Chapter 10: The Sylow Theorems

Matthew Macauley

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

Math 4120, Spring 2014

Overview

This chapter about one question:

What groups are there?

In Chapter 5, we saw five families of groups: cyclic, dihedral, abelian, symmetric, alternating.

In Chapter 8, 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.

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.

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 $|G|$.

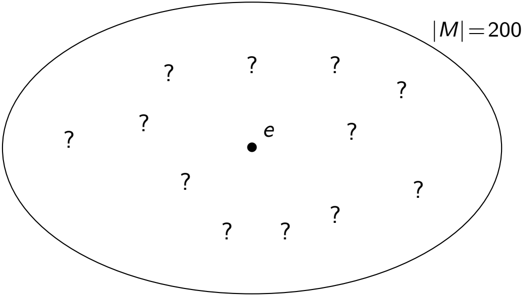
There are three Sylow theorems, and loosely speaking, they describe the following about a group's p-subgroups:

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 this chapter, 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

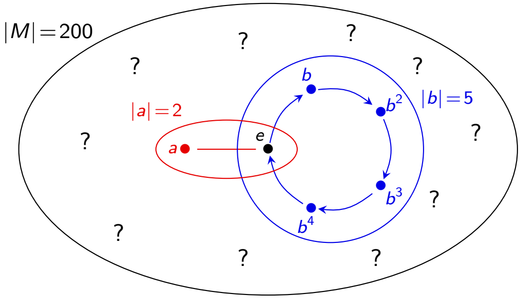
If p is a prime number dividing $|G|$, then G has an element g of order p.

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, $\langle a \rangle \cap \langle b \rangle = \{e\}$.



p-groups

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

Recall that a p-group is any group of order p^n. For example, C_1, C_4, V_4, D_4 and Q_4 are all 2-groups.

p-group Lemma

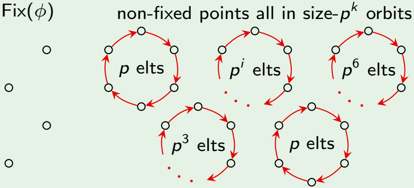
If a p-group G acts on a set S via $\phi\colon G \to \mathrm{Perm}(S)$, then

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

Proof (sketch)

Suppose $|G| = p^n$.

By the Orbit-Stabilizer theorem, the only possible orbit sizes are $1, p, p^2, \dots, p^n$.



p-groups

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 $S = G/H = \{Hx \mid x \in G\}$. 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 $N_G(H)$:

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

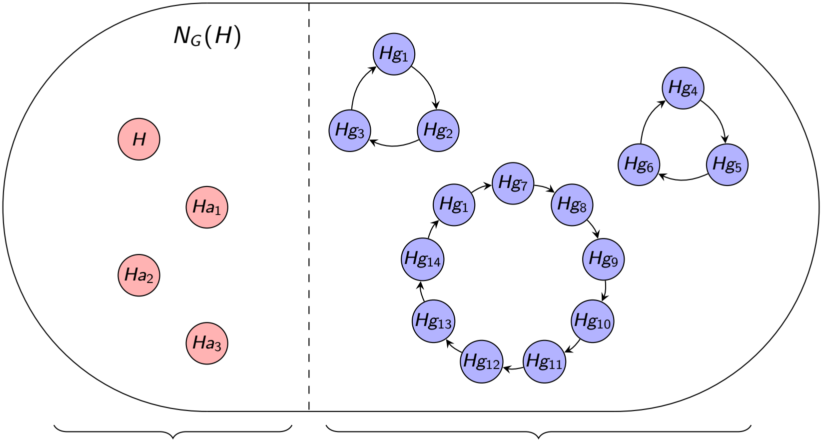
Therefore, $|\operatorname{Fix}(\phi)| = [N_G(H)\colon H]$, and $|S| = [G : H]$. By our p-group Lemma,

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

p-groups

Here is a picture of the action of the p-subgroup H on the set $S = G/H$, from the proof of the Normalizer Lemma.

$S = G/H =$ set of right cosets of H in G



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

Orbits of size > 1 are of various sizes dividing $|H|$, but all lie outside $N_G(H)$

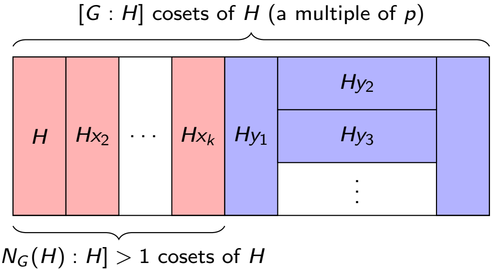
p-subgroups

The following result will be useful in proving the first Sylow theorem.

The 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.

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



Conclusions:

- $H = N_G(H)$ is impossible!
- p^{i+1} divides $|N_G(H)|$.

Proof of the normalizer lemma

The 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 $H \lhd N_G(H)$, we can create the quotient map

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

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. □

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 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 1^{st} 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.

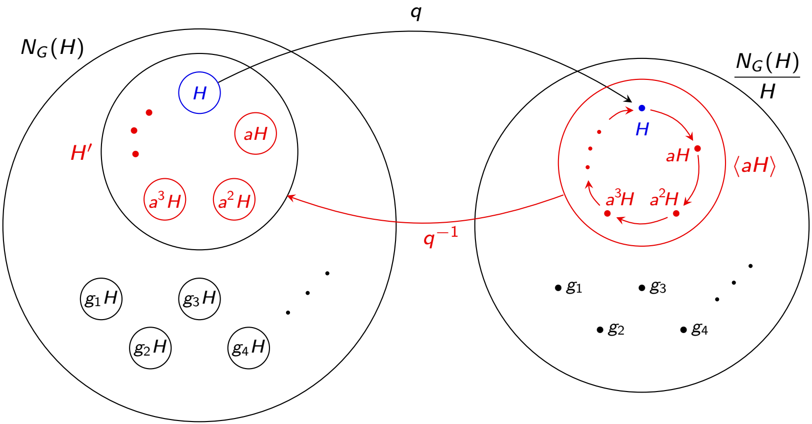
Claim: The preimage of $\langle aH \rangle$ under the quotient $q \colon N_G(H) \to N_G(H)/H$ is the subgroup H' we seek.

The preimages $q^{-1}(H)$, $q^{-1}(aH)$, $q^{-1}(a^2H)$, $\dots$, $q^{-1}(a^{p-1}H)$ 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 $H' = q^{-1}(\langle aH \rangle)$.

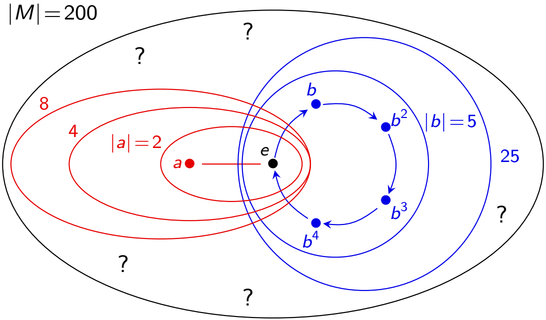


Since $|H| = p^i$, the subgroup $H' = \bigcup_{k=0}^{p-1} a^k H$ contains $p \cdot |H| = p^{i+1}$ elements.

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 2[nd] 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 $\mathrm{Syl}_p(G)$ 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 $S = G/H = \{gH \mid g \in G\}$, 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 $\phi\colon K \to \mathrm{Perm}(S)$, where

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

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

Proof

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

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

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

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

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

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

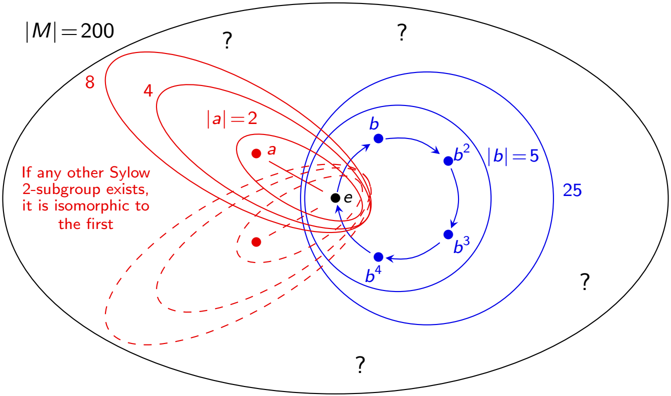
$$|S| = [G\colon H] = \frac{|G|}{|H|} = \frac{p^n m}{p^n} = m, \qquad p \nmid m\,.$$

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

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 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

The group G acts on $S = \mathrm{Syl}_p(G)$ by conjugation, via $\phi\colon G \to \mathrm{Perm}(S)$, 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, $\mathrm{Orb}(H)$, of size $n_p = |S|$.

By the Orbit-Stabilizer Theorem,

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

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, $n_p := |S| \equiv_p |\mathrm{Fix}(\theta)| = 1$. $\square$

Summary of the proofs of the Sylow Theorems

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

For the 2^{nd} and 3^{th} 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 $H \in \operatorname{Syl}_p(G)$.

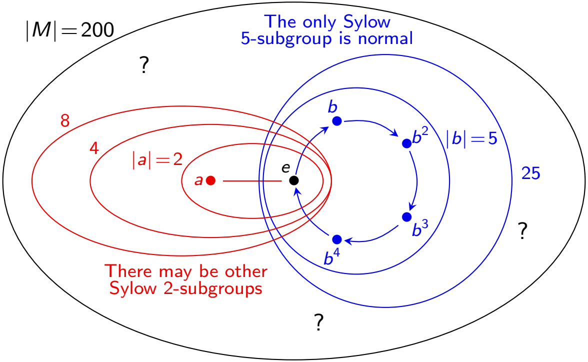
S3a The action of G on $S = \operatorname{Syl}_p(G)$, by conjugation.

S3b The action of $H \in \operatorname{Syl}_p(H)$ 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 $|M| = 2^3 \cdot 5^2 = 200$:

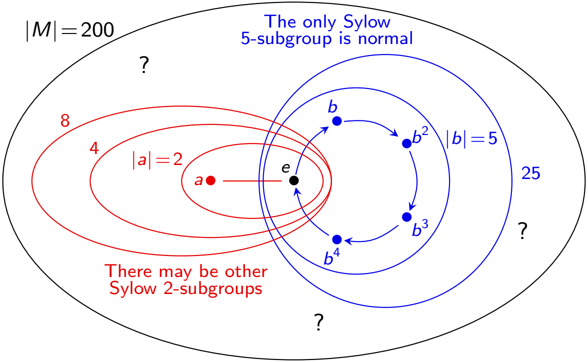
- $n_5 \mid 8$, thus $n_5 \in \{1, 2, 4, 8\}$. But $n_5 \equiv_5 1$, so $n_5 = 1$.
- $n_2 \mid 25$ and is odd. Thus $n_2 \in \{1, 5, 25\}$.
- We conclude that A has a unique (and hence normal) Sylow 5-subgroup P_5 (of order $5^2 = 25$), and either 1, 5, or 25 Sylow 2-subgroups (of order $2^3 = 8$).



Our unknown group of order 200

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 $2^3 = 8$).



Simple groups

Definition

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

Since all Sylow p-subgroups are conjugate, the following result is straightforward:

Proposition (HW)

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

The Sylow theorems are very useful for establishing statements like:

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

To do this, we usually just need to show that $n_p = 1$ for some p dividing $|G|$.

Since we established $n_5 = 1$ for our running example of a group of size $|M| = 200$, there are no simple groups of order 200.

Simple groups: an easy example

Tip

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

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 $n_2 \in \{1, 3, 7, 21\}$.

Simple groups: 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. $\square$

Simple groups: the hardest example

Proposition

If $H \lneq G$ and $|G|$ does not divide $[G:H]!$, then G cannot be simple.

Proof

Let G act on the **right cosets** of H (i.e., $S = G/H$) 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 the kernel of ϕ is the intersection of all conjugate subgroups of H:

$$\mathrm{Ker}\,\phi = \bigcap_{x \in G} x^{-1}Hx.$$

Notice that $\langle e\rangle \leq \mathrm{Ker}\,\phi \leq H \lneq G$, and $\mathrm{Ker}\,\phi \lhd G$.

If $\mathrm{Ker}\,\phi = \langle e\rangle$ then $\phi\colon G \hookrightarrow S_n$ is an embedding. But this is *impossible* because $|G|$ does not divide $|S_n| = [G:H]!$. $\square$

Corollary

There are no simple groups of order 24.

Theorem (classification of finite simple groups)

Every finite simple group is isomorphic to one of the following groups:

- A cyclic group $\mathbb{Z}_p$, with p prime;
- An alternating group A_n, with $n \geq 5$;
- A Lie-type Chevalley group: $\mathrm{PSL}(n, q)$, $\mathrm{PSU}(n, q)$, $\mathrm{PsP}(2n, p)$, and $P\Omega^{\epsilon}(n, q)$;
- A Lie-type group (twisted Chevalley group or the Tits group): $D_4(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(2^n)'$, $G_2(q)$, ${}^2G_2(3^n)$, ${}^2B(2^n)$;
- One of 26 exceptional "sporadic groups."

The two largest sporadic groups are the:

- "baby monster group" B, which has order

$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33};$$

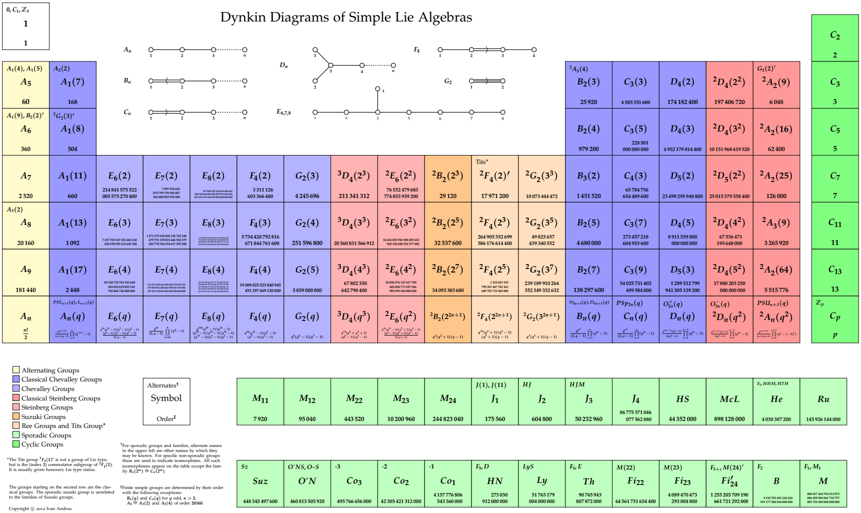
- "monster group" M, which has order

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8.08 \times 10^{53}.$$

The proof of this classification theorem is spread across $\approx$ 15,000 pages in $\approx$ 500 journal articles by over 100 authors, published between 1955 and 2004.

Image by *Ivan Andrus*, 2012

The Periodic Table Of Finite Simple Groups



Finite Simple Group (of Order Two), by The Klein Four™

Musical Fruitcake

View More by This Artist

Klein Four

Open iTunes to preview, buy, and download music.

View in iTunes

$9.99

Genres: Pop, Music
Released: Dec 05, 2005
℗ 2005 Klein Four

Customer Ratings

★★★★½ 13 Ratings

	Name	Artist	Time	Price	
1	Power of One	Klein Four	5:16	$0.99	View In iTunes ▸
2	Finite Simple Group (of Order Two)	Klein Four	3:00	$0.99	View In iTunes ▸
3	Three-Body Problem	Klein Four	3:17	$0.99	View In iTunes ▸
4	Just the Four of Us	Klein Four	4:19	$0.99	View In iTunes ▸
5	Lemma	Klein Four	3:43	$0.99	View In iTunes ▸
6	Calculating	Klein Four	4:09	$0.99	View In iTunes ▸
7	XX Potential	Klein Four	3:42	$0.99	View In iTunes ▸
8	Confuse Me	Klein Four	3:41	$0.99	View In iTunes ▸
9	Universal	Klein Four	4:13	$0.99	View In iTunes ▸
10	Contradiction	Klein Four	3:48	$0.99	View In iTunes ▸
11	Mathematics Paradise	Klein Four	3:51	$0.99	View In iTunes ▸
12	Stefanie (The Ballad of Galois)	Klein Four	4:51	$0.99	View In iTunes ▸
13	Musical Fruitcake (Pass it Around)	Klein Four	2:50	$0.99	View In iTunes ▸
14	Abandon Soap	Klein Four	2:17	$0.99	View In iTunes ▸

14 Songs