Normal subgroups!

Spencer Bagley

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

19 Feb 2025

Goals for today:

1. Define what quotient groups are
2. See some examples
3. Thus, see why we care so much about normal subgroupss

Some review!

Cosets!

Definition

If $H \leq G$, then a (left) coset is a set

$$xH = \{xh \mid h \in H\},$$

for some fixed $x \in G$ called the representative.
Similarly, we can define a right coset as

$$Hx = \{hx \mid h \in H\}.$$

Morally:

A coset of H is a shifted copy of H somewhere else in G.

A coset of H is always / sometimes / never:

- An element of G
- A subset of G
- Equal to H
- A subgroup of G

Conjugate subgroups!

Definition

For a fixed element $g \in G$, the conjugate of H by g is the set

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

A conjugate of H is always / sometimes / never:

- An element of G
- A subset of G
- Equal to H
- A subgroup of G

Definition

The conjugacy class of H in G is the set of all conjugates of H:

$$\mathrm{cl}_G(H) = \{gHg^{-1} \mid g \in G\}.$$

Morally

$\mathrm{cl}_G(H)$ is a list of all the subgroups of G that are "similar to" H.

Normal subgroups!

Formal definition

A subgroup H is a normal subgroup of G if $gH = Hg$ for *all* $g \in G$. We write $H \trianglelefteq G$.

Equivalent definition

. . . if $gHg^{-1} = H$ for *all* $g \in G$.

Equivalent definition #2

. . . if there is only one conjugate subgroup to H, ie., H itself.

Equivalent definition #3

. . . if $\left|\mathrm{cl}_G(H)\right| = 1$.

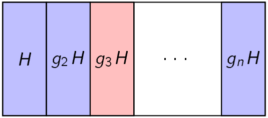
Morally

Normal subgroups are in some way unique in their group.

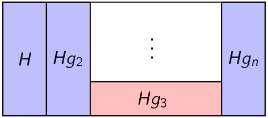
Normal-ish subgroups

Okay, well, if $H \leq G$ isn't normal, then a natural followup question is:

"*How* non-normal?" "*How many* left cosets of H are right cosets?"



Partition of G by the left cosets of H



Partition of G by the right cosets of H

- "Best case" scenario ($H \trianglelefteq G$): all of them
- "Worst case" scenario: only H (I mean for sure the identity coset $eH = He$)
- In general: somewhere between these two extremes

Normalizers!

Definition

The normalizer of H, denoted $N_G(H)$, is the set of elements $g \in G$ that "normalize" H:

$$\begin{aligned} N_G(H) &= \{g \in G \mid gH = Hg\} \\ &= \{g \in G \mid gHg^{-1} = H\} \end{aligned}$$

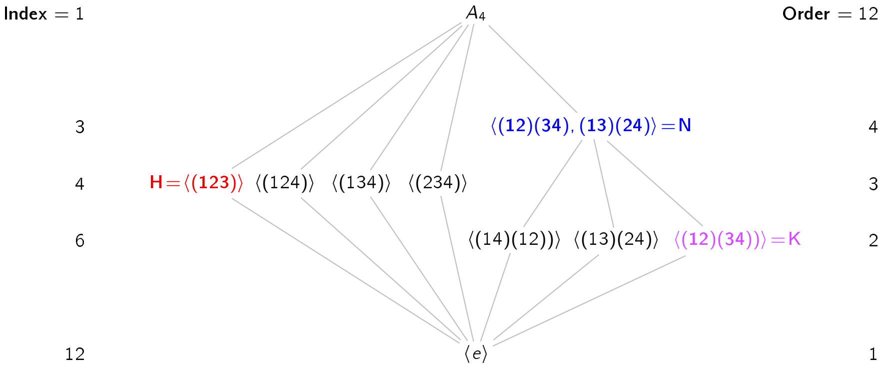
The normalizer of H always / sometimes / never:

- An element of G
- A subset of G
- A subgroup of G
- Equal to H
- Contains H

Three subgroups of A_4 (from Problem 9)

I am highlighting the following three subgroups of A_4:

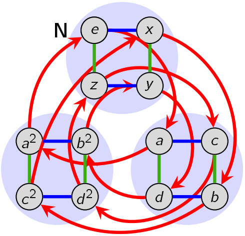
$$N = \big\langle (12)(34), (13)(24) \big\rangle = \big\{ e,\ (12)(34),\ (13)(24),\ (14)(23) \big\} \cong V_4$$
$$H = \big\langle (123) \big\rangle = \big\{ e,\ (123),\ (132) \big\} \cong C_3$$
$$K = \big\langle (12)(34) \big\rangle = \big\{ e,\ (12)(34) \big\} \cong C_2.$$

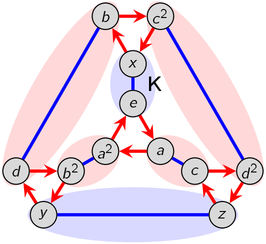


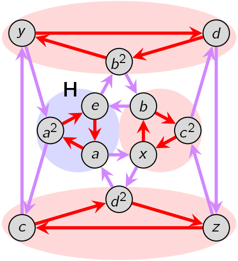
Three subgroups of A_4 (from Problem 9)

Take $a = (123)$, $b = (134)$, $x = (12)(34)$, and $z = (13)(24)$. Then:

$$N = \langle x, z \rangle; \qquad H = \langle a \rangle; \qquad K = \langle x \rangle.$$







(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

$[A_4 : N_{A_4}(N)] = 1$

"normal"

(124)	(234)	(143)	(132)
(123)	(243)	(142)	(134)
e	(12)(34)	(13)(24)	(14)(23)

$[A_4 : N_{A_4}(K)] = 3$

"moderately unnormal"

(14)(23)	(142)	(143)
(13)(24)	(243)	(124)
(12)(34)	(134)	(234)
e	(123)	(132)

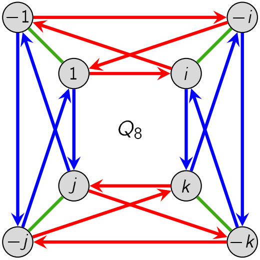
$[A_4 : N_{A_4}(H)] = 4$

"fully unnormal"

Quotients!

Quotients

We have already kinda bumped into the concept a quotient of a group by a subgroup:



	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

$Q_8/\langle -1 \rangle \cong V_4$

	± 1	$\pm i$	$\pm j$	$\pm k$
± 1	± 1	$\pm i$	$\pm j$	$\pm k$
$\pm i$	$\pm i$	± 1	$\pm k$	$\pm j$
$\pm j$	$\pm j$	$\pm k$	± 1	$\pm i$
$\pm k$	$\pm k$	$\pm j$	$\pm i$	± 1

We now know enough algebra to be able to formalize this, but first some examples based on vibes.

Key idea

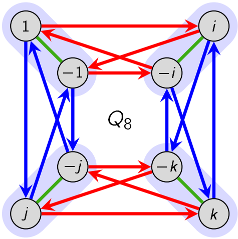
The quotient of G by a subgroup H exists when the (left) cosets of H form a group.

Quotients

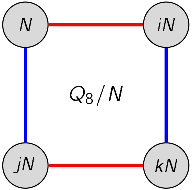
Goals

- Characterize *when* a quotient exists.
- Learn *how* to formalize this algebraically (without Cayley graphs or tables).

First, let's interpret the "*quotient process*" visually, in terms of cosets.



Cluster the left cosets of N



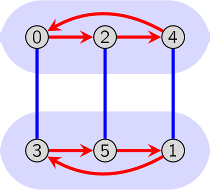
Collapse cosets into single nodes

	N	iN	jN	kN
N	N	iN	jN	kN
iN	iN	N	kN	jN
jN	jN	kN	N	iN
kN	kN	jN	iN	N

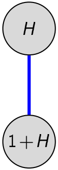
Elements of the quotient are cosets of N

Notice how taking a quotient generally loses information.
(You are squashing cosets together: iN and $-iN$ are the same node.)

Quotients



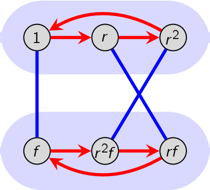
Cluster the
left cosets of $H \leq \mathbb{Z}_6$



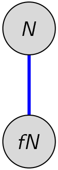
Collapse cosets
into single nodes

	H	$1+H$
H	H	$1+H$
$1+H$	$1+H$	H

Elements of the quotient
are cosets of H



Cluster the
left cosets of $N \leq D_3$



Collapse cosets
into single nodes

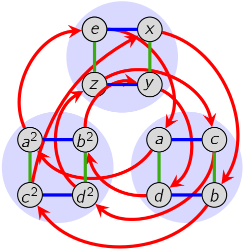
	N	fN
N	N	fN
fN	fN	N

Elements of the quotient
are cosets of N

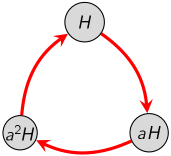
We say that $\mathbb{Z}_6/\langle 2\rangle \cong \mathbb{Z}_2$ and $D_3/\langle r\rangle \cong C_2$.

Quotients

The quotient process succeeds for the group $N = \langle (12)(34), (13)(24) \rangle$ of A_4.



Cluster the left
cosets of $H \leq A_4$



Collapse cosets
into single nodes

	H	aH	a^2H
H	H	aH	a^2H
aH	aH	a^2H	H
a^2H	a^2H	H	aH

Elements of the quotient
are cosets of H

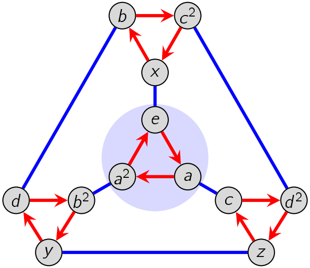
We denote the resulting group by $G/N = \{N,\ aN,\ a^2N\} \cong C_3$. Since it's a group, there is a binary operation on the set of cosets of N.

Questions

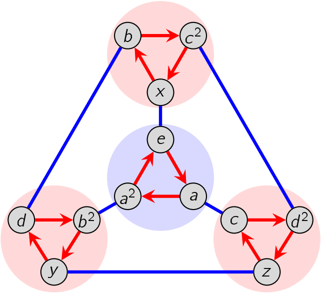
- Do you see *how* to define this binary operation?
- Do you see *why* this works for this particular $N \leq G$?
- Can you think of examples where this "quotient process" would fail, and why?

Quotients

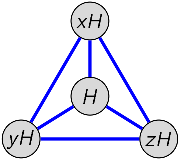
The quotient process fails for the group $H = \langle (123) \rangle$ of A_4.



Here is $H = \langle a \rangle$.



Cluster the left cosets of $H = \langle (123) \rangle$.



Collapse cosets into single nodes

We can still write $G/H := \{H,\ xH,\ yH,\ zH\}$ for the set of (left) cosets of H in G.

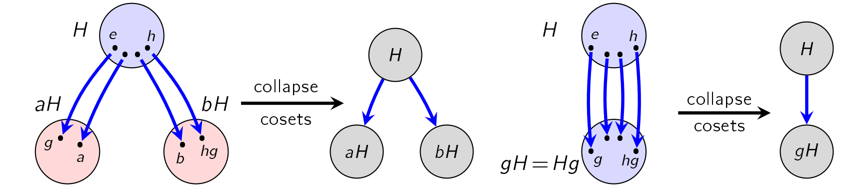
But now what in the hell are the arrows?

Apparently all of those arrows are x arrows, but that doesn't make sense; this is no longer a legit Cayley graph!

When and why the quotient process works

To get some intuition, let's consider collapsing the left cosets of a subgroup $H \leq G$.

In the following: *the right cosets Hg are the "arrowtips"*.



Elements in the right coset Hg are in multiple left cosets

not a valid Cayley graph

Elements in Hg all stay in gH

valid Cayley graph

Key idea

For this process to work, the left cosets (nodes) and right cosets (arrows) must be compatible. So if H is a normal subgroup of G, then this process will work.

If H is not normal, then following the blue arrows from H is ambiguous.

In other words, it depends on where we start within H.

We still need to formalize this and prove it algebraically.

What does it mean to "multiply" two cosets?

Quotient theorem

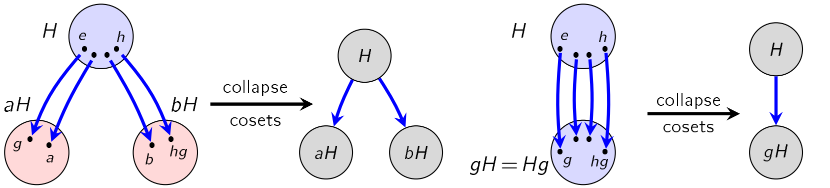
Consider the set of (left) cosets $G/H = \{eH, aH, bH, \ldots\}$.
If $H \trianglelefteq G$, then G/H forms a group, with binary operation

$$aH \cdot bH := abH.$$

It is clear that G/H is closed under this operation.

We have to show that this operation is well-defined.

By that, we mean that it *does not depend on our choice of coset representative*.



our destination depends on where in H we start

the quotient process does not yield a group

destination doesn't depend on where we start in H

quotient process succeeds

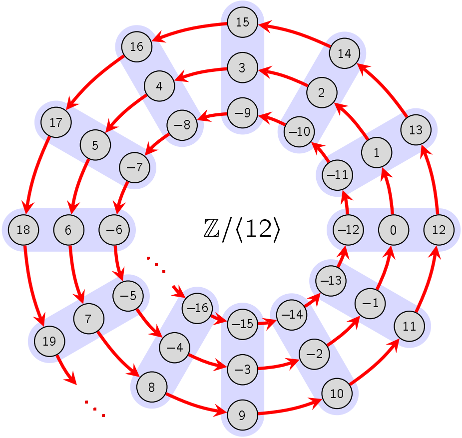
A familiar example

Consider the subgroup $H = \langle 12 \rangle = 12\mathbb{Z}$ of $G = \mathbb{Z}$.

The cosets of H are the congruence classes modulo 12.

Since this group is additive, the condition $aH \cdot bH$ becomes $(a + H) + (b + H) = a + b + H$:

"(the coset containing a) + (the coset containing b) = the coset containing a + b."



Quotient groups, algebraically

Lemma

Let $H \trianglelefteq G$. Multiplication of cosets is well-defined:

$$\text{if } a_1 H = a_2 H \text{ and } b_1 H = b_2 H, \text{ then } a_1 H \cdot b_1 H = a_2 H \cdot b_2 H.$$

Proof

Suppose that $H \trianglelefteq G$, $a_1 H = a_2 H$ and $b_1 H = b_2 H$. Then

Claim			Data / Warrant
$a_1 H \cdot b_1 H$	$=$	$a_1 b_1 H$	(by definition)
	$=$	$a_1 (b_2 H)$	($b_1 H = b_2 H$ by assumption)
	$=$	$(a_1 H) b_2$	($b_2 H = H b_2$ since $H \trianglelefteq G$)
	$=$	$(a_2 H) b_2$	($a_1 H = a_2 H$ by assumption)
	$=$	$a_2 b_2 H$	($b_2 H = H b_2$ since $H \trianglelefteq G$)
	$=$	$a_2 H \cdot b_2 H$	(by definition)

Thus, the binary operation on G/H is well-defined. □

Quotient groups, algebraically

Quotient theorem (restated)

When $H \trianglelefteq G$, the set of cosets G/H forms a group.

Proof

There is a well-defined binary operation on the set of left (equivalently, right) cosets:

$$aH \cdot bH = abH.$$

We need to verify the three remaining properties of a group:

Identity. The coset $H = eH$ is the identity because for any coset $aH \in G/H$,

$$aH \cdot H = aH \cdot eH = aeH = aH = eaH = eH \cdot aH = H \cdot aH. \qquad \checkmark$$

Inverses. Given a coset aH, its inverse is $a^{-1}H$, because

$$aH \cdot a^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H \cdot aH. \qquad \checkmark$$

Closure. This is immediate, because $aH \cdot bH = abH$ is another coset in G/H. $\checkmark$

Quotient groups, algebraically

We just learned that if $H \trianglelefteq G$, then we can define a binary operation on cosets by

$$aH \cdot bH = abH,$$

and *this works*.

Here's another reason why this makes sense.

Given any subgroup $H \leq G$, normal or not, define the product of left cosets:

$$xHyH = \{xh_1yh_2 \mid h_1, h_2 \in H\}.$$

Exercise

If H is normal, then the set $xHyH$ is equal to the left cosets

$$xyH = \{xyh \mid h \in H\}.$$

To show that $xHyH = xyH$, it suffices to verify that $\subseteq$ and $\supseteq$ both hold. That is:

- every element of the form xh_1yh_2 can be written as xyh for some $h \in H$.
- every element of the form xyh can be written as xh_1yh_2 for some $h_1, h_2 \in H$.

Note that one containment is trivial. This will be left for homework.

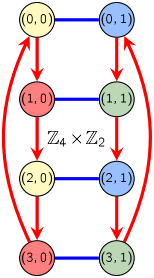
(One last word on quotients)

Remark

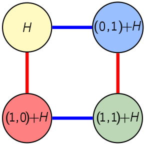
Do you think the following should be true or false, for subgroups H and K?

1. Does $H \cong K$ imply $G/H \cong G/K$?
2. Does $G/H \cong G/K$ imply $H \cong K$?
3. Does $H \cong K$ and $G_1/H \cong G_2/K$ imply $G_1 \cong G_2$?

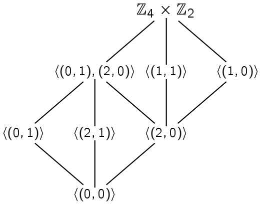
All are false. Counterexamples for all of these can be found using the group $G = \mathbb{Z}_4 \times \mathbb{Z}_2$:



$\mathbb{Z}_4 \times \mathbb{Z}_2 / \langle (2,0) \rangle$



	H	(1,0)+H	(0,1)+H	(1,1)+H
H	H	(1,0)+H	(0,1)+H	(1,1)+H
(1,0)+H	(1,0)+H	H	(1,1)+H	(0,1)+H
(0,1)+H	(0,1)+H	(1,1)+H	H	(1,0)+H
(1,1)+H	(1,1)+H	(0,1)+H	(1,0)+H	H



The end!