p-groups and the Sylow theorems!

Spencer Bagley

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

21 Apr 2025

Overview

Intuitively, a group action occurs when a group G "naturally permutes" a set S *of states*.

Formal definition

A group G acts on a set S if there is a homomorphism $\phi\colon G \longrightarrow \mathrm{Perm}(S)$.
We'll use right group actions,
and we'll write $s.\phi(g)$ to denote "where pushing the g-button sends state s."

Definition

A set S with a (right) action by G is called a (right) G-set.

Big ideas

- An action $\phi\colon G \longrightarrow \mathrm{Perm}(S)$ endows S with an **algebraic structure**.
- *Action graphs are to G-sets, like how Cayley graphs are to groups.*

Notation

Throughout, we'll denote identity elements by $1 \in G$ and $e \in \mathrm{Perm}(S)$.

Five features of every group action

Every group action has **five fundamental features** that we will always try to understand.

	local (about an s or a g)	global (about the whole action ϕ)
subsets of S	$\mathrm{orb}(s)$ $\mathrm{fix}(g)$	$\mathrm{Fix}(\phi) = \bigcap_{g \in G} \mathrm{fix}(g)$
subgroups of G	$\mathrm{stab}(s)$	$\mathrm{Ker}(\phi) = \bigcap_{s \in S} \mathrm{stab}(s)$

"Duality:" columns vs. rows in the fixed-point table:

- the stablizers can be read off the columns: *group elements that fix $s \in S$*
- the kernel is the rows with a check in every column
- the fixators can be read off the rows: *set elements fixed by $g \in G$*
- the fixed points are the columns with a check in every row

More applications of group actions!

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \ldots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \dots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \dots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi \colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \dots, x_p) \xmapsto{\phi(1)} (x_2, x_3 \dots, x_p, x_1)\,.$$

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \ldots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \ldots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi\colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \ldots, x_p) \xmapsto{\phi(1)} (x_2, x_3 \ldots, x_p, x_1)\,.$$

The set P is partitioned into orbits, each of size $|\mathrm{orb}(s)| = [\mathbb{Z}_p : \mathrm{stab}(s)] = 1$ or p.

The only way that the orbit of $(x_1, x_2, \ldots, x_p)$ can have size 1 is if $x_1 = \cdots = x_p$.

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \ldots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \ldots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi \colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \ldots, x_p) \xmapsto{\phi(1)} (x_2, x_3 \ldots, x_p, x_1)\,.$$

The set P is partitioned into orbits, each of size $|\mathbf{orb}(s)| = [\mathbb{Z}_p : \mathbf{stab}(s)] = 1$ or p.

The only way that the orbit of $(x_1, x_2, \ldots, x_p)$ can have size 1 is if $x_1 = \cdots = x_p$.

Clearly, $(e, \ldots, e) \in P$ is a fixed point.

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \dots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \dots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi \colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \dots, x_p) \xmapsto{\phi(1)} (x_2, x_3 \dots, x_p, x_1)\,.$$

The set P is partitioned into orbits, each of size $|\mathbf{orb}(s)| = [\mathbb{Z}_p : \mathbf{stab}(s)] = 1$ or p.

The only way that the orbit of $(x_1, x_2, \dots, x_p)$ can have size 1 is if $x_1 = \cdots = x_p$.

Clearly, $(e, \dots, e) \in P$ is a fixed point.

The $|G|^{p-1} - 1$ other elements in P sit in orbits of size 1 or p.

Since $p \nmid |G|^{p-1} - 1$, there must be other orbits of size 1.

A creative application of a group action

Cauchy's theorem

If p is a prime dividing $|G|$, then G has an element (and hence a subgroup) of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e:

$$(x_1, x_2, \ldots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \ldots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi\colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \ldots, x_p) \xrightarrow{\phi(1)} (x_2, x_3 \ldots, x_p, x_1)\,.$$

The set P is partitioned into orbits, each of size $|\mathrm{orb}(s)| = [\mathbb{Z}_p : \mathrm{stab}(s)] = 1$ or p.

The only way that the orbit of $(x_1, x_2, \ldots, x_p)$ can have size 1 is if $x_1 = \cdots = x_p$.

Clearly, $(e, \ldots, e) \in P$ is a fixed point.

The $|G|^{p-1} - 1$ other elements in P sit in orbits of size 1 or p.

Since $p \nmid |G|^{p-1} - 1$, there must be other orbits of size 1. Thus, some $(x, \ldots, x) \in P$, with $x \neq e$ satisfies $x^p = e$. $\square$

Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

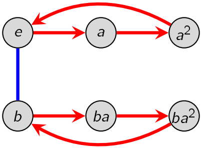
- an element a of order 3
- an element b of order 2.

Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

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

Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":

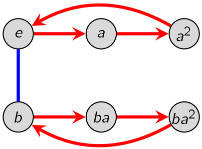


Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

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

Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":



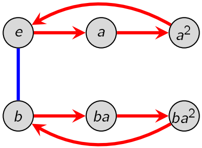
It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

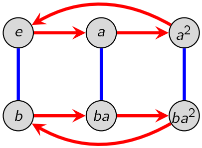
- an element a of order 3
- an element b of order 2.

Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":



It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

$C_6 \cong C_2 \times C_3$

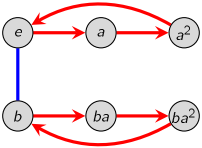


Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

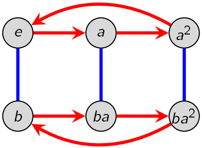
- an element a of order 3
- an element b of order 2.

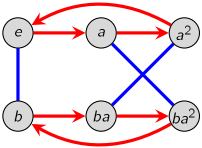
Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":



It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

$C_6 \cong C_2 \times C_3$





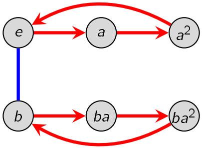
D_3

Classification of groups of order 6

By Cauchy's theorem, every group of order 6 must have:

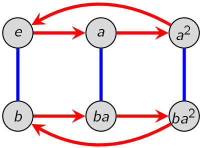
- an element a of order 3
- an element b of order 2.

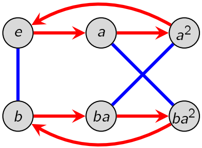
Clearly, $G = \langle a, b \rangle$, and so G must have the following "partial Cayley graph":



It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

$C_6 \cong C_2 \times C_3$





D_3

Exercise. Suppose that $|G| = pq$, where $p < q$ are primes and p doesn't divide $q - 1$. Prove that G is cyclic.

p-groups and the Sylow theorems!

p-groups and the Sylow theorems

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.

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

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

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

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.

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

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.

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

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**: Strong restrictions on the number of p-subgroups a group can have.

p-groups and the Sylow theorems

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.

Can you tell me some examples of 2-groups?

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.)

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**: 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.

Groups of order $12 = 2^2 \cdot 3^1$

Head to LMFDB and look at subgroup lattices of each of the groups of order 12. What do you notice about the p-subgroups?

Groups of order $12 = 2^2 \cdot 3^1$

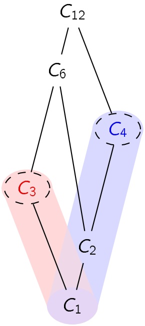
Head to LMFDB and look at subgroup lattices of each of the groups of order 12. What do you notice about the p-subgroups?

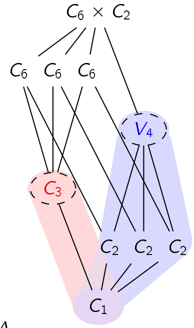
Sylow theorems:

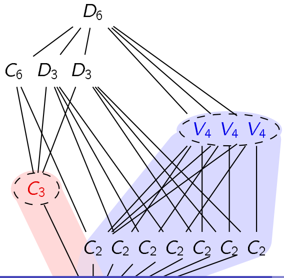
p-subgroups come in "towers."

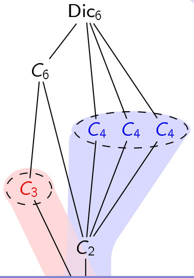
2-subgroups blue; 3-subgroups red.

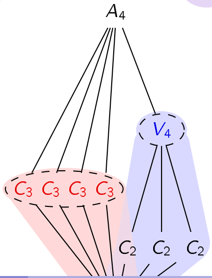
The tops of the towers are conjugate; there are restrictions on the size of their conjugacy classes.











p-groups

Before we introduce the Sylow theorems, we need to better understand p-groups.

Before we introduce the Sylow theorems, we need to better understand p-groups.

p-group Lemma

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

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

Proof (sketch)

p-groups

Before we introduce the Sylow theorems, we need to better understand p-groups.

p-group Lemma

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

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

Proof (sketch)

Suppose $|G| = p^n$.

p-groups

Before we introduce the Sylow theorems, we need to better understand p-groups.

p-group Lemma

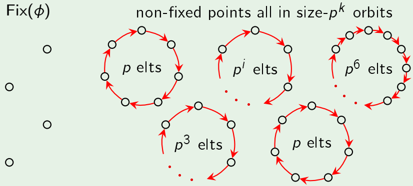
If a p-group G acts on a set S via $\phi \colon G \to \mathbf{Perm}(S)$, then

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

Proof (sketch)

Suppose $|G| = p^n$.

By the orbit-stabilizer theorem, the only possible orbit sizes are $1, p, p^2, \ldots, p^n$.



p-groups

Before we introduce the Sylow theorems, we need to better understand p-groups.

p-group Lemma

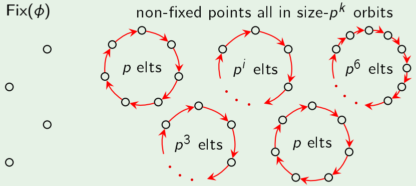
If a p-group G acts on a set S via $\phi\colon G \to \mathbf{Perm}(S)$, then

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

Proof (sketch)

Suppose $|G| = p^n$.

By the orbit-stabilizer theorem, the only possible orbit sizes are $1, p, p^2, \ldots, p^n$.



A lot of proofs about p-groups go like this: two things are equal mod p; set up some action of G on S; one of the things is the number of fixed points; the other thing is the size of S.

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Approach:

- Let H (not G!) act on the (right) cosets of H by (right) multiplication.

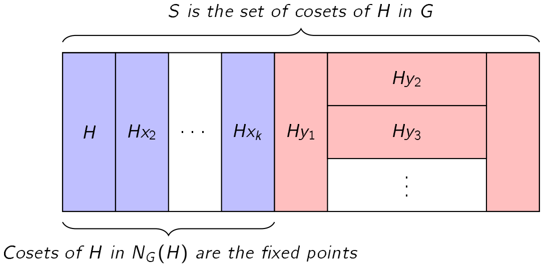
Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Approach:

- Let H (not G!) act on the (right) cosets of H by (right) multiplication.



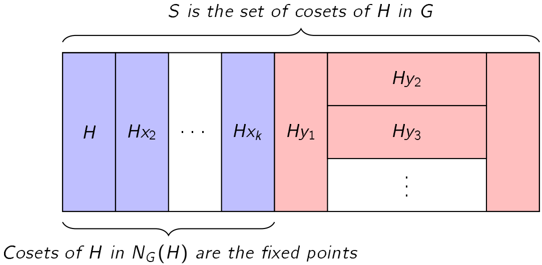
Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Approach:

- Let H (not G!) act on the (right) cosets of H by (right) multiplication.



- Apply our lemma: $|\,\mathrm{Fix}(\phi)| \equiv_p |S|$.

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H \backslash G = \{Hx \mid x \in G\}$.

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H \backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi \colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi \colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$Hxh = Hx, \quad \forall h \in H \qquad \Longleftrightarrow \qquad Hxhx^{-1} = H, \quad \forall h \in H$$

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \quad &\Longleftrightarrow \quad Hxhx^{-1} = H, \quad \forall h \in H \\ &\Longleftrightarrow \quad xhx^{-1} \in H, \quad \forall h \in H \end{aligned}$$

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \qquad &\Longleftrightarrow \qquad Hxhx^{-1} = H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad xhx^{-1} \in H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad x \in N_G(H). \end{aligned}$$

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \qquad &\Longleftrightarrow \qquad Hxhx^{-1} = H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad xhx^{-1} \in H, \quad \forall h \in H \\ &\Longleftrightarrow \qquad x \in N_G(H)\,. \end{aligned}$$

Therefore, $|\mathrm{Fix}(\phi)| = [N_G(H)\colon H]$, and $|S| = [G : H]$.

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \quad &\iff \quad Hxhx^{-1} = H, \quad \forall h \in H \\ &\iff \quad xhx^{-1} \in H, \quad \forall h \in H \\ &\iff \quad x \in N_G(H). \end{aligned}$$

Therefore, $|\mathrm{Fix}(\phi)| = [N_G(H)\colon H]$, and $|S| = [G : H]$. By our p-group Lemma,

$$|\mathrm{Fix}(\phi)| \equiv_p |S| \quad \Longrightarrow$$

Normalizer lemma, Part 1

If H is a p-subgroup of G, then

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

Proof

Let $S = H\backslash G = \{Hx \mid x \in G\}$. The group H acts on S by **right-multiplication**, via $\phi\colon H \to \mathrm{Perm}(S)$, where

$$\phi(h) = \text{the permutation sending each } Hx \text{ to } Hxh.$$

The fixed points of ϕ are the cosets Hx in the normalizer $N_G(H)$:

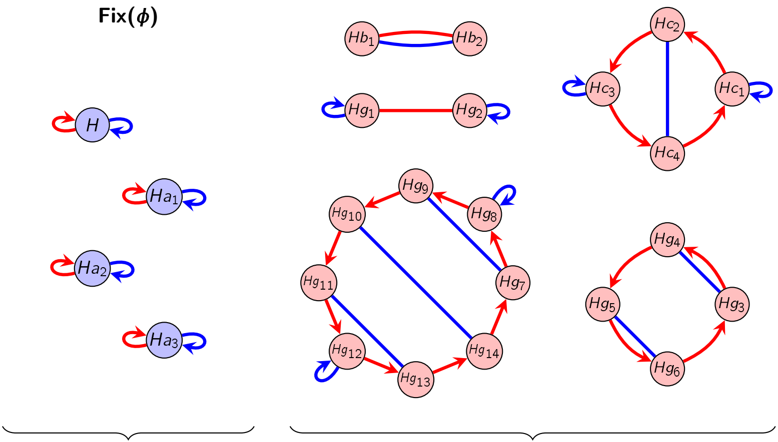
$$\begin{aligned} Hxh = Hx, \quad \forall h \in H \quad &\Longleftrightarrow \quad Hxhx^{-1} = H, \quad \forall h \in H \\ &\Longleftrightarrow \quad xhx^{-1} \in H, \quad \forall h \in H \\ &\Longleftrightarrow \quad x \in N_G(H)\,. \end{aligned}$$

Therefore, $|\operatorname{Fix}(\phi)| = [N_G(H)\colon H]$, and $|S| = [G : H]$. By our p-group Lemma,

$$|\operatorname{Fix}(\phi)| \equiv_p |S| \quad \Longrightarrow \quad [N_G(H)\colon H] \equiv_p [G\colon H]. \qquad \square$$

p-groups

Here is a picture of the action of the p-subgroup H (for $p = 2$) on the set $S = H\backslash G$, from the proof of the normalizer lemma.



The fixed points are the cosets in $N_G(H)$

Cosets not in $N_G(H)$ are in orbits of order p^i, for various $i \geq 1$

p-subgroups

Recall that $H \leq N_G(H)$ (always), and H is fully unnormal if $H = N_G(H)$.

p-subgroups

Recall that $H \leq N_G(H)$ (always), and H is fully unnormal if $H = N_G(H)$.

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.

p-subgroups

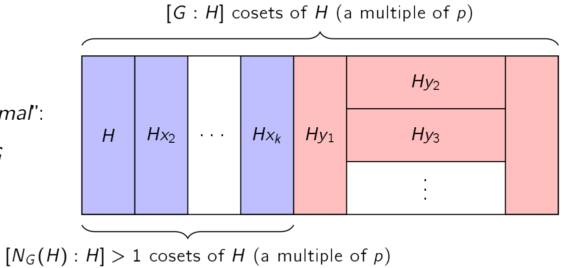
Recall that $H \leq N_G(H)$ (always), and H is fully unnormal if $H = N_G(H)$.

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.

H is not "*fully unnormal*":

$$H \lneq N_G(H) \leq G$$



p-subgroups

Recall that $H \leq N_G(H)$ (always), and H is fully unnormal if $H = N_G(H)$.

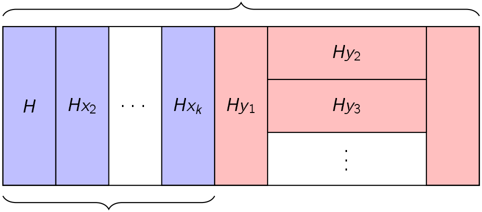
Normalizer lemma, Part 2

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.

H is not "*fully unnormal*":

$$H \lneq N_G(H) \leq G$$

$[G : H]$ cosets of H (a multiple of p)



$[N_G(H) : H] > 1$ cosets of H (a multiple of p)

Important corollaries

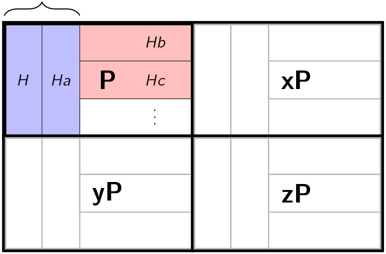
- p-groups cannot have any fully unnormal subgroups (i.e., $H \lneq N_G(H)$).
- In *any* finite group, the only fully unnormal p-subgroups are maximal.

Normalizers of p-subgroups

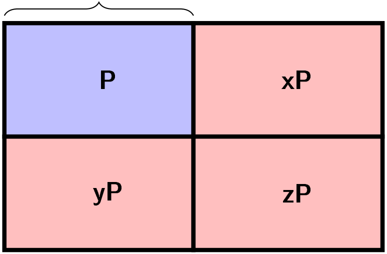
Let H be properly contained in a maximal p-subgroup $P \lneq G$.

- The normalizer of H *must* grow in P (and hence in G)
- The normalizer of P *need not* grow in G.

$\overbrace{H \lneq N_P(H)} \leq N_G(H)$



it may happen that $P = N_G(P)$



Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad \pi \colon g \longmapsto gH\,.$$

Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad \pi \colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H) \colon H]$, the number of cosets of H in $N_G(H)$.

Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad \pi \colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H) \colon H]$, the number of cosets of H in $N_G(H)$.

By the normalizer lemma Part 1, $[N_G(H) \colon H] \equiv_p [G \colon H]$.

Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad \pi \colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H) \colon H]$, the number of cosets of H in $N_G(H)$.

By the normalizer lemma Part 1, $[N_G(H) \colon H] \equiv_p [G \colon H]$. By Lagrange's theorem,

$$[N_G(H) \colon H] \equiv_p [G \colon H] = \frac{|G|}{|H|}$$

Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi\colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad \pi\colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H)\colon H]$, the number of cosets of H in $N_G(H)$.

By the normalizer lemma Part 1, $[N_G(H)\colon H] \equiv_p [G\colon H]$. By Lagrange's theorem,

$$[N_G(H)\colon H] \equiv_p [G\colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^i} = p^{n-i} m \equiv_p 0.$$

Proof of the normalizer lemma

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.

Proof

Since $H \trianglelefteq N_G(H)$, we can create the quotient map

$$\pi \colon N_G(H) \longrightarrow N_G(H)/H\,, \qquad\qquad \pi \colon g \longmapsto gH\,.$$

The size of the quotient group is $[N_G(H) \colon H]$, the number of cosets of H in $N_G(H)$.

By the normalizer lemma Part 1, $[N_G(H) \colon H] \equiv_p [G \colon H]$. By Lagrange's theorem,

$$[N_G(H) \colon H] \equiv_p [G \colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^i} = p^{n-i} m \equiv_p 0.$$

Therefore, $[N_G(H) \colon H]$ is a multiple of p, so $N_G(H)$ must be strictly larger than H. $\square$

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 $|G|$?

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."

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?.*

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

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:

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?

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?

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?

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 $p \nmid m$.

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 $|G|$.

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.

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$.

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$.

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

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*".

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$.

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.

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$.

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.

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$.

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.

Our unknown group of order 12

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

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:

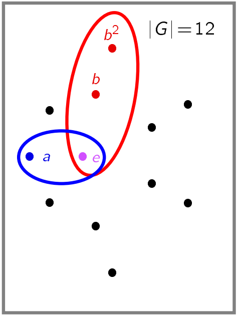
- an element a of order 2, and

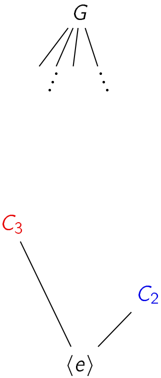
Our unknown group of order 12

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 $|G| = 12$, we will unconver as much about its structure as we can.

The 1^{st} 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

The 1^{st} 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

Take any $H \leq G$ with $|H| = p^i < p^n$.

The 1^{st} 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

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

The 1^{st} Sylow theorem: existence of p-subgroups

First Sylow theorem

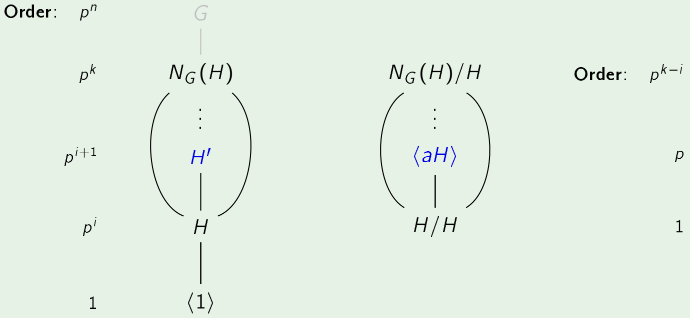
G has a subgroup of order p^k, for each p^k dividing $|G|$.

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

Proof

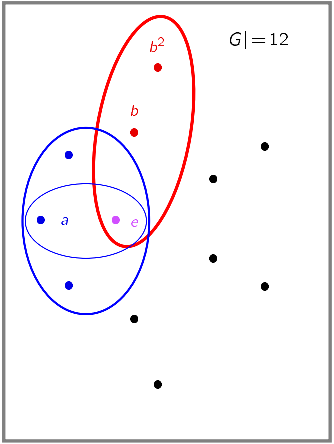
Take any $H \leq G$ with $|H| = p^i < p^n$. We know $H \trianglelefteq N_G(H)$ and p divides $|N_G(H)/H|$.

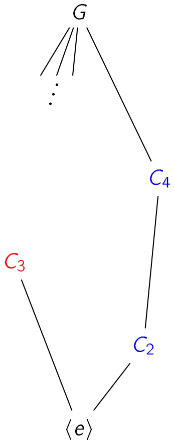
Find an element aH of order p. The union of cosets in $\langle aH \rangle$ is a subgroup of order p^{i+1}.

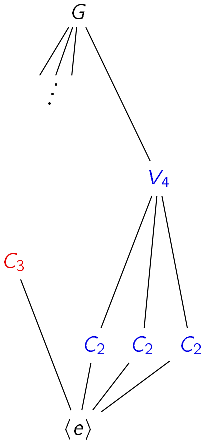


Our unknown group of order 12

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 2^{nd} Sylow theorem: relationship among p-subgroups

Second Sylow theorem

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

The 2^{nd} 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.

The 2^{nd} 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 2nd Sylow theorem: relationship among p-subgroups

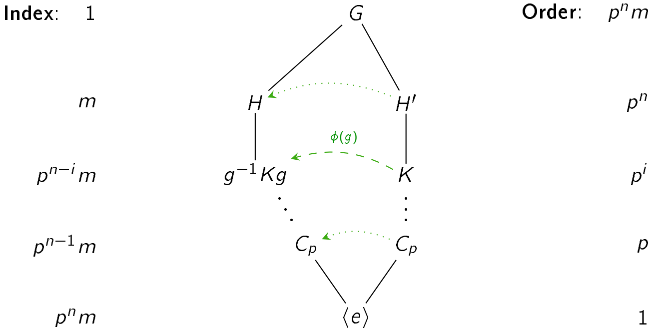
Second Sylow theorem

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 2^{nd} 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 2^{nd} 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

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

The 2nd 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

$$Hgk = Hg\,, \quad \forall k \in K$$

The 2^{nd} 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

$$Hgk = Hg\,, \quad \forall k \in K \qquad \Longleftrightarrow \qquad Hgkg^{-1} = H\,, \quad \forall k \in K$$

The 2^{nd} 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

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

The 2^{nd} 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

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

The 2^{nd} 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 $\phi \colon K \to \mathsf{Perm}(S)$, 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

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

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

The 2^{nd} 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 $|\mathrm{Fix}(\phi)| \not\equiv_p 0$.

The 2^{nd} 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

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

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,

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

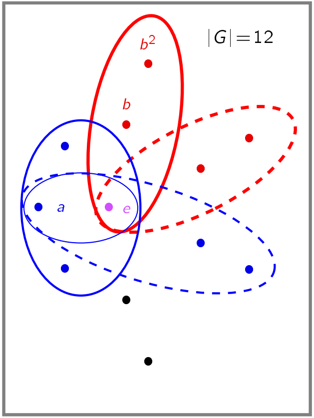
Our unknown group of order 12

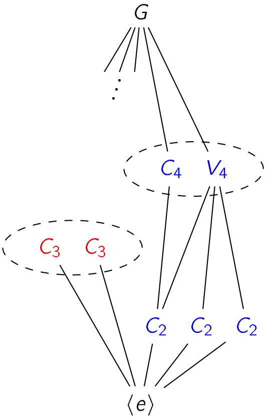
By the second Sylow theorem, all Sylow p-subgroups are conjugate, and hence isomorphic.

Our unknown group of order 12

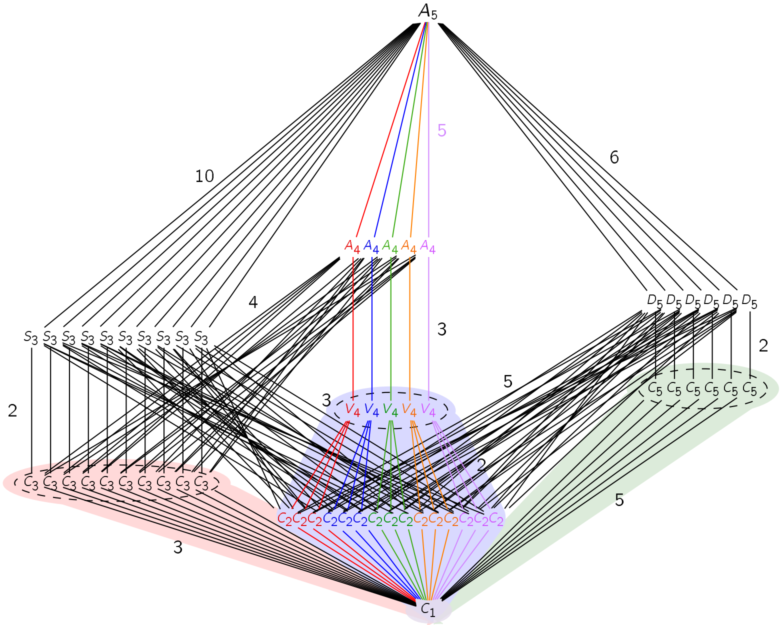
By the second Sylow theorem, all Sylow p-subgroups are conjugate, and hence isomorphic.

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





Example: A_5 has no nontrival proper normal subgroups



The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal.

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

Proposition

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

Proof

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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 $N_G(N_G(P)) = N_G(P)$.

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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 $N_G(P)$.

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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 $N_G(P)$.

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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., $x \in N_G(N_G(P))$).

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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.

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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

$$P \leq N_G(P) \qquad \Longrightarrow$$

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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

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

The normalizer of the normalizer

Notice how in A_5:

- all Sylow p-subgroups are moderately unnormal
- the normalizer of each Sylow p-subgroup is fully unnormal. That is:

$$N_G(N_G(P)) = N_G(P)$$

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 3rd Sylow theorem: number of p-subgroups

Third Sylow theorem

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

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

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 $|G| = p^n \cdot m$.)

The 3^{rd} 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 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

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

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

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

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.*

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

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

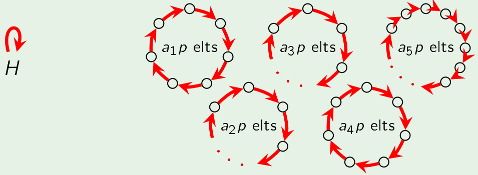
The subgroup H acts on $S = \mathrm{Syl}_p(G)$ by conjugation, via $\phi\colon G \to \mathrm{Perm}(S)$, where

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

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 3$^{\mathrm{rd}}$ Sylow theorem: number of p-subgroups

Proof (cont.)

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

The 3^{rd} Sylow theorem: number of p-subgroups

Proof (cont.)

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

Let $K \in \mathrm{Fix}(\phi)$.

The 3rd 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

$$h^{-1}Kh = K\,, \quad \forall h \in H$$

The 3rd 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

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

The 3rd 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

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

- H and K are p-Sylow in G, and in $N_G(K)$.

The 3[rd] 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.)

The 3rd 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 $N_G(K)$.

The 3rd 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, $\mathrm{Fix}(\phi) = \{H\}$.

The 3rd 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

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

- 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, $n_p := |S|$

The 3rd Sylow theorem: number of p-subgroups

Proof (cont.)

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

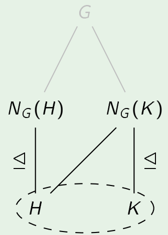
Let $K \in \mathrm{Fix}(\phi)$. Then $K \leq G$ is a Sylow p-subgroup satisfying

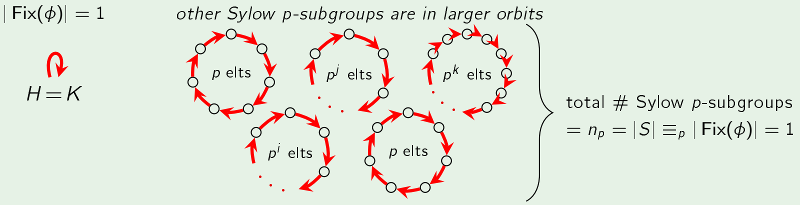
$$h^{-1}Kh = K, \quad \forall h \in H \quad \Longleftrightarrow \quad H \leq N_G(K) \leq G.$$

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

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:

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 $|\,\mathbf{orb}(s)| \cdot |\,\mathbf{stab}(s)| = |G|$.

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 $|\,\mathrm{orb}(s)| \cdot |\,\mathrm{stab}(s)| = |G|$.

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

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 $|\,\mathsf{orb}(s)| \cdot |\,\mathsf{stab}(s)| = |G|$.

(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 $K \in \mathsf{Syl}_p(G)$ on $S = H\backslash G$ by right multiplication for some other $H \in \mathsf{Syl}_p(G)$.

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

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.

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 $|\,\mathrm{orb}(s)| \cdot |\,\mathrm{stab}(s)| = |G|$.

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

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:

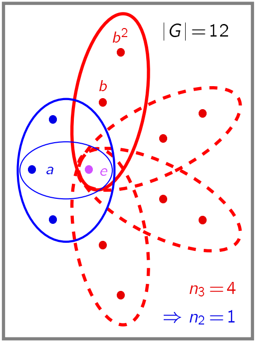
- n_3 Sylow 3-subgroups, each of order 3.

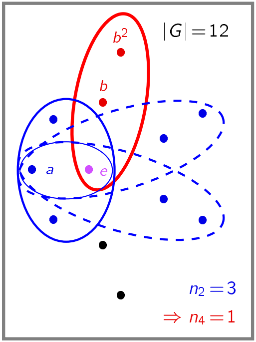
$$n_3 \mid 4, \qquad n_3 \equiv 1 \pmod 3 \qquad \Longrightarrow \qquad n_3 = 1 \text{ or } 4.$$

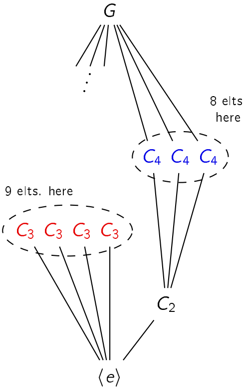
- n_2 Sylow 2-subgroups of order $2^2 = 4$.

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

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





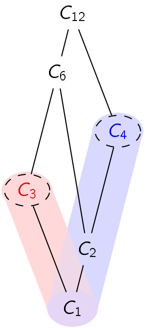


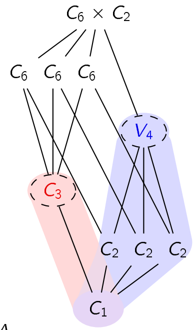
The five groups of order 12

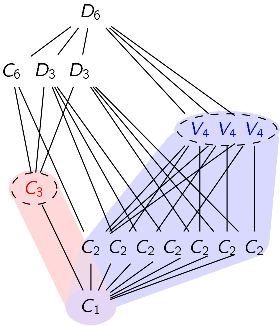
With a little work and the Sylow theorems, we can classify all groups of order 12.

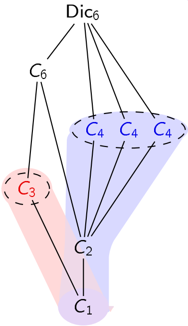
We've already seen them all. Here are their subgroup lattices.

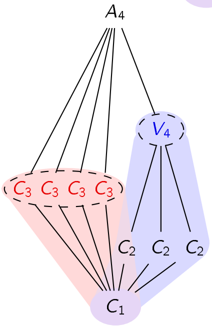
Note that *all* of these decompose as a direct or semidirect product of Sylow subgroups.











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 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.

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)."

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 $n_p = 1$).

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.

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.

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.

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.

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:

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 $n_7 \in \{1, 2, 3, 4, 6, 12\}$)

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 $n_7 \in \{1, 2, 3, 4, 6, 12\}$)
- $n_7 \equiv_7 1$.

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 $n_7 \in \{1, 2, 3, 4, 6, 12\}$)
- $n_7 \equiv_7 1$.

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. $\square$

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. □

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

- n_3 divides $2^2 \cdot 7 = 28$ and $n_3 \equiv_3 1$.

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. □

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 $n_3 \in \{1, \cancel{2}, 4, 7, \cancel{14}, 28\}$.

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. □

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 $n_2 \equiv_2 1$.

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.

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:

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 $n_{13} \in \{1, 3, 9, 27\}$)

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 $n_{13} \in \{1, 3, 9, 27\}$)
- $n_{13} \equiv_{13} 1$.

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 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, $P \cap Q = \{e\}$.

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 possibilities 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 $n_{13} = 27$.

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.

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.

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 $24 = 2^3 \cdot 3$.

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 $n_3 = \{1, 4\}$.

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: $[G : H] = 3$.

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.

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**:

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

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:

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

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 $|G| \nmid n!$. $\square$