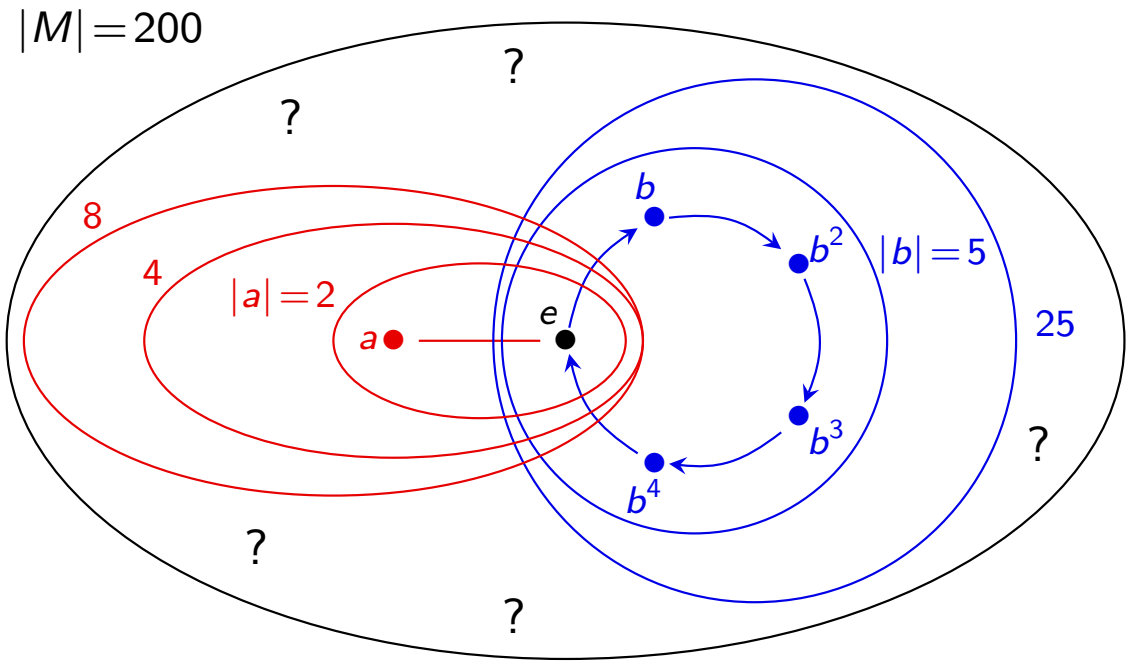


Since $|H| = p^i$, the subgroup $H' = \bigcup_{k=0}^{p-1} a^k H$ contains $p \cdot |H| = p^{i+1}$ elements.

Our unknown group of order 200

We now know a little bit more about the structure of our mystery group of order $|M| = 2^3 \cdot 5^2$:

- M has a 2-subgroup P_2 of order $2^3 = 8$;
- M has a 5-subgroup P_5 of order $25 = 5^2$;
- Each of these subgroups contains a nested chain of p-subgroups, down to the trivial group, $\{e\}$.



The 2nd Sylow Theorem: Relationship among p-subgroups

Definition

A subgroup $H < G$ of order p^n, where $|G| = p^n \cdot m$ with $p \nmid m$ is called a Sylow p-subgroup of G. Let $\text{Syl}_p(G)$ denote the set of Sylow p-subgroups of G.

Second Sylow Theorem

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

Proof

Let $H < G$ be any Sylow p-subgroup of G, and let $S = G/H = \{Hg \mid g \in G\}$, the set of right cosets of H.

Pick *any other* Sylow p-subgroup K of G. (If there is none, the result is trivial.)

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

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

The 2nd Sylow Theorem: All Sylow p-subgroups are conjugate

Proof

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

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

Thus, if ϕ has a fixed point Hg, then H and K are conjugate by g, and we're done!

All we need to do is show that $|\operatorname{Fix}(\phi)| \not\equiv_p 0$.

By the p-group Lemma, $|\operatorname{Fix}(\phi)| \equiv_p |S|$. Recall that $|S| = [G, H]$.

Since H is a Sylow p-subgroup, $|H| = p^n$. By Lagrange's Theorem,

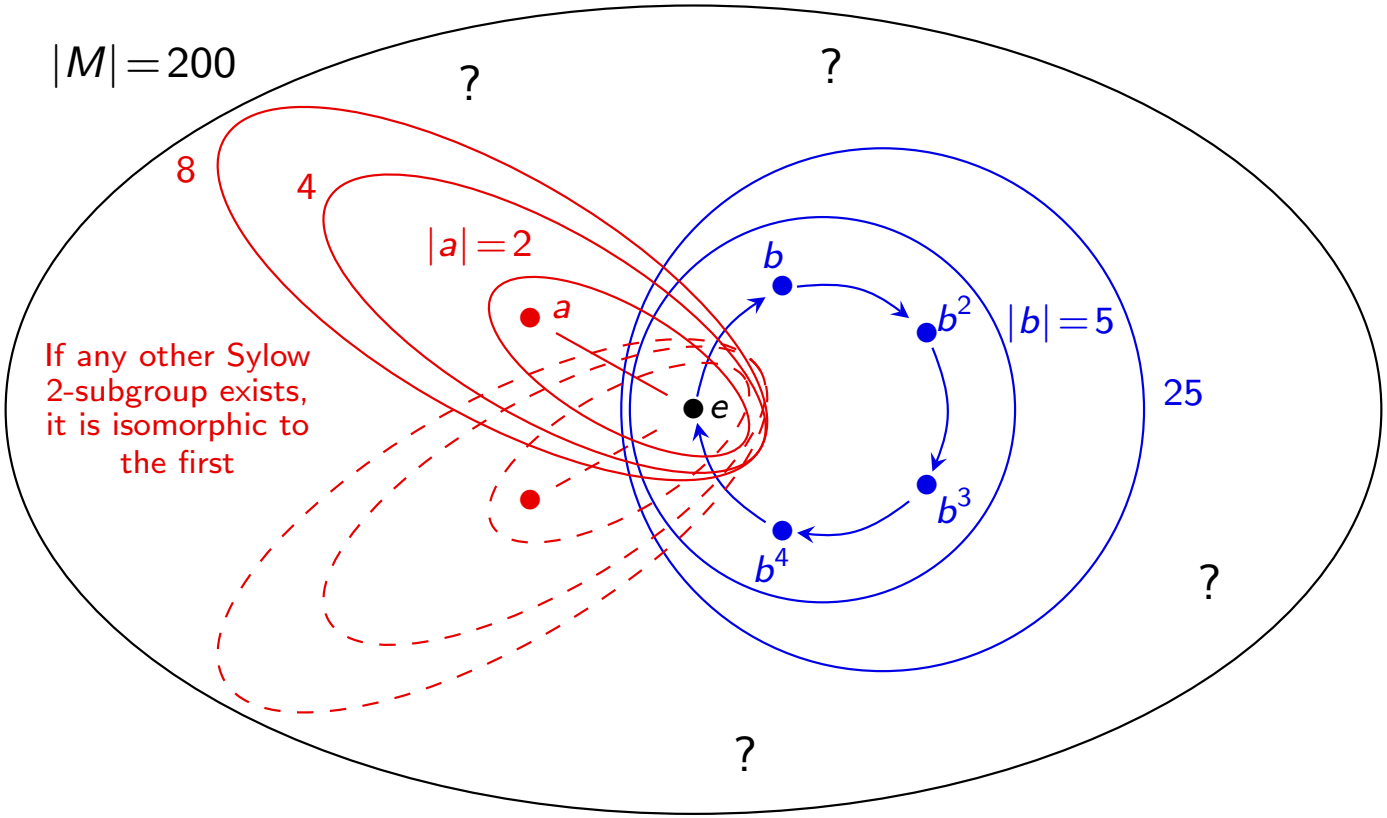
$$|S| = [G\colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^n} = m, \qquad p \nmid m\,.$$

Therefore, $|\operatorname{Fix}(\phi)| \equiv_p m \not\equiv_p 0$. □

Our unknown group of order 200

We now know even more about the structure of our mystery group M, of order $|M| = 2^3 \cdot 5^2$:

- If M has any other Sylow 2-subgroup, it is isomorphic to P_2;
- If M has any other Sylow 5-subgroup, it is isomorphic to P_5.



The 3rd 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

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

$$\phi(g) = \text{the permutation sending each } H \text{ to } g^{-1}Hg.$$

By the Second Sylow Theorem, all Sylow p-subgroups are conjugate! Thus there is only one orbit, $\text{Orb}(H)$, of size $n_p = |S|$.

By the Orbit-Stabilizer Theorem,

$$\underbrace{|\text{Orb}(H)|}_{=n_p} \cdot |\text{Stab}(H)| = |G| \qquad \Longrightarrow \qquad n_p \text{ divides } |G|\,.$$

The 3rd Sylow Theorem: Number of p-subgroups

Proof (cont.)

Now, pick any $H \in \mathrm{Syl}_p(G) = S$. The group H acts on S by conjugation, via $\theta\colon H \to \mathrm{Perm}(S)$, where

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

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

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

We know that:

- H and K are Sylow p-subgroups of G, but also of $N_G(K)$.
- Thus, H and K are conjugate in $N_G(K)$. (2nd Sylow Thm.)
- $K \lhd N_G(K)$, thus the only conjugate of K in $N_G(K)$ is itself.

Thus, $K = H$. That is, $\mathrm{Fix}(\theta) = \{H\}$ contains only 1 element.

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

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 $p, p^2, \ldots, p^n$.

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 $|\operatorname{Orb}(s)| \cdot |\operatorname{Stab}(s)| = |G|$.

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

To summarize, we used:

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

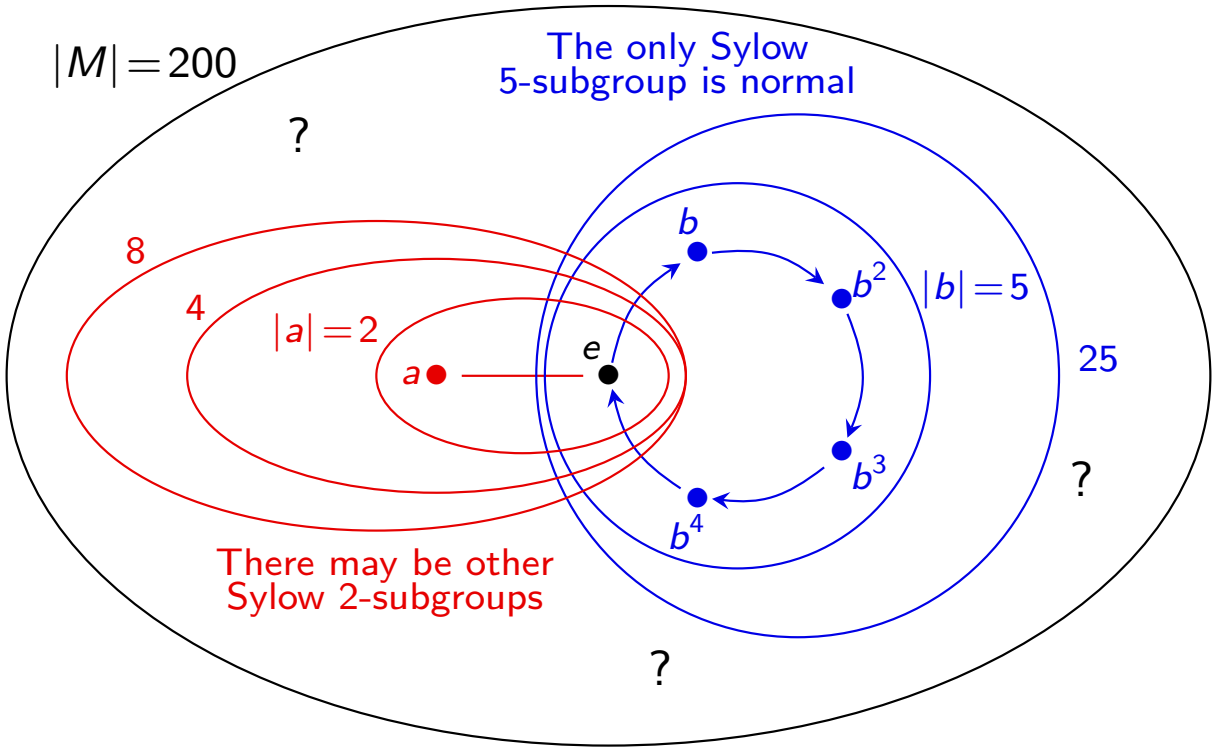
S3a The action of G on $S = \operatorname{Syl}_p(G)$, by conjugation.

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

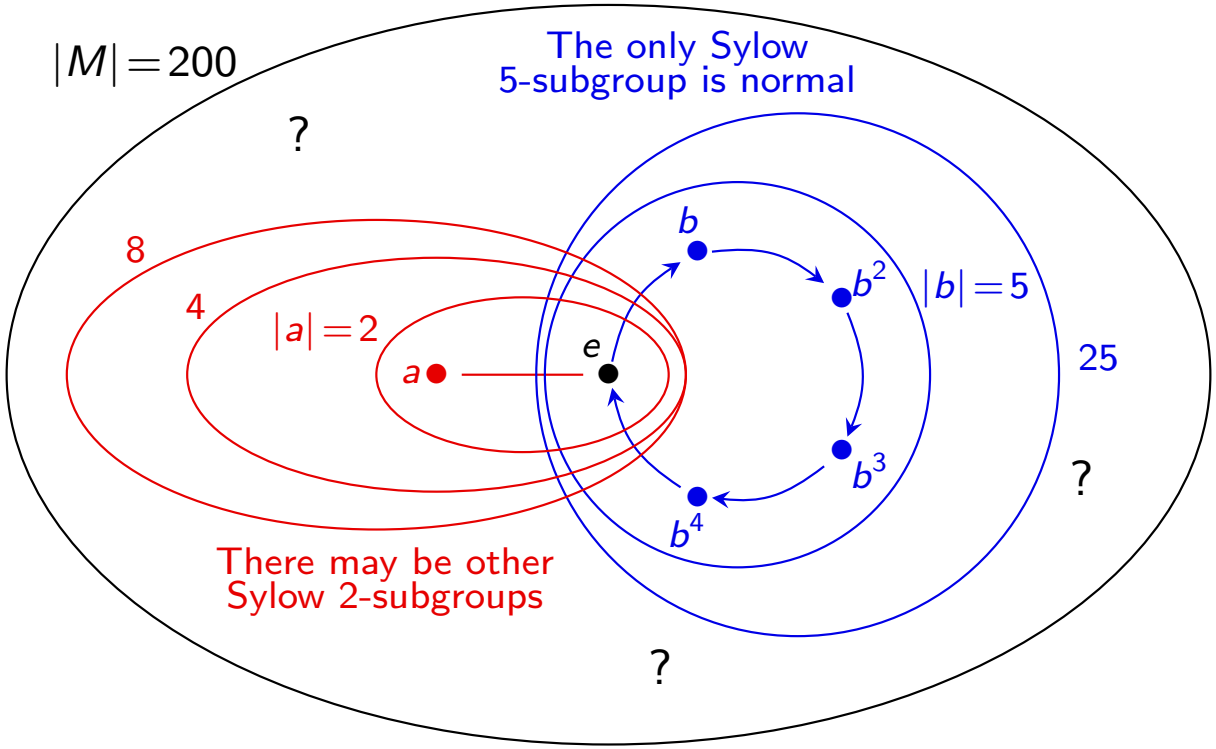
Our unknown group of order 200

We now know a little bit more about the structure of our mystery group M, of order $|M| = 2^3 \cdot 5^2 = 200$:

- $n_5 \mid 8$, thus $n_5 \in \{1, 2, 4, 8\}$. But $n_5 \equiv_5 1$, so $n_5 = 1$.
- $n_2 \mid 25$ and is odd. Thus $n_2 \in \{1, 5, 25\}$.
- We conclude that M has a unique (and hence normal) Sylow 5-subgroup P_5 (of order $5^2 = 25$), and either 1, 5, or 25 Sylow 2-subgroups (of order $2^3 = 8$).



Our unknown group of order 200



Suppose M has a subgroup isomorphic to D_4.

This would be a Sylow 2-subgroup. Since all of them are conjugate, M *cannot* contain a subgroup isomorphic to Q_4, $C_4 \times C_2$, or C_8!

In particular, M cannot even contain an element of order 8. (Why?)