Chapter 6: Extensions of groups

Matthew Macauley

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

Math 8510, Visual Algebra

Chapter overview

Chemistry investigates how matter is assembled from basic "*building blocks*" (atoms).

Main goal

Understand how groups are assembled from basic "building blocks" (simple groups).

This chapter is broken into three parts:

1. Finite abelian groups are products of cyclic groups.
2. The classification of finite simple groups: the "*periodic table of groups*."
3. Extensions of groups: like doing "*all of chemistry* for groups."
   (a) Groups built from simple extensions (all groups)
   (b) Groups built from abelian extensions (solvable groups)
   (c) Groups built from central extensions (nilpotent groups)

Finite abelian groups

Lemma 1

Let $|G| = p^n$. Then G is cyclic iff it has a unique subgroup of order p^k for each $k = 0, 1, \dots, n$.

Proof

If $G \cong C_{p^n} = \langle r \rangle$, then $\langle r^d \rangle$ is the unique subgroup of order p^n/d.

Conversely, suppose G has a subgroup of order p^k for each $k = 0, 1, \dots, n$, and let $|H| = p^{n-1}$.

By the first Sylow theorem, H has a subgroup of each order p^k as well, for $k = 0, 1, \dots, n-1$.

Therefore, it must contain the unique subgroup of G of each of these orders, and hence, every proper subgroup of G.

Now, take any $g \notin H$. The cyclic subgroup $\langle g \rangle$ of G cannot be any of the subgroups of H, so it must be G. $\square$

Finite abelian groups

Lemma 2

If G is an abelian p-group with a unique subgroup of order p, then G is cyclic.

Proof

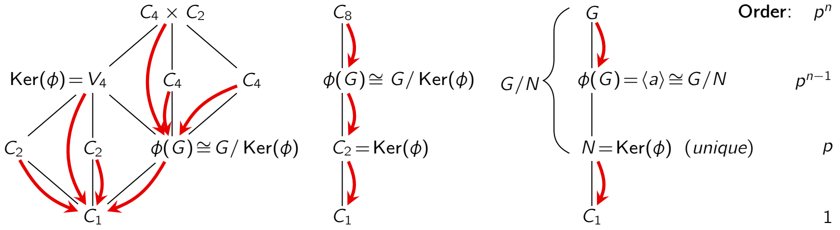
Induct on n, where $|G| = p^n$. The base case is trivial.

Suppose it holds for all p-groups of order up to p^{n-1}. Consider the homomorphism

$$\phi\colon G \longrightarrow G, \qquad \phi(x) = x^p.$$

The kernel is the unique subgroup $N \leq G$ of order p.

By Cauchy's theorem, every nontrivial subgroup of G must contain N.



Finite abelian groups

Lemma 2

If G is an abelian p-group with a unique subgroup of order p, then G is cyclic.

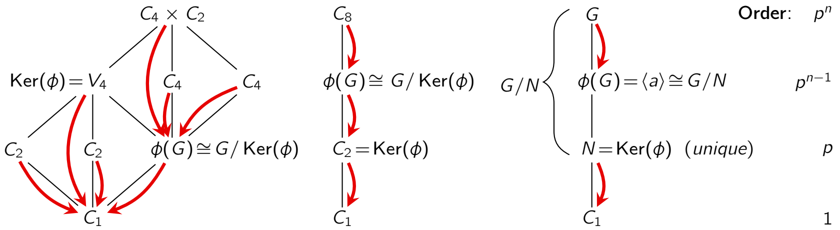
Proof (contin.)

By the FHT, $\phi(G) \cong G/N$ has order p^{n-1}.

However, $\phi(G) \leq G$, so it has a unique subgroup of order p.

By induction, $\phi(G) \cong G/N$ is cyclic, so it has a unique order-p^k subgroup H/N, for each $k \leq n-1$.

By the correspondence theorem, H is the unique subgroup of G of order p^{k-1}. $\square$



Finite abelian groups

Lemma 3

Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

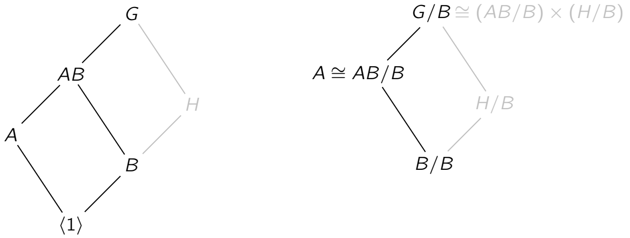
Proof

Induct on n, where $|G| = p^n$. The base case is trivial.

Let $A = \langle a \rangle$ for $|a| = p^k$, and assume the result holds for p-groups of order $< |G| = p^n$.

By the Lemma, there is a subgroup $B \leq G$ of order p, not contained in A.

By the diamond theorem: $AB/B \cong A/(A \cap B) \cong A$.



Finite abelian groups

Lemma 3

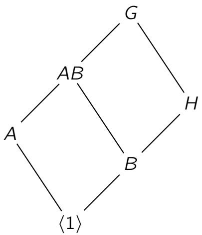
Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

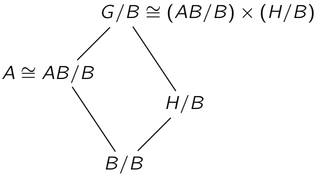
Proof (contin.)

No quotient of G can have a cyclic subgroup of order larger than $|A| = p^k$ (because $|H/N| = |\langle bH \rangle| = p^\ell > p^k$ in would force $|\langle b \rangle| > p^k$).

Therefore, $AB/B \cong A$ is a maximal cyclic subgroup of G/B.

By induction, there is some $H/B \leq G/B$ for which $G/B \cong AB/B \times H/B$.





Finite abelian groups

Lemma 3

Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

Proof (contin.)

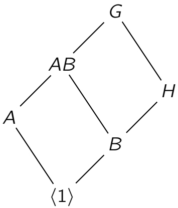
It suffices to show that A and H are lattice complements in G.

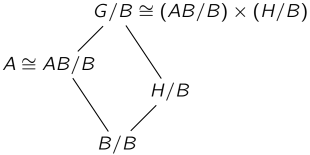
Generate G: Since $B \leq H$, we have $BH = H$ and $AB \subseteq AH$, and hence

$$G = (AB)H = A(BH) = AH.$$

Intersect trivially: Using $A \subseteq AB$ and basic set theory:

$$A \cap H \subseteq A \cap H \cap AB = A \cap (H \cap AB) = A \cap B = \langle 1 \rangle.$$





Finite abelian groups

Lemma 4

Every finite abelian group is a direct product of its Sylow p-groups.

Proof

Induct on the number of primes dividing $|G|$. □

Fundamental theorem of finite abelian groups

Every finite abelian group is a direct product of cyclic groups.

Proof

By Lemma 4, it suffices to consider the case of $|G| = p^n$. We'll induct on n.

The cases of $n = 0$ and $n = 1$ are trivial. Assume the result holds for all groups of order $p^1, \dots, p^{n-1}$.

If G is not cyclic, let A be a maximal cyclic subgroup.

Write $G = A \times H$ using Lemma 3, and apply the induction hypothesis. □

Conjugacy classes in A_n

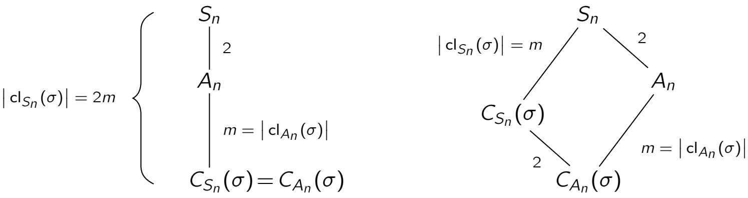
Elements in S_n are conjugate iff they have the same cycle type.

However, 8 of the 12 elements in A_4 are 3-cycles. These cannot all be conjugate.

Take $\sigma \in A_n$. *The size of its conjugacy class is the index of its centralizer.*

There are two cases to consider:

1. $C_{S_n}(\sigma)$ is a subgroup of A_n, or equivalently, $C_{A_n}(\sigma) = C_{S_n}(\sigma)$
2. $C_{S_n}(\sigma)$ is not a subgroup of A_n, or equivalently, $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$.



Key idea

Upon restricting to $A_n \leq S_n$, the conjugacy class of σ is either preserved or splits in two.

Simplicity of A_5

For example, S_5 has 7 conjugacy classes: $\mathrm{cl}_{S_5}(e) = \{e\}$, and

$$\mathrm{cl}_{S_5}((12)), \quad \mathrm{cl}_{S_5}((123)), \quad \mathrm{cl}_{S_5}((1234)), \quad \mathrm{cl}_{S_5}((12345)), \quad \mathrm{cl}_{S_5}((12)(34)), \quad \mathrm{cl}_{S_5}((12)(345)).$$

To find the conjugacy classes of A_5, first disregard the odd permutations. Note that:

- $C_{S_5}(e) = S_5$
- $C_{S_5}((12)(34))$ and $C_{S_5}((123))$ both contain some $(ij) \notin A_5$
- $C_{S_5}((12345)) \leq A_5$

Therefore, the size-24 conjugacy class containing (12345) splits in A_5.

$$\left|\mathrm{cl}_{S_5}((123))\right| = 20, \quad \left|\mathrm{cl}_{S_5}((12345))\right| = 12, \quad \left|\mathrm{cl}_{S_5}((13524))\right| = 12, \quad \left|\mathrm{cl}_{S_5}((12)(34))\right| = 15.$$

Proposition

The alternating group A_5 is simple.

Proof

Any normal subgroup of A_5 must have order 2, 3, 4, 5, 6, 12, 15, ~~20~~, or ~~30~~.

It's also the union of conjugacy classes: $\{e\}$ and other(s) of sizes 12, 12, 15, and 20.

Other than A_5 and $\langle e \rangle$, this is impossible. □

A few basic properties of the alternating group A_n

Lemma

(i) A_n is generated by 3-cycles, if $n \geq 3$.

(ii) all 3-cycles are conjugate to (123), if $n \geq 5$.

Proof

(i) Since $A_3 = \langle (123) \rangle$, take $n \geq 4$.

A_n is generated by products of pairs of transpositions.

- **Type 1**. Disjoint transpositions:

$$(ab)(cd) = (acd)(acb).$$

- **Type 2**. Overlapping transpositions:

$$(ab)(bc) = (acb). \qquad \checkmark$$

(ii) Take any 3-cycle (abc), and write

$$(abc) = \sigma(123)\sigma^{-1}, \qquad \sigma \in S_n.$$

If $\sigma \in A_n$, we're done. Otherwise, conjugate (123) by $\sigma \cdot (45) \in A_n$. ✓

Simplicity of A_n

Theorem

The alternating group A_n is simple, for all $n \geq 5$.

Proof

Consider a nontrivial proper normal subgroup $N \trianglelefteq G$.

All we have to do is show that N *contains a* 3*-cycle*. (Why?)

Pick any nontrivial $\sigma \in N$, and write it as a product of disjoint cycles.

There are several cases to consider separately. We'll either

(i) construct a 3-cycle from σ, or

(ii) construct an element in a previous case.

Case 1. σ contains a k-cycle $(a_1 a_2 \cdots a_k)$ for $k \geq 4$.

Then N contains a 3-cycle:

$$\underbrace{(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_3)(a_1 a_2 \cdots a_k)(a_3 a_2 a_1)(a_k \cdots a_2 a_1) = (a_2 a_3 a_k) \in N. \quad \checkmark$$

In the remaining cases, *we can assume that* σ *is a product of* 2*- and* 3*-cycles*.

Simplicity of A_n

Theorem

The alternating group A_n is simple, for all $n \geq 5$.

Proof (contin.)

Case 2. σ has at least two 3-cycles; $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \cdots$.

If we conjugate σ by $(a_1 a_2 a_4)$, we can also ignore the other (commuting) cycles in σ.

$$\underbrace{(a_1 a_2 a_4)\sigma(a_1 a_2 a_4)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_4)[(a_1 a_2 a_3)(a_4 a_5 a_6) \cdots](a_4 a_2 a_1)[\cdots (a_6 a_5 a_4)(a_3 a_2 a_1)]$$

$$= (a_1 a_2 a_4 a_3 a_6) \in N.$$

We are now back in Case 1. ✓

Case 3. σ has only one 3-cycle; $\sigma = (a_1 a_2 a_3)(a_4 a_5)(a_6 a_7) \cdots\cdots$.

Then $\sigma^2 = (a_1 a_3 a_2) \in N$, and so $\sigma \in N$. ✓

We've exhausted the cases where σ contains a 3-cycle.

In the remaining cases, *we can assume that σ is a product of pairs of 2-cycles*.

Simplicity of A_n

Theorem

The alternating group A_5 is simple, for all $n \geq 5$.

Proof (contin.)

Case 4. σ is a product of 2-cycles; $\sigma = (a_1 a_2)(a_3 a_4) \cdots$.

If we conjugate σ by $(a_1 a_2 a_3)$, we can ignore the other (commuting) 2-cycles in σ.

$$\underbrace{(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}}_{\in N} \cdot \sigma^{-1} = (a_1 a_2 a_3)(a_1 a_2)(a_3 a_4)(a_3 a_2 a_1)(a_1 a_2)(a_3 a_4)$$

$$= (a_1 a_4)(a_2 a_3) \in N.$$

Now, letting $\pi = (a_1 a_4 a_5)$,

$$\underbrace{(a_1 a_4)(a_2 a_3)\pi[(a_1 a_4)(a_2 a_3)]^{-1}}_{\in N} \cdot \pi^{-1} = (a_1 a_4)(a_2 a_3)(a_1 a_4 a_5)(a_1 a_4)(a_2 a_3)(a_5 a_4 a_1)$$

$$= (a_1 a_4 a_5) \in N. \quad \checkmark$$

and this completes the proof. $\square$

Classification of finite simple groups

Theorem (2004)

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 "sporadic groups."

The two largest sporadic groups are the:

- "baby monster group" B, which has order

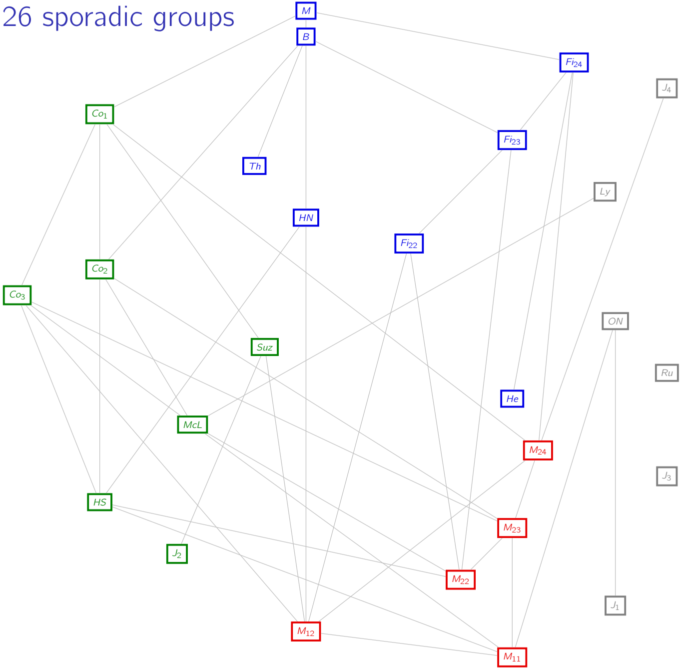
$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33};$$

- "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 ≈15,000 pages in ≈500 journal articles by over 100 authors, published between 1955 and 2004.

The 26 sporadic groups

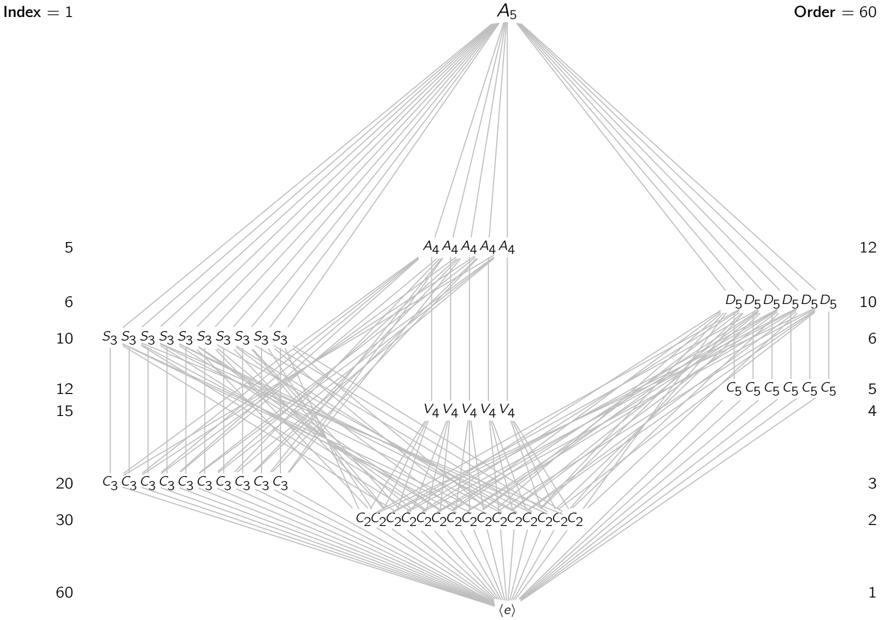


Order $= 8.08 \times 10^{53}$
4.15×10^{33}
1.26×10^{24}
8.68×10^{19}
4.16×10^{18}
4.09×10^{18}
9.07×10^{16}
5.18×10^{16}
2.73×10^{14}
6.46×10^{13}
4.23×10^{13}
4.96×10^{11}
4.61×10^{11}
4.48×10^{11}
1.46×10^{11}
4,030,387,200
898,128,000
244,823,040
50,232,960
44,352,000
10,200,960
604,800
443,520
175,560
95,040
7,920

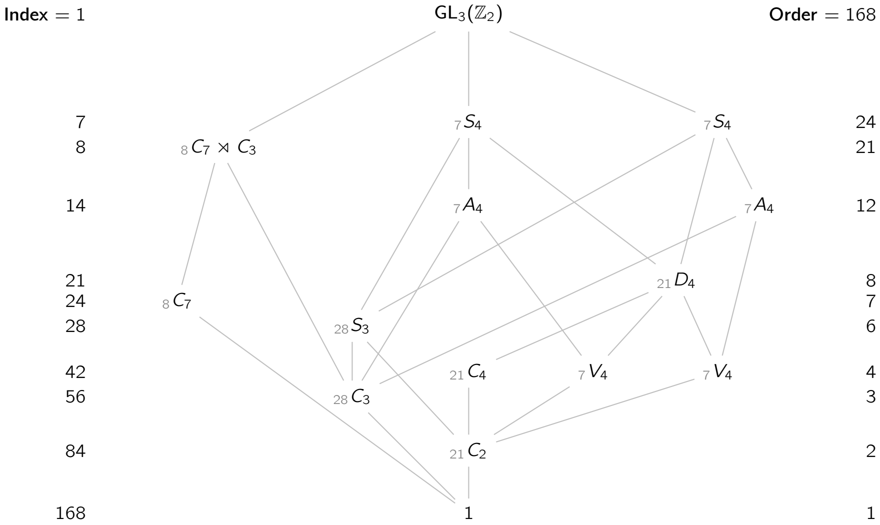
The 31 nonabelian simple groups of order less than 100,000

ID	group	order	$\#\mathrm{cl}_G(g)$	#subgroups	$\#\mathrm{cl}_G(H)$	$\leq S_n$ (min'l)	aka
60.5	A_5	$2^2\cdot3\cdot5$	5	59	9	S_5	$A_1(4)$, $A_1(5)$
168.42	$A_1(7)$	$2^3\cdot3\cdot7$	6	179	15	S_7	$A_2(2)$, $\mathrm{GL}_3(\mathbb{Z}_2)$
360.118	A_6	$2^3\cdot3^2\cdot5$	7	501	22	S_6	$A_1(9)$, $B_2(2)'$
504.156	$A_1(8)$	$2^3\cdot3^2\cdot7$	9	386	12	S_9	${}^2G_2(3)'$, $\mathrm{PSL}_2(\mathbb{F}_8)$
660.13	$A_1(11)$	$2^2\cdot3\cdot5\cdot11$	8	620	16	S_{11}	$\mathrm{PSL}_2(\mathbb{Z}_{11})$
1092.25	$A_1(13)$	$2^2\cdot3\cdot7\cdot13$	9	942	16	S_{14}	$\mathrm{PSL}_2(\mathbb{Z}_{13})$
2448.a	$A_1(17)$	$2^4\cdot3^2\cdot17$	11	2420	22	S_{18}	$\mathrm{PSL}_2(\mathbb{Z}_{17})$
2520.a	A_7	$2^3\cdot3^2\cdot5\cdot7$	9	3786	40	S_7	
3420a	$A_1(19)$	$2^2\cdot3^2\cdot5\cdot19$	12	2912	19	S_{20}	$\mathrm{PSL}_2(\mathbb{Z}_{19})$
4080.a	$A_1(16)$	$2^4\cdot3\cdot5\cdot17$	17	3455	21	S_{17}	$\mathrm{PSL}_2(\mathbb{F}_{16})$
5616.a	$A_2(3)$	$2^4\cdot3^3\cdot13$	12	6374	51	S_{13}	$\mathrm{PSL}_3(\mathbb{Z}_3)$
6048.a	${}^2A_2(3)$	$2^5\cdot3^3\cdot7$	14	5150	36	S_{28}	$G_2(2)'$, $\mathrm{PSU}_3(\mathbb{Z}_3)$
6072.a	$A_1(23)$	$2^3\cdot3\cdot11\cdot23$	14	5915	23	S_{24}	$\mathrm{PSL}_2(\mathbb{Z}_{23})$
7800.a	$A_1(25)$	$2^3\cdot3\cdot5^2\cdot13$	15	9559	37	S_{26}	$\mathrm{PSL}_2(\mathbb{Z}_{25})$
7920.a	M_{11}	$2^4\cdot3^2\cdot5\cdot11$	10	8651	39	S_{11}	
9828.a	$A_1(27)$	$2^2\cdot3^3\cdot7\cdot13$	16	5286	16	S_{28}	$\mathrm{PSL}_2(\mathbb{Z}_{27})$
12180.a	$A_1(29)$	$2^2\cdot3\cdot5\cdot7\cdot29$	17	10040	22	S_{30}	$\mathrm{PSL}_2(\mathbb{Z}_{29})$
14880.a	$A_1(31)$	$2^5\cdot3\cdot5\cdot31$	18	15413	29	S_{32}	$\mathrm{PSL}_2(\mathbb{Z}_{31})$
20160.a	A_8	$2^6\cdot3^2\cdot5\cdot7$	14	48337	137	S_8	$A_3(2)$
20160.b	$A_2(4)$	$2^6\cdot3^2\cdot5\cdot7$	10	44877	95	S_{21}	$\mathrm{PSL}_3(\mathbb{F}_4)$
25308.a	$A_1(37)$	$2^2\cdot3^2\cdot19\cdot37$	21	17731	23	S_{38}	$\mathrm{PSL}_2(\mathbb{Z}_{37})$
25920.a	$A_3(4)$	$2^6\cdot3^4\cdot5$	20	45649	116	S_{27}	$B_2(3)$, $C_2(3)$
29120.a	${}^2B_2(8)$	$2^6\cdot5\cdot7\cdot13$	11	17295	22	S_{65}	
32736.a	$A_1(32)$	$2^5\cdot3\cdot11\cdot31$	33	22328	24	S_{33}	$\mathrm{PSL}_2(\mathbb{F}_{32})$
34440.a	$A_1(41)$	$2^3\cdot3\cdot5\cdot7\cdot41$	23	36129	33	S_{42}	$\mathrm{PSL}_2(\mathbb{Z}_{41})$
39732.a	$A_1(43)$	$2^2\cdot3\cdot7\cdot11\cdot43$	24	25462	20	S_{44}	$\mathrm{PSL}_2(\mathbb{Z}_{43})$
51888.a	$A_1(47)$	$2^4\cdot3\cdot23\cdot47$	26	48837	29	S_{48}	$\mathrm{PSL}_2(\mathbb{Z}_{47})$
58800.a	$A_1(49)$	$2^4\cdot3\cdot5^2\cdot7^2$	27	73945	51	S_{50}	$\mathrm{PSL}_2(\mathbb{Z}_{49})$
62400.a	${}^2A_2(16)$	$2^6\cdot3\cdot5^2\cdot13$	22	31373	34	S_{65}	$U_3(4)$
74412.a	$A_1(53)$	$2^2\cdot3^3\cdot13\cdot53$	29	43254	20	S_{54}	$\mathrm{PSL}_2(\mathbb{Z}_{53})$
95040.a	M_{12}	$2^6\cdot3^3\cdot5\cdot11$	15	214871	147	S_{12}	

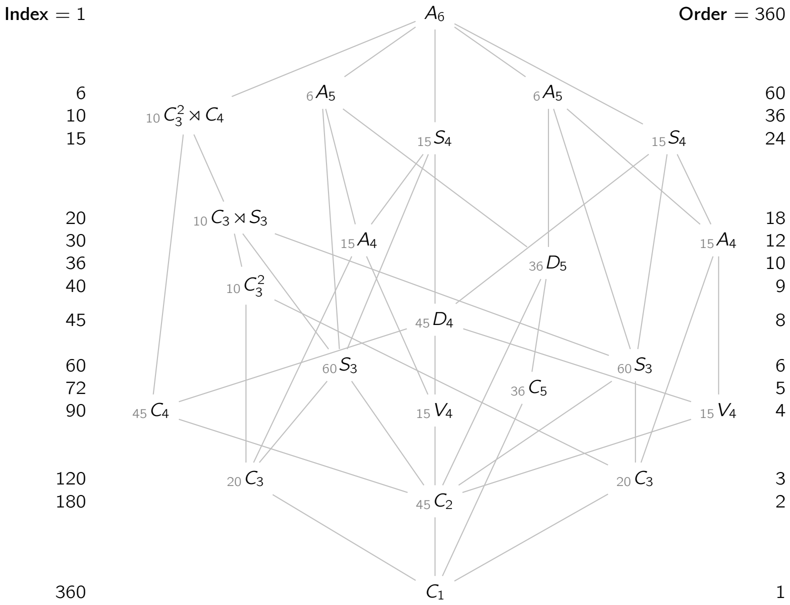
The smallest nonabelian simple group ("group atom")



The second smallest nonabelian simple group ("group atom")



The third smallest nonabelian simple group (“group atom”)



The 71st smallest nonabelian simple group: "Lie type $A_1(173)$"

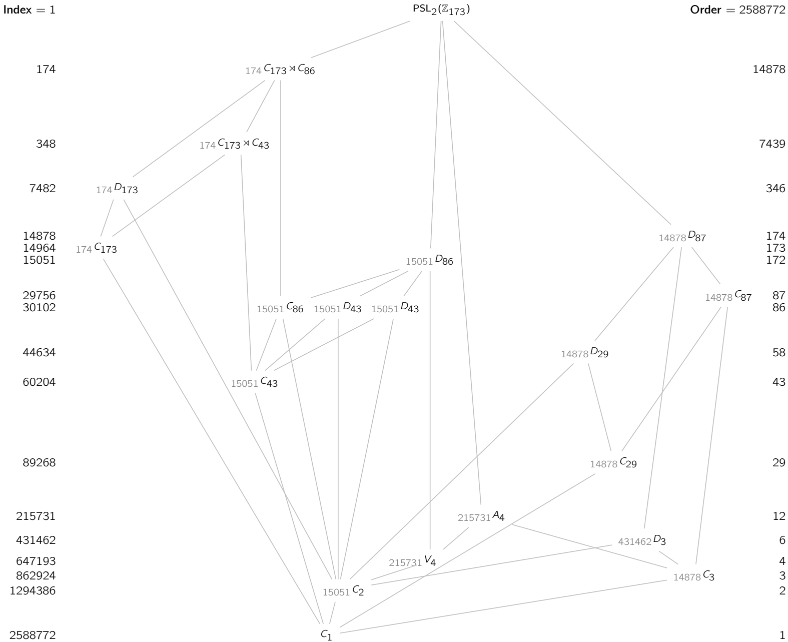
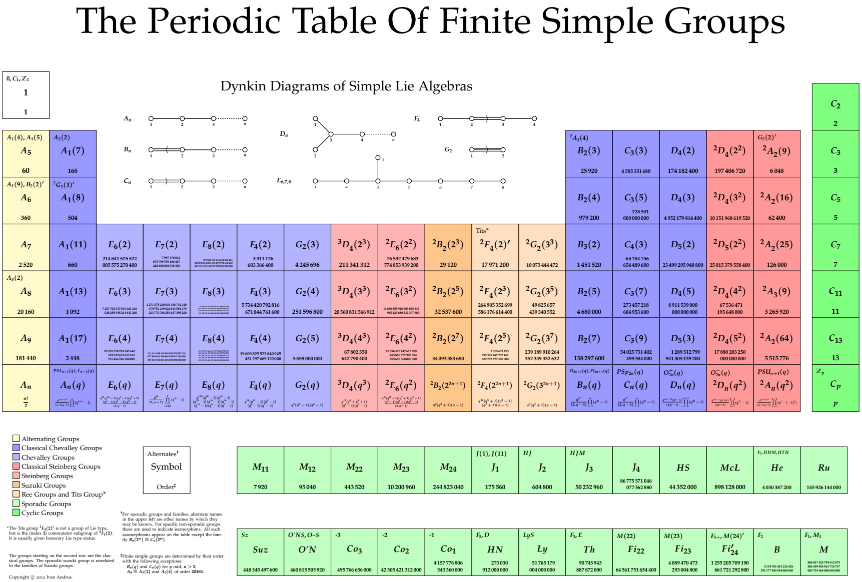


Image by *Ivan Andrus*, 2012



Finite Simple Group (of Order Two), by The Klein Four$^{\text{TM}}$

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

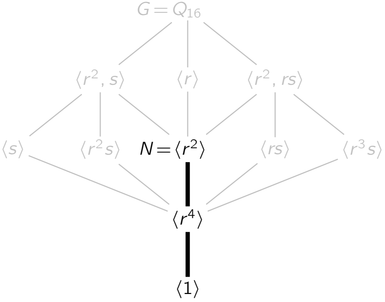
	Name	Artist	Time	Price	
1	Power of One	Klein Four	5:16	$0.99	View In iTunes ▸
2	Finite Simple Group (of Order Two)	Klein Four	3:00	$0.99	View In iTunes ▸
3	Three-Body Problem	Klein Four	3:17	$0.99	View In iTunes ▸
4	Just the Four of Us	Klein Four	4:19	$0.99	View In iTunes ▸
5	Lemma	Klein Four	3:43	$0.99	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

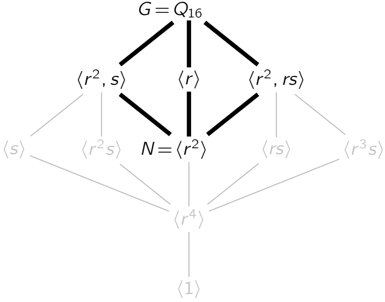
Chopping off subgroup lattices

Going forward, we will iteratively be finding subgroups and quotients of a group G.

It will be convenient to use the following teminology:



"*chopping off above* $N \trianglelefteq G$"



"*chopping off below* $N \trianglelefteq G$"

Group extensions

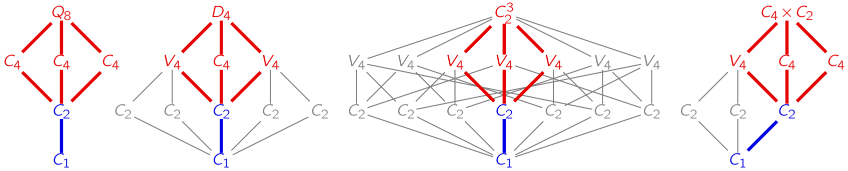
Every normal subgroup $N \trianglelefteq G$ canonically defines two sublattices.

- "*everything above*": the quotient $Q := G/N$
- "*everything below*": the subgroup $N \trianglelefteq G$.

We say that :

"*G is an* **extension** *of Q, by N*".

Here are four extensions of V_4 by C_2.



This can be encoded by a sequence

$$N \xhookrightarrow{\iota} G \xrightarrow{\pi} Q$$

where $\mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$. We say that this sequence is **exact** at G.

Extensions and short exact sesquences

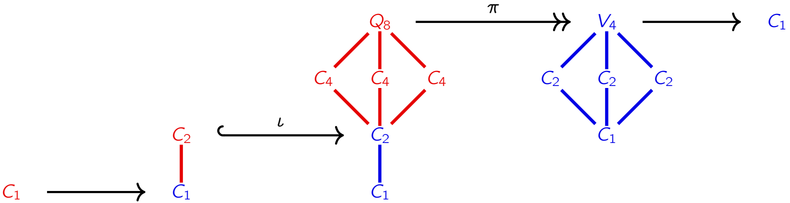
If we write

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1$$

and specifiy that the sequence is exact at N, G, and Q, then

- exactness at N means ι is injective,
- exactness at G means $\mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$,
- exactness at Q means π is surjective.

We call this a **short exact sequence**.



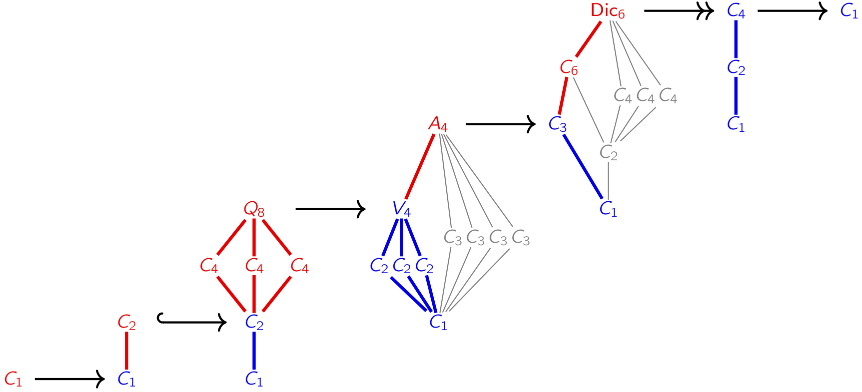
More on exact sequences

Exact sequences arise in algebraic topology, homological algebra, differential geometry, etc.

The "*curl of a conservative vector field is* 0" can be viewed a short exact sequence:

$$0 \longrightarrow L^2 \xrightarrow{\text{grad}} \mathbb{H}_3 \xrightarrow{\text{curl}} \text{Im(curl)} \longrightarrow 0$$

Here is an exact sequence of length 7:



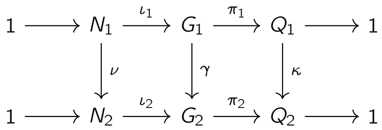
Extensions

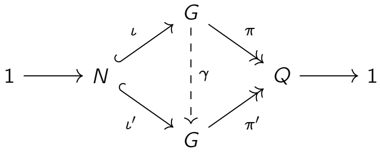
Finding all extensions of a group Q by N amounts to the following.

The "extension problem"

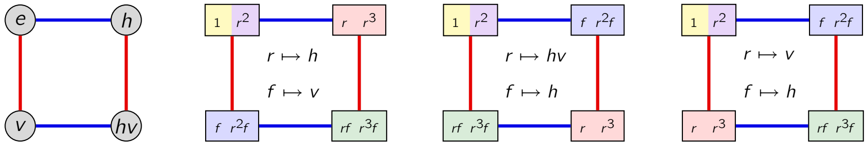
Find all possibilities for the "middle term" G in a short exact sequence, given N and Q.

We define **equivalence** of extensions via commutative diagrams related by automorphisms.





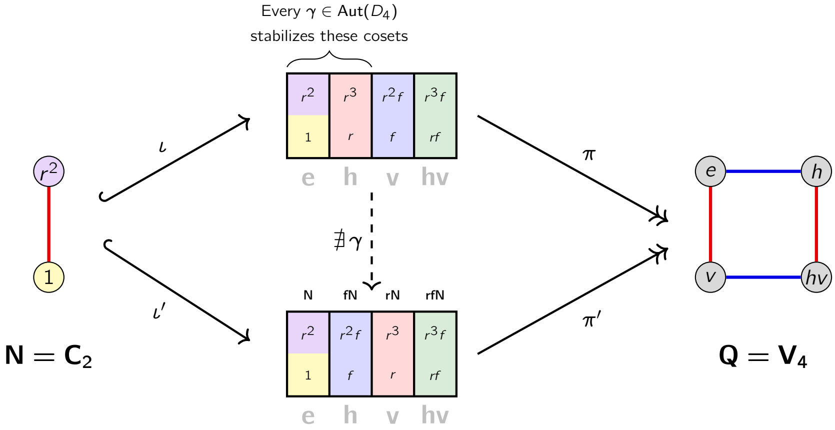
Do you see why these three extensions of V_4 by C_2 do *not* differ by an automorphism?



Extension equivalence

There are three nonequivalent extensions of V_4 by C_2 that give D_4:

$$1 \longrightarrow C_2 \xrightarrow{\iota} D_4 \xrightarrow{\pi} V_4 \longrightarrow 1$$



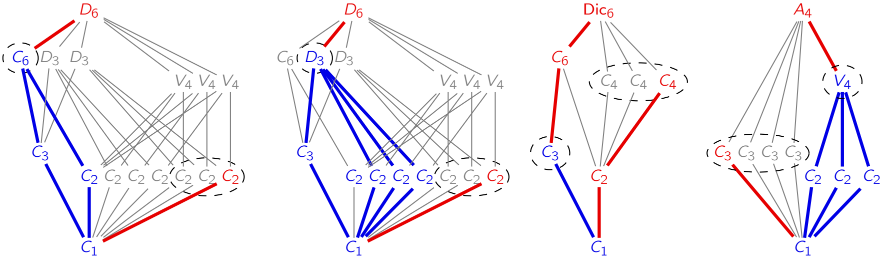
Semidirect products and extensions

A semidirect product $N \rtimes H$ is an extension of H by N.

$$1 \longrightarrow N \xrightarrow{\quad\iota\quad} N \rtimes_\theta H \xrightarrow{\quad\pi\quad} H \longrightarrow 1.$$

In the subgroup lattice, we can see

- $N \leq G$ at the bottom,
- $H \leq G$ at the bottom,
- $Q = G/N \cong H$ at the top.



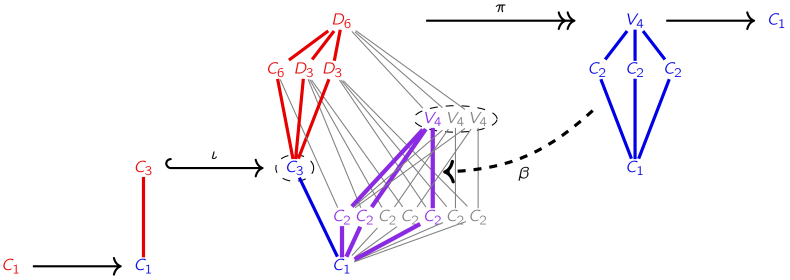
Do you see a canonical injection from $Q \cong G/N \cong H$ "*down to*" $H \leq G$?

Split exact sequences

Definition

A short exact sequence **splits** if there is a backwards map $\beta \colon H \to G$ for which $\pi \circ \beta = \mathrm{Id}_H$:

$$1 \longrightarrow N \xrightarrow{\ \iota\ } G \underset{\beta}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1$$



Split exact sequences and semidirect products

Theorem

A short exact sequence $1 \longrightarrow N \stackrel{\iota}{\longrightarrow} G \underset{\beta}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1$ splits if and only if $G \cong N \rtimes_\theta H$.

Proof

"$\Leftarrow$": We've already seen this. ✓

"$\Rightarrow$": Suppose we have a split exact sequence, and $\beta \colon H \to G$ satisfies $\pi \circ \beta = \mathrm{Id}_H$.

It suffices to show that $\iota(N) \cong N$ and $\beta(H) \cong H$ are lattice complements.

- **Generate** G: Take $g \in G$, we will show that $g = nh \in \underbrace{\iota(N)}_{\cong N}\underbrace{\beta(H)}_{\cong H}$.

  Let $h = \beta(\pi(g)) \in \beta(H)$. ✓

  It suffices to show that $n = gh^{-1}$ is in $\iota(N) = \mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$. By exactness, $\pi(\iota(N)) = 1_H$, and with $\pi \circ \beta = \mathrm{Id}_H$, we get

  $$\pi(n) = \pi(gh^{-1}) = \pi(g)\pi(h)^{-1} = \pi(g) \cdot \pi(\beta(\pi(g)))^{-1} = \pi(g) \cdot \pi(g)^{-1} = 1_H,$$

  hence $n \in \mathrm{Ker}(\pi)$. ✓

Split exact sequences and semidirect products

Theorem

A short exact sequence $1 \longrightarrow N \xrightarrow{\iota} G \underset{\beta}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1$ splits if and only if $G \cong N \rtimes_\theta H$.

Proof

"$\Leftarrow$": We've already seen this. ✓

"$\Rightarrow$": Suppose we have a split exact sequence, and $\beta \colon H \to G$ satisfies $\pi \circ \beta = \mathrm{Id}_H$.

It suffices to show that $\iota(N) \cong N$ and $\beta(H) \cong H$ are lattice complements.

- **Trivial intersection**: Suppose $g \in \iota(N) \cap \beta(H)$, and write $g = \beta(h)$.

  Since $g \in \iota(N) = \mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$,

$$1_H = \pi(g) = \pi(\beta(h)) = (\pi \circ \beta)(h) = \mathrm{Id}_H(h) = h.$$

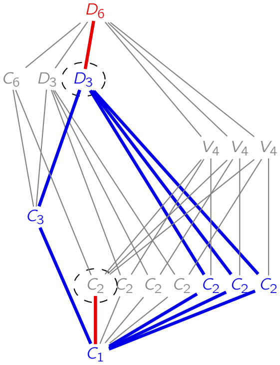
  Therefore, $g = \beta(h) = \beta(1_H) = 1_G$, and hence $\iota(N) \cap \beta(H) = \langle 1_G \rangle$. □

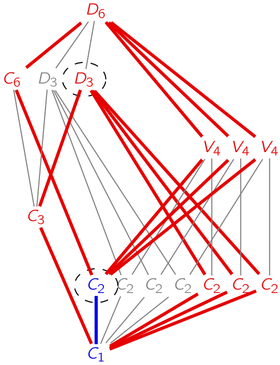
Split exact sequences and direct products

If $G \cong N \times H \cong H \times N$, then G is an extension of N by H, and vice-versa.

$$1 \longrightarrow N \xrightarrow{\iota_1} N \times H \underset{\beta_1}{\overset{\pi_1}{\rightleftarrows}} H \longrightarrow 1 \qquad\qquad 1 \longrightarrow H \xrightarrow{\iota_2} H \times N \underset{\beta_2}{\overset{\pi_2}{\rightleftarrows}} N \longrightarrow 1$$

This gives a certain "duality" to the subgroup lattices. Here is $D_6 \cong D_3 \times C_2 \cong C_2 \times D_3$.



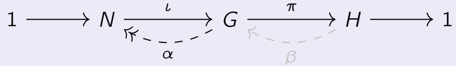


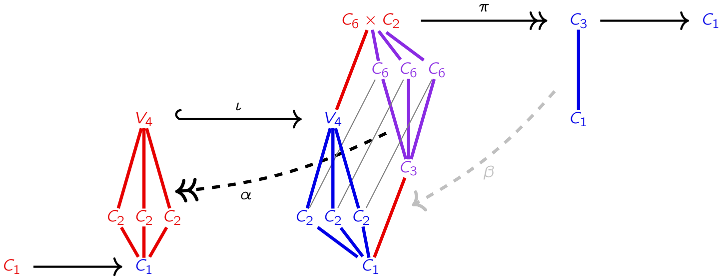
Split exact sequences and direct products

Another way to capture this duality is to distinguish between "right split" and "left split."

Definition

A short exact sequence is **left split** if there is a map $\beta\colon H \to G$ for which $\alpha \circ \iota = \mathrm{Id}_N$:





Split exact sequences and direct products

Proposition (HW)

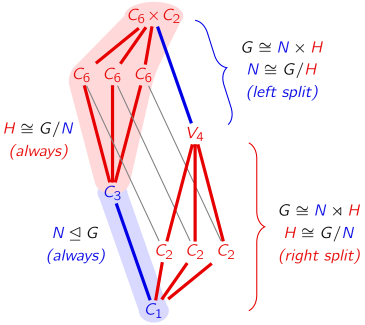
- If a short exact sequence is left split, then it is right split.

  "if it's a direct product, then it's a semidirect product"

- If a short exact sequence is right split and G is abelian, then it is left split.

  "if an abelian group is a semidirect product, then it's a direct product"

$$1 \longrightarrow N \underset{\alpha}{\overset{\iota}{\rightleftarrows}} G \underset{\beta}{\overset{\pi}{\rightleftarrows}} H \longrightarrow 1$$

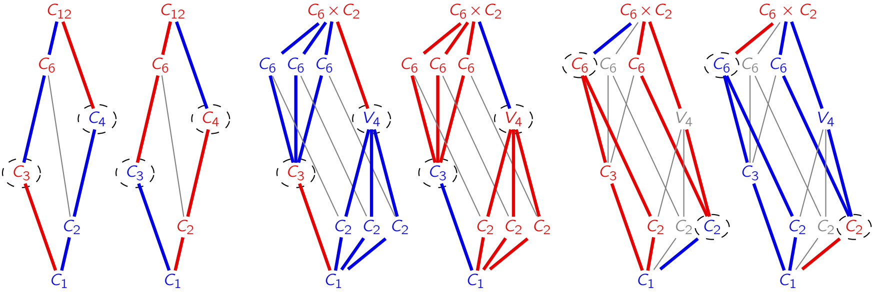


Split exact sequences and direct products

If $G \cong N \times H$, then G is an extension of N by H, and vice-versa.

$$1 \longrightarrow N \overset{\iota_1}{\underset{\alpha_1}{\rightleftarrows}} N \times H \overset{\pi_1}{\underset{\beta_1}{\rightleftarrows}} H \longrightarrow 1 \qquad 1 \longrightarrow H \overset{\iota_2}{\underset{\alpha_2}{\rightleftarrows}} N \times H \overset{\pi_2}{\underset{\beta_2}{\rightleftarrows}} N \longrightarrow 1$$

This gives a certain "duality" to the subgroup lattices. The two abelian groups of order 12 break up as a direct product in three ways:



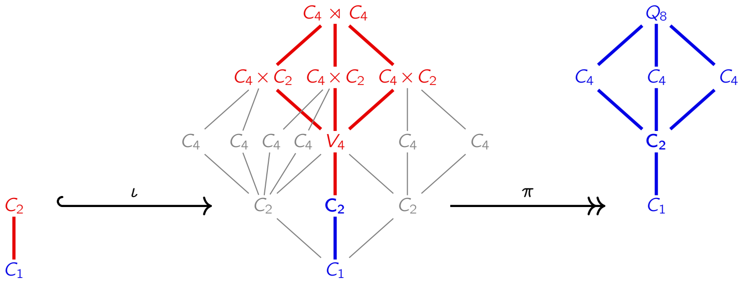
Central and stem extensions

Definition

An extension $1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1$ is

- **abelian** if N is abelian,
- **central** if $\iota(N) \leq Z(G)$,
- a (central) **stem extension** if $\iota(N) \leq Z(G')$.

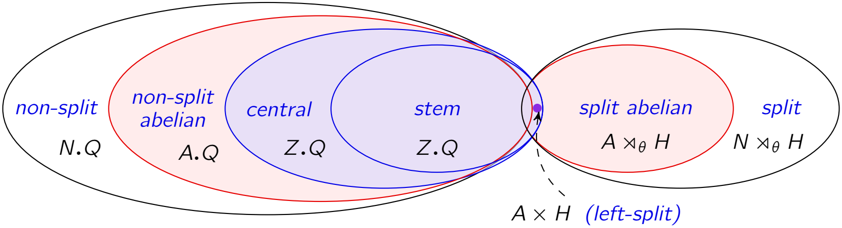
The group $G = C_4 \rtimes C_4$ is a central (and hence abelian), nonsplit extension of $Q = Q_8$ by $N = C_2$.



Types of groups extensions

If G is a (non-split) extension of Q by N, we write $N.Q$.

Here are the different types of extensions and how they are related.



In general, we are interested in understanding how groups can be "built with extensions," via simple groups.

Preview

If G can be broken up into

- abelian extensions, then it is solvable,
- central extensions, then it is nilpotent.

Climbing down subgroups lattices via "simple steps"

Every finite group G has ≥ 1 maximal normal subgroup: $N \trianglelefteq G$ for which G/N is simple.

Let $G_0 = G$, and $G_1 \trianglelefteq G$ be any maximal normal subgroup.

Next, pick any maximal $G_2 \trianglelefteq G_1$. Note that G_2 need not be normal in G.

Iterate this process of taking "simple steps" down the lattice, until we reach the bottom.

Definition

A **composition series** for G is a "*descending subnormal series*"

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \langle 1 \rangle$$

where each G_i/G_{i+1} is simple. The **composition factors** are the quotient groups G_i/G_{i+1}.

Note that each G_i is an extension of G_i/G_{i+1} by G_{i+1}.

Big idea

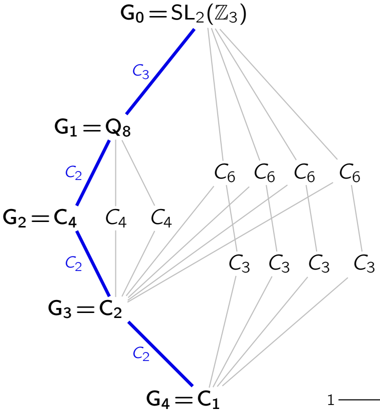
Breaking down a group into composition factors is like factoring a number into primes, or a molecule into atoms. We say:

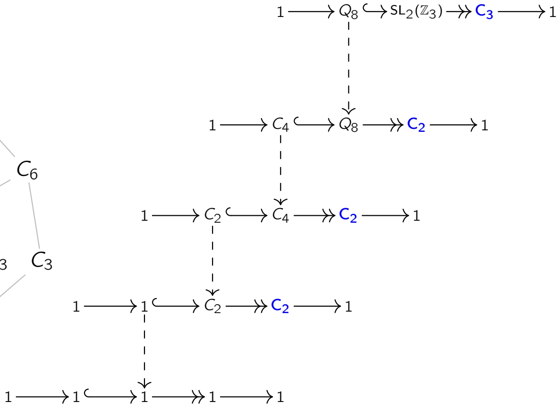
"*Every group can be constructed by 'simple extensions'*"

Composition series and simple extensions

Here is an example of a composition series: $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq G_4 = 1$.

These are all simple extensions. The composition factors are marked.



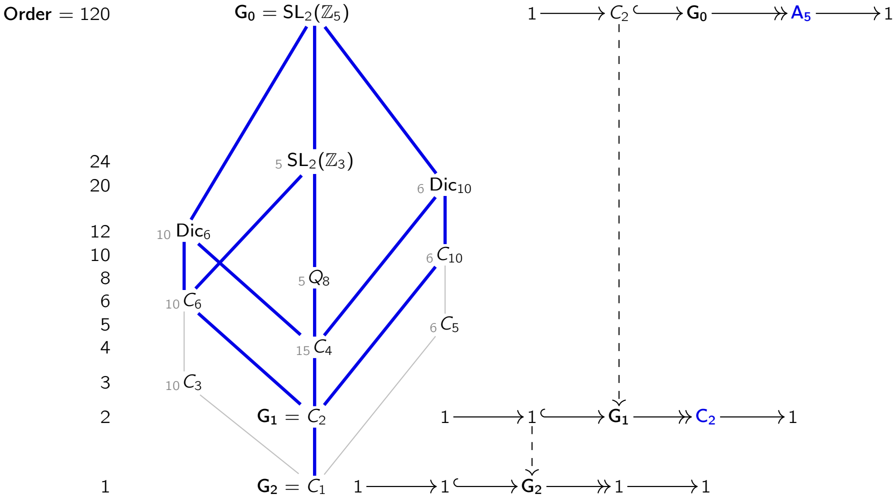


They will always be either *cyclic* or *non-abelian simple* (e.g., A_5, $GL_3(\mathbb{Z}_2)$, $A_6, \ldots$).

Preview: A group is "**solvable**" if they're all cyclic.

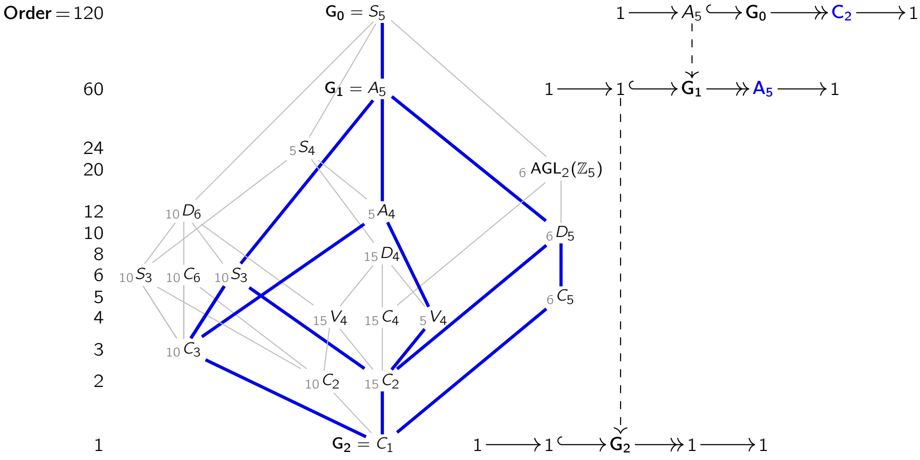
Composition series and simple extensions

The group $G = \mathsf{SL}_2(\mathbb{Z}_5)$ is not solvable because one of its composition factors is a nonabelian simple group.



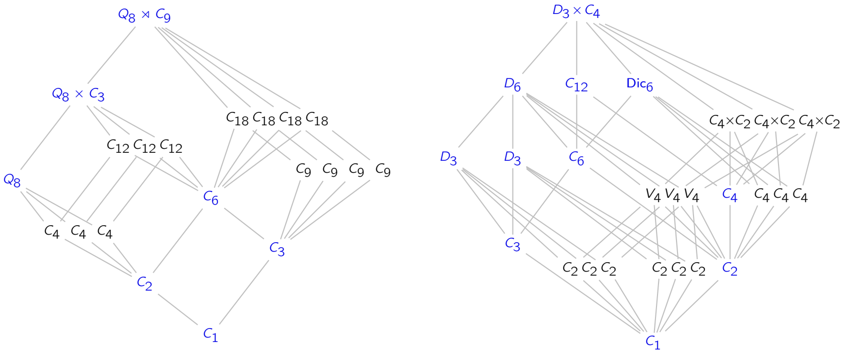
Composition series and simple extensions

The group $G = S_5$ is not solvable because one of its composition factors is a nonabelian simple group.



Composition series and simple extensions

How many composition series do the following groups have? What are their factors?



Do you see why we need to work from "top to bottom" to find them?

The following result is analogous to how integers can be factored uniquely into primes.

Jordan-Hölder theorem (upcoming)

Every composition series of a group has the same multiset of composition factors.

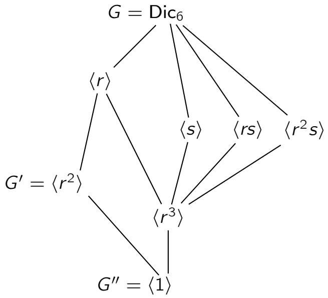
Equivalence of composition series

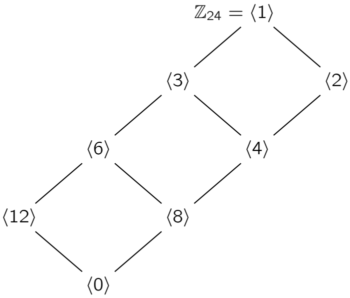
Two composition series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1, \qquad G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_\ell = 1$$

are **equivalent** if $\ell = m$, and they have the same composition factors up to re-ordering.

Notice how all of the composition series of the following groups are equivalent:





This is guaranteed by the Jordan-Hölder theorem.

Equivalence of composition series

Jordan-Hölder theorem

Any two composition series for a finite group are equivalent.

Proof

We proceed by induction (base case is trivial). Suppose we have two composition series:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1, \qquad G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_\ell = 1,$$

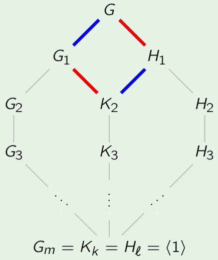
and the result holds for all groups with a composition series of length $\leq m$.

If $G_1 = H_1$, the result follows from the IHOP. So assume otherwise, and let $K_2 = G_1 \cap H_1$. Take a composition series of K_2.

We now have 4 composition series of G.

Reading left-to-right (see lattice):

- The 1st & 2nd, and 3rd & 4th have the same factors by the IHOP.
- The 2nd and 3rd have the same factors by the diamond theorem.



Climbing down subgroups lattices via "abelian descents"

Suppose $G_1 \trianglelefteq G$ and G/G_1 is abelian. We'll call G_1, and the act of jumping from G down to G_1, as an abelian descent.

Equivalently, G is an abelian extension of G/G_1 by G_1.

Proposition (exercise)

If $N \trianglelefteq G$, then G/N is abelian if and only if $G' \leq N$.

In other words, the commutator subgroup G' is the maximal abelian descent from G.

Definition

A group G is solvable if can be constructed iteratively by abelian extensions: there exists

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \langle 1 \rangle$$

where each factor G_i/G_{i+1} is abelian. (Or equivalently: cyclic.)

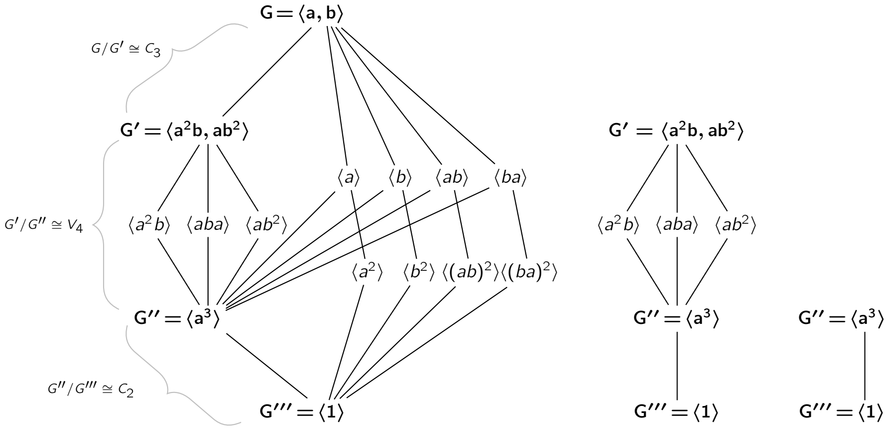
Definition

The derived series of group G is the series

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq G^{(3)} \trianglerighteq \cdots, \qquad \text{where } G^{(k+1)} = (G^{(k)})'.$$

Solvability

The derived series of $G = \mathrm{SL}_2(\mathbb{Z}_3)$ reaches the bottom in 3 steps.



We say that $\mathrm{SL}_2(\mathbb{Z}_3)$ is solvable, with derived length 3.

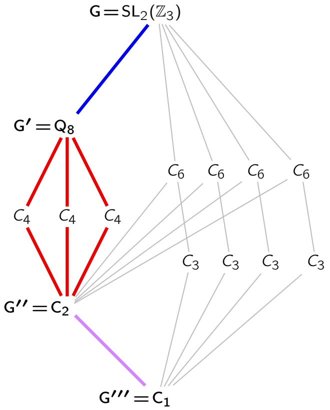
By the correspondence theorem, we can *refine* the derived series to a composition series.

Solvability in terms of abelian extensions

Key idea

A group is solvable if it can be constructed as a series of abelian extensions.

From top-to-bottom: $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq G_3 = \langle 1 \rangle$.



$$1 \longrightarrow Q_8 \hookrightarrow SL_2(\mathbb{Z}_3) \twoheadrightarrow C_3 \longrightarrow 1$$

$$1 \longrightarrow C_2 \hookrightarrow Q_8 \twoheadrightarrow V_4 \longrightarrow 1$$

$$1 \longrightarrow 1 \hookrightarrow C_2 \twoheadrightarrow C_2 \longrightarrow 1$$

$$1 \longrightarrow G' \hookrightarrow G \twoheadrightarrow G/G' \longrightarrow 1$$

$$1 \longrightarrow G'' \hookrightarrow G' \twoheadrightarrow G'/G'' \longrightarrow 1$$

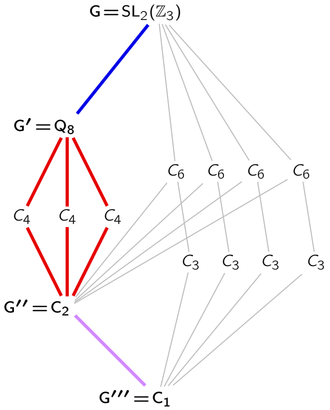
$$1 \longrightarrow G''' \hookrightarrow G'' \twoheadrightarrow G'''/G'' \longrightarrow 1$$

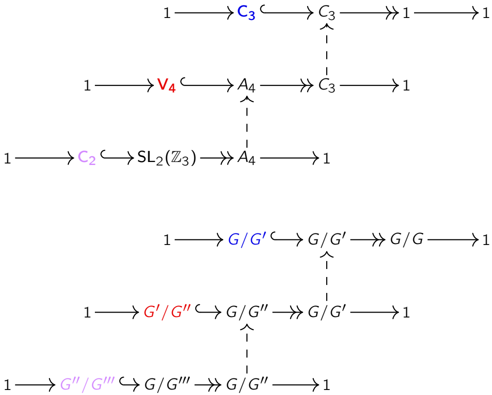
Solvability in terms of abelian extensions

Key idea

A group is solvable if it can be constructed as a series of abelian extensions.

From bottom-to-top: $\langle 1\rangle = G_3 \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$.





Solvability in terms of composition series (simple extensions)

Proposition

A finite group G is solvable if and only if $G^{(m)} = \langle 1 \rangle$ for some $m \in \mathbb{Z}$.

Intuitively: if (non-maximal) abelian descents reach the bottom, so will maximal abelian descents.

Proof

"$\Rightarrow$" is trivial. For "$\Leftarrow$", say G has a subnormal series with $G_m = \langle 1 \rangle$ and abelian factors.

We need to show $G^{(m)} = \langle 1 \rangle$, but we'll prove a stronger statement:

$$G^{(k)} \leq G_k \quad \text{for all} \quad k \in \mathbb{N}.$$

We can do this by induction.

Base case: Since G/G_1 is abelian $G' \leq G_1$. ✓

Bonus base case: Since G_1/G_2 is abelian, G_2 must contain $(G_1)' = G''$.

Suppose $G^{(k)} \leq G_k$ holds; then $G^{(k+1)} \leq G_k'$.

Since G_k/G_{k+1} is abelian, G_{k+1} must contain $G_k' \geq G^{(k+1)}$. □

Solvability and subgroups

Given subgroups H and K of G, define

$$[H,K] = \big\langle [h,k] \mid h \in H,\ k \in K \big\rangle = \big\langle hkh^{-1}k^{-1} \mid h \in H,\ k \in K \big\rangle.$$

Notice that

$$G' = [G,G], \quad G'' = [G',G'], \quad G''' = [G'',G''], \quad \dots \quad , \quad G^{(k+1)} = [G^{(k)},G^{(k)}].$$

Lemma

If $K \leq H \leq G$, then $[K,K] \leq [H,H]$. □

Proposition

If G is solvable and $H \leq G$, then H is solvable.

Proof

By the lemma, $H' = [H,H] \leq [G,G] = G'$, and inductively,

$$H'' = [H',H'] \leq [G',G'] = G'', \quad \dots \quad , \quad H^{(k+1)} = [H^{(k)},H^{(k)}] \leq [G^{(k)},G^{(k)}] = G^{(k+1)}.$$

Since G is solvable, $G^{(m)} = \langle 1 \rangle$ for some $m \in \mathbb{N}$.

Solvability of H follows immediately from $H^{(m)} \leq G^{(m)} = \langle 1 \rangle$.

Solvability and quotients

Proposition

If G is solvable and $N \trianglelefteq G$, then G/N is solvable.

Proof

Let $\pi\colon G \to G/N$. The commutator of the quotient is the quotient of the commutator:

$$\pi([x,y]) = \pi(xyx^{-1}y^{-1}) = xyx^{-1}y^{-1}N = [xN, yN].$$

Therefore, $(G/N)' = \pi(G')$, and $(G/N)^{(k)} = \pi(G^{(k)})$.

Since G is solvable, $G^{(m)} = \langle 1 \rangle$ for some $m \in \mathbb{N}$.

Therefore, $(G/N)^{(m)} = N/N$, and hence G/N is solvable. $\square$

The proof above suggests that commutators behave well under homomorphisms.

Exercise

Suppose $\phi\colon G_1 \to G_2$ is a homomorphism. Then:

(i) $\phi([h,k]) = [\phi(h), \phi(k)]$, for all $h, k \in G_1$.

(ii) $\phi([H,K]) = [\phi(H), \phi(K)]$, for all $H, K \leq G_1$.

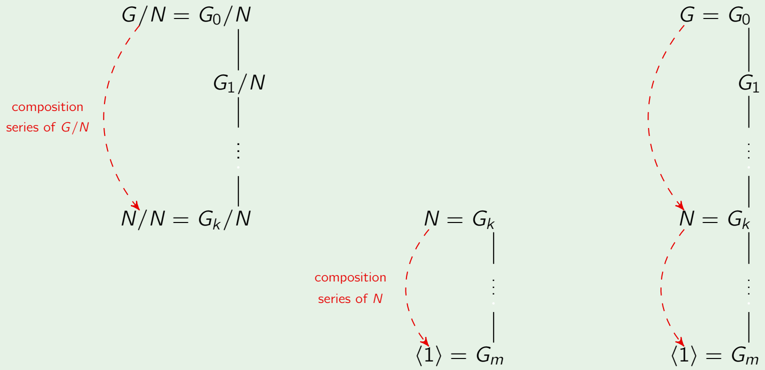
Solvability

Theorem

Suppose $N \trianglelefteq G$. Then G is solvable if and only if G/N and N are solvable.

Proof

Use the correspondence theorem to create a composition series of G:



Solvability and extensions: abelian vs. cyclic

Big ideas

Composition factors are like "atoms" that groups are built with. They are either cyclic, or nonabelian simple groups.

A group G **solvable** if

- we can climb down the subgroup lattice using "*maximal abelian descents*"
- the (minimal) "*simple steps*" down the subgroup lattice are all cyclic.

Theorem

The following groups are solvable.

- p-groups (we'll prove soon)
- All groups of order $p^n q^m$, for primes p and q (Burnside)
- Groups of order $p^n \cdot m$ ($p \nmid m$) that have a subgroup of order m.
- Groups of odd order (Feit-Thompson; 250+ page proof).
- Groups for which all 2-generator subgroups are solvable (Thompson; 475 page proof that uses the Feit-Thompson result).

Central ascents

Starting from any normal subgroup $N \trianglelefteq G$, we can ask:

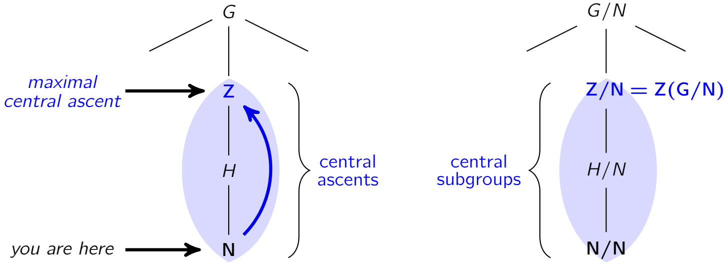
"*if we quotient by N (chop off the lattice below), what subgroup Z/N is the center?*"

We'll give this a memorable name, as we did for (maximal) abelian descents.

Definition

If $N \trianglelefteq G$, then $Z \leq G$ is a

- central ascent from N if $Z/N \leq Z(G/N)$,
- maximal central ascent from N if $Z/N = Z(G/N)$.



By iterating this process from $Z_0 = \langle 1 \rangle$, we can (attempt to) climb *up* a subgroup lattice.

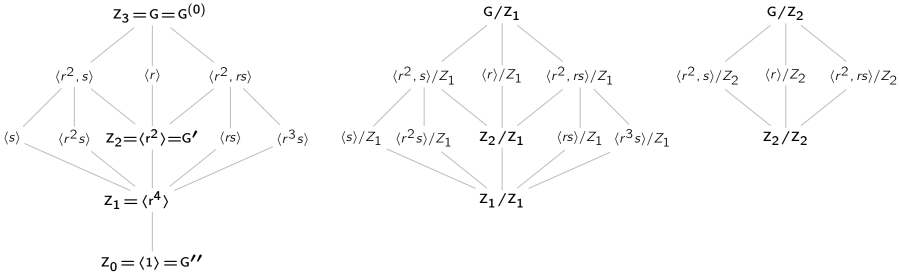
Nilpotent groups and the ascending central series

Definition

Let G be a finite group, and let $Z_0 = \langle 1 \rangle$ and $Z_1 = Z(G)$. The series

$$\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots , \qquad \text{where} \qquad Z_{k+1}/Z_k = Z(G/Z_k)$$

is the **ascending central series** of G, and if $Z_m = G$ for some $m \in \mathbb{N}$, then G is **nilpotent**. The minimal m is the **nilpotency class**.



Big idea

The subgroup Z_{k+1} is the maximal central ascent from Z_k.

Nilpotent groups and central extensions

Proposition

If G is nilpotent, then it is solvable.

Proof

The ascending central series $\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_m = G$ is a normal (and hence subnormal) series of G. (*Why?*)

Since Z_{k+1}/Z_k is the center of the group G/Z_k, it is abelian.

Since G has a subnormal series with abelian factors, it is solvable. □

One easy way to remember this

"*it's easier to fall down than to climb up*."

Corollary

Every p-group is nilpotent, and hence solvable. □

Proof

Since p-groups have nontrivial centers, $Z_i \lneq Z_{i+1}$ for each i. □

Nilpotent groups

Starting from $N \trianglelefteq G$, we can ask:

How can we characterize the central ascents algebraically? Which one is maximal?

Central series lemma

If $N \leq H \leq G$ and $N \trianglelefteq G$, then

$$H/N \leq Z(G/N) \quad \text{if and only if} \quad [G,H] \leq N$$

In particular, the maximal central ascent from N is: $Z = \{z \in G \mid [g,z] \in N,\ \forall g \in G\}$.

Proof

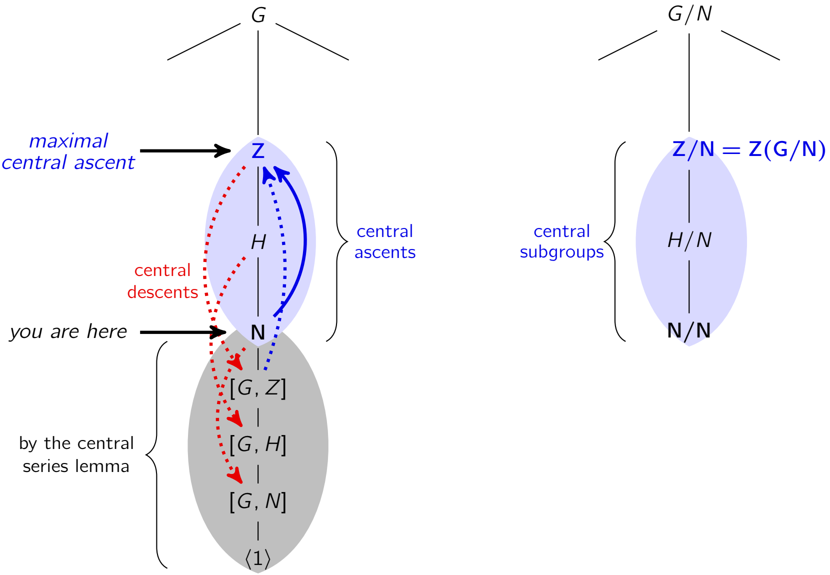
If H/N is in the center of G/N, then for all $h \in H$ and $g \in G$

$$gN \cdot hN = hN \cdot gN \quad \Longleftrightarrow \quad ghg^{-1}h^{-1}N = N \quad \Longleftrightarrow \quad [g,h] \in N \quad \Longleftrightarrow \quad [G,H] \leq N.$$

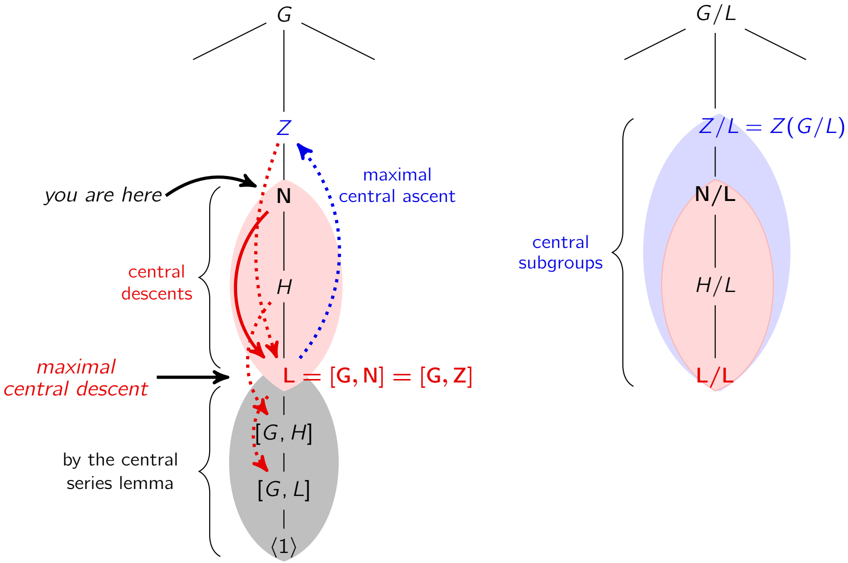
Definition

If $N \trianglelefteq G$, then $L = [G,N]$ is a maximal central descent from N. Intermediate subgroups $L \leq K \leq N$ are central descents.

Central ascents



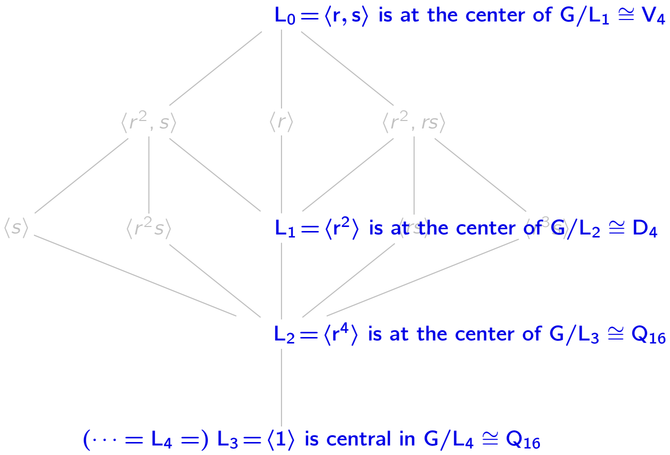
Central descents



The descending central series

To take "maximal central descents" down a subgroup lattice: at each L_k, look down and ask

"*what's the smallest subgroup L_{k+1} where we can chop off so G/L_k remains central?*"



We call this the descending central series of G.

Another way to climb down a subgroup lattice

Definition

The **descending central series** is the normal series

$$G = L_0 \trianglerighteq L_1 \trianglerighteq L_2 \trianglerighteq \cdots, \qquad L_1 = [G, L_0],\ L_2 = [G, L_1], \ldots, L_{k+1} = [G, L_k].$$

It is "harder" to climb down a subgroup lattice in this manner than via the derived series:

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots, \qquad G' = [G, G],\ G'' = [G', G'], \ldots, G_{(k+1)} = [G^{(k)}, G^{(k)}].$$

Proposition

For any group G, we have $G^{(k)} \leq L_k$.

Proof

We start with $G^{(0)} = L_0 = G$ and $G^1 = L_1 = [G, G]$. However, at the second step,

$$G'' = [G', G'] \leq [G, G'] = [G, L_1] = L_2,$$

with the inequality due to $G' \leq G$. Inductively, if $G^{(k-1)} \leq L_{k-1}$, then

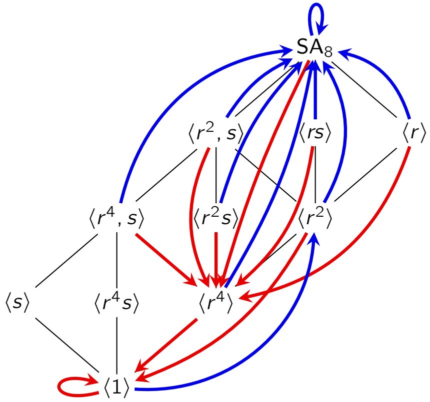
$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \leq [G, L_{k-1}] = L_k,$$

with the inequality holding because $G^{(k-1)} \leq G$ and $G^{(k-1)} \leq L_{k-1}$.

Chutes and Ladders diagrams

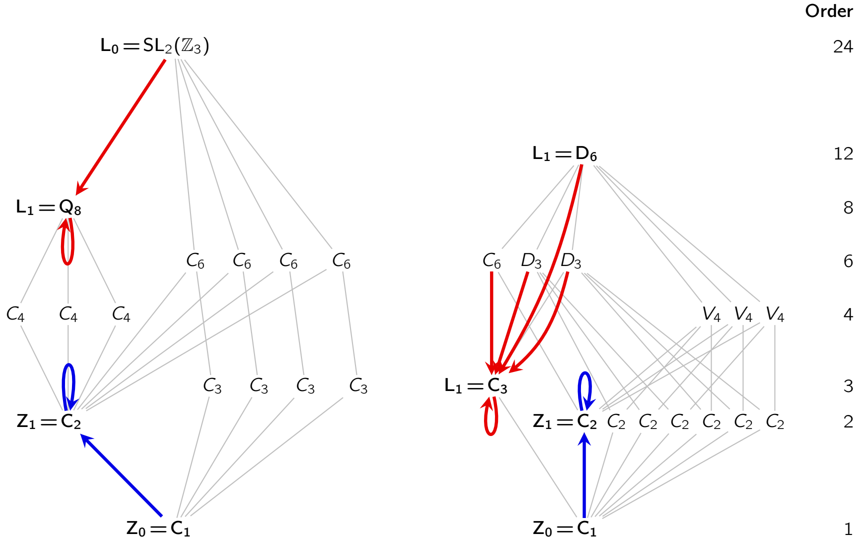
Define the **Chutes and Ladders diagram** of G from its lattice by adding, for each $N \trianglelefteq G$:

- a red arrow for each maximal central descent $N \searrow L$, i.e., $L = [G, N]$,
- a blue arrow for each maximal central ascent, $N \nearrow Z$, i.e., $Z/N = Z(G/N)$.



The ascending and descending central series can be read right off this diagram!

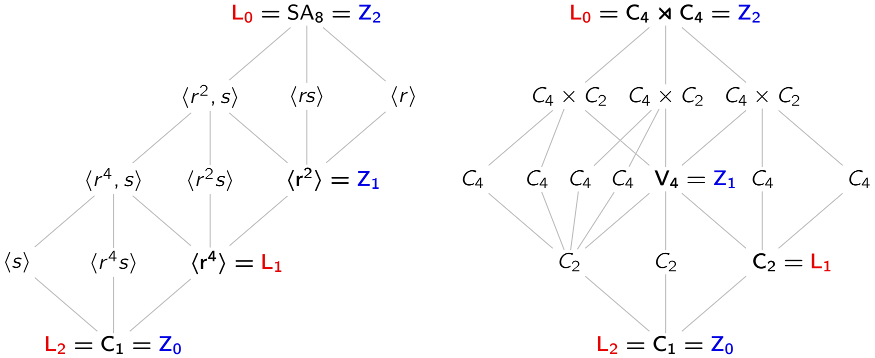
The chutes and ladders diagram of a non-nilpotent group



Ascending vs. descending central series

The ascending and descending central series differ for 6 of 9 nonabelian groups of order 16.

This is the smallest $|G|$ for which this happens.



Key idea (that we'll prove)

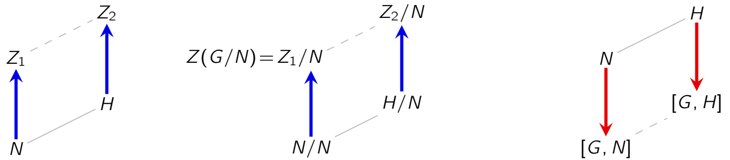
The ascending and descending central series have the same length.

Monotonicity of central ascents and descents

Proposition

Let $N \leq H \leq G$ be a chain of normal subgroups. Then

1. If $Z(G/N) = Z_1/N$ and $Z(G/H) = Z_2/H$, then $Z_1 \leq Z_2$.
2. $[G, N] \leq [G, H]$.



Proof of (i)

For any $z \in Z_1$, the coset zN is central in G/N, which means that, for all $g \in G$,

$$
\begin{aligned}
zNgN = gNzN \quad &\Longleftrightarrow \quad [z,g] \leq N && \textit{by the central series lemma} \\
&\Longrightarrow \quad [z,g] \leq H && \textit{by assumption, } N \leq H \\
&\Longleftrightarrow \quad zHgH = gHzH && \textit{by the central series lemma} \\
&\Longleftrightarrow \quad zH \in Z(G/H) && \textit{by definition of } Z(G/H) \\
&\Longleftrightarrow \quad z \in Z_2 && \textit{by definition; } Z(G/H) = Z_2/H.
\end{aligned}
$$

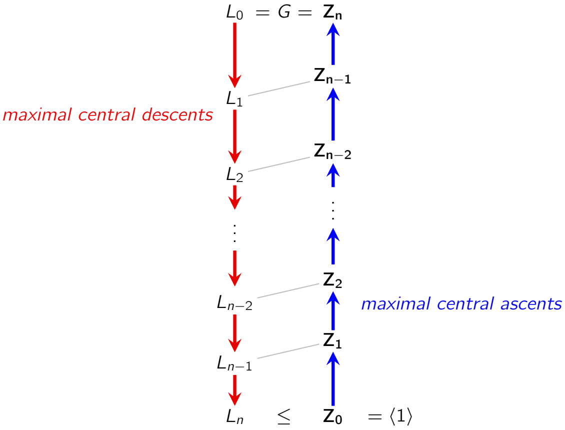
The crooked ladder theorem

Let G be a finite group, and suppose that either of the following hold:

1. The descending central series reaches the bottom: $L_{n-1} \gneq L_n = \langle 1 \rangle$.
2. The ascending central series reaches the top: $Z_{n-1} \lneq Z_n = G$.

Then for all $k = 0, \dots, n$,

$$L_{n-k} \leq Z_k.$$



The crooked ladder theorem

Let G be a finite group, and suppose that either of the following hold:

(i) The descending central series reaches the bottom: $L_{n-1} \gneq L_n = \langle 1 \rangle$.

(ii) The ascending central series reaches the top: $Z_{n-1} \lneq Z_n = G$.

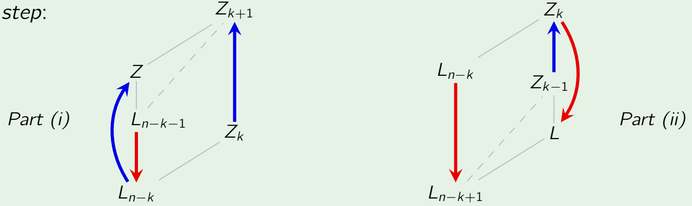
Then for all $k = 0, \dots, n$,

$$L_{n-k} \leq Z_k.$$

Proof of (i); Part (ii) is analogous (HW)

Induct on k. The base case is trivial: $L_n = Z_0 = \langle 1 \rangle$.

Inductive step:



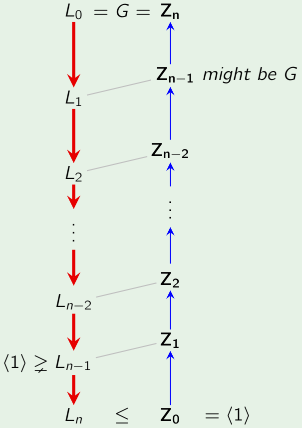
Note that L_{n-k-1} is a central ascent from L_{n-k}: $\overbrace{L_{n-k} \leq L_{n-k-1} \leq Z}^{L_{n+k-1}/L_{n-k} \in Z(G/L_{n-k})} \underbrace{\leq Z_{k+1}}_{\text{monotonicity}}$. □

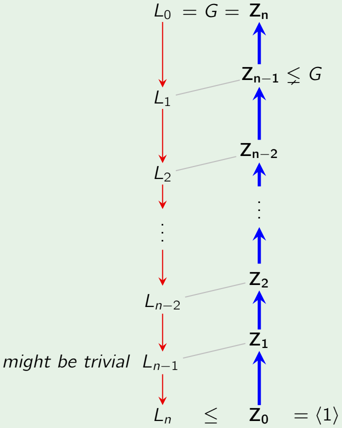
The ascending and descending central series have the same length

Corollary

The ascending central series reaches $Z_n = G$ iff the descending central series reaches $L_m = \langle 1 \rangle$. If this happens, their lengths are the same.

Proof

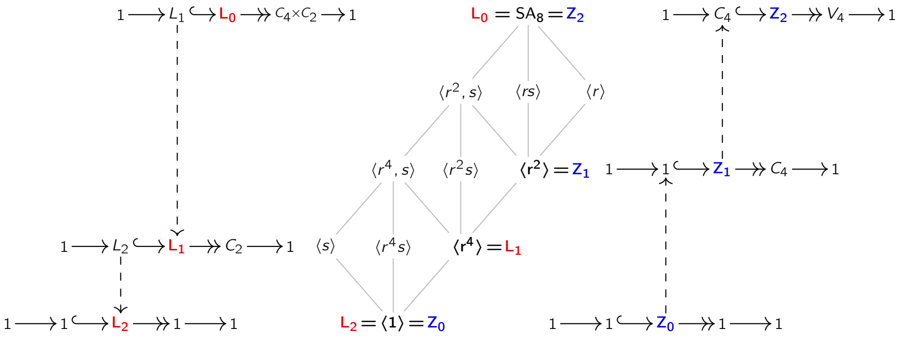




Ascending vs. descending central series

Here's a familiar example, higlighting the "crooked ladder property,"

$$L_{n-k} \leq Z_k, \qquad \textit{or equivalently, } L_k \leq Z_{n-k}.$$



Products of nilpotent groups are nilpotent

Lemma

If $G = H \times K$, then $L_n(G) = L_n(H) \times L_n(K)$ for all n.

Proof

The proof is by induction. The base case is easy:

$$G = L_0(G) = L_0(H) \times L_0(K) = H \times K.$$

Next, suppose that $L_k(G) = L_k(H) \times L_k(K)$. Then

$$\begin{aligned} L_{k+1}(G) = [H \times K, L_k(H \times K)] &= [H \times K, L_k(H) \times L_k(K)] \\ &= [H, L_k(H)] \times [K, L_k(K)] \\ &= L_{k+1}(H) \times L_{k+1}(K), \end{aligned}$$

and the result follows inductively.

Corollary

If H and K are nilpotent, then so is $G = H \times K$.

Normalizers grow in nilpotent groups

In the ascending central series, each Z_{i+1} was defined implictly, via $Z_{i+1}/Z_i = Z(G/Z_i)$.

Since Z_{i+1} is the maximal central ascent from Z_i, we have an explicit formula:

$$Z_{i+1} = \{x \in G \mid [x, g] \in Z_i, \ \forall g \in G\} = \{x \in G \mid xZ_i gZ_i = gZ_i xZ_i, \ \forall g \in G\}$$

Proposition

Subgroups of a nilpotent group G cannot be fully unnormal: if $H \lneq G$, then $H \lneq N_G(H)$.

Proof

Take the maximal Z_k containing H. We'll show that $N_G(H)$ contains Z_{k+1}.

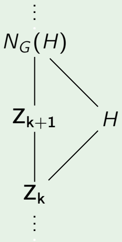
Pick some $x \in Z_{k+1}$. (Need to show it normalizes H.)

For all $g \in G$, we have $[x, g] \in Z_k$.

Thus, $[x, h] = xhx^{-1}h^{-1} \in Z_k \leq H$, for all $h \in H$.

Since $xhx^{-1}h^{-1} \in H$, then $xhx^{-1} \in H$.

Thus, $x \in N_G(H)$.



Sylow p-subgroups of nilpotent groups

Proposition

A finite group is nilpotent iff it is the internal direct product of its Sylow p-subgroups.

Proof

"$\Leftarrow$": by previous lemma.

"$\Rightarrow$": Let $P \in \mathrm{Syl}_p(G)$ be a Sylow p-subgroup.

Then "normalizers must grow", but also $N_G(N_G(P)) = N_G(P)$.

Thus $N_G(P) = G$, so $P \trianglelefteq G$ is the unique Sylow p-subgroup of G.

Let $P_1, \dots, P_k$ be the distinct Sylow p_i-subgroups of G. We need to verify:

1. $G = P_1 P_2 \cdots P_k$. ✓
2. each $P_i \trianglelefteq G$. ✓
3. each P_i trivially intersects

$$Q_i := \langle P_j \mid j \neq i \rangle.$$

If $g \in P_i \cap Q_i$, then $|g| = p_i^\ell$ divides $\prod_{j \neq i} p_j^{d_j}$, which is co-prime to p_i. ✓

Central series

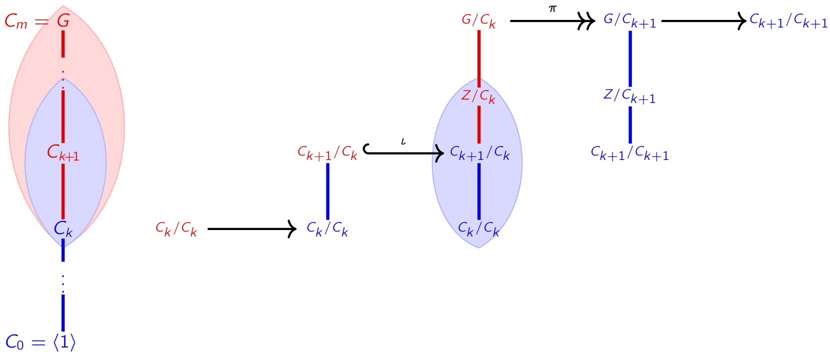
Definition

A **central series** of a group G is a normal series

$$\langle 1\rangle = C_0 \trianglelefteq C_1 \trianglelefteq \cdots \trianglelefteq C_m = G, \quad \text{such that} \quad C_{k+1}/C_k \leq Z(G/C_k).$$

Equivalently, G/C_k **is a central extension of** G/C_{k+1} **by** C_{k+1}/C_k.

$$1 \longrightarrow C_{k+1}/C_k \xrightarrow{\iota_k} G/C_k \xrightarrow{\pi_k} G/C_{k+1} \longrightarrow 1$$



Central series

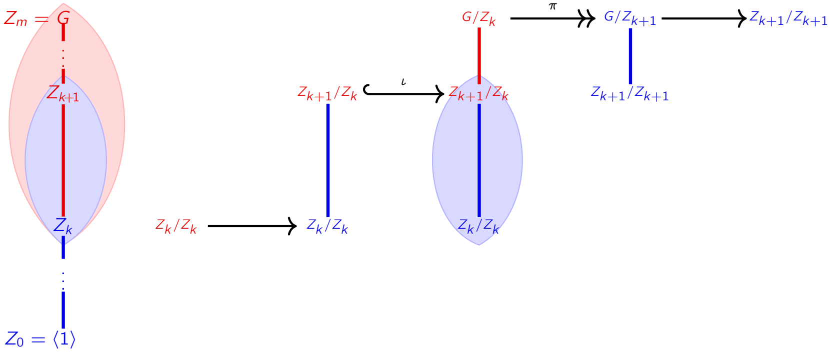
Remark

The **ascending central series** of a nilpotent group G is a normal series

$$\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_m = G, \quad \text{such that} \quad Z_{k+1}/Z_k = Z(G/Z_k).$$

Equivalently, G/Z_k **is the maximal central extension of** G/Z_{k+1} (by Z_{k+1}/Z_k).

$$1 \longrightarrow Z_{k+1}/Z_k \stackrel{\iota_k}{\longrightarrow} G/Z_k \stackrel{\pi_k}{\longrightarrow} G/Z_{k+1} \longrightarrow 1$$



Central series

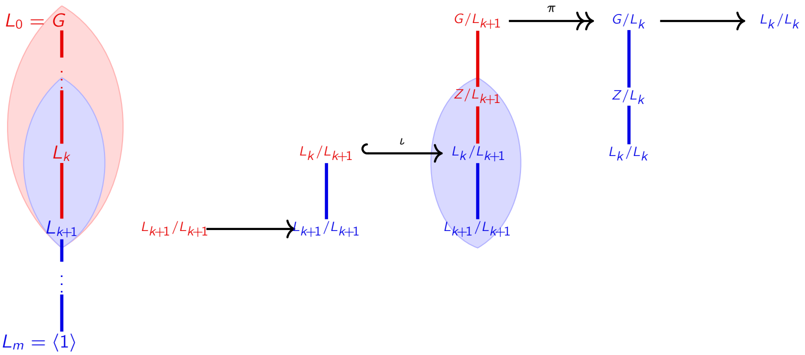
Remark

The **descending central series** of a group G is a normal series

$$G = L_0 \trianglerighteq L_1 \trianglerighteq \cdots \trianglerighteq L_m = G, \quad \text{such that} \quad L_k/L_{k+1} \leq Z(G/L_{k+1}).$$

Equivalently, G/L_{k+1} **is a central extension of** G/C_k **by** L_k/L_{k+1}.

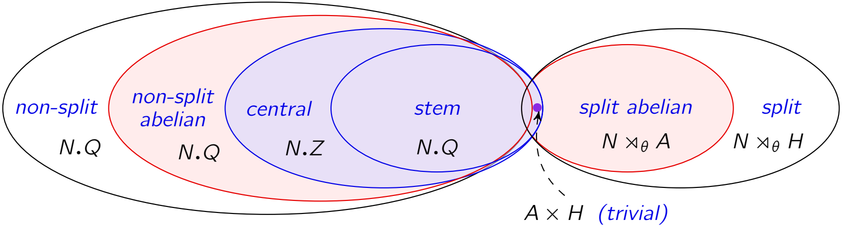
$$1 \longrightarrow L_k/L_{k+1} \xrightarrow{\iota_k} G/L_{k+1} \xrightarrow{\pi_k} G/L_k \longrightarrow 1$$



Solvability and nilpotency in terms of extensions

Summary

- **Every finite group** can be constructed from **extensions of simple groups**.
- Solvable groups can be constructed from abelian extensions.
- Nilpotent groups can be constructed from central extensions.



Summary of nilpotent groups

Theorem

A finite group G is nilpotent if any of the following conditions hold:

1. $Z_n = G$ for some n ("*the ascending central series reaches the top*")
2. $L_m = \langle 1 \rangle$ for some m, ("*descending central series reaches the bottom*")
3. $H \lneq N_G(H)$ for all proper subgroups, ("*no fully unnormal subgroups*")
4. All Sylow p-subgroups are normal.
5. G is the direct product of its Sylow p-subgroups.
6. Every maximal subgroup of G is normal.