Chapter 6: Extensions of groups

Matthew Macauley

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

Math 4130, 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)
   - (d) Groups built from a (right) split extension (semidirect products)
   - (e) Groups built from a left split extension (direct products)

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 $k = 0, 1, \ldots, n$.

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 $k = 0, 1, \ldots, n$, and let $|H| = p^{n-1}$.

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

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

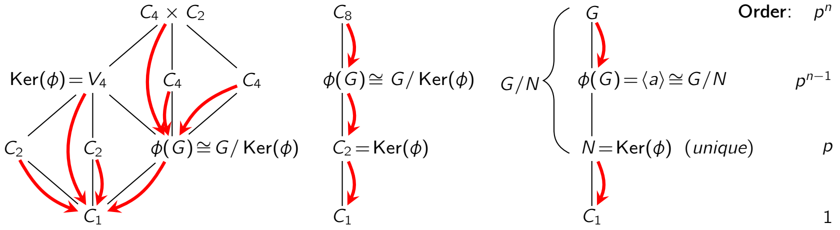
Induct on n, where $|G| = p^n$. The base case is trivial.

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}. $\square$

Index:		
1	G	$G/N \cong \phi(G)$
p	$\phi(G) \cong G/N$	$\phi(G)/N$
$p^{n-(k+1)}$	H	H/N (*unique*)
p^{n-1}	$N = \mathrm{Ker}(\phi)$ (*unique*)	N/N
p^n	$\langle 1 \rangle$	

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.

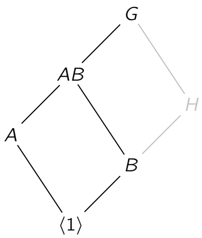
Proof

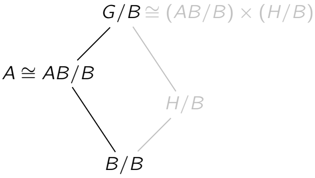
Induct on n, where $|G| = p^n$. The base case is trivial.

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

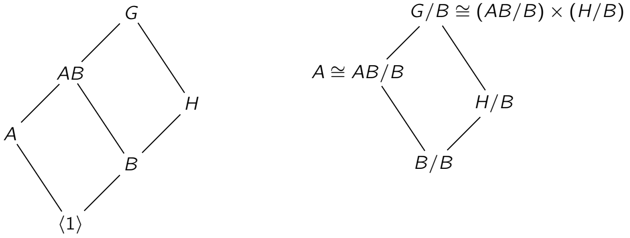
Let G be a finite abelian p-group, and $A \leq G$ a maximal cyclic subgroup. Then $G = A \times H$ for some subgroup H.

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.)

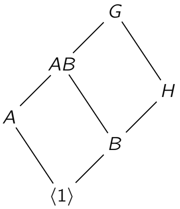
It suffices to show that A and H are lattice complements in G.

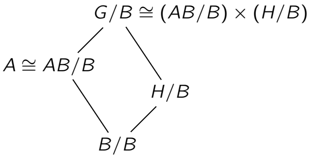
Generate G: Since $B \leq H$, we have $BH = H$ and $AB \subseteq AH$, and hence

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

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 $|G|$. $\square$

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. $\square$

Conjugacy classes in A_n

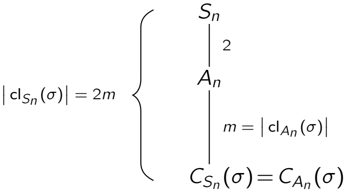
Elements in S_n are conjugate iff they have the same cycle type.

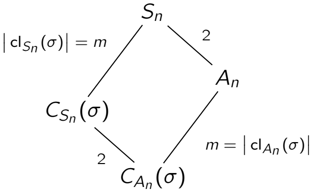
However, 8 of the 12 elements in A_4 are 3-cycles. These cannot all be conjugate.

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: $\text{cl}_{S_5}(e) = \{e\}$, and

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

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.

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

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. $\square$

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.

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

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.

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

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

$$\begin{aligned}\underbrace{(a_1 a_4)(a_2 a_3)\pi[(a_1 a_4)(a_2 a_3)]^{-1}}_{\in N} \cdot \pi^{-1} &= (a_1 a_4)(a_2 a_3)(a_1 a_4 a_5)(a_1 a_4)(a_2 a_3)(a_5 a_4 a_1) \\ &= (a_1 a_4 a_5) \in N. \qquad \checkmark\end{aligned}$$

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

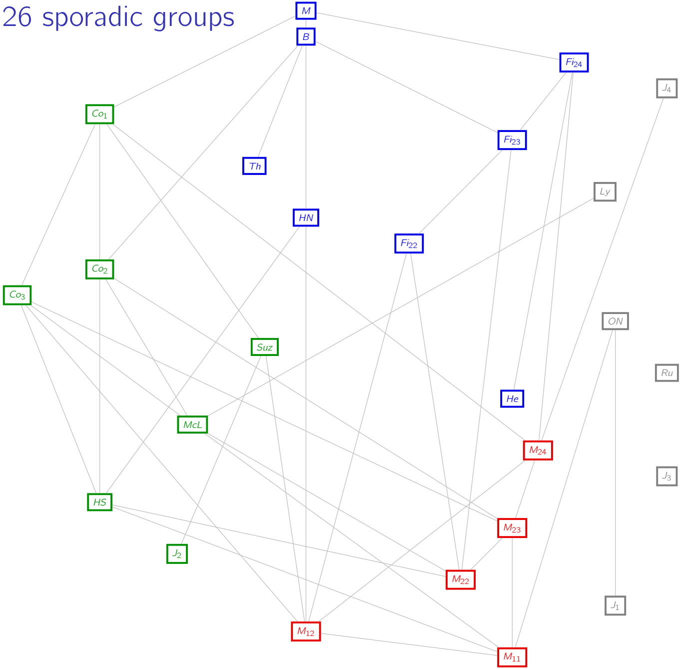
$$|B| = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4.15 \times 10^{33};$$

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

The 26 sporadic groups

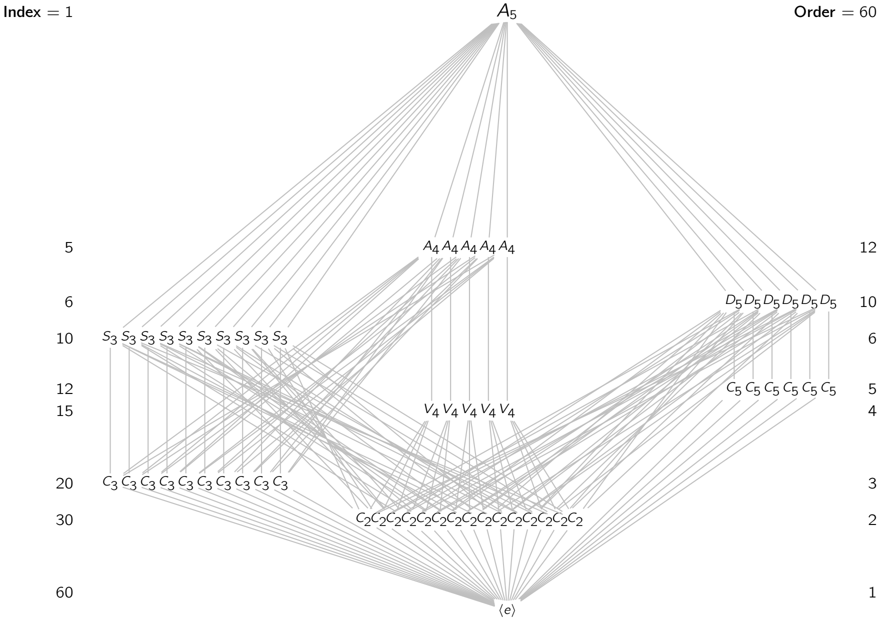


Order $= 8.08 \times 10^{53}$
4.15×10^{33}
1.26×10^{24}
8.68×10^{19}
4.16×10^{18}
4.09×10^{18}
9.07×10^{16}
5.18×10^{16}
2.73×10^{14}
6.46×10^{13}
4.23×10^{13}
4.96×10^{11}
4.61×10^{11}
4.48×10^{11}
1.46×10^{11}
4,030,387,200
898,128,000
244,823,040
50,232,960
44,352,000
10,200,960
604,800
443,520
175,560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

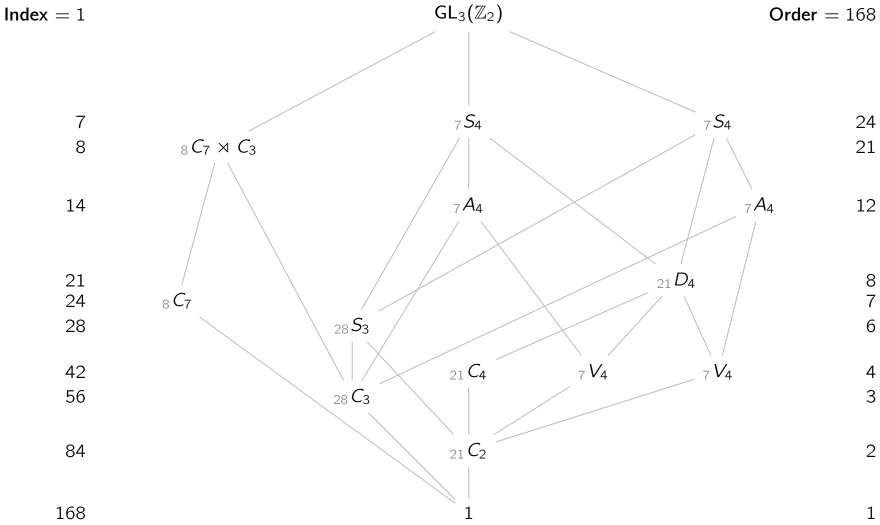
The 31 nonabelian simple groups of order less than 100,000

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

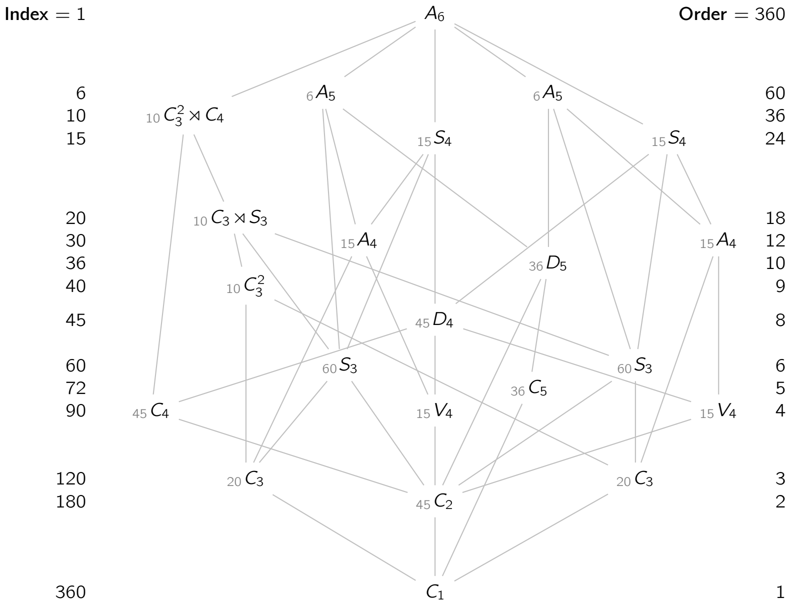
The smallest nonabelian simple group ("group atom")



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



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



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

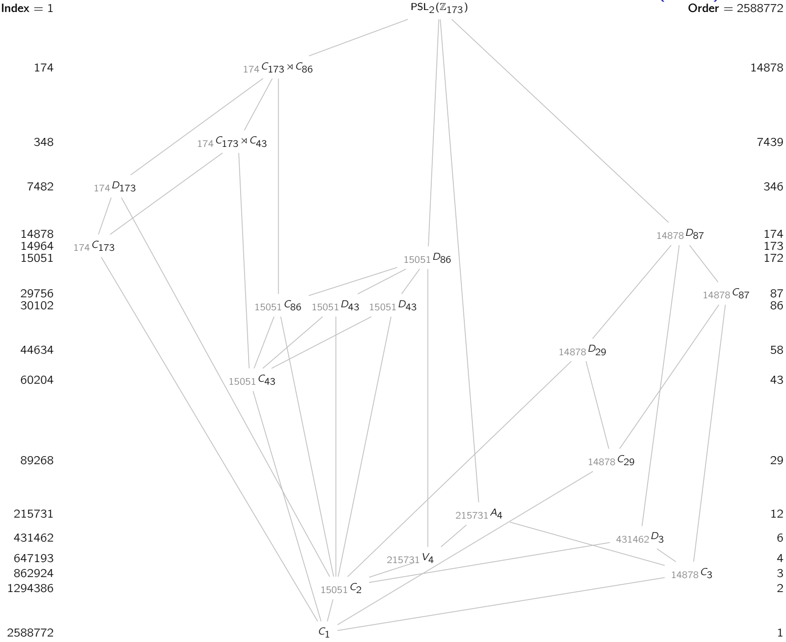
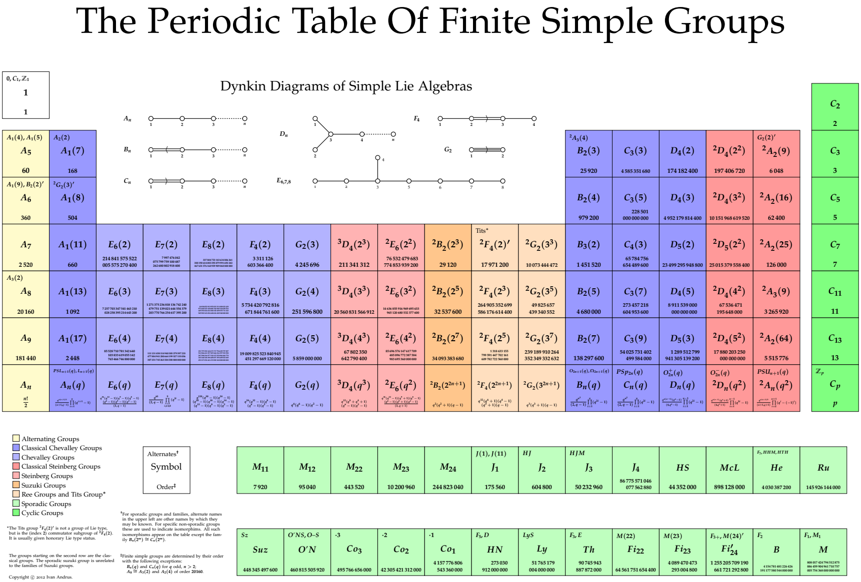


Image by *Ivan Andrus*, 2012



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

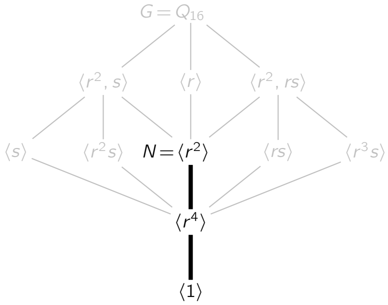
	Name	Artist	Time	Price	
1	Power of One	Klein Four	5:16	$0.99	View In iTunes ▸
2	Finite Simple Group (of Order Two)	Klein Four	3:00	$0.99	View In iTunes ▸
3	Three-Body Problem	Klein Four	3:17	$0.99	View In iTunes ▸
4	Just the Four of Us	Klein Four	4:19	$0.99	View In iTunes ▸
5	Lemma	Klein Four	3:43	$0.99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

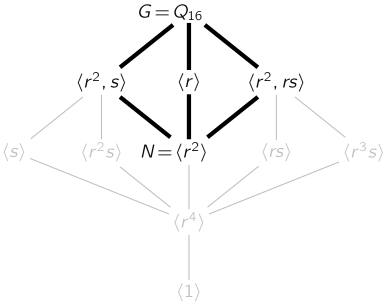
Chopping off subgroup lattices

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 $N \trianglelefteq G$"

What is a group extension?

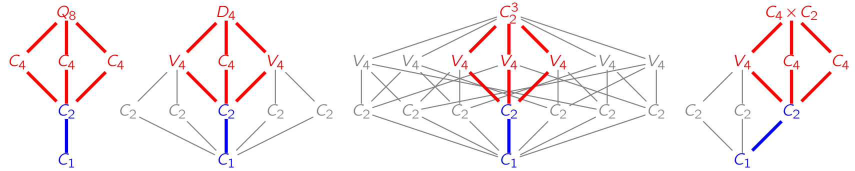
Every normal subgroup $N \trianglelefteq G$ canonically defines two sublattices.

- "*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

$$\begin{tikzcd} N \arrow[r, hook, "\iota"] & G \arrow[r, two heads, "\pi"] & Q \end{tikzcd}$$

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

Extensions and short exact sesquences

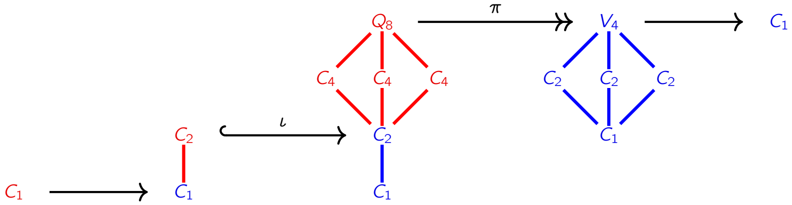
If we write

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

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**.



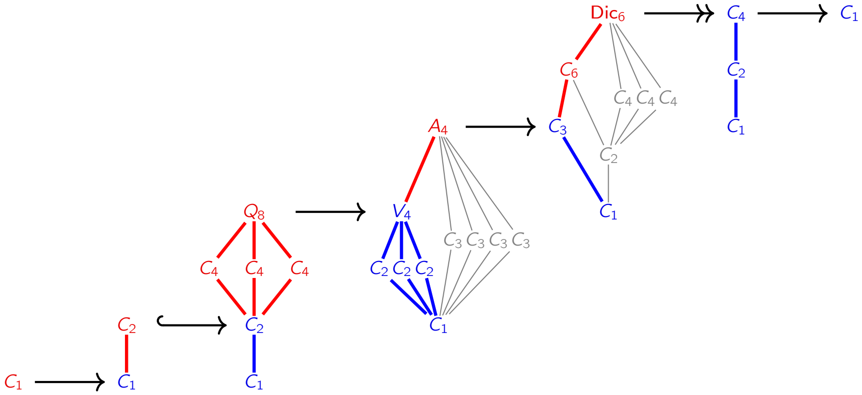
More on exact sequences

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:

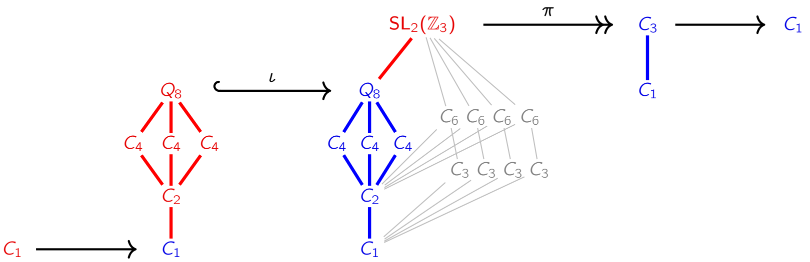
$$0 \longrightarrow L^2 \xrightarrow{\text{grad}} \mathbb{H}_3 \xrightarrow{\text{curl}} \mathrm{Im}(\mathrm{curl}) \longrightarrow 0$$

Here is an exact sequence with 7 groups:

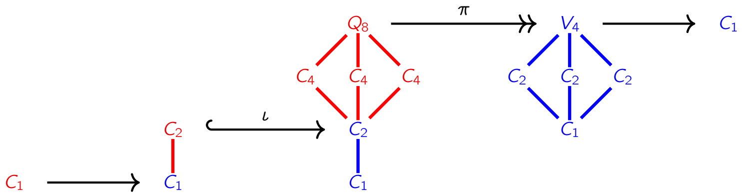


Iterative extensions

The group $\mathsf{SL}_2(\mathbb{Z}_3)$ is an extension of C_3 by Q_8...

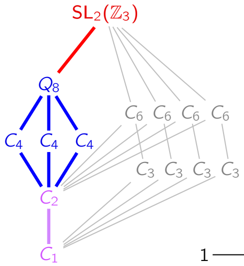


...and Q_8 is an extension of V_4 by C_2:



Iterative extensions

$\mathrm{SL}_2(\mathbb{Z}_3)$ is an extension of C_3 by Q_8, which is an extension of V_4 by C_2:



$$\begin{tikzcd}
 & & & 1 \arrow[r] & Q_8 \arrow[r, hook] \arrow[d, dashed] & \mathrm{SL}_2(\mathbb{Z}_3) \arrow[r, two heads] & C_3 \arrow[r] & 1 \\
 & & 1 \arrow[r] & C_2 \arrow[r, hook] \arrow[d, dashed] & Q_8 \arrow[r, two heads] & V_4 \arrow[r] & 1 & \\
 & 1 \arrow[r] & C_1 \arrow[r, hook] \arrow[d, dashed] & C_2 \arrow[r, two heads] & C_2 \arrow[r] & 1 & & \\
1 \arrow[r] & C_1 \arrow[r, hook] & C_1 \arrow[r, two heads] & C_1 \arrow[r] & 1 & & &
\end{tikzcd}$$

The bottom two exact sequences are unnecessary, but nice to have.

We can represent this as a **subnormal series** of steps down the subgroup lattice:

$$\mathrm{SL}_2(\mathbb{Z}_3) \trianglerighteq Q_8 \trianglerighteq C_2 \trianglerighteq C_1.$$

The subquotients C_3, V_4, and C_2 are the **factors**.

Key idea

Every **descending subnormal series** describes an iterated sequence of extensions.

Extension equivalence

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

The "extension problem"

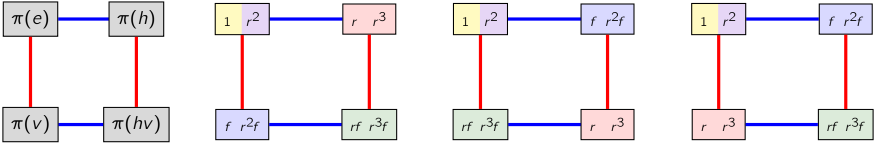
Find all possibilities for the "middle term" G in a short exact sequence, given N and Q.

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

$$\begin{tikzcd}
1 \arrow[r] & N_1 \arrow[r, "\iota_1"] \arrow[d, "\nu"] & G_1 \arrow[r, "\pi_1"] \arrow[d, "\gamma"] & Q_1 \arrow[r] \arrow[d, "\kappa"] & 1 \\
1 \arrow[r] & N_2 \arrow[r, "\iota_2"] & G_2 \arrow[r, "\pi_2"] & Q_2 \arrow[r] & 1
\end{tikzcd}$$

$$\begin{tikzcd}
 & & G \arrow[dr, "\pi"] \arrow[dd, dashed, "\gamma"] & & \\
1 \arrow[r] & N \arrow[ur, hook, "\iota"] \arrow[dr, hook, "\iota'"'] & & Q \arrow[r] & 1 \\
 & & G \arrow[ur, "\pi'"'] & &
\end{tikzcd}$$

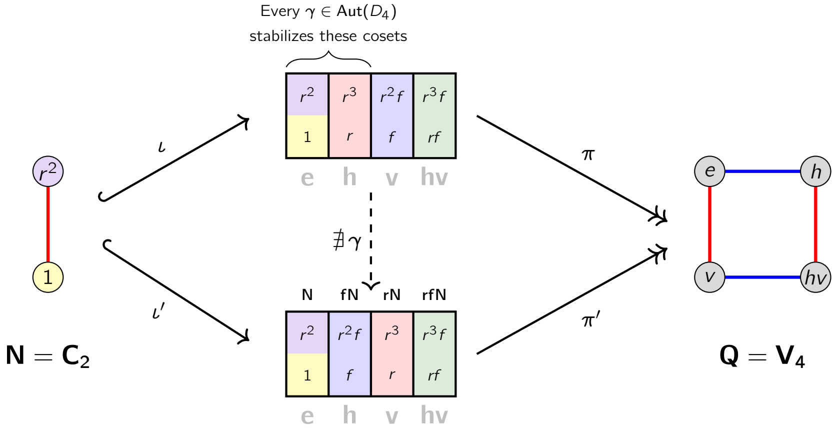
Do you see why these three extensions of V_4 by C_2 do *not* differ by an automorphism?



Extension equivalence

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

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



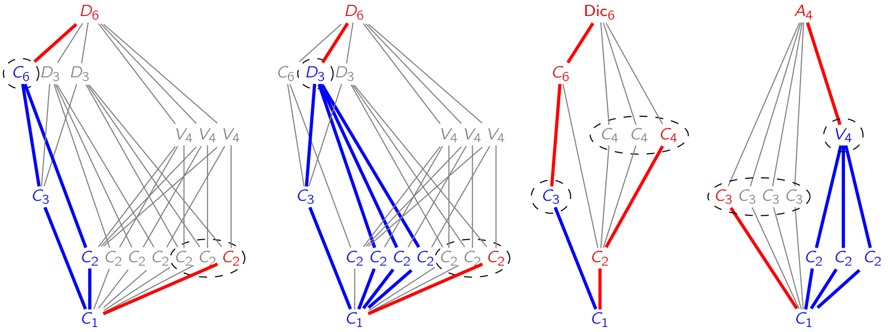
Semidirect products and extensions

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

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

In the subgroup lattice, we can see

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



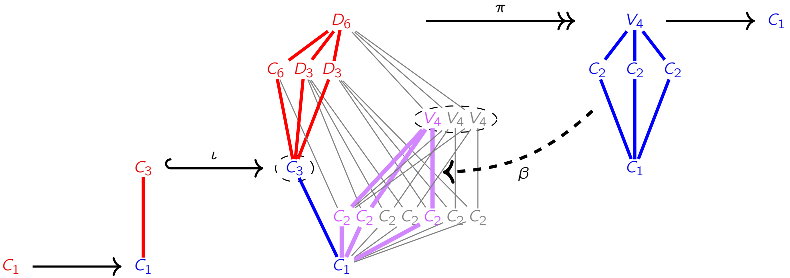
Do you see a canonical injection from $Q \cong G/N \cong H$ "*down to*" $H \le G$?

Split exact sequences

Definition

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

$$
\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] \arrow[l, bend left, dashed, "\beta"] & 1
\end{tikzcd}
$$



Split exact sequences and semidirect products

Theorem

A short exact sequence
$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] \arrow[l, bend left, dashed, "\beta"] & 1 \end{tikzcd}$$
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 $n = gh^{-1} \in \iota(N) = \mathrm{Ker}(\pi)$:

$$\begin{aligned} \pi(n) = \pi(gh^{-1}) = \pi(g)\pi(h)^{-1} &= \pi(g) \cdot \pi(\beta(\pi(g)))^{-1} && \textit{because } h = \beta(\pi(g)) \\ &= \pi(g) \cdot \mathrm{Id}_H\,(\pi(g))^{-1} && \textit{because } \pi \circ \beta = \mathrm{Id}_H \\ &= \pi(g) \cdot \pi(g)^{-1} = 1_H. \end{aligned}$$

✓

Split exact sequences and semidirect products

Theorem

A short exact sequence
$$
\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] \arrow[l, bend left, dashed, "\beta"] & 1
\end{tikzcd}
$$
splits if and only if $G \cong N \rtimes_\theta H$.

Proof

"$\Rightarrow$": 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 $g = \beta(h)$.

  It suffices to show that $g = 1_G$. First, note that

$$
\begin{aligned}
1_H &= \pi(g) && \textit{because } g \in \iota(N) = \mathrm{Im}(\iota) = \mathrm{Ker}(\pi) \\
&= \pi(\beta(h)) && \textit{because } g = \beta(h) \\
&= \mathrm{Id}_H(h) = h. && \textit{because } \pi \circ \beta = \mathrm{Id}_H
\end{aligned}
$$

  Therefore, $g = \beta(h) = \beta(1_H) = 1_G$. $\square$

Split exact sequences and semidirect products

Here is another way that we could formalize the previous result:

"*right split means semidirect product*."

Theorem (exercise)

Given a short exact sequence $1 \to N \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} H \to 1$, the following are equivalent:

(i) There is a backwards map $\beta\colon H \to G$ such that $\pi \circ \beta = \mathrm{Id}_H$.

(ii) There is a homomorphism $\theta\colon H \to \mathrm{Aut}(N)$ and isomorphism $\gamma\colon G \to N \rtimes_\theta H$ that makes the following diagram commute:

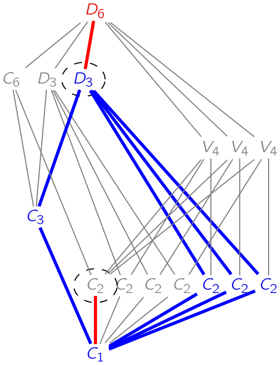
$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "\mathrm{Id}"] & G \arrow[r, "\pi"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\iota'"] & N \rtimes_\theta H \arrow[r, "\pi'"] & H \arrow[r] & 1
\end{tikzcd}$$

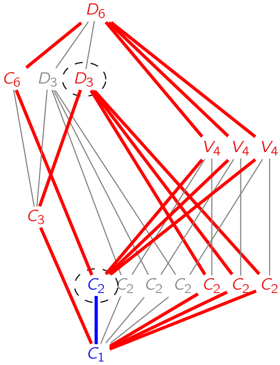
Split exact sequences and direct products

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

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota_1"] & N \times H \arrow[r, "\pi_1"] & H \arrow[r] \arrow[l, bend left, dashed, "\beta_1"] & 1 \end{tikzcd} \qquad \begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\iota_2"] & H \times N \arrow[r, "\pi_2"] & N \arrow[r] \arrow[l, bend left, dashed, "\beta_2"] & 1 \end{tikzcd}$$

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



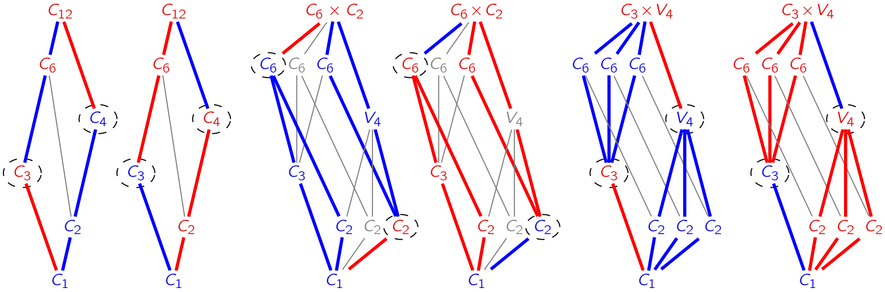


Split exact sequences and direct products

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

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota_1"] & N \times H \arrow[r, "\pi_1"] \arrow[l, dashed, bend left, "\alpha_1"] & H \arrow[r] \arrow[l, dashed, bend left, "\beta_1"] & 1 \end{tikzcd} \qquad \begin{tikzcd} 1 \arrow[r] & H \arrow[r, "\iota_2"] & N \times H \arrow[r, "\pi_2"] \arrow[l, dashed, bend left, "\alpha_2"] & N \arrow[r] \arrow[l, dashed, bend left, "\beta_2"] & 1 \end{tikzcd}$$

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:



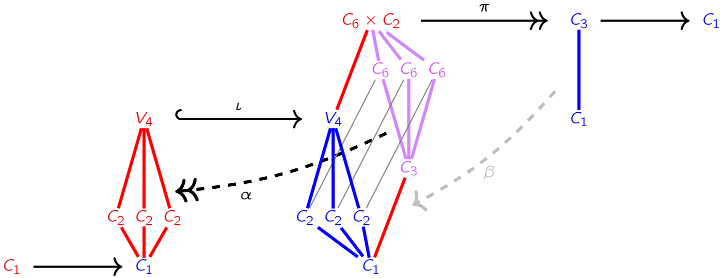
Split exact sequences and direct products

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 $\alpha \circ \iota = \mathrm{Id}_N$:

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[l, bend left, dashed, two heads, "\alpha"] \arrow[r, "\pi"] & H \arrow[l, bend left, dashed, "\beta"] \arrow[r] & 1 \end{tikzcd}$$



Split exact sequences and direct products

Theorem (exercise)

Given a short exact sequence $1 \longrightarrow N \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} H \longrightarrow 1$, the following are equivalent:

(i) There is a backwards map $\alpha \colon G \to N$ such that $\alpha \circ \iota = \mathrm{Id}_N$.

(ii) There is an isomorphism $\gamma \colon G \to N \times H$ that makes the following diagram commute:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "\mathrm{Id}"] & G \arrow[r, "\pi"] \arrow[d, "\gamma"] & H \arrow[r] \arrow[d, "\mathrm{Id}"] & 1 \\
1 \arrow[r] & N \arrow[r, "\iota'"] & N \times H \arrow[r, "\pi'"] & H \arrow[r] & 1
\end{tikzcd}$$

Since every direct product is a semidirect product, we get the following.

Corollary

If a short exact sequence $1 \to N \hookrightarrow G \twoheadrightarrow H \to 1$ is left split, then it is right split. $\square$

Split exact sequences and direct products

Key idea

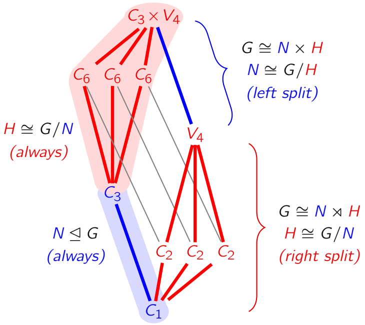
- If a short exact sequence is left split, then it is right split.

  "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"

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] \arrow[l, bend left, dashed, "\alpha"] & H \arrow[r] \arrow[l, bend left, dashed, "\beta"] & 1 \end{tikzcd}$$



An important counterexample

In the exact sequence we've seen,

- $\iota \colon N \hookrightarrow G$ is the inclusion
- $\pi \colon N \times H \twoheadrightarrow H$ is the projection.

If these maps are different, then $1 \to N \overset{\iota}{\hookrightarrow} N \times H \overset{\pi}{\twoheadrightarrow} H \to 1$ need not split!

Consider the groups $N = \prod_{i=0}^{\infty} \mathbb{Z}$ and $H = \prod_{i=0}^{\infty} \mathbb{Z}_2$, and maps

$$\begin{aligned} \iota \colon N &\longrightarrow N \times H \\ \iota \colon (n_i) &\longmapsto \big((2n_i), 0\big), \end{aligned} \qquad \begin{aligned} \pi \colon N \times H &\longrightarrow H \\ \pi \colon \big((n_i), (h_i)\big) &\longmapsto \big(\overline{n_1}, h_1, \overline{n_2}, h_2, \dots\big), \end{aligned}$$

where $\overline{n_i} = n_i \pmod 2$.

Exercise

(i) Prove that $1 \to N \xrightarrow{\iota} N \times H \xrightarrow{\pi} H \to 1$ is exact.

(ii) Show there does *not* exist a backward map $\beta \colon H \to N \times H$ such that $\pi \circ \beta = \mathrm{Id}_H$.

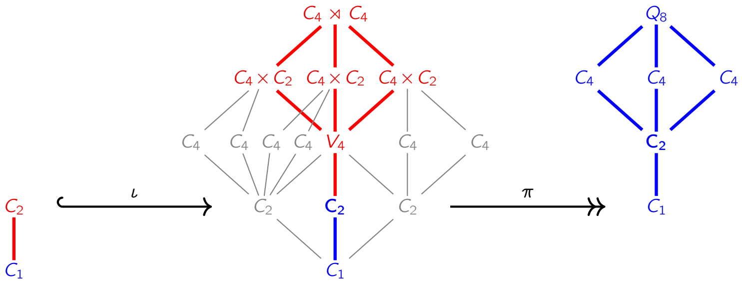
Other types of groups extensions

Definition

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

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

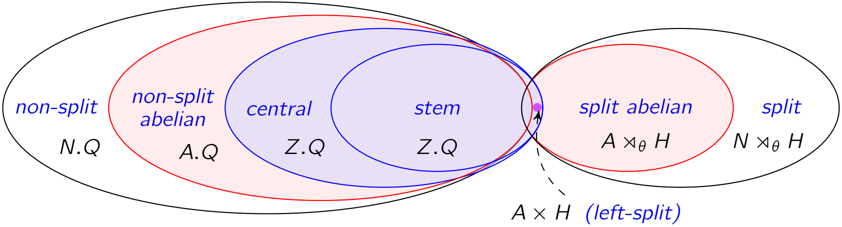
The group $G = C_4 \rtimes C_4$ is a central (and hence abelian), nonsplit extension of $Q = Q_8$ by $N = C_2$.



Other 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 constructed with an iterative sequence of:

- 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

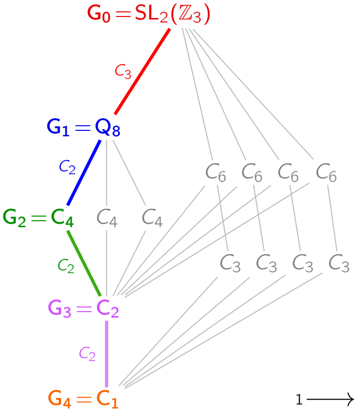
Breaking down a group into composition factors is like factoring a number into primes, or a molecule into atoms. We say:

"*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.

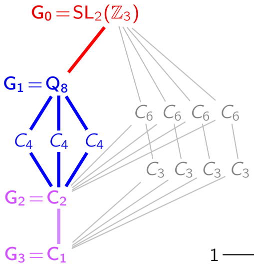


$$\begin{tikzcd}[column sep=small]
 & & & & 1 \arrow[r] & Q_8 \arrow[r, hook] \arrow[d, dashed] & SL_2(\mathbb{Z}_3) \arrow[r, two heads] & \mathbf{C_3} \arrow[r] & 1 \\
 & & & 1 \arrow[r] & C_4 \arrow[r, hook] \arrow[d, dashed] & \mathbf{Q_8} \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & \\
 & & 1 \arrow[r] & C_2 \arrow[r, hook] \arrow[d, dashed] & \mathbf{C_4} \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & & \\
 & 1 \arrow[r] & C_1 \arrow[r, hook] \arrow[d, dashed] & \mathbf{C_2} \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & & & \\
1 \arrow[r] & C_1 \arrow[r, hook] & \mathbf{C_1} \arrow[r, two heads] & C_1 \arrow[r] & 1 & & & &
\end{tikzcd}$$

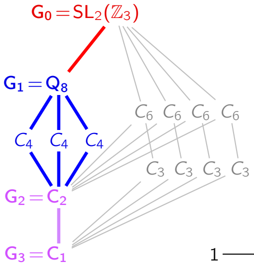
They will always be either *cyclic* or *non-abelian simple* (e.g., A_5, $\mathbf{GL}_3(\mathbb{Z}_2)$, $A_6, \ldots$).

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

Descending vs. ascending series



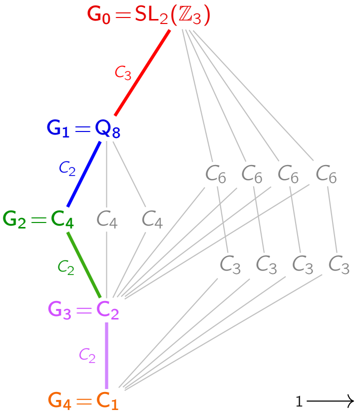
$$\begin{tikzcd}
 & & & 1 \arrow[r] & Q_8 \arrow[r, hook] \arrow[d, dashed] & SL_2(\mathbb{Z}_3) \arrow[r, two heads] & C_3 \arrow[r] & 1 \\
 & & 1 \arrow[r] & C_2 \arrow[r, hook] \arrow[d, dashed] & Q_8 \arrow[r, two heads] & V_4 \arrow[r] & 1 & \\
 & 1 \arrow[r] & C_1 \arrow[r, hook] \arrow[d, dashed] & C_2 \arrow[r, two heads] & C_2 \arrow[r] & 1 & & \\
1 \arrow[r] & C_1 \arrow[r, hook] & C_1 \arrow[r, two heads] & C_1 \arrow[r] & 1 & & &
\end{tikzcd}$$



$$\begin{tikzcd}
 & & & 1 \arrow[r] & C_1 \arrow[r, hook] & C_1 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & C_3 \arrow[r, hook] & C_3 \arrow[r, two heads] & C_1 \arrow[r] \arrow[u, dashed] & 1 & \\
 & 1 \arrow[r] & V_4 \arrow[r, hook] & A_4 \arrow[r, two heads] & C_3 \arrow[r] \arrow[u, dashed] & 1 & & \\
1 \arrow[r] & C_2 \arrow[r, hook] & SL_2(\mathbb{Z}_3) \arrow[r, two heads] & A_4 \arrow[r] \arrow[u, dashed] & 1 & & &
\end{tikzcd}$$

Descending vs. ascending series

Do you see why there's no way to create an iterative sequence of extensions by climbing *up* the lattice?



$$\begin{tikzcd}
 & & & & 1 \arrow[r] & C_1 \arrow[r, hook] & C_1 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & & 1 \arrow[r] & C_3 \arrow[r, hook] & C_3 \arrow[r, two heads] & C_1 \arrow[r] \arrow[u, dashed] & 1 & \\
 & & 1 \arrow[r] & C_2 \arrow[r, hook] & C_4 \arrow[r, two heads] & C_2 \arrow[r] \arrow[u, dashed] & 1 & & \\
 & 1 \arrow[r] & C_2 \arrow[r, hook] & A_4 \arrow[r, two heads] & C_4 \arrow[r] \arrow[u, dashed] & 1 & & & \\
1 \arrow[r] & C_2 \arrow[r, hook] & SL_2(\mathbb{Z}_3) \arrow[r, two heads] & A_4 \arrow[r] \arrow[u, dashed] & 1 & & & &
\end{tikzcd}$$

What's wrong with this picture?!

Descending vs. ascending series

Key idea

Every **subnormal series**

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{m-1} \trianglerighteq G_m = \langle 1 \rangle$$

defines an **iterative descending sequence of extensions**:

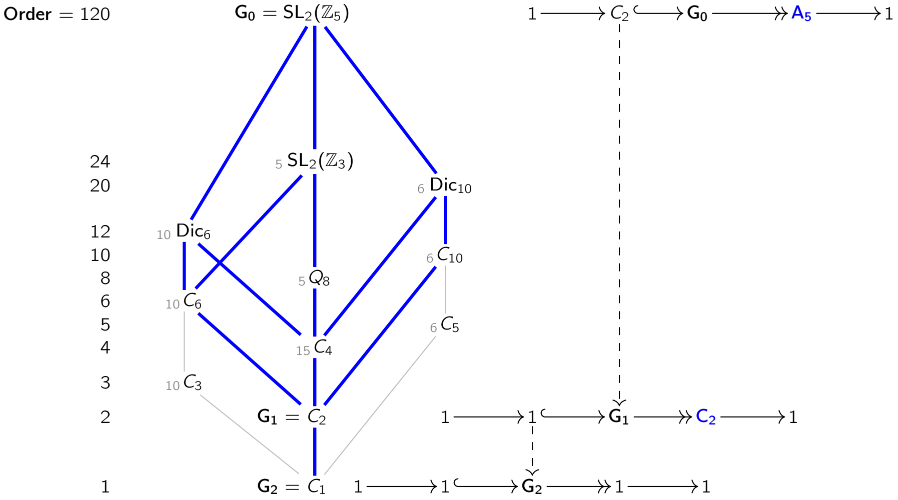
- G_0 is an extension of G_0/G_1 by G_1
- G_1 is an extension of G_1/G_2 by G_2
- $\vdots$
- G_{m-1} is an extension of G_{m-1}/G_m by G_m.

Moreover, if it's a **normal series**, it defines an **iterative ascending sequence of extensions**:

- G_0/G_m is an extension of G_0/G_{m-1} by G_{m-1}/G_m
- G_0/G_{m-1} is an extension of G_0/G_{m-2} by G_{m-2}/G_{m-1}
- $\vdots$
- G_0/G_1 is an extension of G_0/G_0 by G_0/G_1.

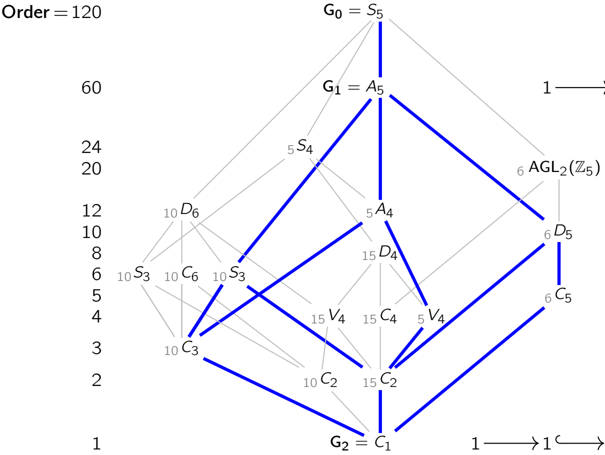
Composition series and simple extensions

The group $G = \mathrm{SL}_2(\mathbb{Z}_5)$ 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.



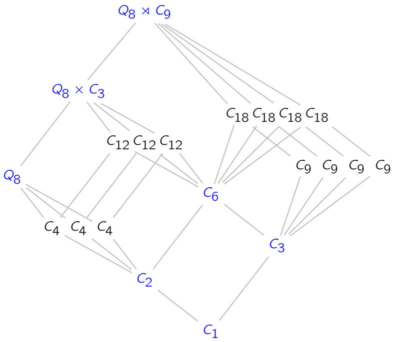
$$
\begin{tikzcd}
 & & 1 \arrow[r] & A_5 \arrow[r, hook] \arrow[d, dashed] & \mathbf{G_0} \arrow[r, two heads] & \color{blue}{\mathbf{C_2}} \arrow[r] & 1 \\
 & 1 \arrow[r] & 1 \arrow[r, hook] \arrow[d, dashed] & \mathbf{G_1} \arrow[r, two heads] & \color{blue}{\mathbf{A_5}} \arrow[r] & 1 & \\
1 \arrow[r] & 1 \arrow[r, hook] & \mathbf{G_2} \arrow[r, two heads] & 1 \arrow[r] & 1 & &
\end{tikzcd}
$$

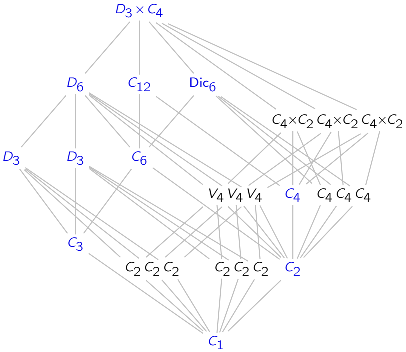
Equivalence of composition series

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.





Jordan-Hölder theorem (upcoming)

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

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:

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

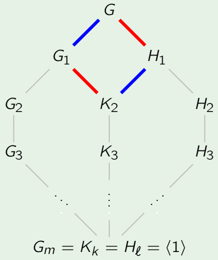
and the result holds for all groups with a composition series of length $\leq m$.

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.



Chief series

Definition

A **chief series** of G is a normal series

$$\langle 1\rangle = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_k = G$$

for which each "**chief factor**" N_{i+1}/N_i is a minimal normal subgroup of G/N_i.

Composition vs. chief series

Construction

- Composition series: descending, iteratively pick maximal normal subgroups
- Chief series: ascending, iteratively pick minimal normal subgroups.

Characterization

- Composition series: any maximal subnormal series
- Chief series: any maximal normal series

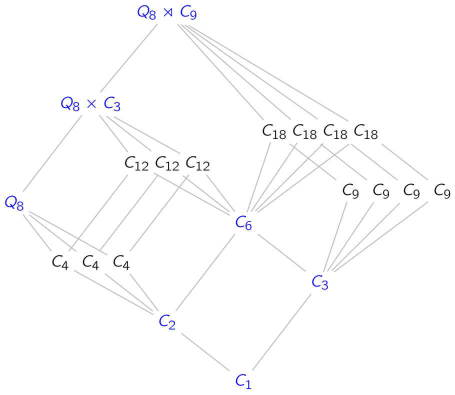
Factors

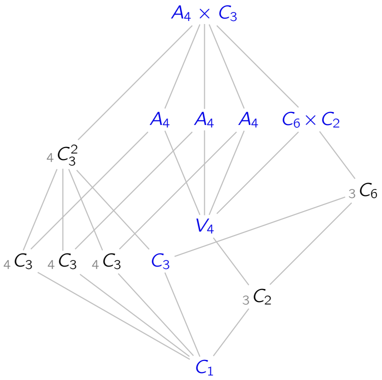
- Composition factors: simple groups
- Chief series: direct products $S \times \cdots \times S$ of a simple group.

There is an analogous "Jordan-Hölder theorem" for chief series.

Composition vs. chief series

Let's compare the composition and chief series in the following groups.





Proposition (exercise)

Every subnormal series can be refined to a composition series.

Solvability and the derived series

Recall that the commutator subgroup is defined as

$$G' = \left\langle xyx^{-1}y^{-1} \mid x, y \in G \right\rangle.$$

This is the "*smallest group N such that G/N is abelian.*"

Given subgroups H and K of G, define

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

We can define higher commutator subgroups,

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

Definition

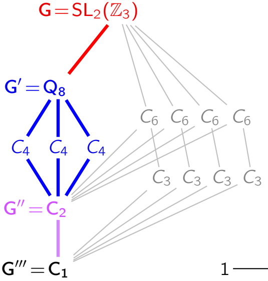
The derived series of a group G is the subnormal series

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

If $G^{(m)} = \langle 1 \rangle$ for some m, then G is solvable. The minimum m is the derived length of G.

Solvability and the derived series

The group $SL_2(\mathbb{Z}_3)$ is solvable, with derived length 3.



$$\begin{tikzcd}
& & & 1 \arrow[r] & G' \arrow[r, hook] \arrow[d, dashed] & G \arrow[r, two heads] & G/G' \arrow[r] & 1 \\
& & 1 \arrow[r] & G'' \arrow[r, hook] \arrow[d, dashed] & G' \arrow[r, two heads] & G'/G'' \arrow[r] & 1 & \\
& 1 \arrow[r] & G''' \arrow[r, hook] \arrow[d, dashed] & G'' \arrow[r, two heads] & G'''/G'' \arrow[r] & 1 & & \\
1 \arrow[r] & G^{(4)} \arrow[r, hook] & G''' \arrow[r, two heads] & G^{(4)}/G''' \arrow[r] & 1 & & &
\end{tikzcd}$$

We say that:

- $SL_2(\mathbb{Z}_3)$ *is an extension of* C_3 *by* Q_8...
- ...*which is an extension of* V_4 *by* C_2...
- ...*which is an extension of* C_2 *by* C_1.

However, the first of these is *not* an abelian extension!

Solvability and abelian descents

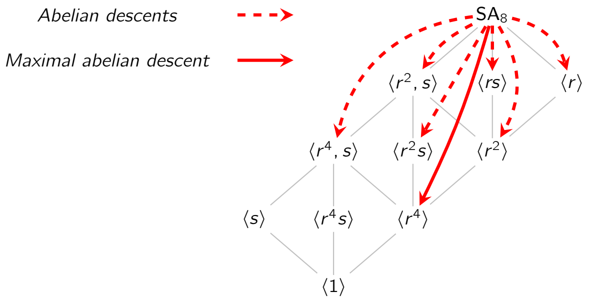
Proposition (exercise)

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

If G/H is abelian, call H, and the act of jumping from G down to H, an abelian descent.

Key point

The commutator subgroup G' is the maximal abelian descent from G.



Solvability and abelian series

Definition

An abelian series for a group G is a subnormal series

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \langle 1 \rangle$$

for which every factor H_k/H_{k+1} is abelian.

Proposition

If $G = H_0 \trianglerighteq \cdots \trianglerighteq H_m = \langle 1 \rangle$ is an abelian series, then

$$G^{(k)} \leq H_k \qquad \text{for all } \; k \in \mathbb{N}.$$

Proof (induction)

Base case: $G^{(0)} = G = H_0$. Suppose $G^{(i)} \leq H_i$. Then

$$\begin{aligned}
G^{(i+1)} &= [G^{(i)}, G^{(i)}] && \textit{by definition} \\
&\leq [H_i, H_i] && \textit{if } K \leq H \leq G, \textit{ then } [K,K] \leq [H,H] \\
&= H_i' && \textit{by definition} \\
&\leq H_{i+1} && \textit{because } H_i/H_{i+1} \textit{ is abelian.}
\end{aligned}$$

Solvability and abelian series

Corollary

If $G = H_0 \trianglerighteq \cdots \trianglerighteq H_m = \langle 1 \rangle$ is an abelian series, then G is solvable with derived length $\leq m$.

$$\begin{tikzcd}
\mathbf{G^{(0)}} \arrow[d] & = G = & H_0 \arrow[d] & \\
\mathbf{G'} \arrow[d] \arrow[rr, dash] & & H_1 \arrow[d] & \\
\mathbf{G''} \arrow[d] \arrow[rr, dash] & & H_2 \arrow[d] & \\
\vdots \arrow[d] & & \vdots \arrow[d] & \\
\mathbf{G^{(m-2)}} \arrow[d] \arrow[rr, dash] & & H_{m-2} \arrow[d] & \\
\mathbf{G^{(m-1)}} \arrow[d] \arrow[rr, dash] & & H_{m-1} \arrow[d] & \\
\mathbf{G^{(m)}} & \leq & H_m & = \langle 1 \rangle
\end{tikzcd}$$

maximal abelian descents

abelian descents

Characterizations of solvability

Proposition

The following are equivalent for a finite group G.

(i) G is solvable, i.e., $G^{(m)} = \langle 1 \rangle$ for some m.

(ii) G has an abelian series $G = H_0 \trianglerighteq \cdots \trianglerighteq H_n = \langle 1 \rangle$.

(iii) Every composition factor of G is cyclic.

Proof

"(i)⇒(ii)" The derived series is an abelian series for G. ✓

"(ii)⇒(i)" The previous Corollary. ✓

"(ii)⇒(iii)" Refine the abelian series to a composition series. ✓

"(i)⇒(ii)" A composition series with abelian factors is an abelian series for G. □

Remark

If G is solvable, then we can create a normal abelian series by removing the non-normal terms from any composition series to get a chief series.

Commutators and homomorphisms

Lemma (exercise)

Suppose $\phi\colon G_1 \longrightarrow G_2$ 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 $H, K \leq G_1$.

Corollary

Each commutator subgroup $G^{(k)}$ is characteristic in G, and thus normal. $\square$

Lemma

Let $N \trianglelefteq G$ and $\pi\colon G \to G/N$ be the canonical quotient map. Then $(G/N)' = \pi(G')$ and $(G/N)^{(k)} = \pi(G^{(k)})$ for all k.

Proof

By the lemma,

$$\pi(G') = \pi([G,G]) = [\pi(G), \pi(G)] = [G/N, G/N] = (G/N)'.$$

The result for higher commutator subgroups follows inductively.

Solvability of subgroups and quotients

Proposition

Subgroups and quotients of a solvable group are solvable.

Proof

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

Subgroups. Let $H \leq G$. Then $H' = [H, H] \leq [G, G] = G'$, and inductively,

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

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

Quotients. Let $\pi \colon G \to G/N$ be the canonical quotient. By the Lemma,

$$(G/N)^{(m)} = \pi(G^{(m)}) = \pi(\langle 1 \rangle) \cong C_1,$$

and so G/N is solvable, with derived length at most m. ✓

The next result will say that the converse holds as well.

Solvability of subgroups and quotients

Theorem

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

Proof (sketch)

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

composition series of G/N

$$\begin{array}{c} G/N = G_0/N \\ | \\ G_1/N \\ | \\ \vdots \\ | \\ N/N = G_k/N \end{array}$$

composition series of N

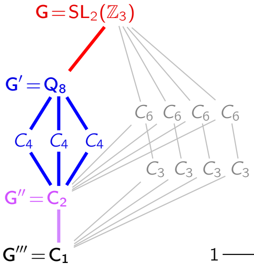
$$\begin{array}{c} N = G_k \\ | \\ \vdots \\ | \\ \langle 1 \rangle = G_m \end{array}$$

$$\begin{array}{c} G = G_0 \\ | \\ G_1 \\ | \\ \vdots \\ | \\ N = G_k \\ | \\ \vdots \\ | \\ \langle 1 \rangle = G_m \end{array}$$

Solvability and abelian extensions

Key idea

Climb *up* the derived series to construct a solvable group with abelian extensions.



$$\begin{tikzcd}
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & \mathbf{G/G} \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & G/G' \arrow[r, hook] & \mathbf{G/G'} \arrow[r, two heads] & G/G \arrow[u, dashed] \arrow[r] & 1 & \\
 & 1 \arrow[r] & G'/G'' \arrow[r, hook] & \mathbf{G/G''} \arrow[r, two heads] & G/G' \arrow[u, dashed] \arrow[r] & 1 & & \\
1 \arrow[r] & G''/G''' \arrow[r, hook] & G/G''' \arrow[r, two heads] & G/G'' \arrow[u, dashed] \arrow[r] & 1 & & &
\end{tikzcd}$$

We say that:

- $\mathrm{SL}_2(\mathbb{Z}_3)$ is an extension of $\mathbf{A_4}$ by C_2, . . .
- . . . and A_4 is an extension of $\mathbf{C_3}$ by V_4, . . .
- . . . and C_3 is an extension of $\mathbf{C_1}$ by C_3.

Solvability and abelian extensions

This is what we would like to formalize:

$$\begin{tikzcd} 1 \arrow[r] & V_4 \arrow[r, hook] & \mathbf{A_4} \arrow[r, two heads] & C_3 \arrow[r] & 1 \end{tikzcd}$$

"*A_4 is constructible with 1 abelian extension*"

$$\begin{tikzcd} 1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{SL_2(\mathbb{Z}_3)} \arrow[r, two heads] & A_4 \arrow[r] \arrow[u, dashed] & 1 \end{tikzcd}$$

"$\mathbf{SL}_2(\mathbb{Z}_3)$ *is constructible with 2 abelian extensions*"

Definition

Say that G is constructible with ...

- ... 1 abelian extension if for some abelian A_1 and Q_0,

$$1 \longrightarrow A_1 \hookrightarrow G \twoheadrightarrow Q_0 \longrightarrow 1$$

- ... k abelian extensions if for some abelian A_k,

$$1 \longrightarrow A_k \hookrightarrow G \twoheadrightarrow Q_{k-1} \longrightarrow 1$$

and Q_{k-1} is constructible with $k-1$ abelian extensions.

Solvability and abelian extensions

If G is constructible with k abelian extensions, then we have the following:

$$
\begin{tikzcd}
 & & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/H_0 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & & 1 \arrow[r] & H_0/H_1 \arrow[r, hook] & G/H_1 \arrow[r, two heads] & G/H_0 \arrow[u, dashed] \arrow[r] & 1 & \\
 & & 1 \arrow[r] & H_1/H_2 \arrow[r, hook] & G/H_2 \arrow[r, two heads] & G/H_1 \arrow[u, dashed] \arrow[r] & 1 & & \\
 & & & & \vdots \arrow[u, dashed] & & & & \\
 & 1 \arrow[r] & H_{k-2}/H_{k-1} \arrow[r, hook] & G/H_{k-1} \arrow[r, two heads] & G/H_{k-2} \arrow[u, dashed] \arrow[r] & 1 & & & \\
1 \arrow[r] & H_{k-1}/H_k \arrow[r, hook] & G/H_k \arrow[r, two heads] & G/H_{k-1} \arrow[u, dashed] \arrow[r] & 1 & & & &
\end{tikzcd}
$$

Note that G has a normal abelian series

$$G = H_0 \trianglerighteq \cdots \trianglerighteq H_k = \langle 1 \rangle, \qquad \text{each } H_i/H_{i+1} \text{ is abelian, and } H_i \trianglelefteq G.$$

Conversely, given a normal abelian series, we can reconstruct the exact sequences.

Summary of solvable groups

Theorem

The following are equivalent for a finite group G:

(i) G is solvable, i.e., $G^{(m)} = \langle 1 \rangle$ for some m.

(ii) G has an abelian series $G = H_0 \trianglerighteq \cdots \trianglerighteq H_n = \langle 1 \rangle$.

(iii) Every composition factor of G is cyclic.

(iv) G can be constructible with abelian extensions.

Proof

We did (i)$\Leftrightarrow$(ii)$\Leftrightarrow$(iii). ✓

(i)$\Rightarrow$(iv): We saw how to build a sequence of abelian extensions from the derived series. ✓

(iv)$\Rightarrow$(ii). Start with the exact sequence picture on the previous slide.

By construction, each extension is

$$1 \longrightarrow H_{i-1}/H_i \hookrightarrow G \twoheadrightarrow G/H_{i-1} \longrightarrow 1$$

and H_{i-1}/H_i is abelian. ✓

Summary of solvable groups

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.
- it can be iteratively built with a abelian extensions.

Theorems

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:

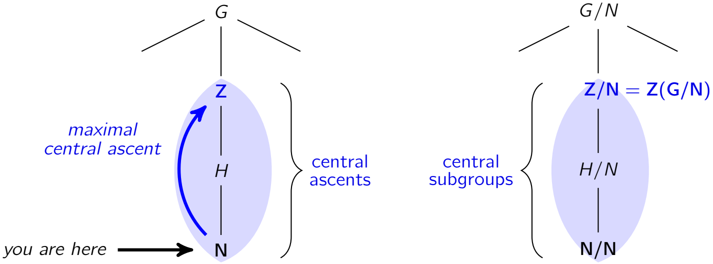
"*if we quotient by N (chop off the lattice below), what subgroup Z/N is the center?*"

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.

Central descents

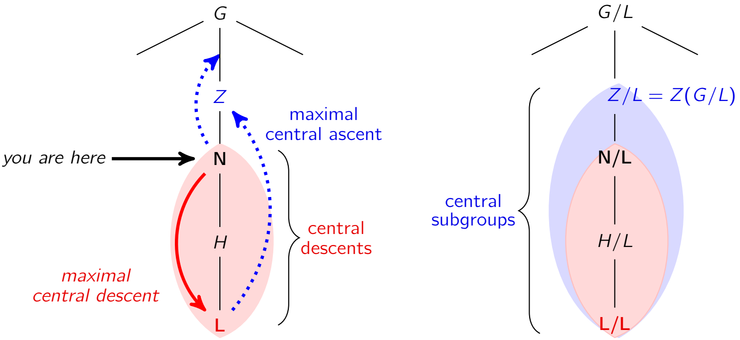
Starting from any normal subgroup $N \trianglelefteq G$, we can ask:

"*what's the smallest subgroup L where we can chop off so G/N remains central?*"

Definition

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

- central descent from N if $N/L \leq Z(G/L)$.
- maximal central descent from N if L is the smallest such subgroup.



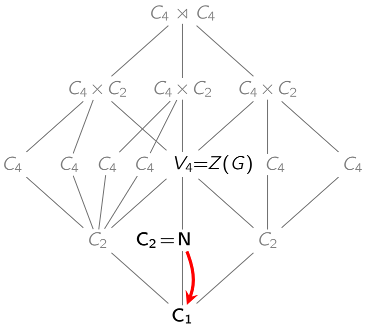
Maximal central ascents and descents

Maximal central descent:

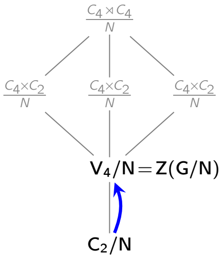
"*how far <u>down</u> the lattice can we jump so that N remains central?*"

Maximal central ascent:

"*how far <u>up</u> the lattice can we climb and remain central in the quotient G/N?*"



"*N/C_1 is central in the quotient G/C_1*"



"*The center of the quotient G/N*"

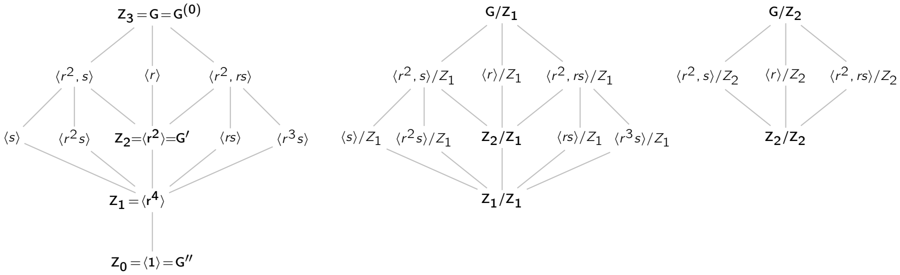
Nilpotent groups and the ascending central series

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**.

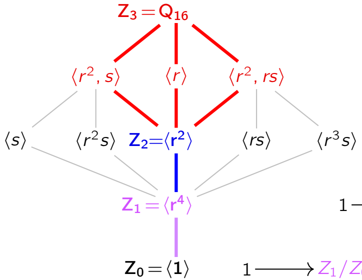


Big idea

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

Nilpotent groups and the ascending central series

"*Iteratively take maximal central steps up the subgroup lattice.*"



$$\begin{tikzcd}
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/G \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & G/Z_2 \arrow[r, hook] & G/Z_2 \arrow[r, two heads] & G/G \arrow[r] \arrow[u, dashed] & 1 & \\
 & 1 \arrow[r] & Z_2/Z_1 \arrow[r, hook] & G/Z_1 \arrow[r, two heads] & G/Z_2 \arrow[r] \arrow[u, dashed] & 1 & & \\
1 \arrow[r] & Z_1/Z_0 \arrow[r, hook] & G/Z_0 \arrow[r, two heads] & G/Z_1 \arrow[r] \arrow[u, dashed] & 1 & & &
\end{tikzcd}$$

We can say:

- *Q_{16} is an extension of $D_4 \cong Q_{16}/Z_1$ by the center $Z(Q_{16}) \cong C_2$,...*
- *...and D_4 is an extension of $V_4 \cong Q_{16}/Z_2$ by the center $Z(D_4) \cong C_2$,...*
- *...and V_4 is an extension of $C_1 \cong Q_{16}/Z_3$ by the center $Z(V_4) \cong V_4$.*

Basic properties of nilpotent groups

Proposition

If G is nilpotent, then it is solvable.

Proof

The ascending central series $\langle 1 \rangle = Z_0 \trianglelefteq \cdots \trianglelefteq Z_m = G$ is an abelian series. (*Why?*) $\square$

Corollary

Every p-group is nilpotent, and hence solvable. $\square$

Proof

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

Remark

For any finite group G with ascending central series $\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots$,

$$\begin{aligned}
Z_{i+1} &= \big\{x \in G \mid xZ_igZ_i = gZ_ixZ_i,\ \forall g \in G\big\} \\
&= \big\{x \in G \mid xZ_igZ_ix^{-1}Z_ig^{-1}Z_i = Z_i,\ \forall g \in G\big\} \\
&= \big\{x \in G \mid [x,g]Z_i = Z_i,\ \forall g \in G\big\} \\
&= \big\{x \in G \mid [x,g] \in Z_i,\ \forall g \in G\big\}.
\end{aligned}$$

Nilpotent groups

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

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

Central ascent 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: $Z = \big\{z \in G \mid [g,z] \in N,\ \forall g \in G\big\}$.

Proof

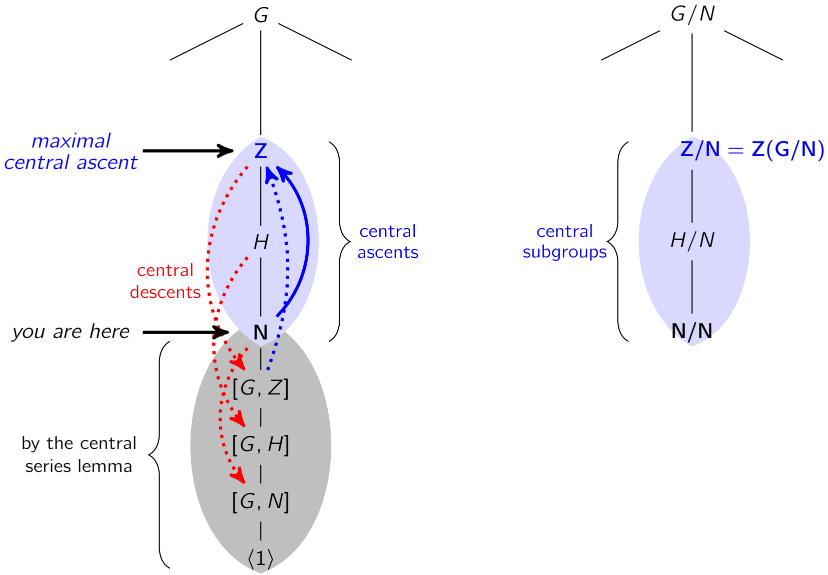
If H/N is in the center of G/N, then for all $h \in H$ and $g \in G$

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

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



Well-defindness of central descents

The following result is why central descents should only be defined for normal subgroups.

Lemma (exercise)

Let $H, K \leq G$.

(i) $[H, K] \leq H$ iff $K \leq N_G(H)$ (i.e., "K normalizes H").

(ii) $[G, H] \leq H$ iff $H \trianglelefteq G$.

If $Z \leq G$ is the maximal central ascent from $N \trianglelefteq G$, and $N \leq H \leq Z$ for some $H \trianglelefteq G$:

$$\begin{aligned} [G, N] &\leq [G, H] && \textit{because } N \leq H \\ &\leq [G, Z] && \textit{because } H \leq Z \\ &\leq N && \textit{by the central ascent lemma}, \text{ applied to } Z/N = Z(G/N). \end{aligned}$$

Since $N/N \leq H/N \leq Z/N$ are central in G/N, it is well-founded to call

$$[G, N] \leq [G, H] \leq [G, Z] \leq N$$

central descents from N.

Moreover, $[G, N]$ is the maximal central descent.

Central descents and commutators

Let's now confirm that our "maximal central descent" term is welll-founded.

Central descent lemma

Let $N \trianglelefteq G$. Then $L := [G, N]$ is the smallest subgroup L for which $N/L \leq Z(G/L)$.

Proof

Centrality of N/L. We know $L = [G, N]$ is normal in G, so G/L exists.

The commutator of $gL \in G/L$ with $nL \in N/L$ is

$$[gL, nL] = gL \cdot nL \cdot (gL)^{-1} \cdot (nL)^{-1} = gng^{-1}n^{-1}L = [g, n]L = L \qquad \checkmark$$

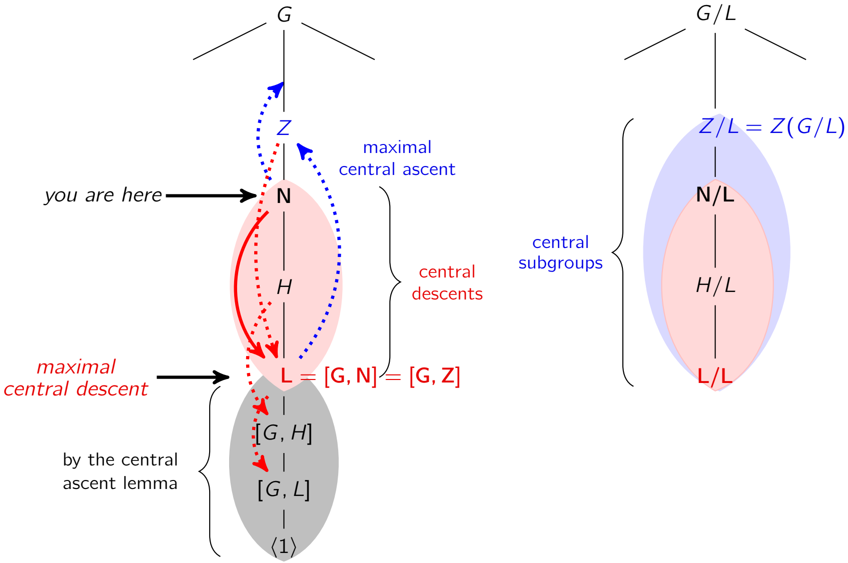
Minimality of L. Suppose $N/K \leq Z(G/K)$; we'll show that $L \leq K$.

Since N/K is central, the commutator of any $gK \in G/K$ with $nK \in N/K$ is trivial:

$$K = [gK, nK] = gK \cdot nK \cdot (gK)^{-1} \cdot (nK)^{-1} = gng^{-1}n^{-1}K = [g, n]K.$$

Thus, $[g, n] \in K$, and so $L := [G, N] \leq K$. ✓

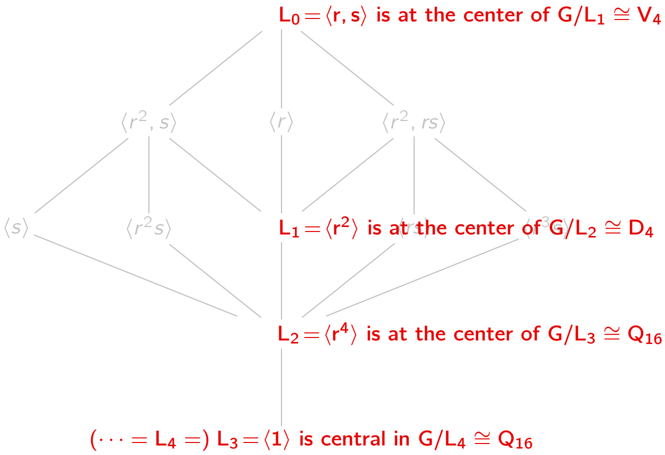
Central descents



The descending central series

At each $L_k \leq G$, look down and ask

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



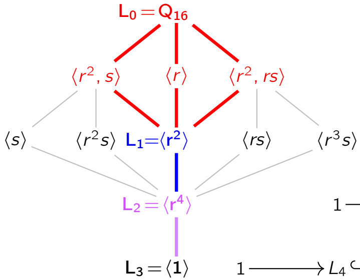
We call this the descending central series of G.

The descending central series

Definition

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

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



$$\begin{tikzcd}
 & & & 1 \arrow[r] & L_1 \arrow[r, hook] \arrow[d, dashed] & L_0 \arrow[r, two heads] & L_0/L_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & L_2 \arrow[r, hook] \arrow[d, dashed] & L_1 \arrow[r, two heads] & L_1/L_2 \arrow[r] & 1 & \\
 & 1 \arrow[r] & L_3 \arrow[r, hook] \arrow[d, dashed] & L_2 \arrow[r, two heads] & L_2/L_3 \arrow[r] & 1 & & \\
1 \arrow[r] & L_4 \arrow[r, hook] & L_3 \arrow[r, two heads] & L_3/L_4 \arrow[r] & 1 & & &
\end{tikzcd}$$

- $L_0 = Q_{16}$ *is an extension of* $L_0/L_1 \cong V_4$ *by* $L_1 \cong C_4, \ldots$
- *. . . which is an extension of* $L_1/L_2 \cong C_2$ *by* $L_2 \cong C_2, \ldots$
- *. . . which is an extension of* $L_2/L_3 \cong C_2$ *by* $L_3 = \langle 1\rangle$.

Maximal abelian vs. maximal central descents

Descending central series:

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

Derived series:

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

Proposition

For any group G, we have $G^{(k)} \leq L_k$, for all $k \in \mathbb{N}$.

Proof

We start with $G^{(0)} = L_0 = G$ and $G' = L_1 = [G, G]$. 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

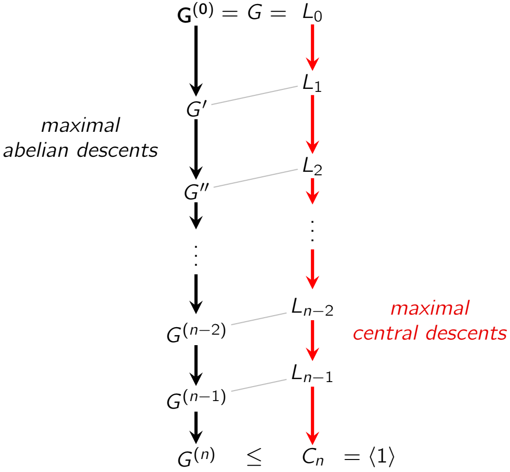
$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \leq [G, L_{k-1}] = L_k,$$

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

Maximal abelian vs. maximal central descents

Proposition

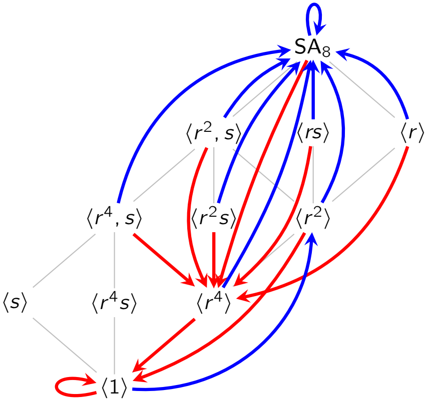
For any group G, we have $G^{(k)} \leq L_k$, for all $k \in \mathbb{N}$.



Chutes and Ladders diagrams

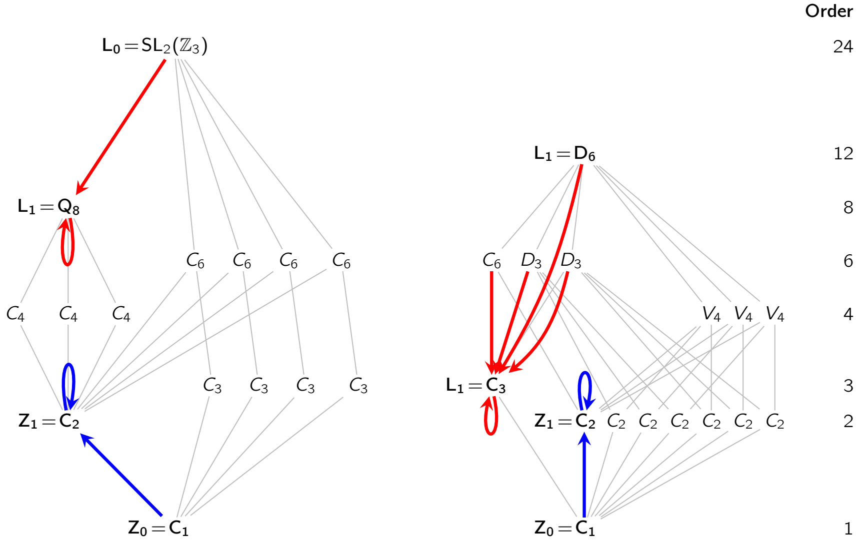
Define the **Chutes and Ladders diagram** of G from its lattice by adding, for each $N \trianglelefteq G$:

- 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!

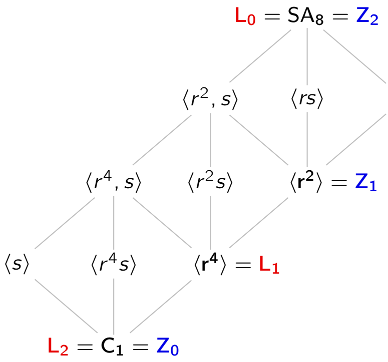
The chutes and ladders diagram of a non-nilpotent group

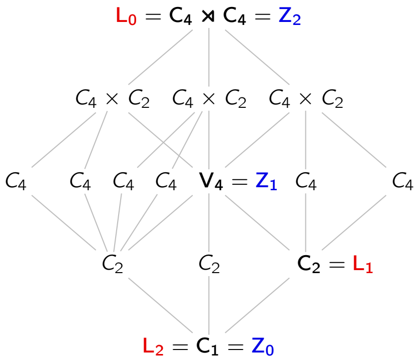


Ascending vs. descending central series

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.





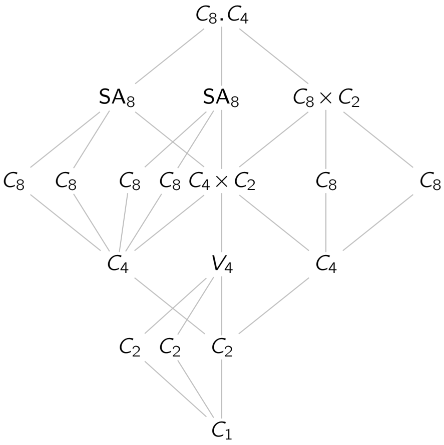
Key idea (that we'll prove)

The ascending and descending central series have the same length.

An example: $G = C_8.C_4$ (GAP ID 32.15)

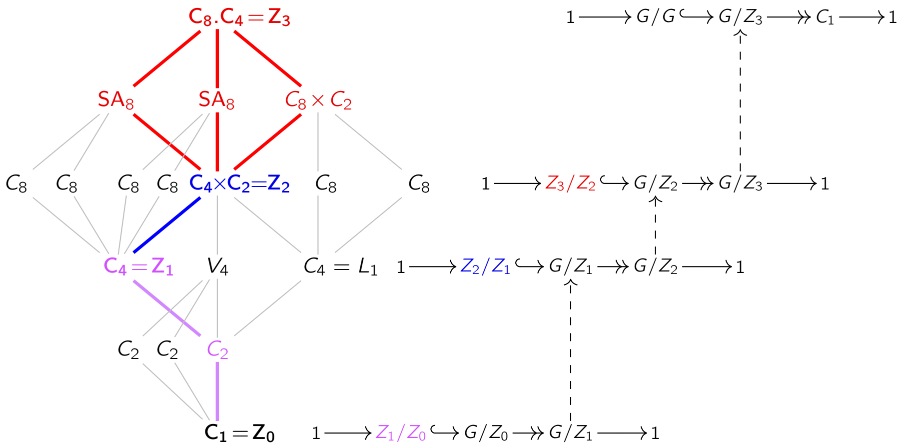
Let's find the ascending and descending central series of the following group of order 32:

$$G = \langle a, b \mid b^8 = 1,\ a^4 = b^4,\ ab = b^7 a \rangle.$$



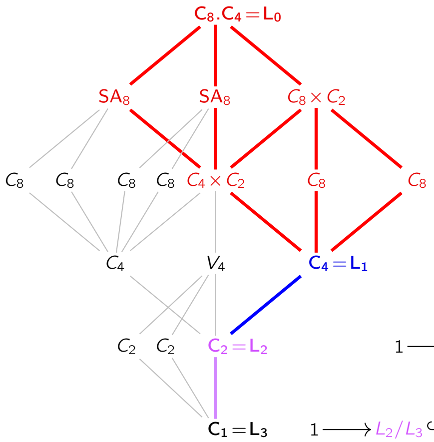
Then, we'll climb up both central series and read off the central extensions.

The ascending central series of $G = C_8.C_4$ (GAP ID 32.15)



- $G = C_8.C_4$ is an extension of $D_4 \cong G/Z_1$ by the center $C_4 \cong Z_1/Z_0 \cong Z(C_8.C_4)$),...
- ...and D_4 is an extension of $V_4 \cong G/Z_2$ by the center $C_2 \cong Z_2/Z_1 \cong Z(D_4)$,...
- ...and V_4 is an extension of $C_1 \cong G/Z_3$ by the center $V_4 \cong Z_3/Z_2 \cong Z(V_4)$.

The descending central series of $G = C_8.C_4$ (GAP ID 32.15)



$$\begin{tikzcd}
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/L_0 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & L_0/L_1 \arrow[r, hook] & G/L_1 \arrow[r, two heads] & G/L_0 \arrow[r] \arrow[u, dashed] & 1 & \\
 & 1 \arrow[r] & L_1/L_2 \arrow[r, hook] & G/L_2 \arrow[r, two heads] & G/L_1 \arrow[r] \arrow[u, dashed] & 1 & & \\
1 \arrow[r] & L_2/L_3 \arrow[r, hook] & G/L_3 \arrow[r, two heads] & G/L_2 \arrow[r] \arrow[u, dashed] & 1 & & &
\end{tikzcd}$$

- $C_8.C_4$ is an extension of $C_4 \rtimes C_4$ by the central subgroup $L_2/L_3 \lneq Z(G/L_3) \cong V_4$,...
- ... $C_4 \rtimes C_4$ is an extension of $C_4 \times C_2$ by central subgroup $L_1/L_2 \lneq Z(C_4 \rtimes C_4) \cong V_4$,...
- ... $C_4 \times C_2$ is an extension of C_1 by central subgroup $L_0/L_1 \cong Z(C_4 \times C_2) \cong C_4 \times C_2$.

Central series

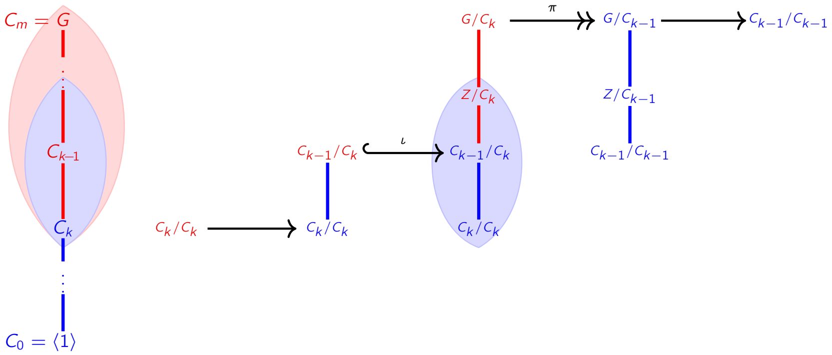
Definition

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

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

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

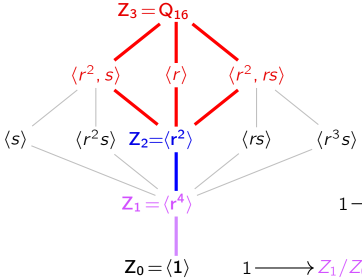
$$1 \longrightarrow C_{k-1}/C_k \xrightarrow{\iota_k} G/C_k \xrightarrow{\pi_k} G/C_{k-1} \longrightarrow 1$$



Nilpotency and central extensions

Key idea

Climb <u>*up*</u> a central series to construct a nilpotent group with central extensions.



$$\begin{tikzcd}
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/G \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & G/Z_2 \arrow[r, hook] & G/Z_2 \arrow[r, two heads] & G/G \arrow[u, dashed] \arrow[r] & 1 & \\
 & 1 \arrow[r] & Z_2/Z_1 \arrow[r, hook] & G/Z_1 \arrow[r, two heads] & G/Z_2 \arrow[u, dashed] \arrow[r] & 1 & & \\
1 \arrow[r] & Z_1/Z_0 \arrow[r, hook] & G/Z_0 \arrow[r, two heads] & G/Z_1 \arrow[u, dashed] \arrow[r] & 1 & & &
\end{tikzcd}$$

We can say:

- Q_{16} is a central extension of $D_4 \cong Q_{16}/Z_1$ by $Z(Q_{16}) \cong C_2$,...
- ...and D_4 is a central extension of $V_4 \cong Q_{16}/Z_2$ by $Z(D_4) \cong C_2$,...
- ...and V_4 is a central extension of $C_1 \cong Q_{16}/Z_3$ by $Z(V_4) \cong V_4$.

Nilpotency and central extensions

$$\begin{tikzcd} & 1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{D_4} \arrow[r, two heads] & V_4 \arrow[r] & 1 \\ 1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{Q_{16}} \arrow[r, two heads] & D_4 \arrow[r] \arrow[u, dashed] & 1 \end{tikzcd}$$

"*D_4 is constructible with 1 central extension*"

"*Q_{16} is constructible with 2 central extensions*"

Definition

Say that G is constructible with ...

- ... 1 central extension if for some abelian A_1 and Q_0,

$$1 \longrightarrow A_1 \hookrightarrow G \twoheadrightarrow Q_0 \longrightarrow 1$$

- ... k central extensions if

$$1 \longrightarrow A_k \hookrightarrow G \twoheadrightarrow Q_{k-1} \longrightarrow 1$$

where $\iota(A_k)$ is central, and Q_{k-1} is constructible with $k-1$ central extensions.

Nilpotency and central extensions

If G is constructible with k central extensions, then we have the following:

$$
\begin{tikzcd}
 & & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/C_0 \arrow[r, two heads] & 1 \arrow[r] & 1 \\
 & & & 1 \arrow[r] & C_0/C_1 \arrow[r, hook] & G/C_1 \arrow[r, two heads] & G/C_0 \arrow[r] \arrow[u, dashed] & 1 & \\
 & & 1 \arrow[r] & C_1/C_2 \arrow[r, hook] & G/C_2 \arrow[r, two heads] & G/C_1 \arrow[r] \arrow[u, dashed] & 1 & & \\
 & 1 \arrow[r] & C_{k-2}/C_{k-1} \arrow[r, hook] & G/C_{k-1} \arrow[r, two heads] & G/C_{k-2} \arrow[r] \arrow[u, dashed, "\vdots"] & 1 & & & \\
1 \arrow[r] & C_{k-1}/C_k \arrow[r, hook] & G/C_k \arrow[r, two heads] & G/C_{k-1} \arrow[r] \arrow[u, dashed] & 1 & & & &
\end{tikzcd}
$$

Note that G has a normal central series

$$G = C_0 \trianglerighteq \cdots \trianglerighteq C_k = \langle 1 \rangle, \qquad \text{each } C_{i-1}/C_i \text{ is central in } G/C_i, \text{ and } C_i \trianglelefteq G.$$

Conversely, given a normal central series, we can reconstruct the exact sequences.

Central series

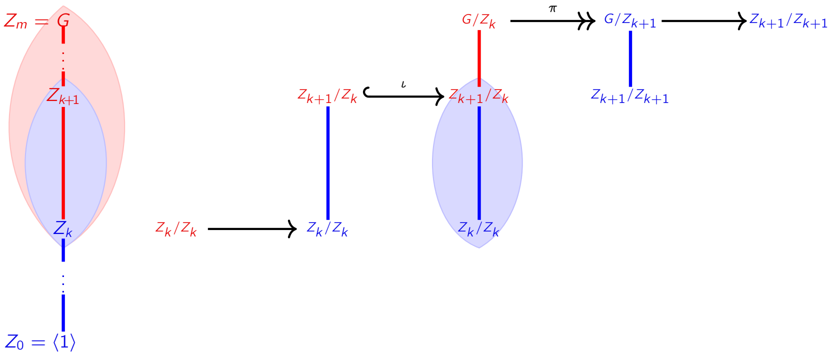
Remark

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).

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



Central series

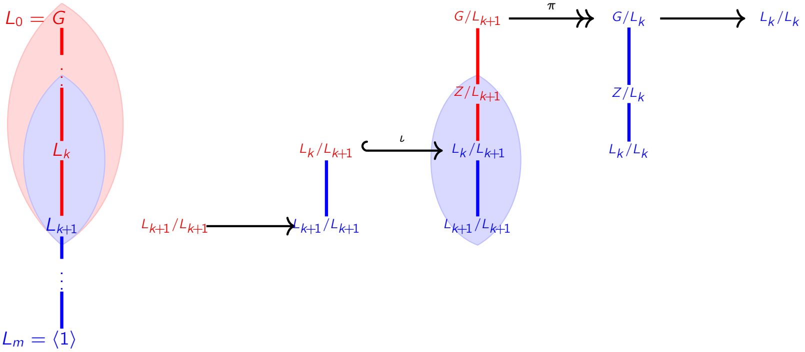
Remark

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

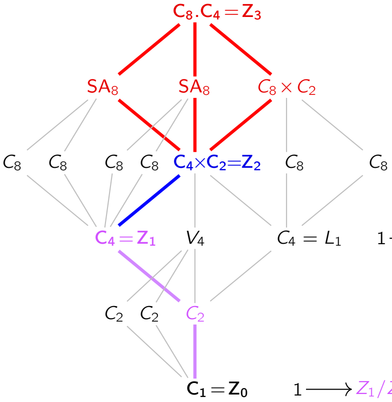
$$G = L_0 \trianglerighteq L_1 \trianglerighteq \cdots \trianglerighteq L_m = \langle 1 \rangle, \quad \text{such that} \quad L_k/L_{k+1} \leq Z(G/L_{k+1}).$$

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

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



The ascending central series of $G = C_8.C_4$ (GAP ID 32.15)



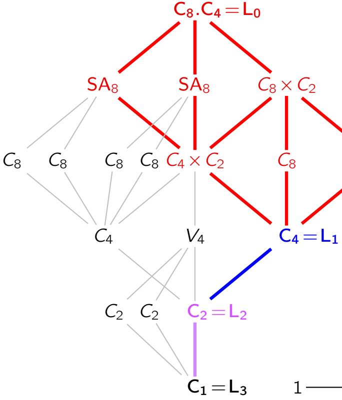
$$\begin{tikzcd}
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/Z_3 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & Z_3/Z_2 \arrow[r, hook] & G/Z_2 \arrow[r, two heads] & G/Z_3 \arrow[r] \arrow[u, dashed] & 1 & \\
 & 1 \arrow[r] & Z_2/Z_1 \arrow[r, hook] & G/Z_1 \arrow[r, two heads] & G/Z_2 \arrow[r] \arrow[u, dashed] & 1 & & \\
1 \arrow[r] & Z_1/Z_0 \arrow[r, hook] & G/Z_0 \arrow[r, two heads] & G/Z_1 \arrow[r] \arrow[u, dashed] & 1 & & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & 1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{D_4} \arrow[r, two heads] & V_4 \arrow[r] & 1 \\
1 \arrow[r] & C_4 \arrow[r, hook] & \mathbf{C_8.C_4} \arrow[r, two heads] & D_4 \arrow[r] \arrow[u, dashed] & 1 &
\end{tikzcd}$$

"*D_4 is constructible with 1 central extension*"

"*$C_8.C_4$ is constructible with 2 central extensions*"

The descending central series of $G = C_8.C_4$ (GAP ID 32.15)



$$
\begin{tikzcd}[column sep=small]
 & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/L_0 \arrow[r, two heads] & C_1 \arrow[r] & 1 \\
 & & 1 \arrow[r] & L_0/L_1 \arrow[r, hook] & G/L_1 \arrow[r, two heads] & G/L_0 \arrow[r] \arrow[u, dashed] & 1 & \\
 & 1 \arrow[r] & L_1/L_2 \arrow[r, hook] & G/L_2 \arrow[r, two heads] & G/L_1 \arrow[r] \arrow[u, dashed] & 1 & & \\
1 \arrow[r] & L_2/L_3 \arrow[r, hook] & G/L_3 \arrow[r, two heads] & G/L_2 \arrow[r] \arrow[u, dashed] & 1 & & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & 1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{C_4 \rtimes C_4} \arrow[r, two heads] & C_4 \times C_4 \arrow[r] & 1 \\
1 \arrow[r] & C_2 \arrow[r, hook] & \mathbf{C_8.C_4} \arrow[r, two heads] & C_4 \rtimes C_2 \arrow[r] \arrow[u, dashed] & 1 &
\end{tikzcd}
$$

"*$C_4 \rtimes C_4$ is constructible with 1 central extension*"

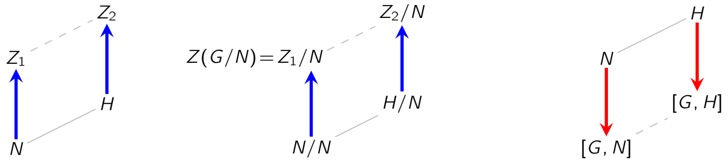
"*$C_8.C_4$ is constructible with 2 central extensions*"

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 $g \in G$,

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

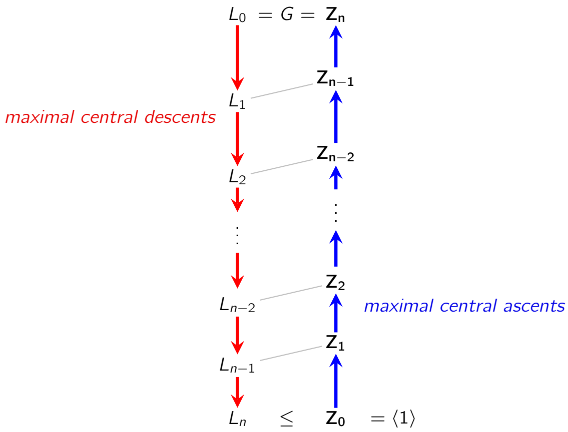
The crooked ladder theorem

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 $k = 0, \dots, n$,

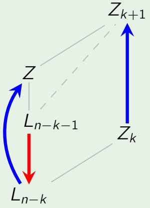
$$L_{n-k} \leq Z_k.$$

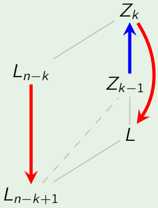
Proof of (i); Part (ii) is analogous (HW)

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

Inductive step:

Part (i)





Part (ii)

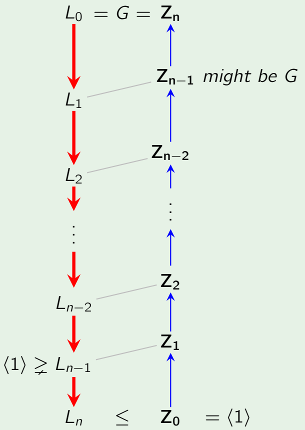
Note that L_{n-k-1} is a central ascent from L_{n-k}: $\overbrace{L_{n-k} \leq L_{n-k-1} \leq Z}^{L_{n+k-1}/L_{n-k} \in Z(G/L_{n-k})} \underbrace{\leq Z_{k+1}}_{\text{monotonicity}}$. $\square$

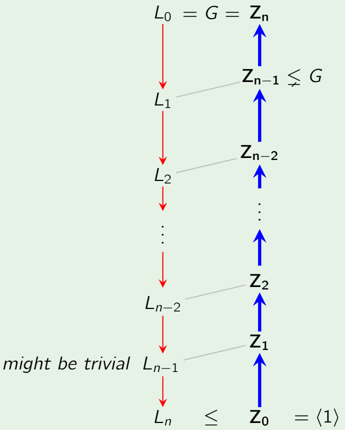
The ascending and descending central series have the same length

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

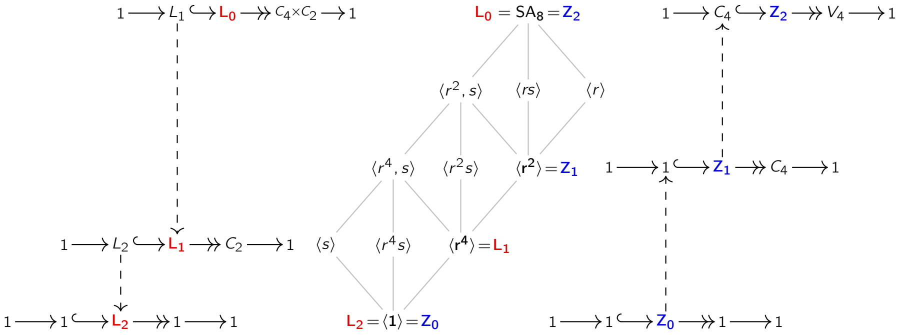




Nilpotent groups

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

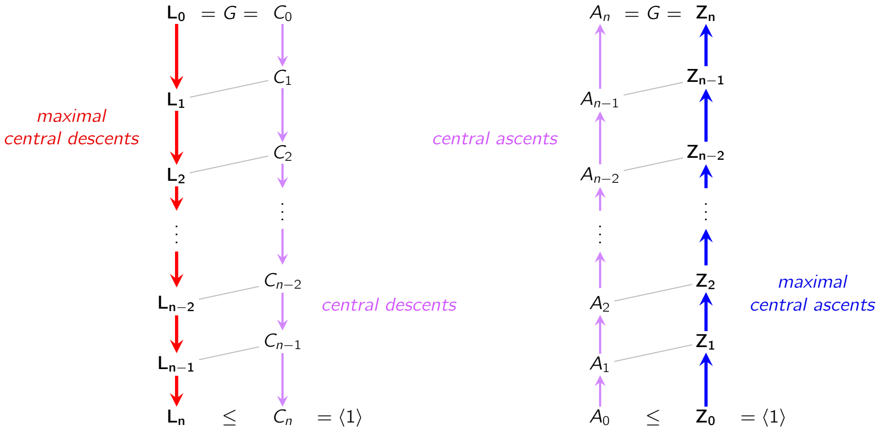
$$L_{n-k} \leq Z_k, \qquad \textit{or equivalently,} \quad L_k \leq Z_{n-k}.$$



Also known as the “upper” and “lower” central series

Aside (exercise)

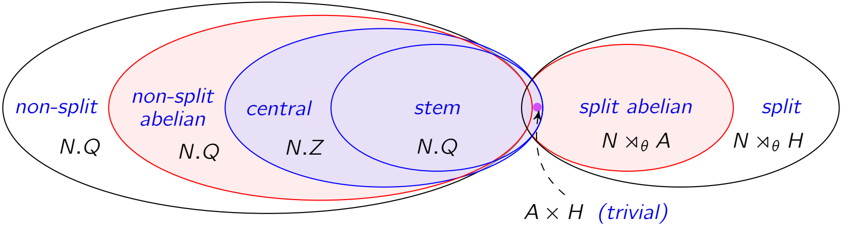
- The L_k's fall faster than every other central series, and thus are term-by-term lower.
- The Z_k's rise faster than every other central series, and thus are term-by-term higher.



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.



The first two characterizations of nilpotency

Original definition

A finite group G is **nilpotent** if the ascending central series reaches the top of the lattice:

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

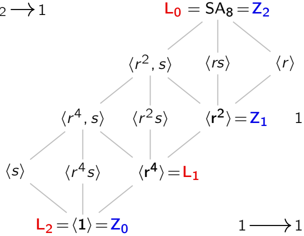
Theorem

The ascending central series reachers the top of the lattice iff the descending central series

$$G = L_0 \trianglerighteq L_1 \trianglerighteq \cdots \trianglerighteq L_m = \langle 1\rangle, \qquad L_{k+1} = [G, L_k]$$

reaches the bottom of the lattice. If this happens, it takes the same number of steps.

$$\begin{tikzcd}
 & & 1 \arrow[r] & L_1 \arrow[r, hook] \arrow[d, dashed] & \mathbf{L_0} \arrow[r, two heads] & C_4\times C_2 \arrow[r] & 1 \\
 & 1 \arrow[r] & L_2 \arrow[r, hook] \arrow[d, dashed] & \mathbf{L_1} \arrow[r, two heads] & C_2 \arrow[r] & 1 & \\
1 \arrow[r] & 1 \arrow[r, hook] & \mathbf{L_2} \arrow[r, two heads] & 1 \arrow[r] & 1 & &
\end{tikzcd}$$



$$\begin{tikzcd}
 & & 1 \arrow[r] & C_4 \arrow[r, hook] & \mathbf{Z_2} \arrow[r, two heads] & V_4 \arrow[r] & 1 \\
 & 1 \arrow[r] & 1 \arrow[r, hook] & \mathbf{Z_1} \arrow[r, two heads] \arrow[u, dashed] & C_4 \arrow[r] & 1 & \\
1 \arrow[r] & 1 \arrow[r, hook] & \mathbf{Z_0} \arrow[r, two heads] \arrow[u, dashed] & 1 \arrow[r] & 1 & &
\end{tikzcd}$$

The 3rd characterization of nilpotency

Lemma

A finite groups is nilpotent if and only if it is constructible with central extensions.

This is equivalent to G having a central series:

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

$$\begin{tikzcd}
 & & & & 1 \arrow[r] & G/G \arrow[r, hook] & G/C_0 \arrow[r, two heads] & 1 \arrow[r] & 1 \\
 & & & 1 \arrow[r] & C_0/C_1 \arrow[r, hook] & G/C_1 \arrow[r, two heads] & G/C_0 \arrow[u, dashed] \arrow[r] & 1 & \\
 & & 1 \arrow[r] & C_1/C_2 \arrow[r, hook] & G/C_2 \arrow[r, two heads] & G/C_1 \arrow[u, dashed] \arrow[r] & 1 & & \\
 & & & & \vdots \arrow[u, dashed] & & & & \\
 & 1 \arrow[r] & C_{k-2}/C_{k-1} \arrow[r, hook] & G/C_{k-1} \arrow[r, two heads] & G/C_{k-2} \arrow[u, dashed] \arrow[r] & 1 & & & \\
1 \arrow[r] & C_{k-1}/C_k \arrow[r, hook] & G/C_k \arrow[r, two heads] & G/C_{k-1} \arrow[u, dashed] \arrow[r] & 1 & & & &
\end{tikzcd}$$

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 $G = H \times K$.

The 4^{th} characterization of nilpotency: normalizers grow

Proposition

A finite group G is nilpotent iff it has no proper fully unnormal subgroups ($H \lneq N_G(H)$).

Proof

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

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

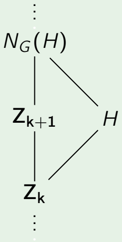
For all $g \in G$, we have $[x, g] \in Z_k$.

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

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

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

"$\Leftarrow$" Exercise. (Need a result on Sylow p-subgroups.) $\square$

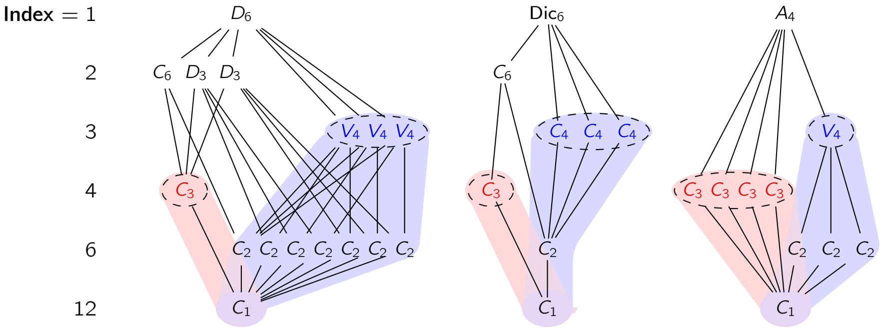


The 4^{th} characterization of nilpotency: normalizers grow

Proposition

A finite group G is nilpotent iff it has no proper fully unnormal subgroups ($H \lneq N_G(H)$).

Since $|\operatorname{cl}_G(H)| = [G : N_G(H)]$, this means that G has no "*maximally wide conjugacy fans*."



The 5th and 6th characterizations of nilpotency: Sylow p-subgroups

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.

$$\begin{aligned} P &\lneq N_G(P) && \textit{by previous Proposition} \\ &= N_G(N_G(P)) && \textit{property of Sylow p-subgroups} \\ &= G && \textit{contrapositive of Prop.: } N_G(H) = H \textit{ implies } H = G. \end{aligned}$$

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. ✓

Corollary

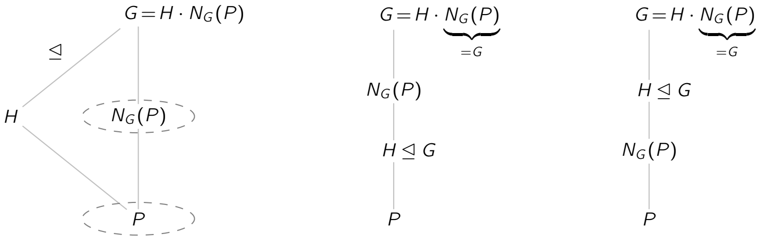
A finite group is nilpotent iff all Sylow p-subgroups are normal.

A technical lemma for the 7^{th} characterization of nilpotency.

Frattini argument (exercise)

If G is a finite group and $P \leq H \trianglelefteq G$ with $P \in \mathrm{Syl}_p(H)$, then $G = N_G(P)H$.

Case 1 *Case 2* *Case 3*



Corollary (Case 3)

If G is a finite group and $P \leq H \trianglelefteq G$ with $P \in \mathrm{Syl}_p(H)$ and $N_G(P) \leq H$, then

(i) $H \trianglelefteq G \;\Rightarrow\; P \trianglelefteq G$, (ii) $P \ntrianglelefteq G \;\Rightarrow\; H \ntrianglelefteq G$.

The 7^{th} characterization of nilpotency.

Frattini argument corollary (Case 3)

If G is a finite group and $P \leq H \trianglelefteq G$ with $P \in \text{Syl}_p(H)$ and $N_G(P) \leq H$, then

(i) $H \trianglelefteq G \;\Rightarrow\; P \trianglelefteq G$,

(ii) $P \ntrianglelefteq G \;\Rightarrow\; H \ntrianglelefteq G$.

Proposition

A finite group is nilpotent iff every maximal subgroup is normal.

Proof

"$\Rightarrow$" Let $M \trianglelefteq G$ be maximal normal. Then $M \lneq N_G(M) \leq G \;\Rightarrow\; N_G(M) = G$. ✓

"$\Leftarrow$" Let $P \leq G$ be a Sylow p-subgroup.

Suppose $P \ntrianglelefteq G$, and let M be a maximal subgroup containing its normalizer:

$$P \leq N_G(P) \leq M \lneq G.$$

By Frattini (Case 3), $P \ntrianglelefteq G \;\Rightarrow\; M \ntrianglelefteq G$, a contradiction. □

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. G is constructible with central extensions.
4. $H \lneq N_G(H)$ for all proper subgroups, ("*no fully unnormal subgroups*")
5. G is the direct product of its Sylow p-subgroups.
6. All Sylow p-subgroups are normal (or equivalently, $n_p = 1$).
7. Every maximal subgroup of G is normal.