Chapter 6: Extensions & universal constructions

Matthew Macauley

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

Math 8510, Abstract Algebra

Group extensions

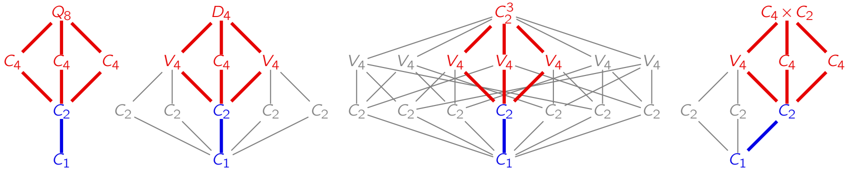
Every normal subgroup $N \trianglelefteq G$ canonically defines two sublattices.

- "*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

$$N \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$$

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

Extensions and short exact sesquences

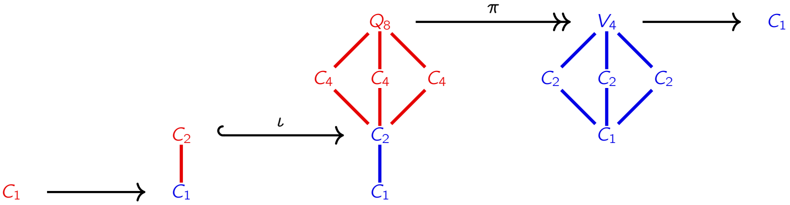
If we write

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

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**.



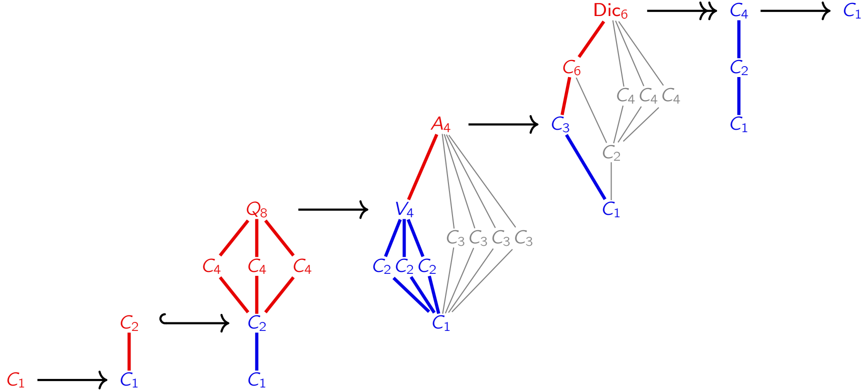
More on exact sequences

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:

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

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"

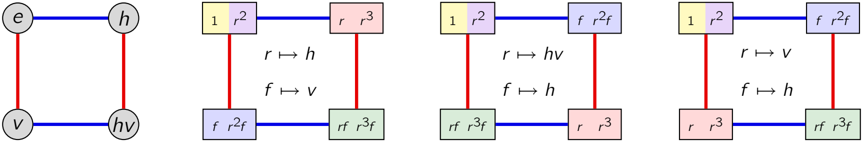
Find all possibilities for the "middle term" G in a short exact sequence, given N and Q.

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

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

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

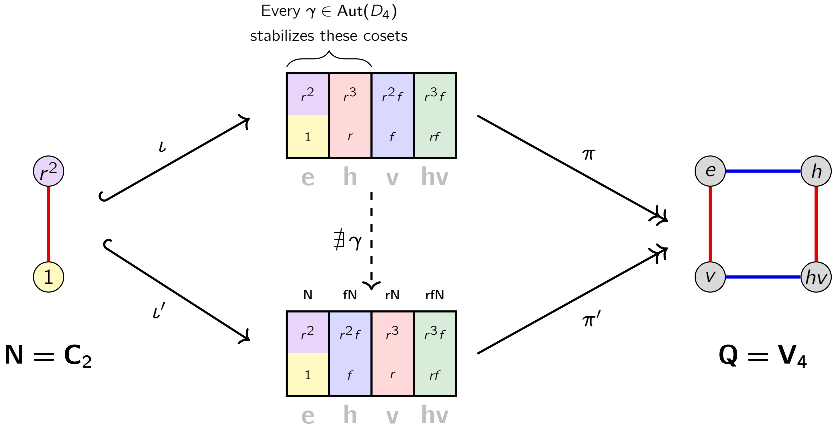
Do you see why these three extensions of V_4 by C_2 do *not* differ by an automorphism?



Extension equivalence

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

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



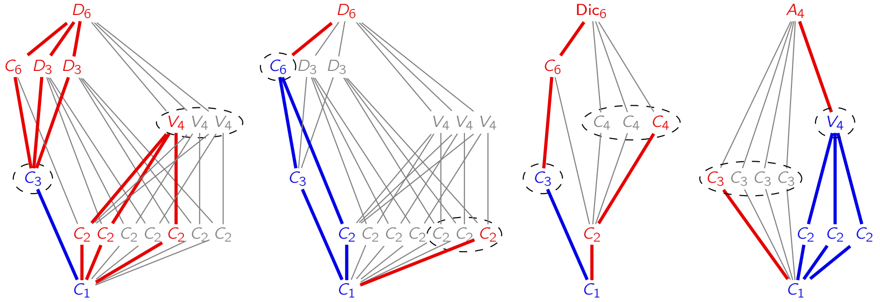
Semidirect products and extensions

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

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



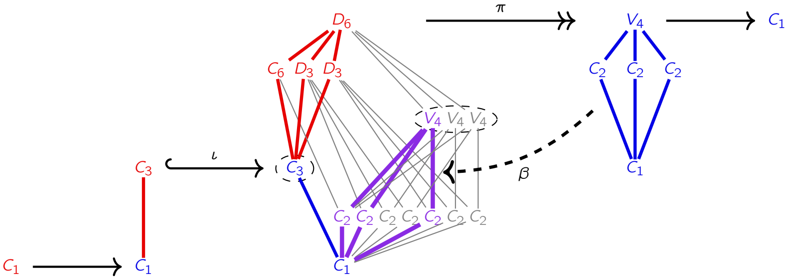
Do you see a canonical injection from $Q \cong G/N \cong H$ "down to" $H \leq G$?

Split exact sequences

Definition

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

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



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 $n = gh^{-1}$ 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 $g \in \iota(N) = \mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$,

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

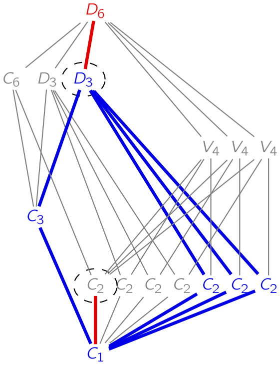
  Therefore, $g = \beta(h) = \beta(1_H) = 1_G$, and hence $\iota(N) \cap \beta(H) = \langle 1_G \rangle$. $\square$

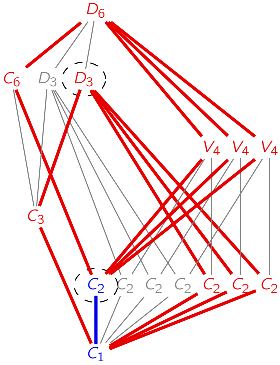
Split exact sequences and direct products

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

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

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





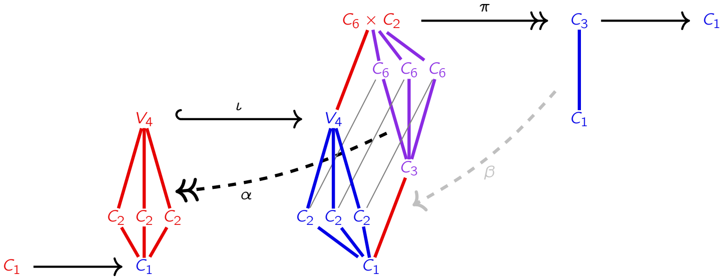
Split exact sequences and direct products

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

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



Split exact sequences and direct products

Proposition (HW)

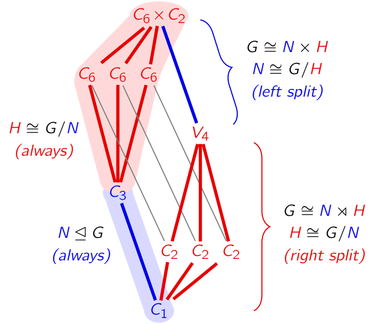
- If a short exact sequence is left split, then it is right split.

  "*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*"

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

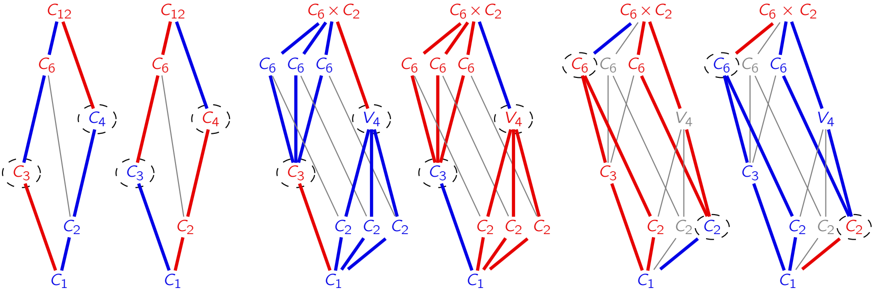


Split exact sequences and direct products

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:



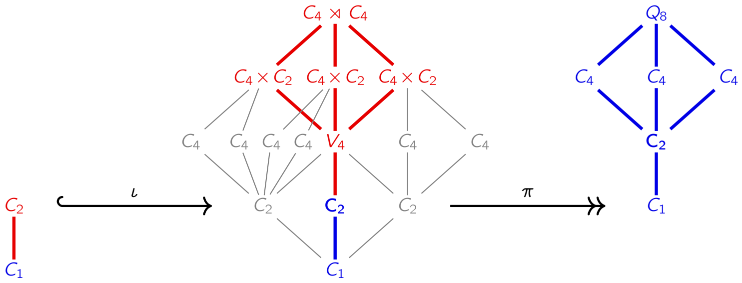
Central and stem extensions

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 $\iota(N) \leq Z(G')$.

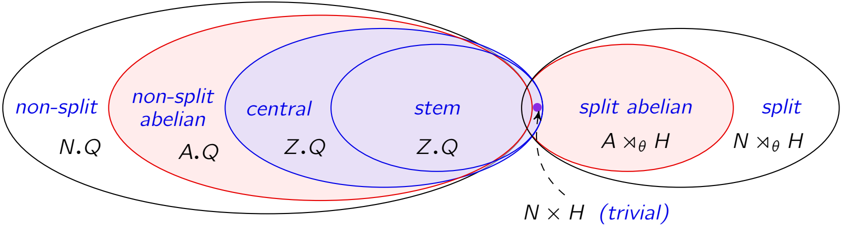
The group $G = C_4 \rtimes C_4$ is a central (and hence abelian), nonsplit extension of $Q = Q_8$ by $N = C_2$.



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

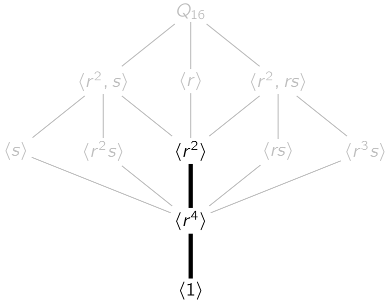
If G can be broken up into

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

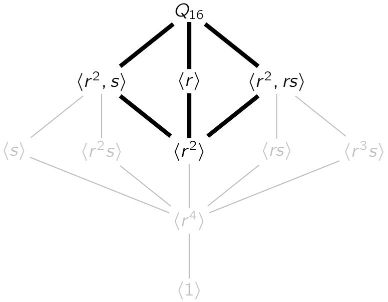
Chopping off subgroup lattices

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* $N = \langle r^2\rangle$"



"*chopping off below* $N = \langle r^2\rangle$"

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

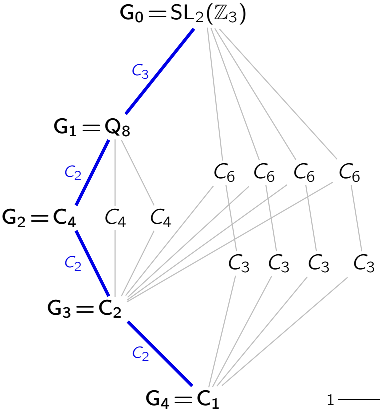
Breaking down a group into composition factors is like factoring a number into primes, or a molecule into atoms. We say:

"*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.



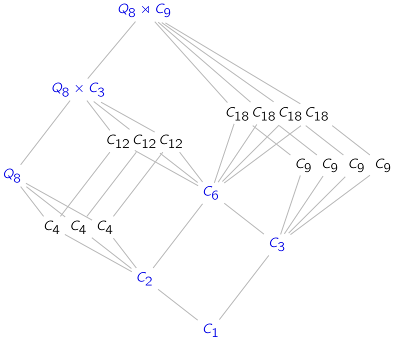
$$
\begin{tikzcd}
 & & & & 1 \arrow[r] & Q_8 \arrow[r, hook] \arrow[d, dashed] & \mathrm{SL}_2(\mathbb{Z}_3) \arrow[r, two heads] & \mathbf{C_3} \arrow[r] & 1 \\
 & & & 1 \arrow[r] & C_4 \arrow[r, hook] \arrow[d, dashed] & Q_8 \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & \\
 & & 1 \arrow[r] & C_2 \arrow[r, hook] \arrow[d, dashed] & C_4 \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & & \\
 & 1 \arrow[r] & 1 \arrow[r, hook] \arrow[d, dashed] & C_2 \arrow[r, two heads] & \mathbf{C_2} \arrow[r] & 1 & & & \\
1 \arrow[r] & 1 \arrow[r, hook] & 1 \arrow[r, two heads] & 1 \arrow[r] & 1 & & & &
\end{tikzcd}
$$

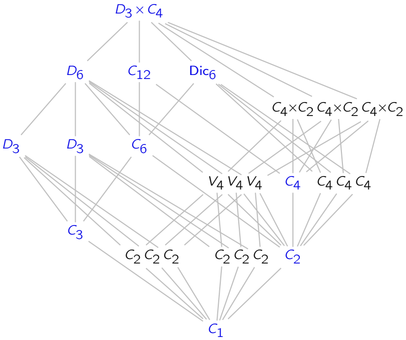
They will always be either *cyclic* or *non-abelian simple* (e.g., A_5, $\mathbf{GL}_3(\mathbb{Z}_2)$, $A_6, \ldots$).

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

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.

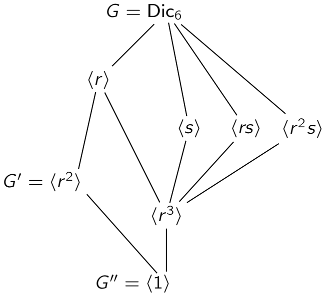
Equivalence of composition series

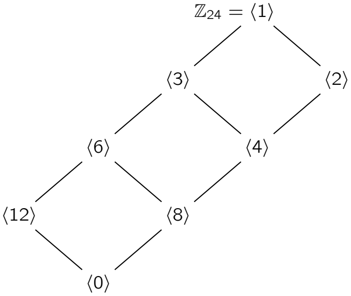
Two composition series

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

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:

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

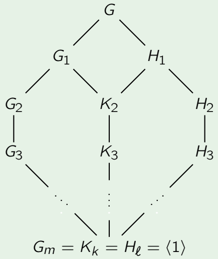
and the result holds for all groups with a composition series of length $\leq m$.

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.

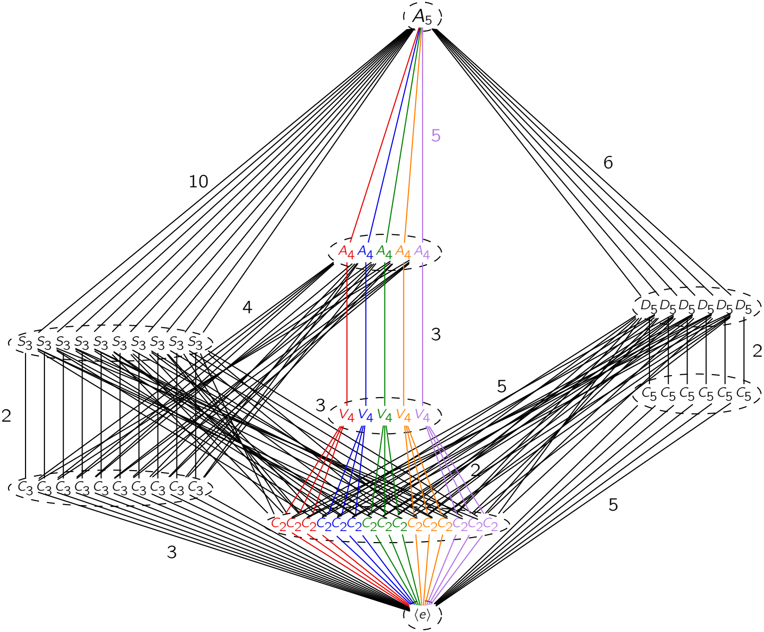
We now have 4 composition series of G.

Reading left-to-right (see lattice):

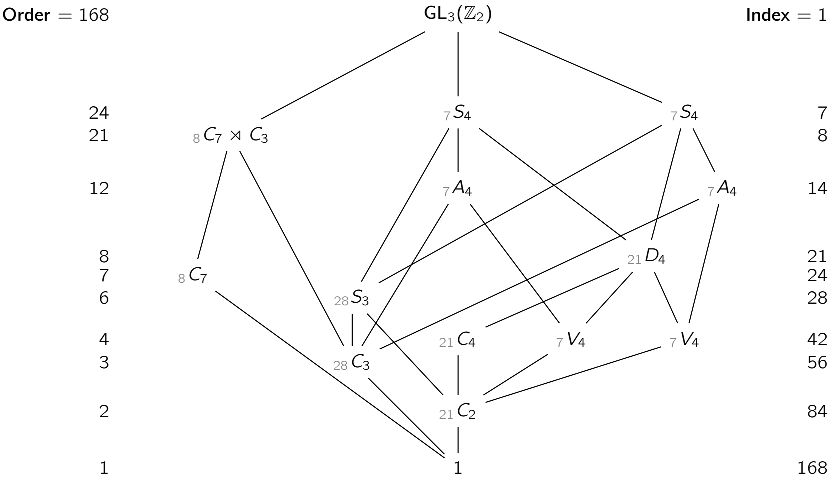
- The 1st & 2nd, and 3rd & 4th have the same factors by the IHOP.
- The 2nd and 3rd have the same factors by the diamond theorem.



The smallest nonsolvable (and smallest nonabelian simple) group

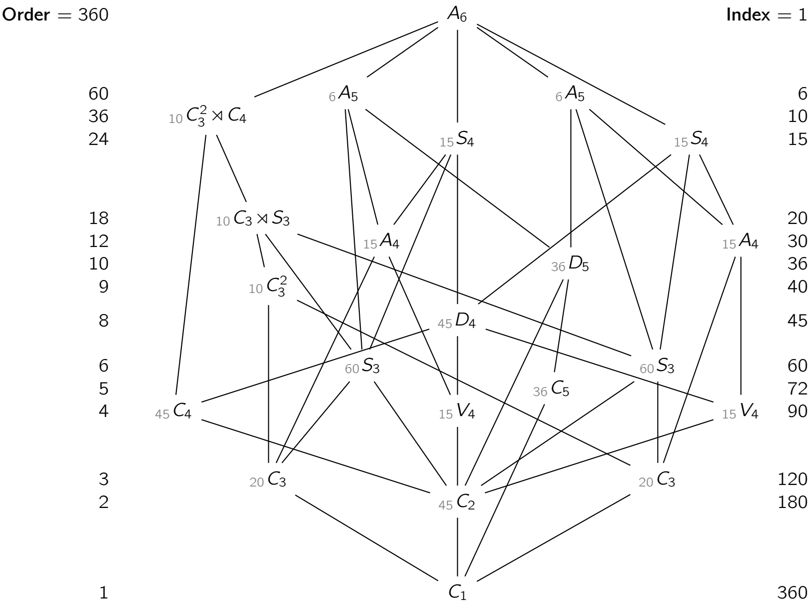


The second smallest nonabelian simple group ("group atom")



Note: There are 3 smaller nonsolvable nonsimple groups: S_5, $A_5 \times C_2$, $\mathsf{SL}_2(\mathbb{Z}_5) \cong A_5 . C_2$.

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



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.)

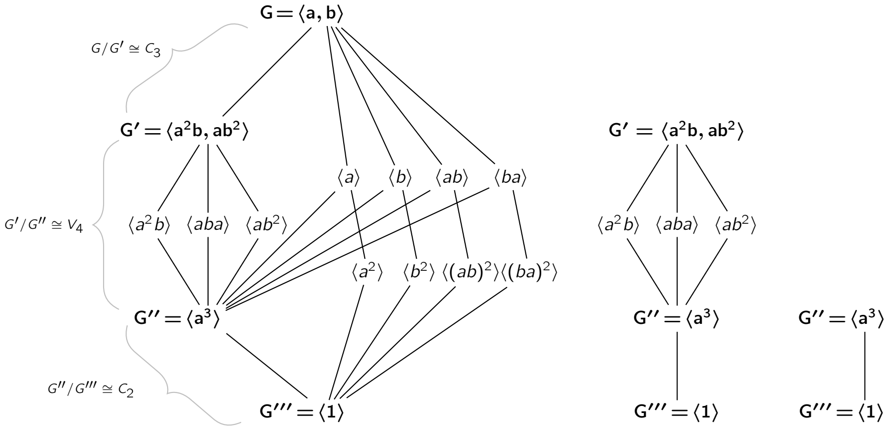
Definition

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.

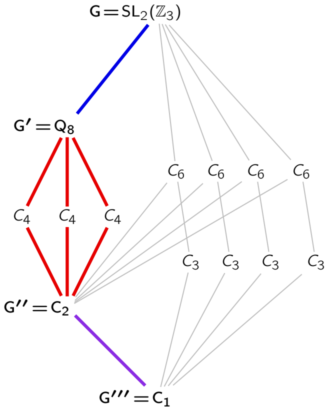
By the correspondence theorem, we can *refine* the derived series to a composition series.

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: $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq G_3 = \langle 1 \rangle$.



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

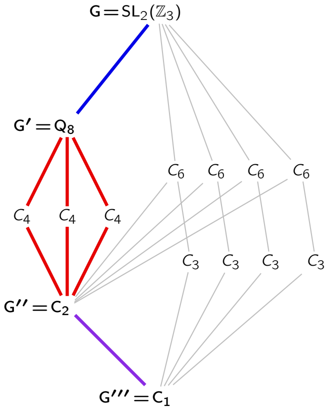
$$\begin{tikzcd}
 & & 1 \arrow[r] & G' \arrow[r, hook] \arrow[d, dashed] & G \arrow[r, two heads] & G/G' \arrow[r] & 1 \\
 & 1 \arrow[r] & G'' \arrow[r, hook] \arrow[d, dashed] & G' \arrow[r, two heads] & G'/G'' \arrow[r] & 1 & \\
1 \arrow[r] & G''' \arrow[r, hook] & G'' \arrow[r, two heads] & G'''/G''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

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: $\langle 1 \rangle = G_3 \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G$.



$$\begin{tikzcd}
 & & 1 \arrow[r] & \mathbf{C_3} \arrow[r, hook] & C_3 \arrow[r, two heads] & 1 \arrow[r] & 1 \\
 & 1 \arrow[r] & \mathbf{V_4} \arrow[r, hook] & A_4 \arrow[r, two heads] & C_3 \arrow[r] \arrow[u, dashed] & 1 & \\
1 \arrow[r] & \mathbf{C_2} \arrow[r, hook] & \mathsf{SL}_2(\mathbb{Z}_3) \arrow[r, two heads] & A_4 \arrow[r] \arrow[u, dashed] & 1 & &
\end{tikzcd}$$

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

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 $[K,K] \leq [H,H]$. $\square$

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:

$$\begin{tikzcd}[column sep=small]
G/N = G_0/N \arrow[dddd, dashed, bend right=60, "\text{composition series of } G/N"'] \arrow[d, dash] \\
G_1/N \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
\\
N/N = G_k/N
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
N = G_k \arrow[dd, dashed, bend right=60, "\text{composition series of } N"'] \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
\langle 1 \rangle = G_m
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
G = G_0 \arrow[ddd, dashed, bend right=60] \arrow[d, dash] \\
G_1 \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
N = G_k \arrow[dd, dashed, bend right=60] \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
\langle 1 \rangle = G_m
\end{tikzcd}$$

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:

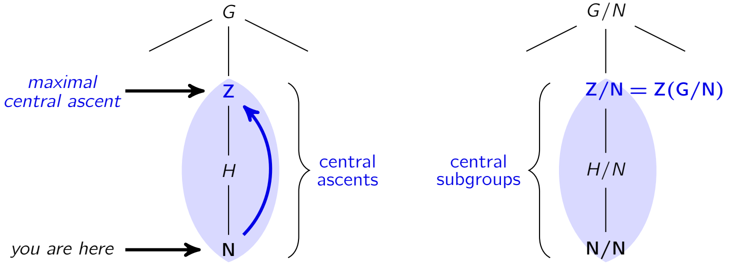
"*if we quotient by* N *(chop off the lattice below), what subgroup* Z/N *is the center?*"

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.

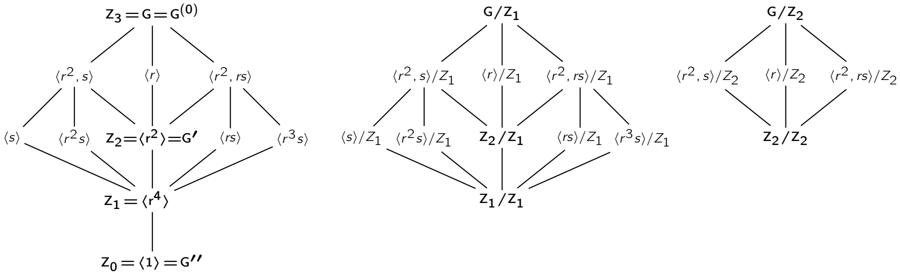
Nilpotent groups and the ascending central series

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. $\square$

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. $\square$

Proof

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

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 $N \le H \le G$ and $N \trianglelefteq G$, then

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

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

Proof

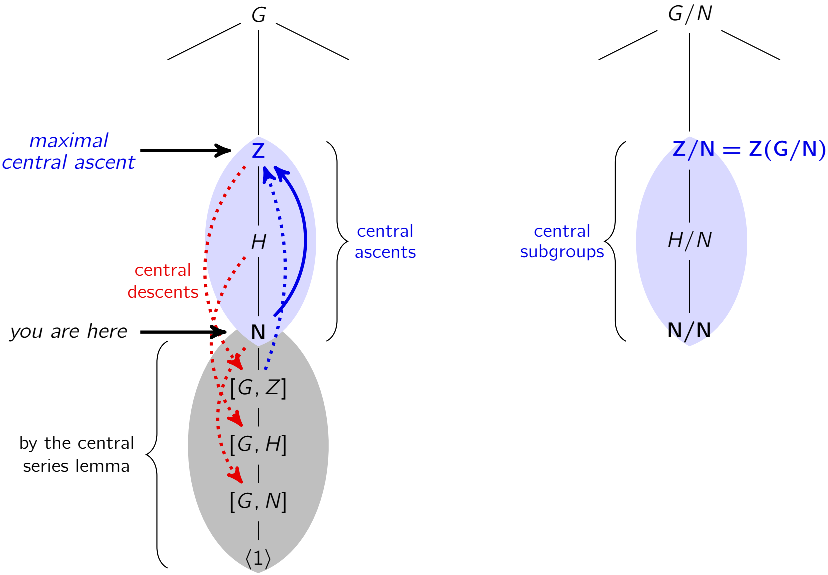
If H/N is in the center of G/N, then for all $h \in H$ and $g \in G$

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

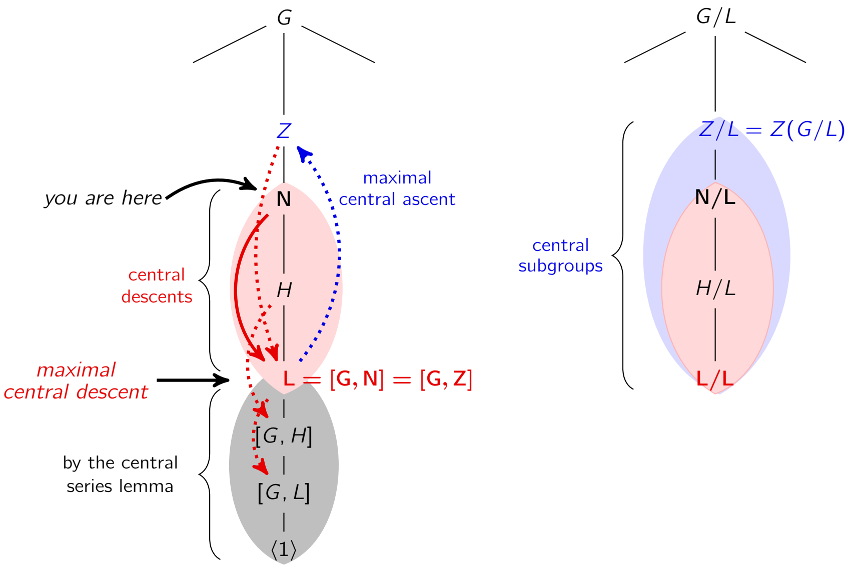
Definition

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

Central ascents



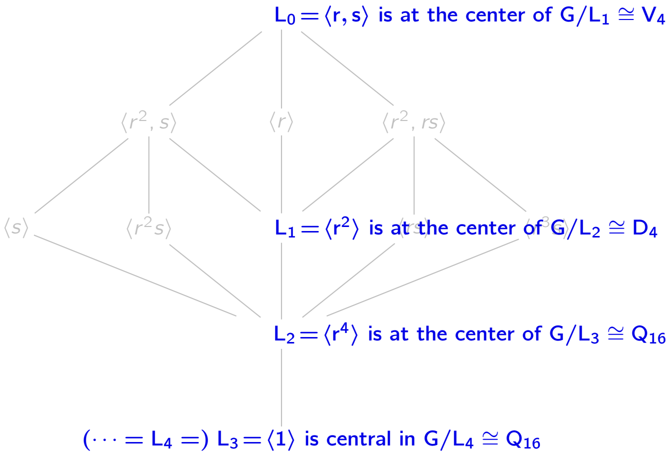
Central descents



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

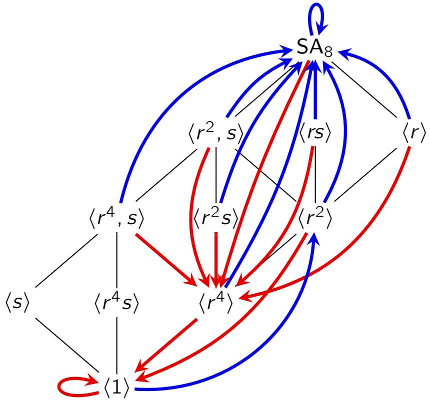
$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \leq [G, L_{k-1}] = L_k,$$

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., $Z/N = Z(G/N)$.

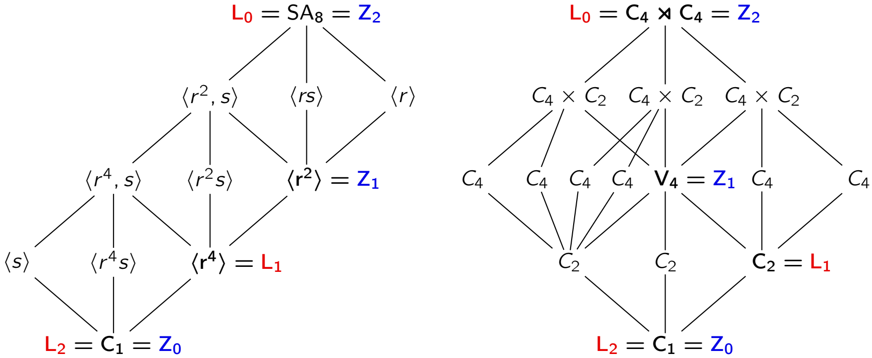


The ascending and descending central series can be read right off this diagram!

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 important technical lemma

The following lemma should come off as uninspiring and non-obvious.

Lemma

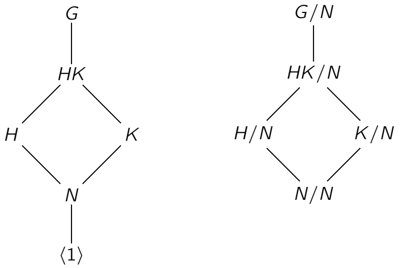
Suppose $N \leq H, K \leq G$ are normal. If $[G, H] \leq N$ and $[G, K] \leq N$, then $[G, HK] \leq N$.

Now, let's restate this using the *central series lemma*: If $N \leq H \leq G$ and $N \trianglelefteq G$, then

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

Lemma, restated

If H/N and K/N are central in G/N, then their product HK/N is as well.



A stronger result than we actually need

Theorem (we'll prove this next)

Let G be a finite group for which $L_{n-1} \gneq L_n = \langle 1 \rangle$. Then for all $k = 0, 1 \ldots, n$,

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

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

If the ACS reaches the top, say $Z_{n-1} \lneq Z_n = G$, then $L_n \leq Z_0 = \langle 1 \rangle$, so the DCS reaches the bottom in *at most n* steps. Hence $\text{length}(DCS) \leq \text{length}(ACS)$. ✓

If the DCS reaches the bottom, say $\langle 1 \rangle = L_m \lneq L_{m-1}$, then $G = L_0 \leq Z_m$, so the ACS reaches the top in *at most m* steps. Hence $\text{length}(ACS) \leq \text{length}(DCS)$. □

Proof of the stronger result

Theorem

Let G be a finite group for which $L_{n-1} \gneq L_n = \langle 1 \rangle$. Then $\mathbf{L_{n-k}} \leq \mathbf{Z_k}$, for all $k = 0, 1 \ldots, n$,

Proof

Throughout, the following facts will be used repeatedly:

$$[G, L_k] = L_{k+1} \quad (\textit{definition}), \qquad [G, Z_k] \leq Z_{k-1} \quad (\textit{by central series lemma}) \tag{1}$$

Suppose G is nilpotent of class n, i.e., $Z_{n-1} \lneq Z_n = G = L_0$.

Start at the top of the lattice and work down. We have $[G, L_0] = [G, Z_n]$, and applying Eq. (1) gives.

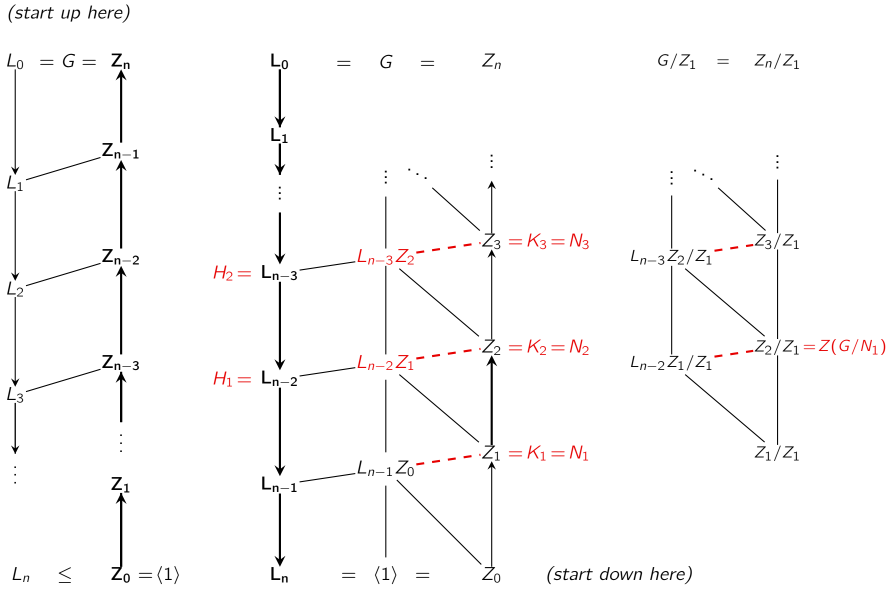
$$L_1 = [G, L_0] = [G, Z_n] \leq Z_{n-1}.$$

Now, we have $[G, L_1] \leq [G, Z_{n-1}]$. Applying Eq. (1) again gives

$$\begin{array}{ccccccc} L_2 & = & [G, L_1] & \leq & [G, Z_{n-1}] & \leq & Z_{n-2} \\ L_3 & = & [G, L_2] & \leq & [G, Z_{n-2}] & \leq & Z_{n-3} \\ & \vdots & & \vdots & & \vdots & \\ L_k & = & [G, L_{k-1}] & \leq & [G, Z_{n+k-1}] & \leq & Z_{n-k}, \end{array}$$

and $L_{n-k} \leq Z_k$ follows. ✓

Picture of the proof we just did (left diagram)



Proof of the stronger result

Theorem

Let G be a finite group for which $L_{n-1} \gneq L_n = \langle 1 \rangle$. Then $\mathbf{L_{n-k}} \leq \mathbf{Z_k}$, for all $k = 0, 1 \ldots, n$,

Proof (contin.)

Next, suppose $L_{n-1} \gneq L_n = \langle 1 \rangle = Z_0$; we'll will work our way *up* the lattice.

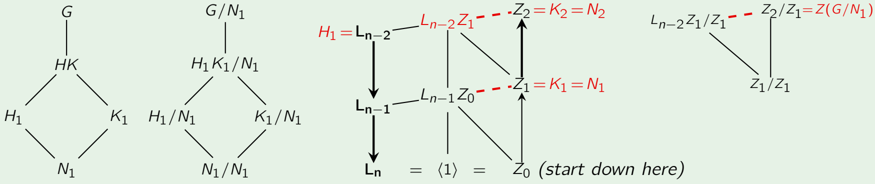
Starting at $L_n = [G, L_{n-1}] = \langle 1 \rangle = Z_0$, apply the *central series lemma* to $[G, L_{n-1}] \leq Z_0$:

$$L_{n-1} \cong L_{n-1}/Z_0 \leq Z(G/Z_0) \cong Z(G) = Z_1.$$

Next goal: Working upwards, show $L_{n-2} \leq Z_2$, $L_{n-3} \leq Z_3$, and inductively, $L_{n-k} \leq Z_k$.

It suffices to show: $$L_{n-k} \leq L_{n-k}Z_{k-1} \leq Z_k.$$

How: Apply our Lemma with $H = L_{n-2}$, $K = Z_1$, and $N = Z_1$.



Proof of the stronger result

Theorem

Let G be a finite group for which $L_{n-1} \gneq L_n = \langle 1 \rangle$. Then $\mathbf{L_{n-k}} \leq \mathbf{Z_k}$, for all $k = 0, 1 \ldots, n$,

Proof (contin.)

It suffices to show: $$L_{n-k} \leq L_{n-k} Z_{k-1} \leq Z_k.$$

How: Taking $H = L_{n-2}$, $K = Z_1$, and $N = Z_1$, we have

$$[G, H] = [G, L_{n-2}] = L_{n-1} \leq Z_1 = N, \qquad [G, K] = [G, Z_1] \leq Z_0 \leq Z_1 = N.$$

and our Lemma ($[G, HK] \leq N$) gives $[G, L_{n-2} Z_1] \leq Z_1$.

Translating this back into quotients, by the central series lemma:

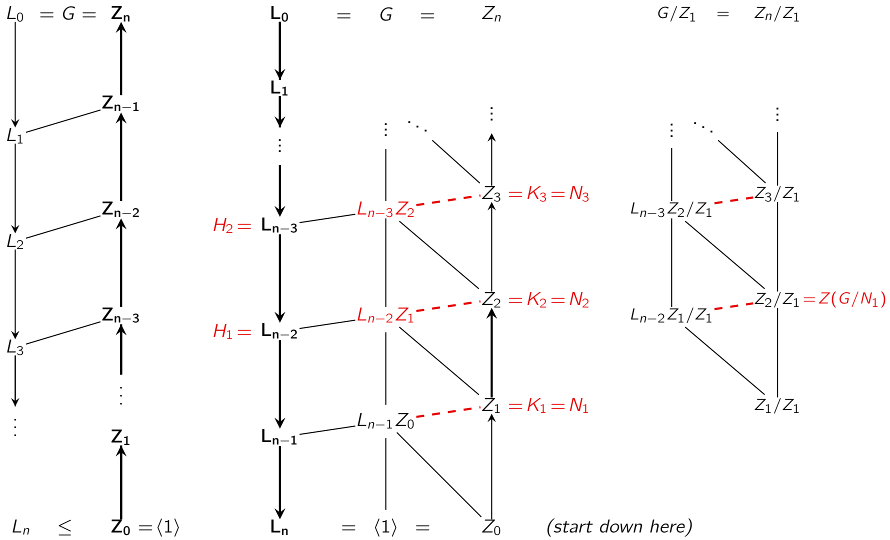
$$\underbrace{L_{n-2} Z_1 / Z_1}_{=HK/N} \leq \underbrace{Z(G/Z_1)}_{=Z(G/N)} := Z_2 / Z_1.$$

The inequality, $L_{n-2} Z_1 \leq Z_2$ now follows from the correspondence theorem.

Repeating this process inductively gives the desired result. $\square$

Picture of the proof we just did

(start up here)



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:

$$Z_{i+1} = \big\{x \in G \mid [x,g] \in Z_i,\ \forall g \in G\big\} = \big\{x \in G \mid xZ_igZ_i = gZ_ixZ_i,\ \forall g \in G\big\}$$

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}.

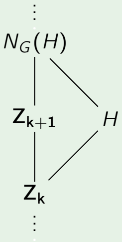
Pick some $x \in Z_{k+1}$. (Need to show it normalizes H.)

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

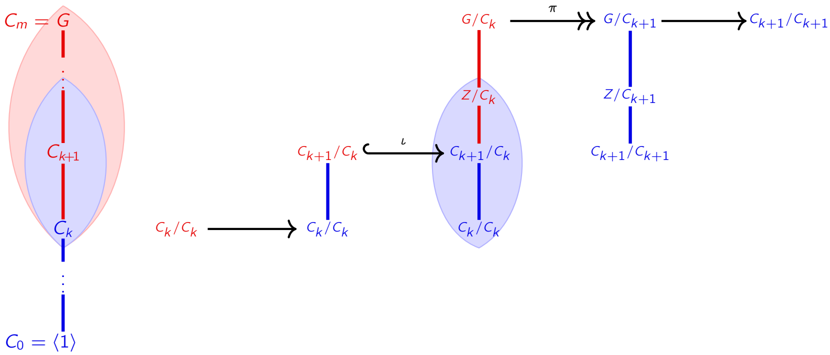
Definition

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

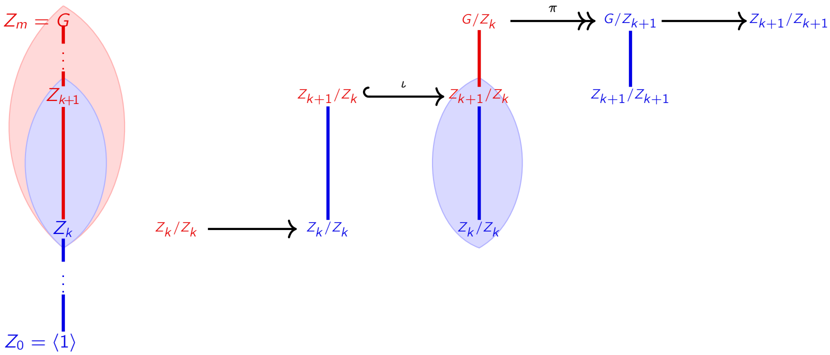
Remark

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 C_{k+1}/C_k).

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



Central series

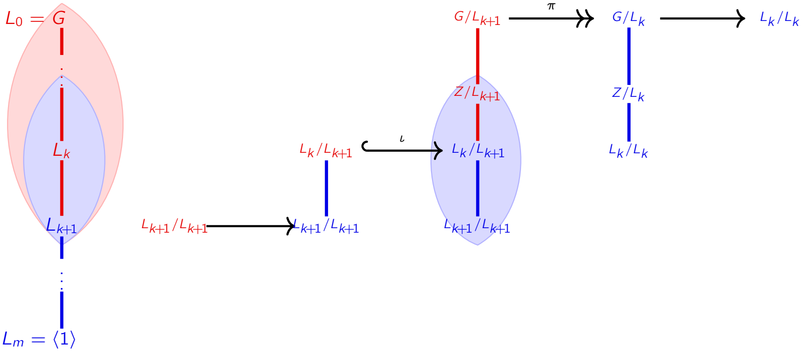
Remark

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

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

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

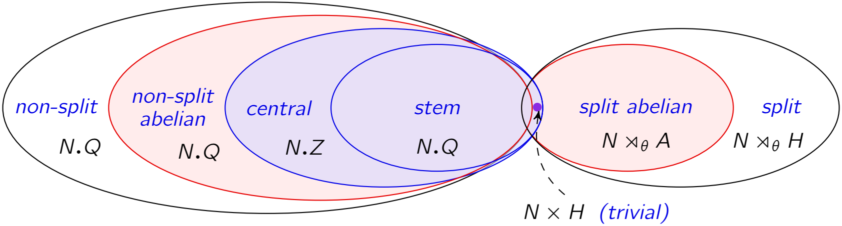
$$1 \longrightarrow L_k/L_{k+1} \xrightarrow{\iota_k} G/L_{k+1} \xrightarrow{\pi_k} G/L_k \longrightarrow 1$$



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.

$$
\begin{tikzcd}
& L_n = \langle 1 \rangle & & \\
\text{max'l} \Rightarrow \text{normal} \arrow[r, Rightarrow, bend left, "\text{HW}"] & Z_n = G \arrow[l, Rightarrow, bend left, "\text{Cor.}"] \arrow[u, Leftrightarrow, "\text{Cor.}"'] \arrow[r, Leftrightarrow, "\text{Prop.}"] \arrow[d, Rightarrow, bend right, "\text{Prop.}"'] & G = P_1 P_2 \cdots P_k \arrow[r, Leftrightarrow, "\text{Exer.}"] & n_p = 1,\ \forall p \\
& \text{normalizers grow} \arrow[u, Rightarrow, bend right, "\text{HW}"'] & &
\end{tikzcd}
$$

Factoring maps

We've discussed a number of properties that can be described as

"*the minimal* ____," or "*the maximal* ____,"

satisfying some condition.

We'll see to express this concisely in terms of maps and commutative diagrams.

This will highlight similarities and patterns that are inherent in seemingly different structures, streamline proofs, and lead to new insight.

Warm-up exercise (easy)

Given maps $g\colon G \to H$ and $h\colon H \to K$, their composition $f := h \circ g$ is a map from G to K.

I.e., there is *always* a map $f\colon G \to K$ making the following diagram commute:

$$\begin{tikzcd} G \arrow[rr, dashed, "f = h \circ g"] \arrow[dr, "g"'] & & K \\ & H \arrow[ur, "h"'] & \end{tikzcd}$$

Factoring maps

Let's now consider two variants of the previous commutative diagram.

Definition

Given two maps...

1. *from the same domain*, $f\colon G \to K$, $g\colon G \to H$, when does there exist $h\colon H \to K$
2. *into the same codomain*, $f\colon G \to K$, $h\colon H \to K$, when does there exist $g\colon G \to H$

such that $f = h \circ g$?

$$\begin{tikzcd}
\mathbf{G} \arrow[rr, "f"] \arrow[dr, "g"'] & & K \\
& H \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, dashed, "g"'] & & \mathbf{K} \\
& H \arrow[ur, "h"'] &
\end{tikzcd}$$

"f factors through g" "f factors through h"

We say that h and g are **factors** of f.

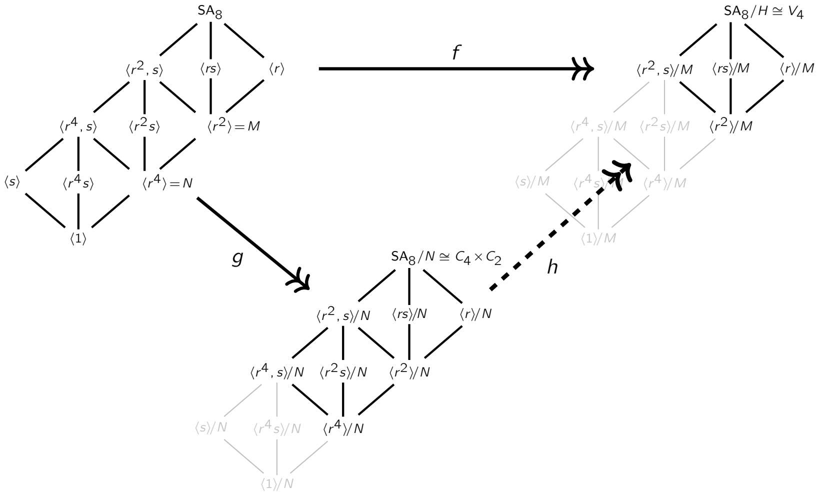
We'll do an example of each that will nicely illustrate when and why this happens.

Both will involve $G = \mathrm{SA}_8 = \langle r, s\rangle$, and its subgroups $N = \langle r^2\rangle \cong C_4$, and $M = \langle r^4\rangle \cong C_2$.

Factoring maps: a quotient between the codomains

Let $G = \mathrm{SA}_8 = \langle r, s\rangle$, and $N = \langle r^2\rangle \cong C_4$, and $M = \langle r^4\rangle \cong C_2$.

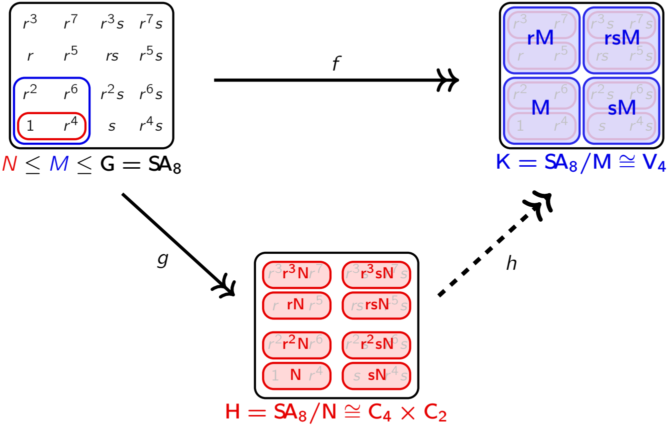
The standard quotient map $f \colon \mathrm{SA}_8 \to V_4$ can be factored:



Factoring maps: a quotient between the codomains

Formally, this map is defined by

$$h\colon \mathrm{SA}_8/N \longrightarrow \mathrm{SA}_8/M, \qquad h\colon gN \longmapsto gM.$$

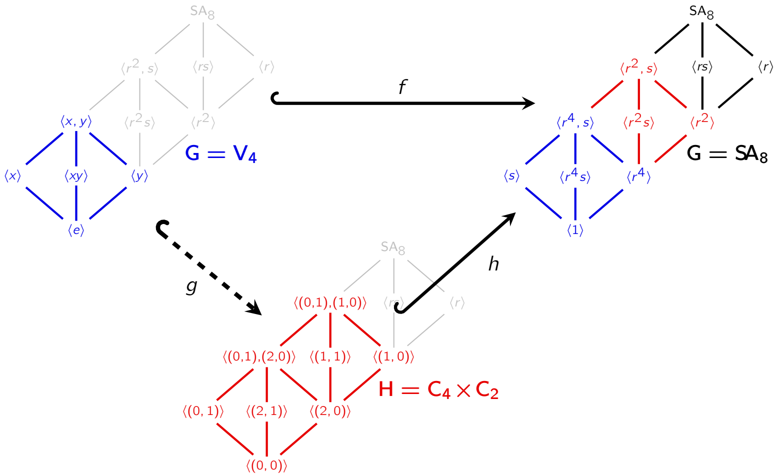


Factoring maps: an embedding between the domains

Let $V_4 = \{e, x, y, xy\}$ and $\mathrm{SA}_8 = \langle r, s\rangle$. The embedding

$$f\colon V_4 \hookrightarrow \mathrm{SA}_8, \qquad x \longmapsto r^4, \quad y \longmapsto s$$

uniquely factors through $h\colon C_4 \times C_2 \to \mathrm{SA}_8$, where $(1,0) \mapsto r^2$ and $(0,1) \mapsto s$.

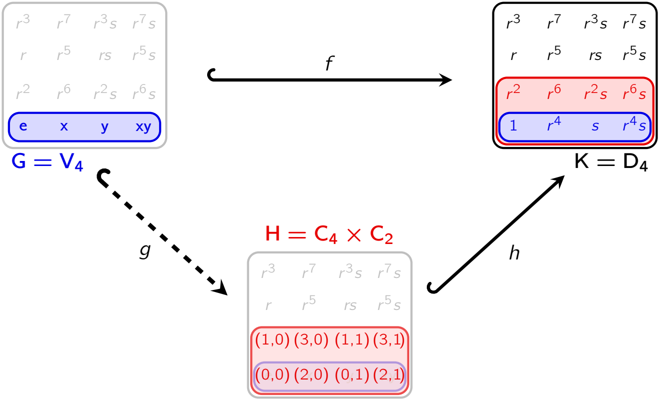


Factoring maps: an embedding between the domains

Let $V_4 = \{e, x, y, xy\}$ and $\mathrm{SA}_8 = \langle r, s \rangle$. Here's that same embedding

$$f\colon V_4 \hookrightarrow \mathrm{SA}_8, \qquad x \longmapsto r^4, \quad y \longmapsto s$$

that uniquely factors through $h\colon C_4 \times C_2 \to \mathrm{SA}_8$, where $(1,0) \mapsto r^2$ and $(0,1) \mapsto s$.



Canceling maps: when does existence imply uniqueness?

Proposition ("cancelation laws")

Suppose we have functions $g_i \colon G \to H$ and $h_i \colon H \to K$ between sets, for $i = 1, 2$.

If g is surjective, then it right-cancels: $\quad h_1 \circ g = h_2 \circ g \quad \Longrightarrow \quad h_1 = h_2.$

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "g"'] & & K \\ & H \arrow[ur, dashed, two heads, "h_1"'] & \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "g"'] & & K \\ & H \arrow[ur, dashed, two heads, "h_2"'] & \end{tikzcd} \quad \Longrightarrow \quad h_1 = h_2.$$

If h is injective, then it left-cancels: $\quad h \circ g_1 = h \circ g_2 \quad \Longrightarrow \quad g_1 = g_2.$

$$\begin{tikzcd} G \arrow[rr, hook, "f"] \arrow[dr, dashed, hook, "g_1"'] & & K \\ & H \arrow[ur, hook, "h"'] & \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[rr, hook, "f"] \arrow[dr, dashed, hook, "g_2"'] & & K \\ & H \arrow[ur, hook, "h"'] & \end{tikzcd} \quad \Longrightarrow \quad g_1 = g_2.$$

Key idea

Injective functions have left inverses; surjective functions have right inverses.

Failure of uniqueness: a quotient between domains

Let $D_4 = \langle r, s \rangle$ with subgroups $N = \langle r^2 \rangle \cong C_2$ and $M = \langle r \rangle \cong C_4$.

Their quotients are $V_4 \cong D_4/N = \{N, rN, sN, rsN\}$ and $C_2 \cong D_4/M = \{M, sM\}$.

Define the functions $f \colon D_4 \to C_2$ and $h \colon V_4 \to C_2$ as follows:

$$\begin{tikzcd} D_4 \arrow[rr, "f"] \arrow[dr, dashed, "g"'] & & C_2 \\ & V_4 \arrow[ur, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} r \arrow[rr, mapsto, "f"] \arrow[dr, dashed, mapsto, "g"'] & & rM \\ & rN \arrow[ur, mapsto, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} s \arrow[rr, mapsto, "f"] \arrow[dr, dashed, mapsto, "g"'] & & sM \\ & sN \arrow[ur, mapsto, "h"'] & \end{tikzcd}$$

We must have $g \colon 1 \mapsto N$. Since $f \colon r \mapsto M$, then $g(r) \in \mathrm{Ker}(h) = \{rN, N\}$.

If $g(r) = N$, then g is not surjective, but we still have $f = h \circ g$.

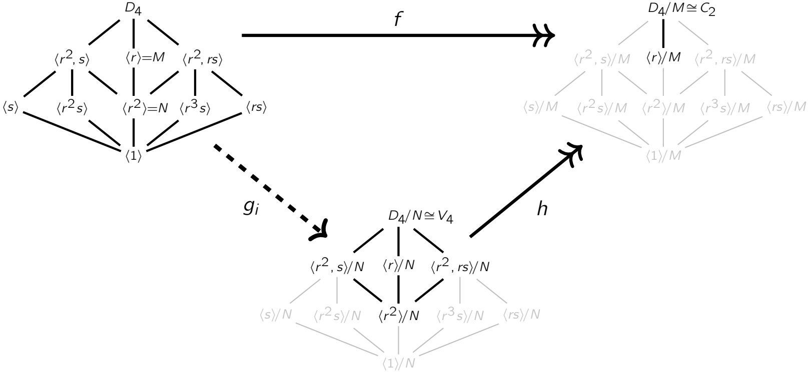
Warning!

The homomorphism $g \colon D_4 \to V_4$ is *not* uniquely defined! ($r \mapsto N$ would work too)

Moral: commutative diagrams can be deceiving!

Failure of uniqueness: a quotient between domains

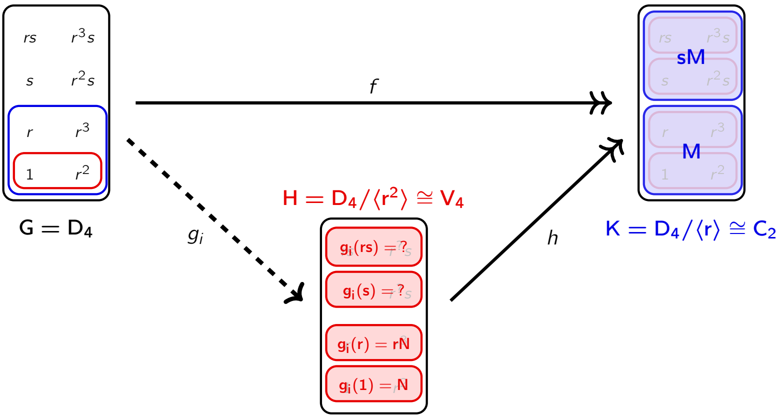
Multiple maps g_i make this diagram commute; both $r \mapsto rN$ and $r \mapsto N$ work.



For surjective maps, $h \circ g_1 = h \circ g_2 \quad \not\Rightarrow \quad g_1 = g_2$.

Failure of uniqueness: a quotient between domains

Note that $g_i \colon D_4 \to V_4$ need not be surjective for the following diagram to commute.



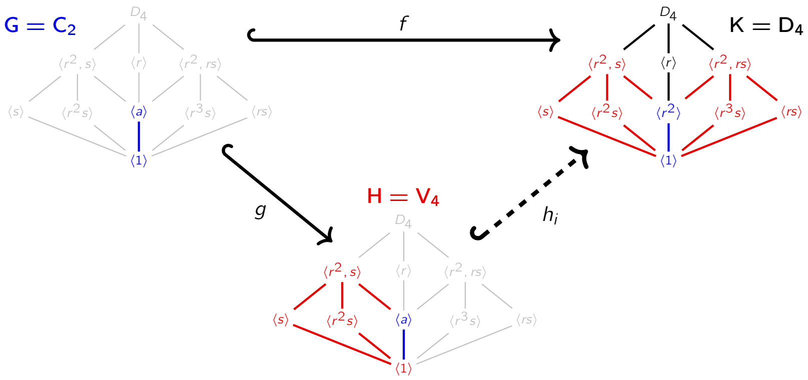
Any choice of $g_i(r) \in \{N, rN\}$ and $g_i(s) \in \{sN, rsN\}$ would work.

Failure of uniqueness: an embedding between codomains

Consider two maps from $G = C_2 = \{1, a\}$ into $H = V_4 = \{e, x, y, xy\}$ and $K = D_4 = \langle r, s\rangle$:

$$f\colon C_2 \longrightarrow D_4, \quad f(a) = r^2, \qquad\qquad g\colon C_2 \longrightarrow V_4, \quad f(a) = x.$$

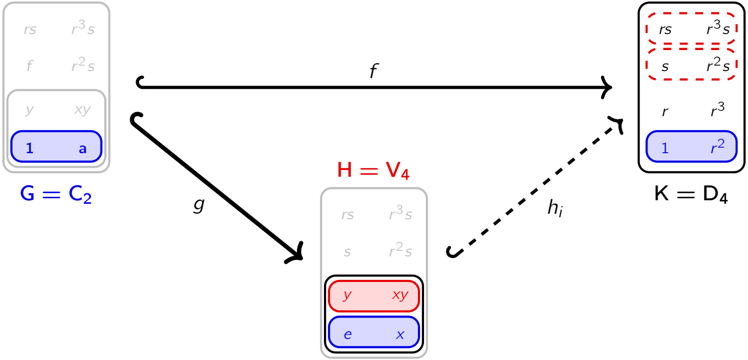
There are multiple embeddings $h_i\colon V_4 \hookrightarrow D_4$ that make this diagram commute:



For injective maps, $h_1 \circ g = h_2 \circ g \quad \not\Rightarrow \quad h_1 = h_2$.

Failure of uniqueness: an embedding between codomains

Here is another way to see why there are multiple embeddings $h_i \colon V_4 \hookrightarrow D_4$ that make this diagram commute:



For injective maps, $h_1 \circ g = h_2 \circ g \quad \not\Rightarrow \quad h_1 = h_2$.

Factoring non-homomorphisms

Definition

Let G/N be a set (not necessarily a group) of equivalence classes. The map ϕ from G **descends to a map from G/N** if it factors through the canonical quotient $\pi\colon G \to G/N$.

For example, we have seen that:

- the map $\phi\colon G \to \mathrm{cl}_G(H)$ **descends to a bijection** $G/N_G(H) \to \mathrm{cl}_G(H)$.

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, two heads, "\pi"'] & & \mathrm{cl}_G(H) \\ & G/N_G(H) \arrow[ur, dashed, "\iota"'] & \end{tikzcd} \qquad \begin{tikzcd} g \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, two heads, "\pi"'] & & g^{-1}Hg \\ & Ng \arrow[ur, dashed, mapsto, "\iota"'] & \end{tikzcd}$$

- the map $\phi\colon G \to \mathrm{cl}_G(g)$ **descends to a bijection** $G/C_G(g) \to \mathrm{cl}_G(g)$.
- For a fixed $s \in S$, $\phi\colon G \to \mathrm{orb}(s)$ **descends to a bijection** $G/\operatorname{stab}(s) \to \mathrm{orb}(s)$.

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, two heads, "\pi"'] & & \mathrm{orb}(s) \\ & G/\operatorname{stab}(s) \arrow[ur, dashed, "\iota"'] & \end{tikzcd} \qquad \begin{tikzcd} g \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, two heads, "\pi"'] & & g.\phi(s) \\ & Hg \arrow[ur, dashed, mapsto, "\iota"'] & \end{tikzcd}$$

Motivating the co-universal property of quotient groups

Definition

Given $H \leq G$, the **canonical inclusion map** is

$$\iota\colon H \hookrightarrow G, \qquad \iota\colon h \longmapsto h.$$

If $H \trianglelefteq G$, the **canonical quotient map is**

$$\pi\colon G \longrightarrow G/H, \qquad \pi\colon g \longmapsto gH.$$

There does not exist a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ with $\phi(1) = 1$. To formalize this:

the canonical quotient $f: \mathbb{Z} \twoheadrightarrow \mathbb{Z}_4$ does not factor through $g: \mathbb{Z} \twoheadrightarrow \mathbb{Z}_3$.

That is, there does *not* exist $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ making this diagram commute:

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\pi"'] & & \mathbb{Z}_4 \\
& \mathbb{Z}_3 \arrow[ur, dashed, "\phi"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & 1 \\
& 1 \arrow[ur, dashed, mapsto, "\phi"'] &
\end{tikzcd}$$

Preview: such a map exists iff $\mathrm{Ker}(\pi) \leq \mathrm{Ker}(f)$, i.e., f collapses at least as much as π.

Motivating the co-universal property of quotient groups

Does $\phi\colon \mathbb{Z}_8 \to \mathbb{Z}_{12}$, where $\phi(1) = 3$, define a homomorphism?

Is there a homomorphism ϕ making the following diagram commute?

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\pi"'] & & \mathbb{Z}_{12} \\ & \mathbb{Z}_8 \arrow[ur, dashed, "\phi"'] & \end{tikzcd} \qquad \begin{tikzcd} 1 \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & 3 \\ & 1 \arrow[ur, dashed, mapsto, "\phi"'] & \end{tikzcd}$$

Note that $\mathrm{Ker}(f) = 4\mathbb{Z}$ is a subgroup of $\mathrm{Ker}(\pi) = 8\mathbb{Z}$, and so f factors through π.

Not only does ϕ exist, it is automatically unique by the cancellation laws.

The co-universal property of quotient groups

Theorem

Let $N \trianglelefteq G$ and $f\colon G \to K$ be a homomorphism such that $N \le \mathrm{Ker}(f)$. Then

1. f uniquely factors through $\pi\colon G \to G/N$ (i.e., $\exists! h\colon G/N \to K$ such that $g = h \circ \pi$).
2. h is injective iff $\mathrm{Ker}(f) = N$.

Proof (i)

Assume WLOG that f is onto (otherwise, take $K = \mathrm{Im}(f)$). Define $h\colon G/N \to H$ by

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, "\pi"'] & & K \\ & G/N \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & f(x) \\ & xN \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Well-defined: If $xN = yN$, then $y^{-1}xN = N$, so $y^{-1}x \in N = \mathrm{Ker}(\pi) \le \mathrm{Ker}(f)$. Now,

$$f(y^{-1}x) = 1 \quad \Longrightarrow \quad f(y)^{-1}f(x) = 1 \quad \Longrightarrow \quad h(xN) = f(x) = f(y) = h(yN). \qquad \checkmark$$

Homomorphism: $\quad h(xNyN) = h(xyN) = f(xy) = f(x)f(y) = h(xH)h(yN). \qquad \checkmark$

Uniqueness: Follows from existence, since f and π are quotients (cancellation laws). $\checkmark$

The co-universal property of quotient groups

Theorem

Let $N \trianglelefteq G$ and $f \colon G \to K$ be a homomorphism such that $N \leq \mathrm{Ker}(f)$. Then

1. f uniquely factors through $\pi \colon G \to G/N$ (i.e., $\exists! h \colon G/N \to K$ such that $g = h \circ \pi$).
2. h is injective iff $\mathrm{Ker}(f) = N$.

Proof (ii)

Assume WLOG that f is onto. We just found the unique h such that

$$
\begin{tikzcd}
G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\pi"'] & & K \\
& G/N \arrow[ur, dashed, two heads, "h"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
x \arrow[rr, maps to, "f"] \arrow[dr, maps to, "\pi"'] & & f(x) \\
& xN \arrow[ur, dashed, maps to, "h"'] &
\end{tikzcd}
$$

Let $H = \mathrm{Ker}(f)$, and note that

$$\mathrm{Ker}(h) = \{xN \mid f(x) = 1_K\} = \{xN \mid x \in H\} = H/N.$$

Note that h is injective iff $|\mathrm{Ker}(h)| = 1$, or equivalently, $H = N$. $\square$

Co-universal property of quotient groups $\Rightarrow$ FHT

Corollary: Fundamental homomorphism theorem

If $f\colon G \to H$ is a homomorphism, then $G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

Proof

Let $K = \operatorname{Im}(f)$ and $N = \operatorname{Ker}(f)$ with canonical quotient map $\pi\colon G \to G/N$.

By construction, $\operatorname{Ker}(f) = N = \operatorname{Ker}(\pi)$.

By the co-universal property of quotient maps, f factors through the quotient:

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, two heads, "\pi"'] & & \operatorname{Im}(f) \\
& G/N \arrow[ur, hook, two heads, dashed, "\iota"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & f(x) \\
& xN \arrow[ur, mapsto, dashed, "\iota"'] &
\end{tikzcd}$$

Since $\operatorname{Ker}(f) = N$, the map ι is injective by Part (ii) of the previous theorem.

Therefore, ι is an isomorphism. $\square$

Abstracting the (co)-universal property

To motivate where we're going, let's rephrase what we just did as

> "*G/N is the largest quotient that collapses N, in that any other homomorphism collapsing N factors through $\pi\colon G \to G/N$ uniquely.*"

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\pi"'] & & K \\ & G/N \arrow[ur, dashed, two heads, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & f(x) \\ & xN \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Compare this to what we know about the commutator subgroup G':

> "*G/G' is the largest abelian quotient of G, in that any other homomorphism to an abelian group factors through $\alpha\colon G \to G/G'$ uniquely.*"

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\alpha"'] & & A \\ & G/G' \arrow[ur, dashed, two heads, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\alpha"'] & & f(x) \\ & xG' \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Abstracting the (co)-universal property

The **co-universal property** of quotients came with a distinguished (maximal)

- group G/N, and
- canonical map $\pi\colon G \to G/N$.

Definition

A **co-universal pair** (C, χ) for a group G w.r.t. a property consists of:

- a group C, with
- an incoming map $\chi\colon G \to C$,

such that every $f\colon G \to H$ with the same property factors through χ uniquely.

I.e., there is a unique homomorphism $h\colon C \to H$ between co-domains such that $f = h \circ \chi$.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\chi"'] & & H \\ & C \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

Abstracting the (co)-universal property

Proposition

If G has a co-universal pair (C, χ) w.r.t. some property, C is unique up to isomorphism.

Proof

Let (C, χ) and (C', χ') be co-universal. Start with (C, χ), and take $H = C'$ and $f = \chi'$.

By definition, $\exists! h \colon C \to C'$ such that $\chi' = h \circ \chi$. Reverse the roles, and we get:

$$\begin{tikzcd}
G \arrow[rr, "\chi'"] \arrow[dr, "\chi"'] & & C' \\
& C \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[rr, "\chi"] \arrow[dr, "\chi'"'] & & C \\
& C' \arrow[ur, dashed, "h'"'] &
\end{tikzcd}$$

We can "stack" one diagrams on the other, and vice-versa:

$$\begin{tikzcd}
G \arrow[rrr, "\chi"] \arrow[drr, "\chi'"] \arrow[ddr, "\chi"'] & & & C \\
& & C' \arrow[ur, dashed, "h'"] & \\
& C \arrow[ur, dashed, "h"] \arrow[uurr, dashed, bend right, "\mathrm{Id}_C"'] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[rrr, "\chi'"] \arrow[drr, "\chi"] \arrow[ddr, "\chi'"'] & & & C' \\
& & C \arrow[ur, dashed, "h"] & \\
& C' \arrow[ur, dashed, "h'"] \arrow[uurr, dashed, bend right, "\mathrm{Id}_{C'}"'] & &
\end{tikzcd}$$

By uniqueness, $h \circ h' = \mathrm{Id}_C$ (left), and $h' \circ h = \mathrm{Id}_{C'}$ (right). Thus, $C \cong C'$. $\square$

A co-universal property and nilpotency

Recall that we characterized nilpotent groups via iterative "maximal central descents."

Given $N \trianglelefteq G$, the maximal central descent $[G, N]$ is characterized as being

"*the smallest subgroup L such that N/L is central in G/L*".

We can phrase this as a co-universal property.

Consider (L, λ), where $L = [G, N]$ and $\lambda \colon G \to G/L$ is the canonical quotient.

Co-universal property of central descents (HW)

Let $N \trianglelefteq G$ and $f \colon G \to K$ for which $f(N)$ is central. Then f uniquely factors through the canonical quotient map $\lambda \colon G \to G/L$, where $L = [G, N]$.

That is, there is a unique homomorphism $h \colon G/L \to K$ for which $f = h \circ \lambda$.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\lambda"'] & & K \\ & G/L \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\lambda"'] & & f(x) \\ & xL \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Universal vs. co-universal properties

We call the examples we've seen co-universal because the map is between the co-domains.

The "dual" version, where the maps is between the domains, are universal properties.

Most books don't distinguish these two, and use "universal" for both.

The examples we've seen were maximal quotients. Let's now look at maximal subgroups.

Universal property of centers

Let $H \leq G$ for which $xz = zx$ for all $z \in H$ and $x \in G$. The canonical inclusion $g \colon H \hookrightarrow G$ uniquely factors through $\zeta \colon Z(G) \hookrightarrow G$.

That is, there is a unique embedding $g \colon H \hookrightarrow Z(G)$ for which $f = \zeta \circ g$.

$$
\begin{tikzcd}
H \arrow[rr, hook, "f"] \arrow[dr, hook, dashed, "g"'] & & G \\
& Z(G) \arrow[ur, hook, "\zeta"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
z \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, dashed, "g"'] & & z \\
& z \arrow[ur, mapsto, "\zeta"'] &
\end{tikzcd}
$$

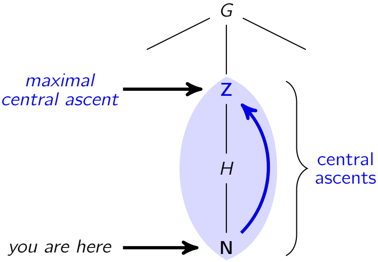
Another universal property

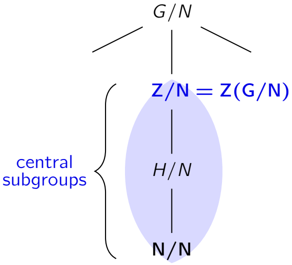
Universal property of central ascents

Given $N \trianglelefteq G$, suppose that $H/N \leq Z(G/N)$. The canonical inclusion $H/N \hookrightarrow G/N$ uniquely factors through $\zeta\colon Z(G/N) \hookrightarrow G/N$.

That is, there is a unique embedding $g\colon H/N \hookrightarrow Z(G/N)$ for which $f = \zeta \circ g$.

$$
\begin{tikzcd}
H/N \arrow[rr, hook, "f"] \arrow[dr, hook, dashed, "g"'] & & G/N \\
& Z(G/N) \arrow[ur, hook, "\zeta"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
hN \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, dashed, "g"'] & & hN \\
& hN \arrow[ur, mapsto, "\zeta"'] &
\end{tikzcd}
$$





Universal pairs and universal constructions

Definition

A **universal pair** (U, υ) for G w.r.t. a property consists of a group U and map $\upsilon\colon U \to G$, such that every other $f\colon H \to G$ with the same property factors through υ uniquely.

That is, $\exists! g\colon H \to U$ between the *domains* such that $f = \upsilon \circ g$.

$$\begin{tikzcd} H \arrow[rr, "f"] \arrow[dr, dashed, "g"'] & & G \\ & U \arrow[ur, "\upsilon"'] & \end{tikzcd}$$

Proposition (HW)

If G has a universal pair (U, υ) w.r.t. some property, then U is unique up to isomorphism.

It's not standard or necessary to characterize a simple concept like $Z(G)$ with a universal property. We did it as a "warm up."

Soon, we'll *define* concepts by a (co-)universal property.

These are examples of universal constructions.

Motivation: direct product vs. direct sums

Open-ended question

What is the limit of $\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R}\}$, as $n \to \infty$?

- Define $\mathbb{R}^\infty$ to be the space of all infinite sequences

$$\mathbb{R}^\infty := \prod_{i=1}^{\infty} \mathbb{R} := \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \cdots = \big\{(a_1, a_2, a_3, \dots) \mid a_i \in \mathbb{R}\big\}.$$

This space contains "vectors" such as $(1, 1, 1, \dots)$. We'll call it the "**direct product**."

- Define $\mathbb{E}^\infty$ to be the space of all finite sums, like

$$\mathbf{e} = a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n = \sum_{i=1}^{n} a_i\mathbf{e}_i, \qquad ||\mathbf{v}|| = \sqrt{a_1^2 + \cdots + a_n^2}.$$

We'll call this the "**direct sum**".

$$\mathbb{E}^\infty := \bigoplus_{i=1}^{\infty} \mathbb{R}\mathbf{e}_i : = \mathbb{R}\mathbf{e}_1 \oplus \mathbb{R}\mathbf{e}_2 \oplus \mathbb{R}\mathbf{e}_3 \oplus \cdots = \left\{\sum_{i=1}^{k} a_i\mathbf{e}_i \mid a_i \in \mathbb{R},\ k \geq 1\right\}$$

$$\cong \big\{(a_1, a_2, a_3, \dots) \mid a_i \in \mathbb{R},\ \text{all but finitely many } a_j \text{ are zero}\big\}.$$

Motivation: direct product vs. direct sums

Define the canonical quotient maps for each $i = 1, 2, \ldots$ as

$$\pi_i \colon \mathbb{R} \times \mathbb{R} \times \cdots \longrightarrow \mathbb{R}, \qquad \pi_i \colon (a_1, a_2, \ldots) \longmapsto a_i.$$

The direct product is the "*smallest P that projects onto each factor*."

Given any family $f_i \colon X \to \mathbb{R}$ of maps, each f_i factors through the projection $\pi_i \colon P \to \mathbb{R}$.

$$\begin{tikzcd}
 & X \arrow[dl, "f_1"'] \arrow[d, dashed, "f"] \arrow[dr, "f_2"] & \\
\mathbb{R} & \mathbb{R}\times\mathbb{R}\times\cdots \arrow[l, two heads, "\pi_1"] \arrow[r, two heads, "\pi_2"'] & \mathbb{R}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & x \arrow[dl, mapsto, "f_1"'] \arrow[d, mapsto, dashed, "f"] \arrow[dr, mapsto, "f_2"] & \\
a_1 & (a_1, a_2, \ldots) \arrow[l, mapsto, "\pi_1"] \arrow[r, mapsto, "\pi_2"'] & a_2
\end{tikzcd}$$

Let's see why this fails if we tried to use $\mathbb{E}^\infty$ for P:

$$\begin{tikzcd}
 & X = \mathbb{R}\times\mathbb{R}\times\cdots \arrow[dl, "f_1"'] \arrow[d, dashed, two heads, "f"] \arrow[dr, "f_2"] & \\
\mathbb{R} & \underbrace{\mathbb{R}\mathbf{e}_1 \oplus \mathbb{R}\mathbf{e}_2 \oplus \cdots}_{\text{"\textit{too small}"}} \arrow[l, two heads, "\pi_1"] \arrow[r, two heads, "\pi_2"'] & \mathbb{R}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & x = (a_1, a_2, \ldots) \arrow[dl, mapsto, "f_1"'] \arrow[d, mapsto, dashed, "\nexists f"] \arrow[dr, mapsto, "f_2"] & \\
a_1 & ??? \arrow[l, mapsto, "\pi_1"] \arrow[r, mapsto, "\pi_2"'] & a_2
\end{tikzcd}$$

Motivation: direct product vs. direct sums

Define the natural inclusion map for each $j = 1, 2, \dots$ as

$$\iota_j \colon \mathbb{R}\mathbf{e}_j \hookrightarrow \bigoplus_{i=1}^{\infty} \mathbb{R}\mathbf{e}_i, \qquad \iota_j \colon a_j\mathbf{e}_j \longmapsto a_j\mathbf{e}_j$$

The direct sum is the "*smallest S that each factor embeds into*."

Given any family $f_j \colon \mathbb{R}\mathbf{e}_j \to X$ of maps, each ι_j factors through the embedding $\iota_j \colon \mathbb{R}\mathbf{e}_j \hookrightarrow S$.

$$\begin{tikzcd}
& X & \\
\mathbb{R}\mathbf{e}_1 \arrow[ur, "f_1"] \arrow[r, hook, "\iota_1"'] & \mathbb{R}\mathbf{e}_1 \oplus \mathbb{R}\mathbf{e}_2 \oplus \cdots \arrow[u, dashed, "f"] & \mathbb{R}\mathbf{e}_2 \arrow[ul, "f_2"'] \arrow[l, hook', "\iota_2"]
\end{tikzcd}
\qquad
\begin{tikzcd}
& x_j & \\
a_1\mathbf{e}_1 \arrow[ur, mapsto, "f_1"] \arrow[r, mapsto, "\iota_1"'] & a_j\mathbf{e}_j \arrow[u, dashed, mapsto, "f"] & a_2\mathbf{e}_2 \arrow[ul, mapsto, "f_2"'] \arrow[l, mapsto, "\iota_2"]
\end{tikzcd}$$

Let's see why this fails if we try to use $\mathbb{R}^\infty$ for S:

$$\begin{tikzcd}
& \mathbb{R}\mathbf{e}_1 \oplus \mathbb{R}\mathbf{e}_2 \oplus \cdots & \\
\mathbb{R}\mathbf{e}_1 \arrow[ur, hook, "\iota_1"] \arrow[r, hook, "\iota_1"'] & \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots}_{\text{“\textit{too big}”}} \arrow[u, dashed, hook, "f"] & \mathbb{R}\mathbf{e}_2 \arrow[ul, hook', "\iota_2"'] \arrow[l, hook', "\iota_2"]
\end{tikzcd}
\qquad
\begin{tikzcd}
??? \\
(1, 1, \dots) \arrow[u, dashed, hook, "\nexists f"]
\end{tikzcd}$$

Returning to groups

Let $\{G_\alpha \mid \alpha \in A\}$ be a nonempty family of groups. We will define their product and co-product via a universal construction.

$$
\begin{tikzcd}
H \arrow[rr, "f_\alpha"] \arrow[dr, dashed, "g"'] \arrow[rr, phantom, shift right=4ex, "\text{``product''}"] & & G_\alpha \\
& P \arrow[ur, two heads, "\pi_\alpha"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
G_\alpha \arrow[rr, "f_\alpha"] \arrow[dr, hook, "\iota_\alpha"'] \arrow[rr, phantom, shift right=4ex, "\text{``co-product''}"] & & H \\
& S \arrow[ur, dashed, "h"'] &
\end{tikzcd}
$$

Remark

Existence of the map needed to make these diagrams commute does *not* imply uniqueness from the cancellation laws – each is the "wrong type" of diagram for that.

The fact that there are such groups that guarantee uniqueness indicates that the definitions are capturing something fundamentally important.

Definition

The **product** of $\{G_\alpha \mid \alpha \in A\}$ is a group P with a family of homomorphisms $\{\pi_\alpha \colon P \to G_\alpha \mid \alpha \in A\}$, satisfying:

> *Given any group H and homomorphisms $f_\alpha \colon H \to G_\alpha$, there is a unique homomorphism $g \colon H \to P$ such that $\pi_\alpha \circ g = f_\alpha$ for all $\alpha \in A$.*

Products: surjectivity and uniqueness

Proposition

If $\{G_\alpha \mid \alpha \in A\}$ has a product, it is unique up to isomorphism, and each π_α is surjective.

Proof

We've shown uniqueness.

To show that π_α is surjective, consider $\pi_\beta \colon P \to G_\beta$, and take $H = G_\alpha$.

Define f_β to be the identity map if $\beta = \alpha$ and the trivial map otherwise. That is,

$$f_\alpha \colon G_\alpha \longrightarrow G_\beta, \qquad f_\alpha(x) = \begin{cases} x, & \alpha = \beta \\ 1, & \alpha \neq \beta. \end{cases}$$

Every element $x \in G_\beta$ has a π_β-preimage, $g(x) \in P$.

$$\begin{tikzcd} G_\alpha \arrow[rr, "f_\alpha\ \text{(trivial)}"] \arrow[dr, dashed, "g"'] & \arrow[d, phantom, "\alpha \neq \beta"] & G_\beta \\ & P \arrow[ur, "\pi_\beta"'] & \end{tikzcd}
\qquad
\begin{tikzcd} G_\alpha \arrow[rr, "f_\alpha = \mathrm{Id}_\beta"] \arrow[dr, dashed, "g"'] & \arrow[d, phantom, "\alpha = \beta"] & G_\beta \\ & P \arrow[ur, "\pi_\beta"'] & \end{tikzcd}
\qquad
\begin{tikzcd} x \arrow[rr, mapsto, "f_\alpha = \mathrm{Id}_\beta"] \arrow[dr, dashed, mapsto, "g"'] & \arrow[d, phantom, "\alpha = \beta"] & x \\ & g(x) \arrow[ur, mapsto, "\pi_\beta"'] & \end{tikzcd}$$

Products: existness

Proposition

The product of $\{G_\alpha \mid \alpha \in A\}$ is the Cartesian product, $P = \prod_{\alpha \in A} G_\alpha$.

Proof

Define the canonical projection maps as

$$\pi_\beta \colon P \longrightarrow G_\beta, \qquad \pi_\beta \colon (x_\alpha)_{\alpha \in A} \longmapsto x_\beta.$$

Suppose we have another family of maps $f_\alpha \colon H \to G_\alpha$, for each $\alpha \in A$.

Goal. Show $\exists! g \colon H \to P$ such that $f_\alpha = \pi_\alpha \circ g$ for all $\alpha \in A$.

$$\begin{tikzcd}
H \arrow[rr, "f_\beta"] \arrow[dr, dashed, "g"'] & & G_\beta \\
& \prod_{\alpha \in A} G_\alpha \arrow[ur, "\pi_\beta"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
x \arrow[rr, mapsto, "f_\beta"] \arrow[dr, mapsto, dashed, "g"'] & & f_\beta(x) \\
& (f_\alpha(x))_{\alpha \in A} \arrow[ur, mapsto, "\pi_\beta"'] &
\end{tikzcd}$$

Uniqueness. Suppose $\exists h \colon H \to P$ for which $f_\alpha = \pi_\alpha \circ h$ for all $\alpha \in A$.

This means $\pi_\alpha \circ g = \pi_\alpha \circ h$. Take $x \in H$, note that

$$h(x)_\beta = \pi_\beta\big(h(x)\big) = f_\beta(x) = \pi_\beta\big(g(x)\big) = g(x)_\beta. \qquad \square$$

Co-products

Definition

The **co-product** of $\{G_\alpha \mid \alpha \in A\}$ is a group S with a family of homomorphisms $\{\iota_\alpha \colon G_\alpha \to S \mid \alpha \in A\}$, satisfying:

> *Given any group H and homomorphisms $f_\alpha \colon G_\alpha \to H$, there is a unique homomorphism $h \colon S \to H$ such that $h \circ \iota_\alpha = f_\alpha$ for all $\alpha \in A$.*

$$\begin{tikzcd} G_\alpha \arrow[rr, "f_\alpha"] \arrow[dr, "\iota_\alpha"'] & & H \\ & S \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

Exercise (HW)

If $\{G_\alpha \mid \alpha \in A\}$ has a co-product, it is unique up to isomorphism, and each ι_α is injective.

Showing existence of a co-product is trickier – it a construction that we have not yet seen.

The product of C_2 and C_2 has order 4. The co-product is infinite.

Categories

Some constructions we've recently seen have analogues for other mathematical objects.

We can define the product and coproduct of sets, topological spaces, rings, vector spaces, etc.

Many structural results carry over, so we'd like to generalize these in a common framework.

The mathematical field that addresses these questions is called **category theory**.

Definition

A **category** $\mathcal{C}$ consists of

- a class $\mathrm{Ob}(\mathcal{C})$ of **objects**,
- a class $\mathrm{Hom}(\mathcal{C})$ of **morphisms** between objects, with identities, closure, and associativity.

- Examples of "objects" include sets, groups, rings, vector spaces, topological spaces, etc.,
- "Morphisms" are meant to be "structure-preserving maps."

Categories

Think of the category $\mathcal{C} = \textbf{Grp}$ of groups as a massive directed multigraph, where

- each node represents a group
- there is a directed edge from A to B for each homomorphism $f\colon A \to B$.

We require: identity, composition, and associativity.

$$\begin{tikzcd} A \arrow[loop above, "\mathrm{Id}_A"] \arrow[r, bend left, "f"] & B \arrow[loop above, "\mathrm{Id}_B"] \arrow[l, bend left, "g"] \end{tikzcd} \qquad \begin{tikzcd} A \arrow[loop above, "\mathrm{Id}_A"] \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[loop above, "\mathrm{Id}_A"] \arrow[r, "g"] & C \arrow[loop above, "\mathrm{Id}_C"] \end{tikzcd}$$

Denote the morphisms from A to B by $\mathrm{Hom}_{\mathcal{C}}(A, B)$.

(i) Every group has an **identity morphism**: for every $A \in \mathrm{Ob}(\mathcal{C})$, there is $\mathrm{Id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ satisfying

$$f \circ \mathrm{Id}_A = f, \ \text{ for all } f \in \mathrm{Hom}_{\mathcal{C}}(A, B), \qquad \mathrm{Id}_A \circ g = g, \ \text{ for all } h \in \mathrm{Hom}_{\mathcal{C}}(B, A).$$

(ii) Morphisms are **closed under composition**:

$$\text{If } f \in \mathrm{Hom}_{\mathcal{C}}(A, B) \ \text{ and } \ g \in \mathrm{Hom}_{\mathcal{C}}(B, C), \ \text{ then } \ g \circ f \in \mathrm{Hom}_{\mathcal{C}}(A, C).$$

(iii) Composition of morphisms is **associative**:

$$\text{If } f \in \mathrm{Hom}_{\mathcal{C}}(A, B), \ g \in \mathrm{Hom}_{\mathcal{C}}(B, C), \ h \in \mathrm{Hom}_{\mathcal{C}}(C, D), \ \text{ then } h \circ (g \circ f) = (h \circ g) \circ f.$$

Abstracting the notion of "one-to-one" and "onto"

Definition

Let $f, f_1, f_2 \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $g, g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, C)$. Then

1. g is a **monomorphism** if $g \circ f_1 = g \circ f_2$ implies $f_1 = f_2$.
2. f is an **epimorphism** if $g_1 \circ f = g_2 \circ f$ implies $g_1 = g_2$,

Sometimes, we'll say "*mono*" and "*epi*" (noun) or "*epic*" (adjective).

A morphism $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an **isomorphism** if it has a two-sided inverse.

That is, if $\exists g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$.

We say A and B are **equivalent**.

$$\begin{tikzcd} A \arrow[r, shift left, "f_1"] \arrow[r, shift right, "f_2"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

"monomorphism" (one-to-one)

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & C \end{tikzcd}$$

"epimorphism" (onto)

$$\begin{tikzcd} A \arrow[loop above, "\mathrm{Id}_A = g \circ f"] \arrow[r, bend left, "f"] & B \arrow[loop above, "\mathrm{Id}_B = f \circ g"] \arrow[l, bend left, "g"] \end{tikzcd}$$

"equivalent" (isomorphic)

Abstracting the notion of "product" and "coproduct"

Definition

Consider a category $\mathcal{C}$ and a non-empty collection $\{B_i \mid i \in I\}$ of objects.

A **product** for $\{B_i\}$ is $P \in \mathrm{Ob}(\mathcal{C})$ with a family $\{\pi_i \in \mathrm{Hom}(P, B_i) \mid i \in I\}$ such that:

> *Given any $A \in \mathrm{Ob}(\mathcal{C})$ and $\left\{f_i \in \mathrm{Hom}_{\mathcal{C}}(A, B_i) \mid i \in I\right\}$, there is a unique $g \in \mathrm{Hom}_{\mathcal{C}}(A, P)$ such that $\pi_i \circ g = f_i$ for all $i \in I$.*

A **coproduct** for $\{B_i\}$ is $S \in \mathrm{Ob}(\mathcal{C})$ with $\{\iota_i \in \mathrm{Hom}(A_i, S) \mid i \in I\}$ such that:

> *Given any $B \in \mathrm{Ob}(\mathcal{C})$ and family $\left\{f_i \in \mathrm{Hom}_{\mathcal{C}}(A_i, B) \mid i \in I\right\}$, there is a unique $h \in \mathrm{Hom}_{\mathcal{C}}(S, B)$ such that $h \circ \iota_i = f_i$ for all $i \in I$.*

$$
\begin{tikzcd}
A \arrow[rr, "f_i"] \arrow[dr, dashed, "g"'] & \text{``product''} & B_i \\
& P \arrow[ur, "\pi_i"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
A_i \arrow[rr, "f_i"] \arrow[dr, hook, "\iota_i"'] & \text{``co-product''} & B \\
& S \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\tag{2}
$$

It can be shown that the π_i's are epimorphisms, and ι_i's are monomorphisms.

A few counterintuitive facts

- *Isomorphisms need not be bijective!* In the category **Rng**, the non-surjective morphism

$$g \colon \mathbb{Z} \longrightarrow \mathbb{Q}, \qquad g(n) = n$$

is both mono and an epic.

$$\begin{tikzcd} R \arrow[r, shift left, "g_1"] \arrow[r, shift right, "g_2"'] & \mathbb{Z} \arrow[r, "f"] & \mathbb{Q} \end{tikzcd} \qquad\qquad \begin{tikzcd} \mathbb{Z} \arrow[r, "g"] & \mathbb{Q} \arrow[r, shift left, "h_1"] \arrow[r, shift right, "h_2"'] & \mathbb{R} \end{tikzcd}$$

The equality $f \circ g_1 = f \circ g_2$, implies $g_1 = g_2$, and $h_1 \circ g = h_2 \circ g$, forces $h_1 = h_2$.

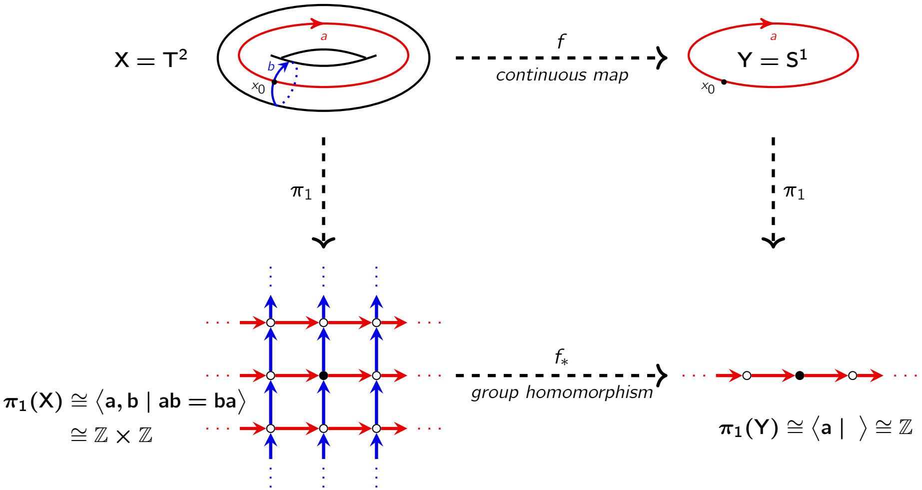
However, g is not an isomorphism because it does not have a left or a right inverse.

- *The same concept across different categories can seem very different!*

Category	Objects	Morphisms	Product	coproduct
Set	sets	functions	Cartesian product	disjoint union
Grp	groups	homomorphisms	direct product	free product
Ab	abelian groups	homomorphisms	direct product	direct sum
Ring	rings w/ 1	ring homomorphisms	direct product	free product
Field	fields	field embeddings	none	none
$\mathbf{Vect}_{\mathbb{F}}$	$\mathbb{F}$-vector spaces	linear functions	direct product	direct sum
Top	topological spaces	continuous maps	product topology	disjoint union

A functor from **Top** to **Grp**

Sometimes, there are structure-preserving maps between categories.



This is an example of a **functor**.

A functor from **Top** to **Grp**

The fundamental group of X is the group $\pi_1(X)$ of all "loops up to equivalence."

A continuous map $f\colon X \to Y$ induces a homomorphism

$$f_*\colon \pi_1(T^2) \longrightarrow \pi_1(S^1), \qquad f_*\colon (a,b) \longmapsto a.$$

Formally, π_1 is a functor from $\mathbf{Top}_\bullet$ to $\mathbf{Grp}$, defined as:

$$\pi_1\colon\ \mathrm{Ob}(\mathbf{Top}_\bullet) \longrightarrow \mathrm{Ob}(\mathbf{Grp}) \qquad\qquad \mathcal{F}\colon\ \mathrm{Hom}(\mathbf{Top}_\bullet) \longrightarrow \mathrm{Hom}(\mathbf{Grp})$$

$$X \longmapsto \pi_1(X) \qquad\qquad X \xrightarrow{f} Y \quad\longmapsto\quad \pi_1(X) \xrightarrow{f_*} \pi_1(Y)$$

For arbitrary (pointed) topological spaces (X, x_0) and (Y, y_0):

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi_1"'] & Y \arrow[d, "\pi_1"] \\ \pi_1(X) \arrow[r, "f_*"] & \pi_1(Y) \end{tikzcd}$$

f is a contin. b/w topological spaces, with $f(x_0) = y_0$

f_* is a homomorphism b/w fundamental groups

Covariant and contravariant functors

Definition

A (**covariant**) **functor** $\mathcal{F}$ from $\mathcal{C}$ to $\mathcal{D}$ is a function that sends

- objects A of $\mathcal{C}$ to objects $\mathcal{F}(A)$ of $\mathcal{D}$,
- morphisms $f\colon A \to B$ in $\mathcal{C}$ to morphisms $\mathcal{F}(f)\colon \mathcal{F}(A) \to \mathcal{F}(B)$ in D satisfying:
  - $\mathcal{F}(\mathrm{Id}_A) = \mathrm{Id}_{\mathcal{F}(A)}$ for all $A \in \mathrm{Ob}(\mathcal{C})$
  - $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$ for all morphisms $f\colon A \to B$ and $g\colon B \to C$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd} \qquad \begin{tikzcd} \mathcal{F}(A) \arrow[r, "\mathcal{F}(f)"] \arrow[rr, bend right, "\mathcal{F}(g) \circ \mathcal{F}(f)"'] & \mathcal{F}(B) \arrow[r, "\mathcal{F}(g)"] & \mathcal{F}(C) \end{tikzcd}$$

There is a "dual" type of functor, called **contravariant**, that reverses the arrows.

That is, they send $A \xrightarrow{f} B$ to $\mathcal{F}(B) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(A)$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd} \qquad \begin{tikzcd} \mathcal{F}(A) & \mathcal{F}(B) \arrow[l, "\mathcal{F}(f)"'] & \mathcal{F}(C) \arrow[l, "\mathcal{F}(g)"'] \arrow[ll, bend left, "\mathcal{F}(g) \circ \mathcal{F}(f)"] \end{tikzcd}$$

A contravariant function from linear algebra

Let $V \in \mathrm{Ob}(\mathbf{Vect}_{\mathbb{R}})$ be an n-dimensional vector space.

The **dual space** $V^* \in \mathrm{Ob}(\mathbf{Vect}_{\mathbb{R}})$ consists of all *linear scalar functions* $\ell \colon V \to \mathbb{R}$.

Think of:

- elements in V as columns vectors,
- elements in V^* as row vectors.

$$\ell \colon V \longrightarrow \mathbb{R}, \qquad \ell(v) = \underbrace{\begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}}_{\ell \in V^*} \underbrace{\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}}_{v \in V} = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.$$

A linear map $A \colon V \to W$ can be represented by an $m \times n$ matrix, where $\mathbf{dim}(W) = m$.

Think of this as *left-multiplication by column vectors*, $Av = w$:

$$A \colon V \longrightarrow W, \qquad \underbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}}_{A \in \mathbf{Hom}(V,W)} \underbrace{\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}}_{v \in V} = \underbrace{\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix}}_{w \in W}.$$

A contravariant function from linear algebra

The *transpose* is a linear map $A^t \colon W^* \to V^*$.

Think of this as *right-multiplication by row vectors*, $w^t A^t = v^t$:

$$A^t \colon W^* \longrightarrow V^*, \qquad \underbrace{\begin{bmatrix} w_1 & w_2 & \cdots & w_m \end{bmatrix}}_{w^t \in W^*} \underbrace{\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \cdots & a_{nm} \end{bmatrix}}_{A^t \in \mathrm{Hom}(W^*, V^*)} = \underbrace{\begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix}}_{v^t \in V^*}$$

Formally, we have a contravariant functor:

$$\mathcal{F} \colon \mathrm{Ob}(\mathbf{Vect}_{\mathbb{F}}) \longrightarrow \mathrm{Ob}(\mathbf{Vect}_{\mathbb{F}}) \qquad \mathcal{F} \colon \mathrm{Hom}(\mathbf{Vect}_{\mathbb{F}}) \longrightarrow \mathrm{Hom}(\mathbf{Vect}_{\mathbb{F}})$$

$$V \longmapsto V^* \qquad\qquad v \overset{A}{\mapsto} w \quad \longmapsto \quad w^t \overset{A^*}{\mapsto} v^t$$

Notice how the arrow on the bottom of the following commutative diagram is reversed; this is contravariance.

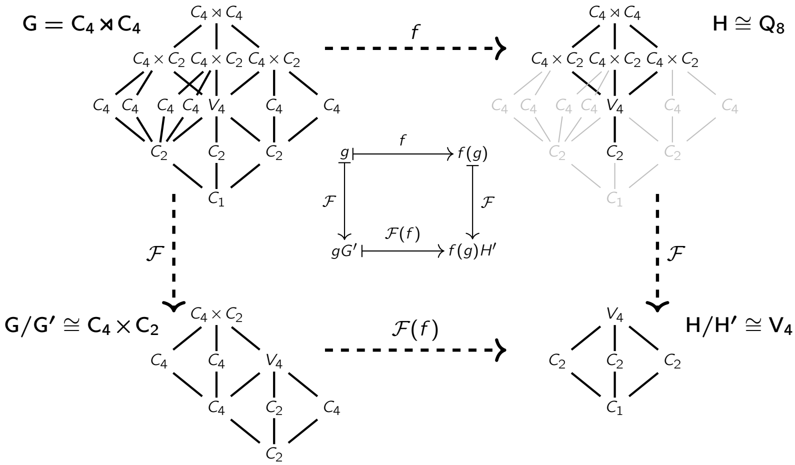
$$\begin{tikzcd} V \arrow[r, "A"] \arrow[d, "\mathcal{F}"'] & W \arrow[d, "\mathcal{F}"] \\ V^* & W^* \arrow[l, "A^*"'] \end{tikzcd} \qquad \begin{array}{l} A \in \mathrm{Hom}(V, W) \\ \\ A^* \in \mathrm{Hom}(W^*, V^*) \end{array}$$

Abelianization, as a functor from **Grp** to **Ab**

Consider the functor sending a group G to its abelianization $A \cong G/G' = G/[G,G]$:

$$\mathcal{F}\colon\ \mathrm{Ob}(\mathbf{Grp}) \longrightarrow \mathrm{Ob}(\mathbf{Ab}) \qquad\qquad \mathcal{F}\colon\ \mathrm{Hom}(\mathbf{Grp}) \longrightarrow \mathrm{Hom}(\mathbf{Ab})$$

$$G \longmapsto G/G' \qquad\qquad g \mapsto f(g) \quad \longmapsto \quad gG' \mapsto f(g)H'$$



Initial and terminal objects

Definition

An object $I \in \mathrm{Ob}(\mathcal{C})$ is **initial** if for each $C_i \in \mathrm{Ob}(\mathcal{C})$, there is a unique $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(I, C_i)$.

An object $T \in \mathrm{Ob}(\mathcal{C})$ is **terminal** if for each $C_i \in \mathrm{Ob}(\mathcal{C})$, there is a unique $\iota_i \in \mathrm{Hom}_{\mathcal{C}}(C_i, T)$.

An object that is initial and terminal is called a **zero object**.

Sometimes, initial objects are called *universal* or *coterminal*, and terminal objects are *final* or *couniversal*.

Category	Objects	Initial objects	Terminal objects	Zero objects
Set	sets	$\emptyset$	every $\{x\}$	none
Grp	groups	$\langle e\rangle$	$\langle e\rangle$	$\langle e\rangle$
Ab	abelian groups	$\langle 0\rangle$	$\langle 0\rangle$	$\langle 0\rangle$
Rng	rings	$\{0\}$	$\{0\}$	$\{0\}$
Ring	rings w/ 1	$\mathbb{Z}$	$\{0\}$	none
Field	fields	none	none	none
Field$_p$	fields w/ char. $p > 0$	$\mathbb{Z}_p$	none	none
Vect$_{\mathbb{F}}$	$\mathbb{F}$-vector spaces	$\{0\}$	$\{0\}$	$\{0\}$
Top	topological spaces	$\emptyset$	every $\{x\}$	none

Initial and terminal objects

Proposition

Any two initial objects in a category $\mathcal{C}$ are equivalent.

Proof

Let I and J be initial.

Since I is initial, there is a unique morphism $f \in \mathbf{Hom}_{\mathcal{C}}(I, J)$.

Since J is initial, there is a unique morphism $g \in \mathbf{Hom}_{\mathcal{C}}(J, I)$.

The morphism $g \circ f$ is in $\mathbf{Hom}_{\mathcal{C}}(I, I)$, as is $\mathbf{Id}_I$ (below, left).

$$\begin{tikzcd} I \arrow[r, bend left, "g \circ f"] \arrow[r, bend right, "\mathbf{Id}_I"'] & I \end{tikzcd} \qquad \begin{tikzcd} J \arrow[r, bend left, "f \circ g"] \arrow[r, bend right, "\mathbf{Id}_J"'] & J \end{tikzcd}$$

However, since I is initial, there must be a unique morphism in $\mathbf{Hom}_{\mathcal{C}}(I, I)$, so $g \circ f = \mathbf{Id}_I$.

Similarly, $f \circ g$ and $\mathbf{Id}_J$ are both in $\mathbf{Hom}_{\mathcal{C}}(J, J)$ (above, right).

By uniqueness, $f \circ g = \mathbf{Id}_J$, hence $I \cong J$. $\square$

Uniquess of products

Suppose $\{B_i \mid i \in I\}$ in $\mathcal{C}$ has product P, with projections $\pi_i \colon P \to B_i$.

Define a new category $\mathcal{B}$:

- objects: families of maps $\{A \xrightarrow{f_i} B_i\}$
- morphisms: $A \xrightarrow{g} C$ that makes the following diagram commute.

$$g \in \mathbf{Hom}_{\mathcal{B}}\left((A \xrightarrow{f_i} B_i,\ C \xrightarrow{h_i} B_i\right)$$

$$\begin{tikzcd} A \arrow[rr, "f_i"] \arrow[dr, dashed, "g"'] & & B_i \\ & C \arrow[ur, "h_i"'] & \end{tikzcd}$$

A terminal object in $\mathcal{B}$ is a family $\{P \xrightarrow{\pi_i} B_i\}$ such that for any $\{A \xrightarrow{f_i} B_i\}$, there exists a unique $g \in \mathbf{Hom}_{\mathcal{C}}(A, P)$ that makes the diagram (left) commute:

$$\begin{tikzcd} A \arrow[rr, "f_i"] \arrow[dr, dashed, "\exists! g"'] & & B_i \\ & P \arrow[ur, "\pi_i"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[rr, "f_i"] \arrow[dr, dashed, "\exists! g"'] & & B_i \\ & \prod_{i \in I} B_i \arrow[ur, "\pi_i"'] & \end{tikzcd}$$

That is, the terminal object is the product! Thus, products are unique up to equivalence.

Uniquess of coproducts and zero morphisms

We can construct an analogus category where the initial object is the coproduct.

$$\begin{tikzcd} A_i \arrow[rr, "f_i"] \arrow[dr, "g_i"'] \arrow[rr, phantom, shift right=3ex, "\text{``\emph{initial}''}"] & & B \\ & S \arrow[ur, dashed, "\exists! h"'] & \end{tikzcd} \qquad \begin{tikzcd} A \arrow[rr, "f_i"] \arrow[dr, dashed, "\exists! g"'] \arrow[rr, phantom, shift right=3ex, "\text{``\emph{terminal}''}"] & & B_i \\ & P \arrow[ur, "h_i"'] & \end{tikzcd}$$

$$h \in \mathbf{Hom}_{\mathcal{A}}\left(A_i \xrightarrow{g_i} S, A_i \xrightarrow{f_i} B\right) \qquad g \in \mathbf{Hom}_{\mathcal{B}}\left(A \xrightarrow{f_i} B_i, P \xrightarrow{h_i} B_i\right)$$

Though each $\pi_i \in \mathbf{Hom}_{\mathcal{C}}(P, B_i)$ need not be epic, there are conditions that guarantee this.

Definition

Let $\mathcal{C}$ be a category with a zero object, $\mathbf{0} \in \mathrm{Ob}(\mathcal{C})$. The **zero morphism** $0_{AB} \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is the composition of the unique maps $A \to \mathbf{0} \to B$.

$$\begin{tikzcd} A \arrow[r, "0_{AB}"] \arrow[d, "f"'] \arrow[dr, "0_{AC}"] & B \arrow[d, "g"] \\ B \arrow[r, "0_{B\mathbf{0}}"] & C \end{tikzcd}$$

Zero morphisms

Proposition

If $\mathbf{0} \in \mathrm{Ob}(\mathcal{C})$, the projection morphisms $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(P, B_i)$ of a product are epimorphisms.

Proof

Fix $\alpha \in I$, and define the family of maps $\left\{f_i \in \mathrm{Hom}_{\mathcal{C}}(B_\alpha, B_i) \mid i \in I\right\}$ as

$$f_i \colon B_\alpha \longrightarrow B_i, \qquad f_i = \begin{cases} \mathrm{Id}_{B_\alpha}, & i = \alpha \\ 0_{B_i\mathbf{0}}, & i \neq \alpha. \end{cases}$$

By the universal property of products, for each $i \in I$, we have:

$$\begin{tikzcd} B_\alpha \arrow[rr, "f_i = \mathrm{Id}_{B_\alpha}"] \arrow[dr, dashed, "\exists! g_i = g_\alpha"'] \arrow[rr, phantom, shift right=6ex, "i=\alpha"] & & B_i \\ & P \arrow[ur, "\pi_i = \pi_\alpha"'] & \end{tikzcd} \qquad \begin{tikzcd} B_\alpha \arrow[rr, "f_i = 0_{B_i\mathbf{0}}"] \arrow[dr, dashed, "\exists! g_i"'] \arrow[rr, phantom, shift right=6ex, "i\neq\alpha"] & & B_i \\ & P \arrow[ur, "\pi_i"'] & \end{tikzcd}$$

To show π_α is epic, we need to verify left-cancelization.

Consider $f, g \in \mathrm{Hom}_{\mathcal{C}}(B_\alpha, C)$ such that $f \circ \pi_\alpha = g \circ \pi_\alpha$.

Zero morphisms

Proposition

If $\mathbf{0} \in \mathrm{Ob}(\mathcal{C})$, the projections $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(P, B_i)$ from a product are epimorphisms.

Proof

It suffices to show that $f = g$.

$$\begin{tikzcd}
B_\alpha \arrow[rr, "f_\alpha = \mathrm{Id}_{B_\alpha}"] \arrow[dr, dashed, "g_\alpha"'] & & B_\alpha \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & C \\
& P \arrow[ur, "\pi_\alpha"'] & &
\end{tikzcd}$$

By the commuativity of the diagram, we have

$$f = f \circ \mathrm{Id}_{B_\alpha} = f \circ (\pi_\alpha \circ g_\alpha) = (f \circ \pi_\alpha) \circ g_\alpha = (g \circ \pi_\alpha) \circ g_\alpha = g \circ (\pi_\alpha \circ g_\alpha) = g \circ \mathrm{Id}_{B_\alpha} = g,$$

whence π_α is an epimorphism. $\square$

Proposition (HW)

If $\mathbf{0} \in \mathrm{Ob}(\mathcal{C})$, the inclusions $\iota_i \in \mathrm{Hom}_{\mathcal{C}}(B_i, S)$ into a coproduct are monomorphisms.

Free groups

Throughtout, let S be a nonempty set.

Definition

The **free group on S** is

$$F = F_S := \langle S \mid \ \rangle.$$

That is, F_S is generated by S, subject to no relations.

We can think of the free groups as groups where:

- elements are words in $T = S \sqcup S^{-1}$, where $S^{-1} := \{s^{-1} \mid s \in S\}$.
- the binary operation is concatenation.

The only way to modify words are by substitutions of form $ss^{-1} = 1$ and $s^{-1}s = 1$.

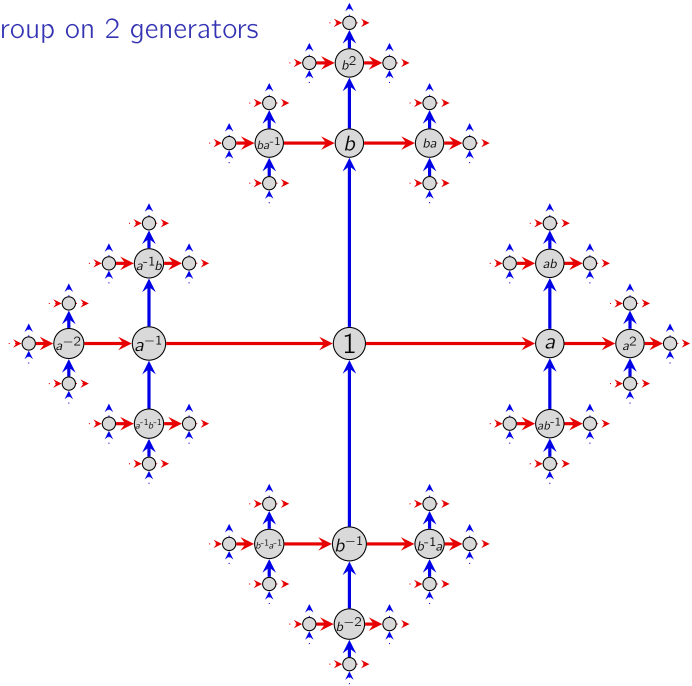
If $|S| = |T|$, then $F_S \cong F_T$.

If $|S| = n < \infty$, then $F_n := F_S$ is *free group on n generators*, or the *free group of rank n*.

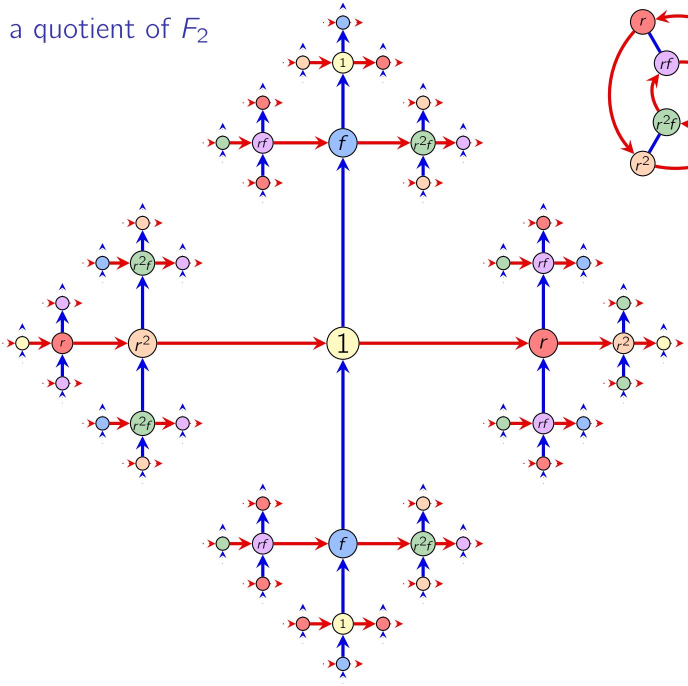
We'll soon see how every group is a quotient of a free group.

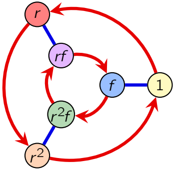
This can be formalized via a couniversal property.

The free group on 2 generators



D_3 as a quotient of F_2





Free groups

Definition

A group F is **free** on $S \neq \emptyset$ if there is a function $\iota\colon S \to F$ such that for any other $\theta\colon S \to G$, there exists a unique homomorphism $\pi\colon F \to G$ such that $\theta = \pi \circ \iota$.

$$\begin{tikzcd} S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & & G \\ & F \arrow[ur, dashed, "\pi"'] & \end{tikzcd}$$

Proposition

If a free group exists on $S \neq \emptyset$, it is unique up to isomorphism, and $\iota\colon S \to F$ is injective.

Proof

We've seen uniqueness. Suppose ι is not 1-to-1; take $a \neq b$ in S for which $\iota(a) = \iota(b)$.

Consider the map $\theta\colon S \longrightarrow \mathbb{Z}$, $\qquad \theta(s) = \begin{cases} 1 & s = a \\ 2 & s = b \\ 0 & s \notin \{a, b\}. \end{cases}$

This forces $1 = \theta(a) = \pi(\iota(a)) = \pi(\iota(b)) = \theta(b) = 2$, a contradiction. $\square$

Free semigroups

Definition

A **semigroup** is a set $X \neq \emptyset$ with associative binary operation.

A **homomorphism** is a function $f\colon X \to Y$ with $f(x_1x_2) = f(x_1)f(x_2)$ for all $x_1, x_2 \in X$.

Let **Sgp** denote the category of semigroups.

Free semigroups exists, are unique up to isomorphism, the map $\iota\colon S \to F$ is injective.

$$\begin{tikzcd}
S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & & Y \\
& X \arrow[ur, dashed, "\pi"'] &
\end{tikzcd}$$

The free semigroup on $S = \{s\}$ is isomorphic to $\mathbb{N} = \{1, 2, \ldots, \}$ under addition.

Free semigroups

Proposition

If $S \neq \emptyset$, then there is a free semigroup over S.

Proof

Let X be the set of nonempty words over S, under concatenation:

$$X = S \cup (S \times S) \cup (S \times S \times S) \cup \cdots, \qquad (a_1, \dots, a_n) * (b_1, \dots, b_m) = (a_1, \dots, a_n, b_1, \dots, b_m).$$

We'll show this is free over S, with inclusion map

$$\iota \colon S \longrightarrow X, \qquad \iota(x) = x.$$

Given a function $\theta \colon S \to Y$ to another semigroup, define

$$\pi \colon X \longrightarrow Y, \qquad \pi \colon (a_1, \dots, a_n) \longmapsto \theta(a_1) \cdots \theta(a_n).$$

Exercise. Check that π is a semigroup homomorphism, and $\pi \circ \iota = \theta$.

$$\begin{tikzcd} S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & & Y \\ & X \arrow[ur, dashed, "\pi"'] & \end{tikzcd}$$

Free semigroups

Proposition

If $S \neq \emptyset$, then there is a free semigroup over S.

Proof (contin.)

Given $\theta\colon S \to Y$, the function

$$\pi\colon X \longrightarrow Y, \qquad \pi\colon (a_1, \dots, a_n) \longmapsto \theta(a_1)\cdots\theta(a_n).$$

satisfyies $\pi \circ \iota = \theta$.

Uniqueness: Suppose $\sigma\colon X \to Y$ also satisfies $\sigma \circ \iota = \theta$. Then

$$\begin{aligned}
\sigma\big((a_1, \dots, a_n)\big) &= \sigma\big(\iota(a_1)\cdots\iota(a_n)\big) \\
&= \sigma(\iota(a_1))\cdots\sigma(\iota(a_n)) \\
&= \theta(a_1)\cdots\theta(a_n) \\
&= \pi(\iota(a_1))\cdots\pi(\iota(a_n)) \\
&= \pi\big(\iota(a_1)\cdots\iota(a_n)\big) \\
&= \pi\big((a_1, \dots, a_n)\big).
\end{aligned}$$

$$\begin{tikzcd}
S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & & G \\
& F \arrow[ur, dashed, "\pi"'] &
\end{tikzcd}$$

Therefore, X satisfies the co-universal property of free semigroups. $\square$

Quotient semigroups

Since semigroups lack an inverse, we don't have kernels, or isomorphism theorems.

But there is a co-universal property of quotient maps.

The group homomorphism $f\colon G \to K$ partitions G into cosets of $\mathrm{Ker}(f)$.

If this is coarser than the parition of G into cosets of $N = \mathrm{Ker}(\pi)$, then f factors through π:

$$\begin{tikzcd} G \arrow[rr, two heads, "f"] \arrow[dr, two heads, "\pi"'] & & K \\ & G/N \arrow[ur, dashed, two heads, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & f(x) \\ & xN \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

A relation R on a semigroup Y is **well-defined** with respect to $*$ if

$$xRy \quad \text{and} \quad zRw \quad \Longrightarrow \quad xzRyw.$$

Let xR be the equivalence class containing x, and call

$$\pi\colon Y \longrightarrow Y/R, \qquad \pi\colon y \longmapsto yR$$

the **canonical quotient map**.

The **quotient semigroup** of Y is Y/R, with $xR \cdot yR := xyR$.

Co-universal property of quotient semigroups

Proposition

The quotient semigroup Y/R satisfies the following co-universal property:

> *If $f\colon Y \to Z$ is a semigroup homomorphism such that xRy implies $f(x) = f(y)$, then $\exists! h\colon Y/R \to Z$ such that $f = h \circ \pi$.*

$$\begin{tikzcd}
Y \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Z \\
& Y/R \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
y \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & z \\
& yR \arrow[ur, dashed, mapsto, "h"'] &
\end{tikzcd}$$

Proof

Existence follows from the definition: $h(yR) = h(\pi(y)) = f(y)$, with well-definedness automatic from $xRy \;\Rightarrow\; f(x) = f(y)$.

Uniqueness by the cancellation laws, because π is surjective. $\square$

Construction of a free group over S

Given $S \neq \emptyset$, construct a disjoint set S' of "formal inverses":

$$S' = \{s' \mid s \in S\}, \qquad T = S \cup S'.$$

The bijection $s \mapsto s'$ and inverse $s' \mapsto s'' := s$ define a bijection $T \to T$, where $t \mapsto t'$.

Let X be the free semigroup on $T \subseteq X$ (under natural inclusion).

Call a homomorphism $\phi \colon X \to G$ **proper** if $\phi(s') = \phi(s)^{-1}$ for all $s \in S$.

If ϕ is proper, then $\phi(t') = \phi(t)^{-1}$ for all $t \in T$.

The only "relation" in a free group group: $ss^{-1} = s^{-1}s = 1$ for all $s \in S \subseteq F$.

We'll construct the this from the free semigroup by forcing $ss't = t$, for all $t \in T \subseteq X$.

If ϕ is proper, then

$$\phi(ss't) = \phi(s)\phi(s')\phi(t) = \phi(s)\phi(s)^{-1}\phi(t) = \phi(t).$$

Define an equivalence relation on X where $xx'yRy$ for all $x, y \in X$, where

$$xRy \quad \text{iff} \quad \phi(x) = \phi(y) \text{ for every proper } \phi \colon X \to G.$$

Exercise: this is well-defined, and so X/R is a group.

Construction of a free group over S

We just showed that that X/R is a semigroup. Now'll we'll show it's a group.

We'll write $\bar{x}$ (not xR), so $\bar{x}\bar{y} = \overline{xy}$, and $\overline{x'} = \bar{x}^{-1}$.

Let $\pi \colon X \twoheadrightarrow X/R$ be the canonical quotient.

Identity. Choose any $s \in S$ and $x \in X$; we claim that $\overline{ss'} = 1$.

If $\phi \colon X \to G$ is proper, then $\phi(ss'x) = \phi(x)$, which means that $xRss'x$ in X, thus

$$\bar{x} = \overline{ss'x} = \overline{ss'} \cdot \overline{x}, \qquad \text{and} \qquad \bar{x} = \overline{xss'} = \overline{x} \cdot \overline{ss'}.$$

Thus, $\overline{ss'}$ is the identity. ✓

Inverses. Let $x = t_1 \cdots t_k \in X$.

We'll show that the inverse of $\bar{x}$ is $\bar{y}$, where $y = t_k' \cdots t_1'$.

If ϕ is proper, then

$$\begin{aligned} \phi(xy) &= \phi(t_1 \cdots t_k t_k' \cdots t_1') \\ &= \phi(t_1) \cdots \phi(t_k)\phi(t_k') \cdots \phi(t_1') \\ &= \phi(t_1) \cdots \phi(t_k)\phi(t_k)^{-1} \cdots \phi(t_1)^{-1} \\ &= 1_G = \phi(ss') \qquad \text{for any } s \in S. \end{aligned}$$ ✓

Thus X/R is a group. □

Showing that our free semigroup quotient X/R is free

Goal

Given $\iota\colon S \to X/R$ defined by $\iota(s) = \bar{s}$, show that for any map $\phi\colon S \to G$, there is a unique homomorphism $h\colon X/R \to G$ such that $\phi = h \circ \iota$

$$\begin{tikzcd}
S \arrow[rr, "\phi"] \arrow[dr, hook, "\iota"'] & & G \\
& X/R \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
s \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, "\iota"'] & & \phi(s) \\
& \bar{s} \arrow[ur, dashed, mapsto, "h"'] &
\end{tikzcd}$$

We'll build up this diagram in "pieces", culminating with the following:

$$\begin{tikzcd}
S \arrow[rrrr, "\phi"] \arrow[dr, hook, "i"] \arrow[dddrr, bend right, "\iota"'] & & & & G \\
& T \arrow[urrr, "\theta"] \arrow[dr, hook, "j"] & & & \\
& & X \arrow[uurr, "f"] \arrow[dr, two heads, "\pi"] & & \\
& & & X/R \arrow[uuur, dashed, "h"'] &
\end{tikzcd}$$

Showing that our free semigroup quotient X/R is free

Extend $\phi\colon S \to G$ to a map $\theta\colon T \longrightarrow G$ by setting $\theta(s') = \phi(s)^{-1}$.

$$\begin{tikzcd}
S \arrow[rr, "\phi"] \arrow[dr, hook, "i"'] & & G \\
& T \arrow[ur, dashed, "\theta"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
s \arrow[rr, mapsto, "\phi"] \arrow[dr, mapsto, "i"'] & & \phi(s) \\
& s \arrow[ur, mapsto, dashed, "\theta"'] &
\end{tikzcd}$$

Applying the co-universal property of free semigroups to $\theta\colon T \to G$ gives the following:

$$\begin{tikzcd}
T \arrow[rr, "\theta"] \arrow[dr, hook, "j"'] & & G \\
& X \arrow[ur, dashed, "f"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
s \arrow[rr, mapsto, "\theta"] \arrow[dr, mapsto, "j"'] & & \theta(s) \\
& s \arrow[ur, mapsto, dashed, "f"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
s' \arrow[rr, mapsto, "\theta"] \arrow[dr, mapsto, "j"'] & & \theta(s')=\phi(s)^{-1} \\
& s' \arrow[ur, mapsto, dashed, "f"'] &
\end{tikzcd}$$

Since the homomorphism f is proper, the co-universal property of quotient semigroups gives:

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, two heads, "\pi"'] & & G \\
& X/R \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\pi"'] & & f(x) \\
& \bar{x} \arrow[ur, mapsto, dashed, "h"'] &
\end{tikzcd}$$

Showing that our free semigroup quotient X/R is free

We know $\exists! h\colon X/R \to G$ such that $f = h \circ \pi$, but not necessarily $\phi = h \circ \iota$.

$$
\begin{tikzcd}
S \arrow[rrrr, "\phi"] \arrow[dr, hook, "i"] \arrow[dddrrr, bend right, "\iota"'] & & & & G \\
& T \arrow[urrr, "\theta"] \arrow[dr, hook, "j"] & & & \\
& & X \arrow[uurr, "f"] \arrow[dr, two heads, "\pi"] & & \\
& & & X/R \arrow[uuur, dashed, "h"'] &
\end{tikzcd}
$$

Suppose $\exists g\colon X/R \to G$ such that $\phi = g \circ \iota$. (Need $h = g$.)

We have $h \circ \pi \circ j \circ i = g \circ \pi \circ j \circ i$, and we claim that $h \circ \pi \circ j = g \circ \pi \circ j$.

It is clear that $h(\pi(j(s))) = f(\pi(j(s))$ for all $s \in S$. By construction,

$$h(\pi(j(s'))) = h(\overline{s'}) = h(\bar{s}^{-1}) = h(s)^{-1} = g(s)^{-1} = g(\bar{s}^{-1}) = g(\overline{s'}) = g(\pi(j(s'))).$$

Therefore, $\theta = h \circ \pi \circ j = g \circ \pi \circ j$.

By the co-universal property of free semigroups, $\exists! f\colon X \to G$ such that $\theta = f \circ j$.

But both $h \circ \pi$ and $g \circ \pi$ satisfy this, and so $f = h \circ \pi = g \circ \pi \quad \Rightarrow \quad h = g$ $\square$

Properties of free groups

Proposition

Suppose $S, U \neq \emptyset$. Then $F_S \cong F_U$ if and only if $|S| = |U|$.

Proof

"$\Rightarrow$" **Case 1**: $|S| < \infty$.

Each nonempty $R \subseteq S$ defines an index-2 subgroup, the kernel of

$$f_R \colon F_S \longrightarrow \mathbb{Z}_2, \qquad f_R(s) = \begin{cases} 0 & s \in R \\ 1 & s \notin R \end{cases}$$

Since F_U has the same number of index-2 subgroups, $2^{|S|} - 1 = 2^{|U|} - 1 \Rightarrow |S| = |U|$.

Case 2: $|S| = \infty$.

Let $T = S \subseteq S^{-1}$. Then $|F_S| = |S|$ because.

$$|F_S| \leq 1 + |T| + |T \times T| + |T \times T \times T| + \cdots = \aleph_0 |T| = |S|.$$

Reversing roles gives $|F_U| = |U| = |S| = |F_S|$. ✓

Properties of free groups

Proposition

Suppose $S, U \neq \emptyset$. Then $F_S \cong F_U$ if and only if $|S| = |U|$.

Proof

"$\Leftarrow$" Fix a bijection $\beta \colon S \to U$ and use the co-universal property to get

$$\begin{tikzcd}
S \arrow[r, "\beta"] \arrow[dr, "\iota_S"'] & U \arrow[r, "\iota_U"] & F_U \\
& F_S \arrow[ur, dashed, "f"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
U \arrow[r, "\beta^{-1}"] \arrow[dr, "\iota_U"'] & S \arrow[r, "\iota_S"] & F_S \\
& F_U \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

We can "stack" these diagrams, two ways, to get:

$$\begin{tikzcd}
S \arrow[rrr, "\iota_S"] \arrow[dr, "\beta"] \arrow[ddr, "\iota_S"'] & & & F_S \\
& U \arrow[r, "\iota_U"] & F_U \arrow[ur, dashed, "g"] & \\
& F_S \arrow[ur, dashed, "f"] \arrow[uurr, dashed, bend right, "\mathrm{Id}_{F_S}"'] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
U \arrow[rrr, "\iota_U"] \arrow[dr, "\beta^{-1}"] \arrow[ddr, "\iota_U"'] & & & F_U \\
& S \arrow[r, "\iota_S"] & F_S \arrow[ur, dashed, "f"] & \\
& F_U \arrow[ur, dashed, "g"] \arrow[uurr, dashed, bend right, "\mathrm{Id}_{F_U}"'] & &
\end{tikzcd}$$

By uniqueness, $g \circ f = \mathrm{Id}_{F_S}$ and $f \circ g = \mathrm{Id}_{F_U}$, so f and g are inverse isomorphisms. $\square$

Free objects

A functor $\mathcal{F} \colon \mathcal{C} \to \mathcal{D}$ is **faithful** if $\mathcal{F} \colon \operatorname{Hom}(\mathcal{C}) \to \operatorname{Hom}(\mathcal{D})$ is injective.

A concrete category is a category $\mathcal{C}$ with a faithful functor $\mathcal{F} \colon \mathcal{C} \to \mathbf{Set}$.

Definition

Let $\mathcal{C}$ be concrete, $F \in \operatorname{Ob}(\mathcal{C})$, and $\iota \colon S \to F$ a map of sets, where $S \neq \emptyset$.

Then F is free on S if for any $A \in \operatorname{Ob}(\mathcal{C})$ and $\theta \colon S \to A$, there is a unique $f \in \operatorname{Hom}_{\mathcal{C}}(F, A)$ such that $f \circ \phi = \iota$.

$$\begin{tikzcd}
S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & & A \\
& F \arrow[ur, dashed, "\pi"'] &
\end{tikzcd}$$

Like we did with products, we can construct a category where free objects are initial:

$$\begin{tikzcd}
S \arrow[rr, "\theta"] \arrow[dr, "\iota"'] & \text{“initial”} & A \\
& F \arrow[ur, dashed, "\exists! h"'] &
\end{tikzcd}
\qquad \pi \in \operatorname{Hom}_{\mathcal{A}}\left(S \xrightarrow{\iota} F, S \xrightarrow{\theta} A\right)$$

Free objects

Let **Nil** be the category of nilpotent groups.

Suppose $\iota\colon S \to F$ is a free object in **Nil**.

This means that every other nilpotent group G generated by S is a quotient of F:

> *"if G is nilpotent with set map $f\colon S \to G$, then there exists a unique $\pi\colon F \to G$ such that $f = \pi \circ \iota$."*

$$\begin{tikzcd}
S \arrow[rr, "f"] \arrow[dr, "\iota"'] & & G \\
& F \arrow[ur, dashed, "\pi"'] &
\end{tikzcd}$$

Suppose F has nilpotency class n. Then every quotient has nilpotency class $\leq n$. (Why?)

Thus, if $G = \langle S \rangle$ has nilpotency class $n+1$, then $\nexists\ \pi\colon F \twoheadrightarrow G$.

Free objects

Let $\mathbf{Nil}_{\leq n}$ be the category of nilpotent groups of class $\leq n$.

If G is a nilpotent group of class $\leq n$, then $L_n(G) = \langle 1 \rangle$.

$$\begin{array}{ccccccc}
L_1(G) & = & [G, L_0] & = & [G, G] & = & \langle [g_1, g_0] \mid g_i \in G \rangle \\
L_2(G) & = & [G, L_1] & = & [G, [G, G]] & = & \langle [g_2, [g_1, g_0]] \mid g_i \in G \rangle \\
L_3(G) & = & [G, L_2] & = & [G, [G, [G, G]]] & = & \langle [g_3, [g_2, [g_1, g_0]]] \mid g_i \in G \rangle \\
 & \vdots & & \vdots & & \vdots & \\
L_n(G) & = & [G, L_{k-1}] & = & [G, [G, \dots [G, G]]] & = & \langle [g_n, [g_{n-1}, \dots [g_1, g_0]]] \mid g_i \in G \rangle
\end{array}$$

Proposition

Let F be free on a set S. Then $F/L_n(F)$ is free in $\mathbf{Nil}_{\leq n}$.

"if G is nilpotent of class $\leq n$ and $f \colon S \to G$, then there exists a unique $\pi \colon F_n/L_n(F_n) \to G$ such that $f = \pi \circ \iota$."

$$\begin{tikzcd}
S \arrow[rr, "f"] \arrow[dr, "\iota"'] & & G \\
& F/L_n(F) \arrow[ur, dashed, "\pi"'] &
\end{tikzcd}$$

Free objects

Proposition

Let F be free on S. Then $F/L_n(F)$ is free in $\mathbf{Nil}_{\leq n}$.

The existence of $h\colon F \to G$ is because F is free on S.

$$\begin{tikzcd}
S \arrow[rrr, "f"] \arrow[dr, hook, "\iota_1"] \arrow[ddrr, bend right, "\iota"'] & & & G \\
& F \arrow[urr, "h"] \arrow[dr, "g"] & & \\
& & F/L_n(F) \arrow[uur, dashed, "\pi"'] &
\end{tikzcd}$$

Since G has nilpotent class $\leq n$, we have $\mathrm{Ker}(g) = L_n(F) \leq \mathrm{Ker}(h)$.

Now, π is guaranteed by the co-universal property of quotient maps.

Exercise: Verify that π is the unique map satsifying $f = \pi \circ \iota$.

Direct sums and bases

The direct sum of a family $\{A_i \mid i \in I\}$ of groups is

$$\bigoplus_{i\in I} A_i = \Big\{(a_i)_{i\in I} \in \prod_{i\in I} A_i \ \text{ with finite support}\Big\}.$$

If all are abelian, let $\mathbf{e}_j := (a_i)_{i\in I}$ with $a_j = \delta_{ij}$. Every $x \in \bigoplus A_i$ can be written as

$$x = \sum_{i=1}^{n} a_i \mathbf{e}_i, \qquad a_i \in \mathbb{Z}, \quad n \in \mathbb{N}.$$

If A is abelian, the subgroup generated by $X \subseteq S$ are the finite linear combinations:

$$\langle X \rangle = \big\{a_1x_1 + \cdots + a_nx_n \mid a_i \in \mathbb{Z},\ x_i \in X\big\}.$$

A basis of A is a subset $X \subseteq A$ for which:

1. $A = \langle X \rangle$.
2. Given distinct $x_1, \dots, x_n \in X$,

$$a_1x_1 + \cdots + a_nx_n = 0 \qquad \Longrightarrow \qquad a_i = 0 \ \text{ for all } i = 1, \dots, n.$$

Exercise

Given a family $\{A_i \mid i \in I\}$ of abelian groups, $\{\mathbf{e}_i \mid i \in I\}$ is a basis of

$$\bigoplus_{i\in I} A_i = \Big\{a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n \mid a_j \in \mathbb{Z}\Big\} = \Big\{\sum_{j=1}^{n} a_j\mathbf{e}_j,\ a_j \in \mathbb{Z}\Big\}.$$

Direct sums and bases

Assuming the axiom of choice, in a vector space, Every generating set has a basis.

This fails for abelian groups; e.g., $\mathbb{Z} = \langle 2, 3 \rangle$.

Every vector space has a basis, and every $v \neq 0$ is contained in one.

If an abelian group A has an element x of finite order, no basis can contain it.

Proposition

Let A be an abelian group with basis X. Then every $a \in A$ can be written as a unique (finite) linear combination of elements from X.

Proof

The following defines a homomorphism

$$f \colon \bigoplus_{i \in I} \mathbb{Z} \longrightarrow A, \qquad f \colon \sum_{j=1}^{n} a_j \mathbf{e}_j \longmapsto \sum_{j=1}^{n} a_j x_j.$$

It is surjective by Property (1) of a basis, and has trivial kernel by Property (2).

Each way to write x as a linear combination of the basis elements corresponds to an f-preimage of x.

Uniqueness follows because f is bijective. $\square$

Free abelian groups

Definition

The **free abelian group** on $S \neq \emptyset$ is $\displaystyle\bigoplus_{s \in S} \mathbb{Z}$.

Theorem

Let $S \neq \emptyset$. The group $\bigoplus_{s\in S} \mathbb{Z}$ with $\iota(s) = \mathbf{e}_s$ is a free object for S in **Ab**.

That is, given any $f\colon S \to A$ there exists a unique h: $\bigoplus_s \mathbb{Z} \to A$ such that $f = h \circ \iota$.

$$\begin{tikzcd} S \arrow[rr, "f"] \arrow[dr, hook, "\iota"'] & & A \\ & \displaystyle\bigoplus_{s\in S}\mathbb{Z} \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} s \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\iota"'] & & x \\ & \mathbf{e}_s \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Proof (sketch)

Existence and uniqueness of the desired function h is constructive:

$$h\Big(\sum_{i=1}^{n} a_{s_i}\mathbf{e}_{s_i}\Big) = \Big(\sum_{i=1}^{n} a_{s_i} h(\mathbf{e}_{s_i})\Big) = \Big(\sum_{i=1}^{n} a_{s_i} h(\iota(s_i))\Big) = \sum_{i=1}^{n} a_{s_i} f(s_i). \qquad \square$$

Group presentations, formalized

Definition

For any subset $R \subseteq F_S$, the group $G = \langle S \mid R \rangle$ is the quotient F_S/N where

$$N := \bigcap_{R \leq N_\alpha \trianglelefteq F_S} N_\alpha .$$

Elements in R are called relators.

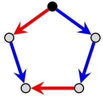
Big idea

The group $\langle S \mid R \rangle$ is the quotient of F_S by the *smallest normal subgroup containing* R.

Exercise: show that

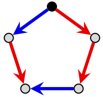
$$G = \langle a, b \mid ab = b^2 a,\ ba = a^2 b \rangle = \langle 1 \rangle .$$

In terms of Cayley graphs and motfis, this means that



$aba^{-1}b^{-2} = 1$

and



$bab^{-1}a^{-2} = 1$

$\Longrightarrow$

$G = \langle a, b, \mid a = b = 1 \rangle = \langle 1 \rangle$

Group presentations, formalized

Given $G_1 = \langle S \mid R_1 \rangle$, define $G_2 = \langle S \mid R_2 \rangle$ by adding relations: $R_1 \subseteq R_2$.

We have two quotient maps,

$$\pi_1 \colon F_S \longrightarrow F_S/N_1 \cong G_1, \qquad\qquad \pi_2 \colon F_S \longrightarrow F_S/N_2 \cong G_2,$$

Since $N_1 = \mathrm{Ker}(\pi_1) \leq \mathrm{Ker}(\pi_2) = N_2$, the co-universal property of quotients gives us:

$$\begin{tikzcd} F_S \arrow[rr, two heads, "\pi_2"] \arrow[dr, two heads, "\pi_1"'] & & G_2 \\ & G_1 \arrow[ur, dashed, two heads, "h"'] & \end{tikzcd}$$

Now, suppose $G_1 = \langle S_1 \mid R \rangle$ and $G_2 = \langle S_2 \mid R \rangle$ with $S_1 \supseteq S_2$.

Defining $R' = S_1 \setminus S_2$, we have

$$G_1 = \langle S_1 \mid R \rangle, \qquad G_2 = \langle S_1 \mid R \cup R' \rangle,$$

and hence a quotient $G_1 \twoheadrightarrow G_2$.

Proposition

Given $G_1 = \langle S_1 \mid R_1 \rangle$ and $G_2 = \langle S_2 \mid R_2 \rangle$ for which $S_1 \supseteq S_2$ and $R_1 \subseteq R_2$, there is a quotient $G_1 \twoheadrightarrow G_2$. $\square$

Group presentations, formalized

In many cases, two generating sets that we wish to compare are not subsets of each other.

For example, if $S_1 = \{a, b, c\}$ and $S_2 = \{r, f\}$, then $S_1 \not\supseteq S_2$.

However, there is $\theta\colon S_1 \twoheadrightarrow S_2$ that can be thought of as a "relabeling."

Saying that "*every relation is G_1 is a relation in G_2*" means that every $\theta(r_1)$ is a relator.

We say that such a map θ *respects relations*, because it extends to a map $\theta\colon R_1 \longrightarrow R_2$.

Proposition

Suppose $G_1 = \langle S_1 \mid R_1 \rangle$ and $G_2 = \langle S_2 \mid R_2 \rangle$ and the following holds:

1. there exists $\theta\colon S_1 \twoheadrightarrow S_2$ extending to $\theta\colon R_1 \longrightarrow R_2$,
2. $r_2 := \theta(r_1) = 1$ for all $r \in R_1$.

Then there is a quotient $h\colon G_1 \twoheadrightarrow G_2$. $\square$

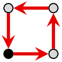
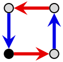
$$\begin{tikzcd}
F_S \arrow[rr, two heads, "\pi_2"] \arrow[dr, two heads, "\pi_1"'] & & G_2 \\
& G_1 \arrow[ur, two heads, dashed, "h"'] &
\end{tikzcd}$$

Group presentations, formalized

Consider the "mystery group"

$$M = \langle a, b \mid a^4 = b^2 = 1,\ (ab)^2 = 1 \rangle,$$

Visually, we are asking what the largest Cayley graph is given several motifs:

 *and*  *and*  $\Longrightarrow$???

$a^4 = 1$ $\qquad$ $(ab)^2 = 1$ $\qquad$ $b^2 = 1$

Elements in M can be written as $a^i b^j$, for $i = \{0, 1, 2, 3\}$ and $j = \{0, 1\}$. Thus, $|M| \leq 8$.

We'll show $|M|$ is a multiple of 8, by constructing a homomorphism

$$\theta\colon M \longrightarrow D_4, \qquad \theta(a) = 90^\circ \text{ CCW rotation}, \qquad \theta(b) = \text{horizontal reflection}.$$

This respect relations because

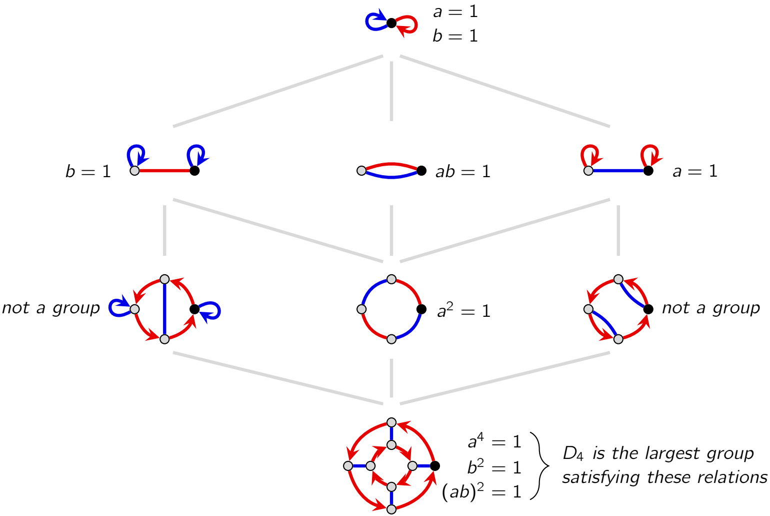
$$\big(\theta(a)\big)^4 = 0^\circ \text{ rotation} = \text{identity symmetry}, \qquad \big(\theta(b)\big)^2 = \text{identity symmetry},$$

$$\big(\theta(a)\theta(b)\big)^2 = (\text{another reflection})^2 = \text{identity symmetry}.$$

Thus, there is a quotient $g\colon M \twoheadrightarrow D_4$, and so $M \cong D_4$.

Group presentations, formalized

Every group $G = \langle a, b \rangle$ satisfying $a^4 = 1$, $b^2 = 1$, and $(ab)^2 = 1$ is a quotient of D_4.



Group presentations, formalized

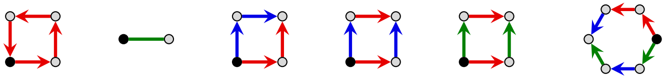
Overview of the strategy

Given a "mystery" $M = \langle S_1 \mid R_1 \rangle$ that we suspect is a "familiar" $F = \langle S_2 \mid R_2 \rangle$:

1. Using the relations, show that $|M| \leq |F|$.
2. Identify generators of F that satisfy the relations in M, via a "relabling map" $\theta\colon S_1 \twoheadrightarrow S_2$ that extends to $\theta\colon R_1 \to R_2$.

Together, $|M| \leq |F|$ and $M \twoheadrightarrow F$ forces $M \cong F$.

Consider the group $M = \langle a, b, c \mid a^4 = c^2 = 1,\ a^2 = b^2,\ ab = ba,\ ac = ca,\ a^2b = cbc \rangle$.



$a^4 = 1$ $\quad$ $c^2 = 1$ $\quad$ $a^2 = b^2$ $\quad$ $ab = ba$ $\quad$ $ac = ca$ $\quad$ $a^2 b = cbc$

Homework: Establish $|M| \leq 16$ by showing that every word in M can be written

$$a^i b^j c^k, \qquad i \in \{0,1,2,3\}, \quad j \in \{0,1\}, \quad k \in \{0,1\},$$

Then, find a "familiar group" F of order 16 whose generator satisfies these relations.

That will define a quotient $\pi\colon M \twoheadrightarrow F$, and hence $|M| \geq |F| = 16$.

Free products

Proposition

The coproduct of $\{A_i \mid i \in I\}$ in **Ab** is the direct sum, $S = \bigoplus_i A_i$:

$$\begin{tikzcd} A_j \arrow[rr, "f_j"] \arrow[dr, hook, "\iota_j"'] & & B \\ & \displaystyle\bigoplus_{i\in I} A_i \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} a_j \arrow[rr, mapsto, "f_j"] \arrow[dr, mapsto, "\iota_j"'] & & b_j \\ & \iota(a_j) \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Proof

Let C be the coproduct of the factors, with $\iota_j \colon A_j \hookrightarrow C$.

Consider the group $B \le C$ generated by the images of all individual factors,

$$B = \langle \iota_j(A_j) \mid j \in I \rangle, \qquad \text{and let } \; g \colon B \hookrightarrow C.$$

Each $b \in B$ can be written as

$$b = \sum_{j=1}^{k} \iota(a_{i_j}), \qquad a_{i_j} \in A_{i_j},$$

and so $B \cong S$. Let $f_j \colon A_j \hookrightarrow B$ be the natural inclusion map.

Free products

Proposition

The coproduct of $\{A_i \mid i \in I\}$ in **Ab** is the direct sum, $S = \bigoplus_i A_i$:

$$\begin{tikzcd} A_j \arrow[rr, "f_j"] \arrow[dr, hook, "\iota_j"'] & & B \\ & \bigoplus\limits_{i \in I} A_i \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} a_j \arrow[rr, mapsto, "f_j"] \arrow[dr, mapsto, "\iota_j"'] & & b_j \\ & \iota(a_j) \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

Proof (cont.)

By the co-universal property of coproducts, we have:

$$\begin{tikzcd} A_j \arrow[rr, hook, "f_j"] \arrow[dr, hook, "\iota_j"'] & & B \\ & C \cong S \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} a_j \arrow[rr, mapsto, "f_j"] \arrow[dr, mapsto, "\iota_j"'] & & \iota(a_j) \\ & \iota(a_j) \arrow[ur, dashed, mapsto, "h"'] & \end{tikzcd}$$

It is clear that $h \circ g = \mathrm{Id}_B$. It suffices to show that $g \circ h = \mathrm{Id}_C$.

Free products

Proposition

The coproduct of $\{A_i \mid i \in I\}$ in **Ab** is the direct sum, $S = \bigoplus_i A_i$:

$$\begin{tikzcd} A_j \arrow[rr, "f_j"] \arrow[dr, hook, "\iota_j"'] & & B \\ & \bigoplus_{i \in I} A_i \arrow[ur, dashed, "h"'] & \end{tikzcd} \qquad \begin{tikzcd} a_j \arrow[rr, mapsto, "f_j"] \arrow[dr, mapsto, "\iota_j"'] & & b_j \\ & \iota(a_j) \arrow[ur, mapsto, dashed, "h"'] & \end{tikzcd}$$

Proof (cont.)

Since $\iota_j = g \circ f_j$ and $f_j = h \circ \iota_j$, the "small triangles" in the following diagram commute:

$$\begin{tikzcd} A_j \arrow[rr, "\iota_j"] \arrow[dr, "f_j"] \arrow[ddr, "\iota_j"'] & & C \\ & B \arrow[ur, dashed, "g"] & \\ & C \arrow[u, dashed, "h"] \arrow[uur, dashed, bend right, "\mathrm{Id}_C"'] & \end{tikzcd}$$

It follows that $\iota_j = g \circ h \circ \iota_j$, but we also have $\iota_j = \mathrm{Id}_C \circ \iota_j$.

By uniqueness from the co-universal property, $g \circ h = \mathrm{Id}_C$. $\square$

Free products

The coproduct of two groups A and B in **Grp** is a construction called the **free product**.

Given groups $A = \langle S_1 \mid R_1 \rangle$ and $B = \langle S_2 \mid R_2 \rangle$, their *free product* is

$$A * B := \big\langle S_1 \sqcup S_2 \mid R_1 \sqcup R_2 \big\rangle.$$

If $A = \langle a \mid \ \rangle = C_\infty \cong \mathbb{Z}$ and $B = \langle b \mid \ \rangle \cong C_\infty$, then $A * B$ is the free group $F_2 = \langle a, b \mid \ \rangle$.

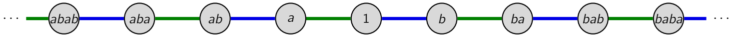
If A and B are nontrivial, their free product is infinite, because

$$a, \quad ab, \quad aba, \quad abab, \quad ababa, \quad ababab, \dots$$

are all distinct, assuming $a, b \neq 1$.

The free product of the groups $A = \langle a \mid a^2 = 1 \rangle \cong C_2$ and $B = \langle b \mid b^2 = 1 \rangle \cong C_2$ is

$$A * B = \big\langle a, b \mid a^2 = 1, \ b^2 = 1 \big\rangle \cong D_\infty$$



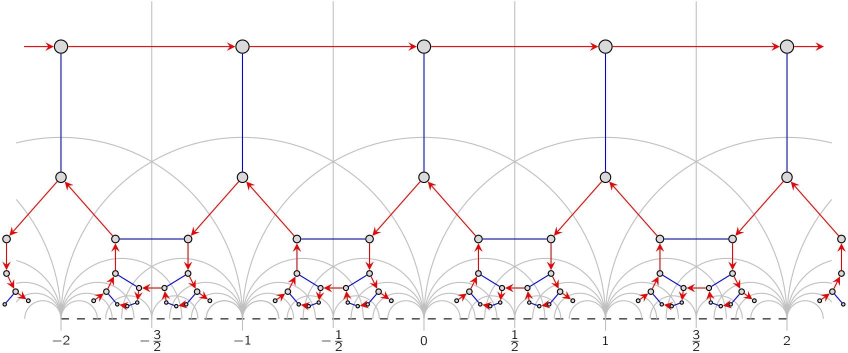
Free products

The free product $C_3 * C_2$ is isomorphic to the projective linear group

$$\mathsf{PSL}_2(\mathbb{Z}) = \mathsf{SL}_2(\mathbb{Z})/\langle -I\rangle, \qquad \text{where } \mathsf{SL}_2(\mathbb{Z}) = \Big\langle \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}_{T} \Big\rangle.$$

This is in no way obvious from the generators that we've seen, which represent

$$S\colon z \longmapsto \frac{0z-1}{z+0} = -\frac{1}{z}, \qquad \text{and} \qquad T\colon z \longmapsto \frac{z+1}{0z+1} = z+1.$$



Free products

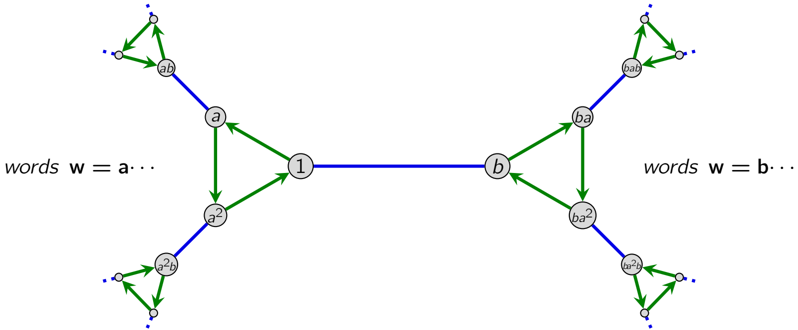
Let's see why the free product $C_3 * C_2$ is isomorphic to the projective linear group

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\langle -I \rangle.$$

Elements of $\mathrm{PSL}_2(\mathbb{Z})$ are cosets of $\langle -I \rangle = \pm I$. Let

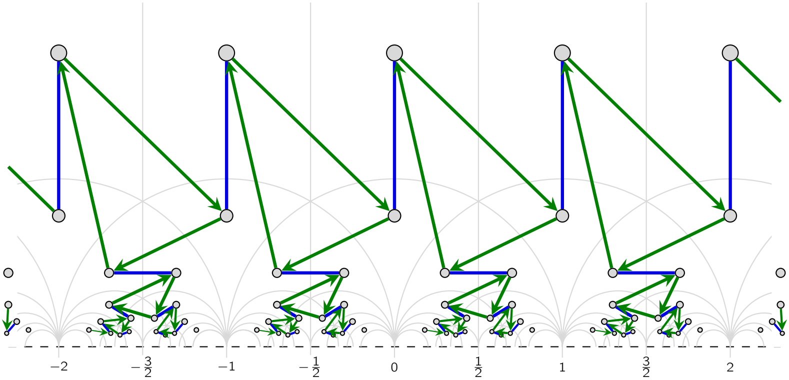
$$\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \mid S^2 = (ST)^6 = I \rangle, \qquad S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad ST = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix},$$

Then $\mathrm{PSL}_2(\mathbb{Z}) \cong \langle A, B \rangle$, where $A = \pm ST$ and $B = \pm S$.



Free products

A Cayley graph of $\mathsf{PSL}_2(\mathbb{Z}) = \langle A, B \mid A^3 = B^2 = 1 \rangle \cong C_3 * C_2$:



To verify $\mathsf{PSL}_2(\mathbb{Z}) \cong C_3 * C_2$, it suffices to show that we can't nontrivially write

$$I = A^{i_1} B^{j_1} A^{i_2} B^{j_2} \cdots A^{i_{m-1}} B^{j_{m-1}} A^{i_m}, \qquad i_k \in \{0, 1, 2\}, \quad j_k \in \{0, 1\}.$$

This will be left as HW.

Free products

Definition

The free product of a family $G_i = \langle S_i \mid R_i \rangle$ of groups is

$$\mathop{\ast}_{i \in I} G_i = \Big\langle \bigsqcup_{i \in I} S_i \;\Big|\; \bigsqcup_{i \in I} R_i \Big\rangle, \qquad \text{where } \iota_j \colon G_j \hookrightarrow \mathop{\ast}_{i \in I} G_i, \qquad \iota_j(x_j) = x_j,$$

Proposition

The coproduct of $\{G_i \mid i \in I\}$ in **Grp** is their free product.

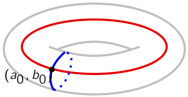
That is, given any H and $\{f_j \colon G_j \to H \mid j \in I\}$, there is a unique $h \colon \ast_i G_i \to H$ such that $f_j = \iota_j \circ h$ for all $j \in I$.

$$\begin{tikzcd}
G_j \arrow[rr, "f_j"] \arrow[dr, hook, "\iota_j"'] & & H \\
& \mathop{\ast}_{i \in I} G_i \arrow[ur, dashed, "h"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
x_j \arrow[rr, mapsto, "f_j"] \arrow[dr, mapsto, "\iota_j"'] & & y_j \\
& \iota(x_j) \arrow[ur, dashed, mapsto, "h"'] &
\end{tikzcd}$$

Fiber coproducts in **Grp**: free products with amalgamation

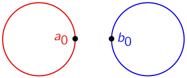
Suppose A and B are disjoint circles. Gluing them at a point is called their wedge sum.

Product



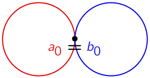
$\mathbf{A} \times \mathbf{B}$: "*Cartesian product*"

Coproduct



$\mathbf{A} \sqcup \mathbf{B}$: "*disjoint union*"

Coproduct w/ amalgamation



$\mathbf{A} \vee \mathbf{B}$: "*wedge sum*"

In general, we can identify or "glue" two objects along a common subset. Gluing two disks along their boundaries gives a sphere.

Suppose $A \trianglelefteq G_i$ for $i = 1, 2$, with embeddings $\alpha_i \colon A \hookrightarrow G_i$.

Goal: Take the the coproduct of G_1 with G_2, and "identify" the common subgroup A.

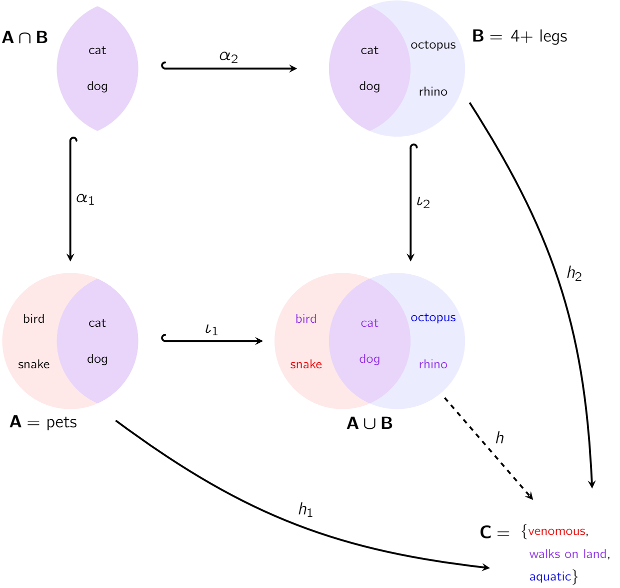
We can "force" $\alpha_1(a) \in G_1$ and $\alpha_2(a) \in G_2$ (in $G_1 * G_2$) to be the same by adding relations

$$\alpha_1(a)\alpha_2^{-1}(a) = 1, \qquad \text{for all } a \in A,$$

and then quotient $A * B$ by the smallest normal subgroup N that contains these relators.

The group $G_1 *_A G_2 := (G_1 * G_2)/N$ is the free product of G_1 and G_2 amalgamated at A.

Fiber coproducts in **Set**: unions



Fiber coproducts in **Grp**: free products with amalgamation

$G_1 * G_2$ is the smallest group in which both G_1 and G_2 embeds into "independently."

I.e., for any other H with this property, those embeddings factor through via $G_1 * G_2 \to H$.

For $i = 1, 2$, let $\iota_i \colon G_i \to (G_1 * G_2)/N = G_1 *_A G_2$ be the map $\iota_i \colon g_i \mapsto g_i N$.

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & G_1 \arrow[d, "\iota_1"] \\ G_2 \arrow[r, "\iota_2"] & (G_1 * G_2)/N \end{tikzcd} \tag{3}$$

$G_1 *_A G_2$ is the smallest group in which both G_1 and G_2 embeds into "independently," while keeping A identified.

The central product, e.g., $\mathrm{DQ}_8 \cong D_4 \circ C_4 \cong Q_8 \circ C_4$, is a *direct product with amalgamation*.

Fiber coproducts in **Grp**: free products with amalgamation

Suppose G_1 and G_2 embed into H while keeping A identified:

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & G_1 \arrow[d, "h_1"] \\ G_2 \arrow[r, "h_2"] & H \end{tikzcd}$$

Then $\exists! h \colon G_1 *_A G_2 \longrightarrow H$ that makes the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & G_1 \arrow[d, "\iota_1"] \arrow[ddr, bend left, "h_1"] & \\ G_2 \arrow[r, "\iota_2"] \arrow[drr, bend right, "h_2"'] & G_1 *_A G_2 \arrow[dr, dashed, "h"] & \\ & & H \end{tikzcd}$$

Fiber coproducts in a general category

Definition

Let $A, B_1, B_2 \in \mathbf{Ob}(\mathcal{C})$ and $\alpha_i \in \mathrm{Hom}_{\mathcal{C}}(A, B_i)$ for $i = 1, 2$. A fiber coproduct (or **pushout**) for them is a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \\ B_2 \arrow[r, "\iota_2"] & C \end{tikzcd}$$

satisfying the following couniversal property:

> *For any $D \in \mathbf{Ob}(\mathcal{C})$ and $h_i \in \mathrm{Hom}_{\mathcal{C}}(B_i, D)$ such that if $h_1 \circ \alpha_1 = h_2 \circ \alpha_2$, there exists a unique $h \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ such that $h \circ \iota_i = h_i$.*

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \arrow[ddr, bend left, "h_1"] & \\ B_2 \arrow[r, "\iota_2"] \arrow[drr, bend right, "h_2"'] & C \arrow[dr, dashed, "h"] & \\ & & D \end{tikzcd}$$

Fiber coproducts (pushouts)

Proposition

Pushouts are unique up to equivalence.

Proof

Suppose we have two pushouts for A, B_1, B_2:

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \\ B_2 \arrow[r, "\iota_2"] & C \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\delta_1"] \\ B_2 \arrow[r, "\delta_2"] & D \end{tikzcd}$$

By the co-universal property, we have $h \in \mathbf{Hom}_{\mathcal{C}}(C, D)$ and $g \in \mathbf{Hom}_{\mathcal{C}}(D, C)$ such that:

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \arrow[ddr, bend left, "\delta_1"] & \\ B_2 \arrow[r, "\iota_2"] \arrow[drr, bend right, "\delta_2"'] & C \arrow[dr, dashed, "h"] & \\ & & D \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\delta_1"] \arrow[ddr, bend left, "\iota_1"] & \\ B_2 \arrow[r, "\delta_2"] \arrow[drr, bend right, "\iota_2"'] & D \arrow[dr, dashed, "g"] & \\ & & C \end{tikzcd}$$

Fiber coproducts (pushouts)

Proposition

Pushouts are unique up to equivalence.

Proof (cont.)

We can "stack" these diagrams to get:

$$\begin{tikzcd}
A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \arrow[ddr, bend left, "\delta_1"] \arrow[dddrr, bend left, "\iota_1"] & & \\
B_2 \arrow[r, "\iota_2"] \arrow[drr, bend right, "\delta_2"] \arrow[ddrrr, bend right, "\iota_2"'] & C \arrow[dr, dashed, "h"] & & \\
 & & D \arrow[dr, dashed, "g"] & \\
 & & & C
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\alpha_1"] \arrow[d, "\alpha_2"'] & B_1 \arrow[d, "\iota_1"] \arrow[ddr, bend left, "\iota_1"] & \\
B_2 \arrow[r, "\iota_2"] \arrow[drr, bend right, "\iota_2"'] & C \arrow[dr, dashed, "\mathrm{Id}_C"] & \\
 & & C
\end{tikzcd}$$

By uniqueness from the co-universal property, $g \circ h = \mathrm{Id}_C$.

Stacking them the other way gives $h \circ g = \mathrm{Id}_D$.

Therefore, h and g are inverse isomorphisms, and hence $C \cong D$. $\square$

Fiber coproducts (pushouts)

In **Set** and **Top**, pushouts are ordinary unions:

$$\begin{tikzcd} Y \cap Z \arrow[r, hook, "\alpha_Z"] \arrow[d, hook, "\alpha_Y"'] & Z \arrow[d, hook, "\iota_Z"] \\ Y \arrow[r, hook, "\iota_Y"] & Y \cup Z \end{tikzcd}$$

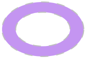
Siefert van-Kampen theorem

The functor $\pi_1 \colon \textbf{Top} \to \textbf{Grp}$ preserves pushouts.

$$\begin{tikzcd} \mathcal{F}(Y \cap Z) \arrow[r, "\alpha_Z^*"] \arrow[d, "\alpha_Y^*"'] & \mathcal{F}(Z) \arrow[d, "\iota_Z^*"] \\ \mathcal{F}(Y) \arrow[r, "\iota_Y^*"] & \mathcal{F}(Y \cup Z) \end{tikzcd} \qquad \begin{tikzcd} \pi_1(Y \cap Z) \arrow[r, "\alpha_Z^*"] \arrow[d, "\alpha_Y^*"'] & \pi_1(Z) \arrow[d, "\iota_Z^*"] \\ \pi_1(Y) \arrow[r, "\iota_Y^*"] & \pi_1(Y \cup Z) \end{tikzcd}$$

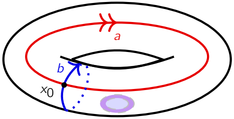
The Siefert van-Kampen theorem

$\pi_1(Y \cap Z) = \langle aba^{-1}b^{-1} \rangle \cong \mathbb{Z}$



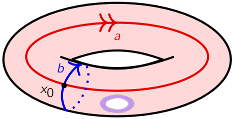
Y ∩ Z

$\pi_1(Z) = \langle 1 \rangle$



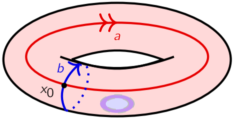
Z = D²

$$\begin{tikzcd}
Y \cap Z \arrow[r, hook, "\alpha_Z"] \arrow[d, hook, "\alpha_Y"'] & Z \arrow[d, hook, "\iota_Z"] \\
Y \arrow[r, hook, "\iota_Y"] & X
\end{tikzcd}$$



Y = T² − D²

$\pi_1(Y) = \langle a, b \mid \; \rangle$



X = Y ∪ Z = T²

$$\pi_1(Y \cup Z) = \pi_1(Y) *_{\pi_1(Y \cap Z)} \pi_1(Z) \cong \big\langle a, b \mid \; \big\rangle *_{\langle aba^{-1}b^{-1} \rangle} \langle 1 \rangle$$

$$= \big\langle a, b \mid aba^{-1}b^{-1} = 1 \big\rangle \cong \mathbb{Z} \times \mathbb{Z}$$

Fiber products / pullbacks (HW)

Definition

Let $A_1, A_2, B \in \mathbf{Ob}(\mathcal{C})$ and $\alpha_i \in \mathrm{Hom}_{\mathcal{C}}(A_i, B)$ for $i = 1, 2$. A fiber product (or **pullback**) for them is a commutative diagram

$$\begin{tikzcd} P \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & A_1 \arrow[d, "\alpha_1"] \\ A_2 \arrow[r, "\alpha_2"] & B \end{tikzcd}$$

satisfying the following universal property:

> *For any $Q \in \mathbf{Ob}(\mathcal{C})$ and $h_i \in \mathrm{Hom}_{\mathcal{C}}(Q, A_i)$ such that if $\pi_1 \circ h_1 = \pi_2 \circ h_2$, there exists a unique $h \in \mathrm{Hom}_{\mathcal{C}}(Q, P)$ such that $h_i = \pi_i \circ h$.*

$$\begin{tikzcd} Q \arrow[dr, dashed, "h"] \arrow[drr, bend left, "h_1"] \arrow[ddr, bend right, "h_2"'] & & \\ & P \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & A_1 \arrow[d, "\alpha_1"] \\ & A_2 \arrow[r, "\alpha_2"] & B \end{tikzcd}$$