Chapter 7: Products and quotients

Matthew Macauley

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

Math 4120, Spring 2014

Overview

In the previous chapter, we looked inside groups for smaller groups lurking inside.

Exploring the subgroups of a group gives us insight into the group's internal structure.

There are two main topics that we will discuss in this chapter.

1. direct products: a method for making *larger* groups from smaller groups.
2. quotients: a method for making *smaller* groups from larger groups.

Before we begin, we'll note that we can *always* form a direct product of two groups.

In constrast, we cannot always take the quotient of two groups. In fact, quotients are restricted to some pretty specific circumstances, as we shall see.

Direct products, algebraically

It is easiest to think of direct product of groups algebraically, rather than visually.

If A and B are groups, there is a natural group structure on the set

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Definition

The **direct product** of groups A and B consists of the set $A \times B$, and the group operation is done component-wise: if $(a, b), (c, d) \in A \times B$, then

$$(a, b) * (c, d) = (ac, bd).$$

We call A and B the factors of the direct product.

Note that the binary operations on A and B could be different. One might be $*$ and the other $+$.

For example, in $D_3 \times \mathbb{Z}_4$:

$$(r^2, 1) * (fr, 3) = (r^2 fr, 1 + 3) = (rf, 0).$$

These elements do *not* commute:

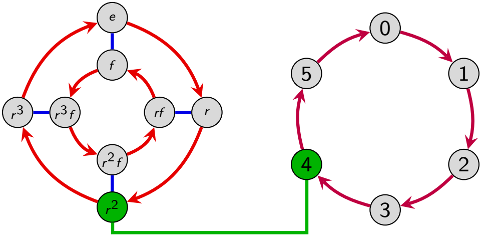
$$(fr, 3) * (r^2, 1) = (fr^3, 3 + 1) = (f, 0).$$

Direct products, visually

Here's one way to think of the direct product of two cyclic groups, say $\mathbb{Z}_n \times \mathbb{Z}_m$: Imagine a slot machine with two wheels, one with n spaces (numbered 0 through $n-1$) and the other with m spaces (numbered 0 through $m-1$).

The actions are: spin one or both of the wheels. Each action can be labeled by where we end up on each wheel, say (i, j).

Here is an example for a more general case: the element $(r^2, 4)$ in $D_4 \times \mathbb{Z}_6$.



Key idea

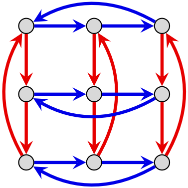
The direct product of two groups joins them so they act independently of each other.

Cayley diagrams of direct products

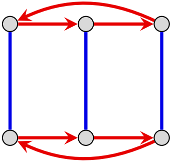
Remark

Just because a group is not written with $\times$ doesn't mean that there isn't some hidden direct product structure lurking. For example, V_4 is really just $C_2 \times C_2$.

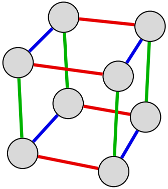
Here are some examples of direct products:



$C_3 \times C_3$



$C_3 \times C_2$



$C_2 \times C_2 \times C_2$

Even more surprising, the group $C_3 \times C_2$ is actually isomorphic to the cyclic group C_6!

Indeed, the Cayley diagram for C_6 using generators r^2 and r^3 is the same as the Cayley diagram for $C_3 \times C_2$ above.

We'll understand this better in Chapter 8 when we study homomorphisms. For now, we will focus our attention on direct products.

Cayley diagrams of direct products

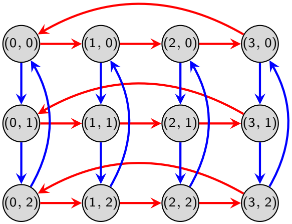
Let e_A be the identity of A and e_B the identity of B.

Given a Cayley diagram of A with generators $a_1, \dots, a_k$, and a Cayley diagram of B with generators $b_1, \dots, b_\ell$, we can create a Cayley diagram for $A \times B$ as follows:

- Vertex set: $\{(a, b) \mid a \in A,\ b \in B\}$.
- Generators: $(a_1, e_b), \dots, (a_k, e_b)$ and $(e_a, b_1), \dots, (e_k, b_\ell)$.

Frequently it is helpful to arrange the vertices in a rectangular grid.

For example, here is a Cayley diagram for the group $\mathbb{Z}_4 \times \mathbb{Z}_3$:



What are the subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_3$? There are six (did you find them all?), they are:

$$\mathbb{Z}_4 \times \mathbb{Z}_3, \qquad \{0\} \times \{0\}, \qquad \{0\} \times \mathbb{Z}_3, \qquad \mathbb{Z}_4 \times \{0\}, \qquad \mathbb{Z}_2 \times \mathbb{Z}_3, \qquad \mathbb{Z}_2 \times \{0\}.$$

Subgroups of direct products

Remark

If $H \leq A$, and $K \leq B$, then $H \times K$ is a subgroup of $A \times B$.

For $\mathbb{Z}_4 \times \mathbb{Z}_3$, *all* subgroups had this form. However, this is not always true.

For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is really just V_4. Since $\mathbb{Z}_2$ has two subgroups, the following four sets are subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$:

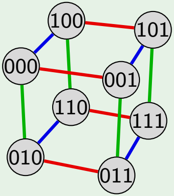
$$\mathbb{Z}_2 \times \mathbb{Z}_2, \qquad \{0\} \times \{0\}, \qquad \mathbb{Z}_2 \times \{0\} = \langle (1,0) \rangle, \qquad \{0\} \times \mathbb{Z}_2 = \langle (0,1) \rangle.$$

However, one subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is missing from this list: $\langle (1,1) \rangle = \{(0,0),(1,1)\}$.

Exercise

What are the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$?

Here is a Cayley diagram, writing the elements of the product as abc rather than (a,b,c).



Did you find all 16 subgroups?

Direct products, visually

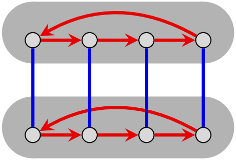
It's not needed, but one can construct the Cayley diagram of a direct product using the following "inflation" method.

Inflation algorithm

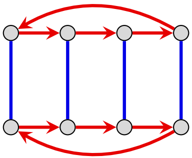
To make a Cayley diagram of $A \times B$ from the Cayley diagrams of A and B:

1. Begin with the Cayley diagram for A.
2. Inflate each node, and place in it a copy of the Cayley diagram for B. (Use different colors for the two Cayley diagrams.)
3. Remove the (inflated) nodes of A while using the arrows of A to connect corresponding nodes from each copy of B. That is, remove the A diagram but treat its arrows as a blueprint for how to connect corresponding nodes in the copies of B.

Cyclic group $\mathbb{Z}_2$



each node contains a copy of $\mathbb{Z}_4$



direct product group $\mathbb{Z}_4 \times \mathbb{Z}_2$

Properties of direct products

Recall the following definition from the end of the previous chapter.

Definition

A subgroup $H < G$ is normal if $xH = Hx$ for all $x \in G$. We denote this by $H \lhd G$.

Assuming A and B are not trivial, the direct product $A \times B$ has *at least* four normal subgroups:

$$\{e_A\} \times \{e_B\}\,, \qquad A \times \{e_B\}\,, \qquad \{e_A\} \times B\,, \qquad A \times B\,.$$

Sometimes we "abuse notation" and write $A \lhd A \times B$ and $B \lhd A \times B$ for the middle two. (Technically, A and B are not even subsets of $A \times B$.)

Here's another observation: "A-arrows" are independent of "B-arrows."

Observation

In a Cayley diagram for $A \times B$, following "A-arrows" neither impacts or is impacted by the location in group B.

Algebraically, this is just saying that $(a, e_b) * (e_a, b) = (a, b) = (e_a, b) * (a, e_b)$.

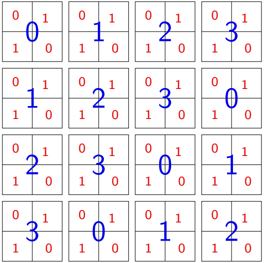
Multiplication tables of direct products

Direct products can also be visualized using multiplication tables.

However, the general process should be clear after seeing the following example; constructing the table for the group $\mathbb{Z}_4 \times \mathbb{Z}_2$:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

multiplication table for the group $\mathbb{Z}_4$



inflate each cell to contain a copy of the multiplication table of $\mathbb{Z}_2$

(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)
(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)
(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)
(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,0)
(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)

join the little tables and element names to form the direct product table for $\mathbb{Z}_4 \times \mathbb{Z}_2$

Quotients

Direct products make larger groups from smaller groups. It is a way to *multiply* groups.

The opposite procedure is called taking a quotient. It is a way to *divide* groups.

Unlike what we did with direct products, we will first describe the quotient operation using Cayley diagrams, and then formalize it algebraically explore properties of the resulting group.

Definition

To divide a group G by one of its subgroups H, follow these steps:

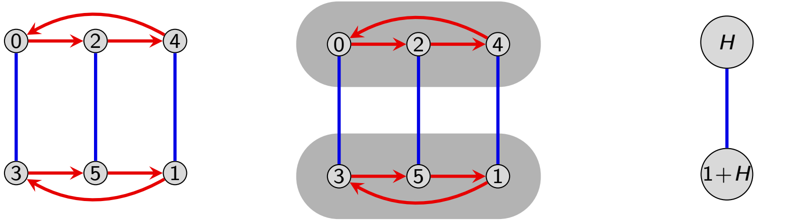
1. Organize a Cayley diagram of G by H (so that we can "see" the subgroup H in the diagram for G).
2. Collapse each left coset of H into one large node. Unite those arrows that now have the same start and end nodes. This forms a new diagram with fewer nodes and arrows.
3. IF (and *only* if) the resulting diagram is a Cayley diagram of a group, you have obtained the quotient group of G by H, denoted G/H (say: "G mod H".) If not, then G cannot be divided by H.

An example: $\mathbb{Z}_3 < \mathbb{Z}_6$

Consider the group $G = \mathbb{Z}_6$ and its normal subgroup $H = \langle 2 \rangle = \{0, 2, 4\}$.

There are two (left) cosets: $H = \{0, 2, 4\}$ and $1 + H = \{1, 3, 5\}$.

The following diagram shows how to take a quotient of $\mathbb{Z}_6$ by H.



$\mathbb{Z}_6$ organized by the subgroup $H = \langle 2 \rangle$

Left cosets of H are near each other

Collapse cosets into single nodes

In this example, the resulting diagram *is* a Cayley diagram. So, we *can* divide $\mathbb{Z}_6$ by $\langle 2 \rangle$, and we see that $\mathbb{Z}_6/H$ is isomorphic to $\mathbb{Z}_2$.

We write this as $\mathbb{Z}_6/H \cong \mathbb{Z}_2$.

A few remarks

- Step 3 of the Definition says "IF the new diagram is a Cayley diagram ..." Sometimes it won't be, in which case there is no quotient.
- The elements of G/H are the cosets of H. Asking if G/H exists amounts to asking if the set of left (or right) cosets of H forms a group. (More on this later.)
- In light of this, given *any* subgroup $H < G$ (normal or not), we will let

  $$G/H := \{gH \mid g \in G\}$$

  denote the set of left cosets of H in G.
- Not surprisingly, if $G = A \times B$ and we divide G by A (technically $A \times \{e\}$), the quotient group is B. (We'll see why shortly).

Caveat!

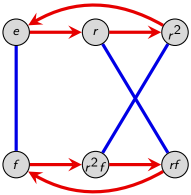
The converse of the previous statement is generally *not* true. That is, if G/H is a group, then G is in general *not* a direct product of H and G/H.

An example: $C_3 < D_3$

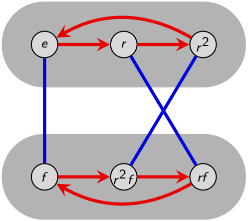
Consider the group $G = D_3$ and its normal subgroup $H = \langle r \rangle \cong C_3$.

There are two (left) cosets: $H = \{e, r, r^2\}$ and $fH = \{f, rf, r^2f\}$.

The following diagram shows how to take a quotient of D_3 by H.



D_3 organized by the subgroup $H = \langle r \rangle$



Left cosets of H are near each other

Collapse cosets into single nodes

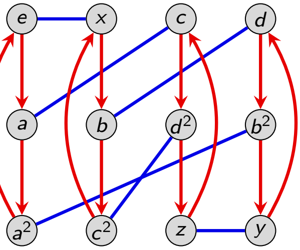
The result is a Cayley diagram for C_2, thus

$$D_3/H \cong C_2 . \qquad \text{However...} \qquad C_3 \times C_2 \not\cong D_3 .$$

Note that $C_3 \times C_2$ is abelian, but D_3 is not.

Example: $G = A_4$ and $H = \langle x, z \rangle \cong V_4$

Consider the following Cayley diagram for $G = A_4$ using generators $\langle a, x \rangle$.

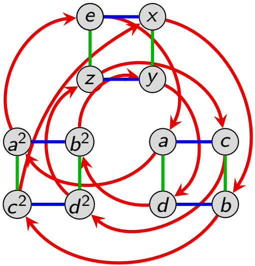


Consider $H = \langle x, z \rangle = \{e, x, y, z\} \cong V_4$. This subgroup is not "visually obvious" in this Cayley diagram.

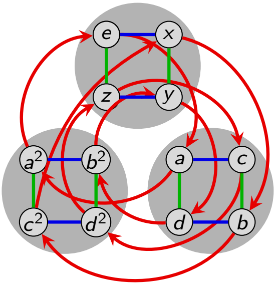
Let's add z to the generating set, and consider the resulting Cayley diagram.

Example: $G = A_4$ and $H = \langle x, z \rangle \cong V_4$

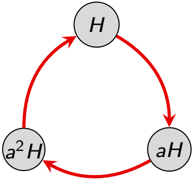
Here is a Cayley diagram for A_4 (with generators x, z, and a), organized by the subgroup $H = \langle x, z \rangle$ which allows us to see the left cosets of H clearly.



A_4 organized by the subgroup $H = \langle x, z \rangle$



Left cosets of H are near each other



Collapse cosets into single nodes

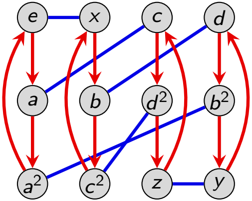
The resulting diagram is a Cayley diagram! Therefore, $A_4/H \cong C_3$. However, A_4 is *not* isomorphic to the (abelian) group $V_4 \times C_3$.

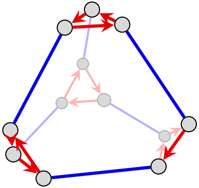
Example: $G = A_4$ and $H = \langle a \rangle \cong C_3$

Let's see an example where we cannot divide G by a particular subgroup H.

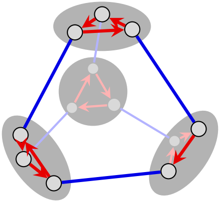
Consider the subgroup $H = \langle a \rangle \cong C_3$ of A_4.

Do you see what will go wrong if we try to divide A_4 by $H = \langle a \rangle$?

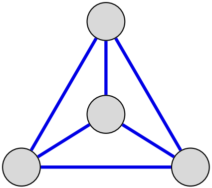




A_4 organized by the subgroup $H = \langle a \rangle$



Left cosets of H are near each other



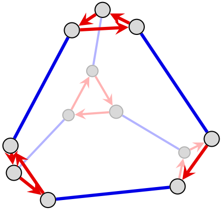
Collapse cosets into single nodes

This resulting diagram is *not* a Cayley diagram! There are multiple outgoing blue arrows from each node.

When can we divide G by a subgroup H?

Consider $H = \langle a \rangle \leq A_4$ again.

The left cosets are easy to spot.



Remark

The right cosets are *not* the same as the left cosets! The blue arrows out of any single coset scatter the nodes.

Thus, $H = \langle a \rangle$ is *not* normal in A_4.

If we took the effort to check our first 3 examples, we would find that in each case, the left cosets and right cosets coincide. In those examples, G/H existed, and H was normal in G.

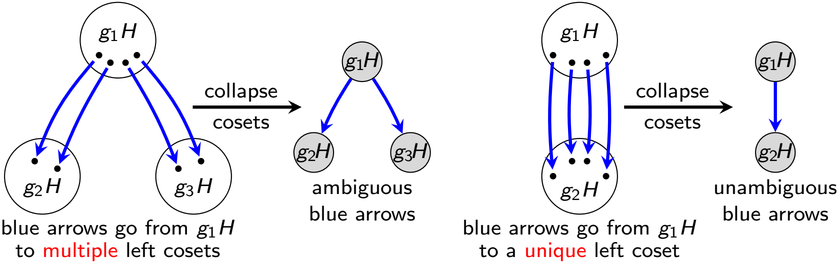
However, these 4 examples do not constitute a proof; they only provide evidence that the claim is true.

When can we divide G by a subgroup H?

Let's try to gain more insight. Consider a group G with subgroup H. Recall that:

- each **left coset** gH is the set of nodes that the H-arrows can reach from g (which looks like a copy of H at g);
- each **right coset** Hg is the set of nodes that the g-arrows can reach from H.

The following figure depicts the potential ambiguity that may arise when cosets are collapsed in the sense of our quotient definition.



The action of the blue arrows above illustrates multiplication of a left coset on the right by some element. That is, the picture shows how left and right cosets *interact*.

When can we divide G by a subgroup H?

When H is normal, $gH = Hg$ for all $g \in G$.

In this case, to whichever coset one g arrow leads from H (the left coset), *all* g *arrows lead unanimously and unambiguously* (because it is also a right coset Hg).

Thus, in this case, collapsing the cosets is a *well-defined* operation.

Finally, we have an answer to our original question of when we can take a quotient.

Quotient theorem

If $H < G$, then the quotient group G/H can be constructed *if and only if* $H \lhd G$.

To summarize our "visual argument": The quotient process succeeds iff the resulting diagram is a valid Cayley diagram.

Nearly all aspects of valid Cayley diagrams are guaranteed by the quotient process: Every node has exactly one incoming and outgoing edge of each color, because $H \lhd G$. The diagram is regular too.

Though it's convincing, this argument isn't quite a formal proof; we'll do a rigorous algebraic proof next.

Quotient groups, algebraically

To prove the Quotient Theorem, we need to describe the quotient process algebraically.

Recall that even if H is not normal in G, we will still denote the set of left cosets of H in G by G/H.

Quotient theorem (restated)

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

This means there is a well-defined binary operation on the set of cosets. But how do we "multipy" two cosets?

If aH and bH are left cosets, define

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

Clearly, G/H is closed under this operation. But we also need to verify that this definition is well-defined.

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

Quotient groups, algebraically

Lemma

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

$$\text{if } a_1H = a_2H \text{ and } b_1H = b_2H, \text{ then } a_1H \cdot b_1H = a_2H \cdot b_2H.$$

Proof

Suppose that $H \lhd G$, $a_1H = a_2H$ and $b_1H = b_2H$. Then

$$\begin{aligned}
a_1H \cdot b_1H &= a_1b_1H && \text{(by definition)} \\
&= a_1(b_2H) && (b_1H = b_2H \text{ by assumption}) \\
&= (a_1H)b_2 && (b_2H = Hb_2 \text{ since } H \lhd G) \\
&= (a_2H)b_2 && (a_1H = a_2H \text{ by assumption}) \\
&= a_2b_2H && (b_2H = Hb_2 \text{ since } H \lhd G) \\
&= a_2H \cdot b_2H && \text{(by definition)}
\end{aligned}$$

Thus, the binary operation on G/H is well-defined. $\square$

Quotient groups, algebraically

Quotient theorem (restated)

When $H \lhd G$, 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 $aH \in G/H$,

$$aH \cdot H = aeH = aH = eaH = H \cdot aH\,.$$

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

$$aH \cdot a^{-1}H = eH = a^{-1}H \cdot aH\,.$$

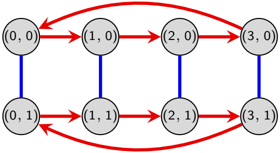
Closure. This is immediate, because $aH \cdot bH = abH$ is another coset in G/H. $\square$

Properties of quotients

Question

If H and K are subgroups and $H \cong K$, then are G/H and G/K isomorphic?

For example, here is a Cayley diagram for the group $\mathbb{Z}_4 \times \mathbb{Z}_2$:



It is visually obvious that the quotient of $\mathbb{Z}_4 \times \mathbb{Z}_2$ by the subgroup $\langle (0,1) \rangle \cong \mathbb{Z}_2$ is the group $\mathbb{Z}_4$.

The quotient of $\mathbb{Z}_4 \times \mathbb{Z}_2$ by the subgroup $\langle (2,0) \rangle \cong \mathbb{Z}_2$ is a bit harder to see. Algebraically, it consists of the cosets

$$\langle (2,0) \rangle, \qquad (1,0) + \langle (2,0) \rangle, \qquad (0,1) + \langle (2,0) \rangle, \qquad (1,1) + \langle (2,0) \rangle.$$

It is now apparent that this group is isomorphic to V_4.

Thus, the answer to the question above is "no." Surprised?

Normalizers

Question

If $H < G$ but H is *not* normal, can we measure "how far" H is from being normal?

Recall that $H \lhd G$ iff $gH = Hg$ for all $g \in G$. So, one way to answer our question is to check how many $g \in G$ satisfy this requirement. Imagine that each $g \in G$ is voting as to whether H is normal:

$gH = Hg$ "yea" $\qquad$ $gH \neq Hg$ "nay"

At a *minimum*, every $g \in H$ votes "yea." (Why?)

At a *maximum*, every $g \in G$ could vote "yea," but this only happens when H really is normal.

There can be levels between these 2 extremes as well.

Definition

The set of elements in G that vote in favor of H's normality is called the normalizer of H in G, denoted $N_G(H)$. That is,

$$N_G(H) = \{g \in G : gH = Hg\} = \{g \in G : gHg^{-1} = H\}.$$

Normalizers

Let's explore some possibilities for what the normalizer of a subgroup can be. In particular, is it a subgroup?

Observation 1

If $g \in N_G(H)$, then $gH \subseteq N_G(H)$.

Proof

If $gH = Hg$, then $gH = bH$ for all $b \in gH$. Therefore, $bH = gH = Hg = Hb$. □

The deciding factor in how a left coset votes is whether it is a right coset (members of gH vote as a block – exactly when $gH = Hg$).

Observation 2

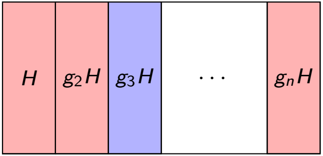
$|N_G(H)|$ is a multiple of $|H|$.

Proof

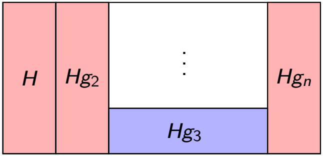
By Observation 1, $N_G(H)$ is made up of whole (left) cosets of H, and all (left) cosets are the same size and disjoint. □

Normalizers

Consider a subgroup $H \leq G$ of index n. Suppose that the left and right cosets partition G as shown below:



Partition of G by the left cosets of H



Partition of G by the right cosets of H

The cosets H, and $g_2H = Hg_2$, and $g_nH = Hg_n$ all vote "yea".

The left coset g_3H votes "nay" because $g_3H \neq Hg_3$.

Assuming all other cosets vote "nay", the normalizer of H is

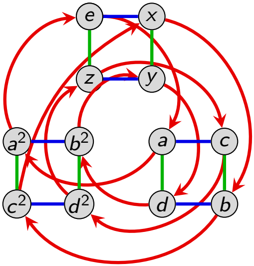
$$N_G(H) = H \cup g_2H \cup g_nH\,.$$

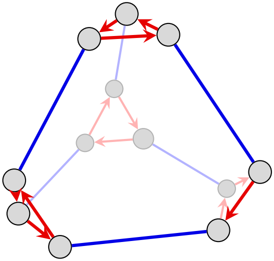
In summary, the two "extreme cases" for $N_G(H)$ are:

- $N_G(H) = G$: iff H is a normal subgroup
- $N_G(H) = H$: H is as "unnormal as possible"

An example: A_4

We saw earlier that $H = \langle x, z \rangle \lhd A_4$. Therefore, $N_{A_4}(H) = A_4$.





At the other extreme, consider $\langle a \rangle < A_4$ again, which is as far from normal as it can possibly be: $\langle a \rangle \not\lhd A_4$.

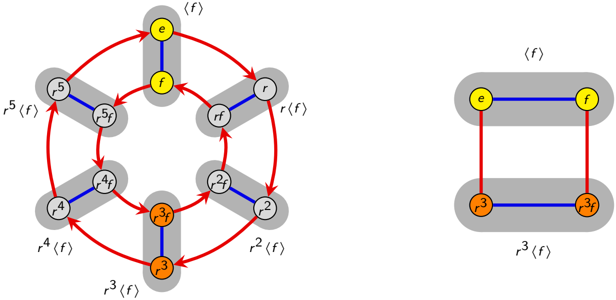
No right coset of $\langle a \rangle$ coincides with a left coset, other than $\langle a \rangle$ itself. Thus, $N_{A_4}(\langle a \rangle) = \langle a \rangle$.

Observation 3

In the Cayley diagram of G, the normalizer of H consists of the copies of H that are connected to H by unanimous arrows.

How to spot the normalizer in the Cayley diagram

The following figure depicts the six left cosets of $H = \langle f \rangle = \{e, f\}$ in D_6.



Note that $r^3 H$ is the *only* coset of H (besides H, obviously) that cannot be reached from H by more than one element of D_6.

Thus, $N_{D_6}(\langle f \rangle) = \langle f \rangle \cup r^3 \langle f \rangle = \{e, f, r^3, r^3 f\} \cong V_4$.

Observe that the normalizer is also a subgroup satisfying: $\langle f \rangle \lneq N_{D_6}(\langle f \rangle) \lneq D_6$.

Do you see the pattern for $N_{D_n}(\langle f \rangle)$? (It depends on whether n is even or odd.)

Normalizers are subgroups!

Theorem 7.7

For any $H < G$, we have $N_G(H) < G$.

Proof (different than VGT!)

Recall that $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$; "*the set of elements that normalize H.*" We need to verify three properties of $N_G(H)$:

(i) Contains the identity;

(ii) Inverses exist;

(iii) Closed under the binary operation.

Identity. Naturally, $eHe^{-1} = \{ehe^{-1} \mid h \in H\} = H$.

Inverses. Suppose $g \in N_G(H)$, which means $gHg^{-1} = H$. We need to show that $g^{-1} \in N_G(H)$. That is, $g^{-1}H(g^{-1})^{-1} = g^{-1}Hg = H$. Indeed,

$$g^{-1}Hg = g^{-1}(gHg^{-1})g = eHe = H\,.$$

Normalizers are subgroups!

Proof (cont.)

Closure. Suppose $g_1, g_2 \in N_G(H)$, which means that $g_1Hg_1^{-1} = H$ and $g_2Hg_2^{-1} = H$. We need to show that $g_1g_2 \in N_G(H)$.

$$(g_1g_2)H(g_1g_2)^{-1} = g_1g_2Hg_2^{-1}g_1^{-1} = g_1(g_2Hg_2^{-1})g_1^{-1} = g_1Hg_1^{-1} = H\,.$$

Since $N_G(H)$ contains the identity, every element has an inverse, and is closed under the binary operation, it is a (sub)group! □

Corollary

Every subgroup is normal in its normalizer:

$$H \lhd N_G(H) \leq G\,.$$

Proof

By definition, $gH = Hg$ for all $g \in N_G(H)$. Therefore, $H \lhd N_G(H)$. □

Conjugacy classes

Recall that for $H \leq G$, the conjugate subgroup of H by a fixed $g \in G$ is

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

Additionally, H is normal iff $gHg^{-1} = H$ for all $g \in G$.

We can also fix the element we are conjugating. Given $x \in G$, we may ask:

"*which elements can be written as gxg^{-1} for some $g \in G$?*"

The set of all such elements in G is called the conjugacy class of x, denoted $\mathrm{cl}_G(x)$. Formally, this is the set

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

Remarks

- In any group, $\mathrm{cl}_G(e) = \{e\}$, because $geg^{-1} = e$ for any $g \in G$.
- If x and g commute, then $gxg^{-1} = x$. Thus, when computing $\mathrm{cl}_G(x)$, we only need to check gxg^{-1} for those $g \in G$ that *do not commute* with x.
- Moreover, $\mathrm{cl}_G(x) = \{x\}$ iff x commutes with everything in G. (Why?)

Conjugacy classes

Lemma

Conjugacy is an equivalence relation.

Proof

- *Reflexive*: $x = exe^{-1}$.
- *Symmetric*: $x = gyg^{-1} \Rightarrow y = g^{-1}xg$.
- *Transitive*: $x = gyg^{-1}$ and $y = hzh^{-1} \Rightarrow x = (gh)z(gh)^{-1}$. □

Since conjugacy is an equivalence relation, it partitions the group G into equivalence classes (conjugacy classes).

Let's compute the conjugacy classes in D_4. We'll start by finding $\mathrm{cl}_{D_4}(r)$. Note that we only need to compute grg^{-1} for those g that *do not* commute with r:

$$frf^{-1} = r^3, \qquad (rf)r(rf)^{-1} = r^3, \qquad (r^2f)r(r^2f)^{-1} = r^3, \qquad (r^3f)r(r^3f)^{-1} = r^3.$$

Therefore, the conjugacy class of r is $\mathrm{cl}_{D_4}(r) = \{r, r^3\}$.

Since conjugacy is an equivalence relation, $\mathrm{cl}_{D_4}(r^3) = \mathrm{cl}_{D_4}(r) = \{r, r^3\}$.

Conjugacy classes in D_4

To compute $\mathrm{cl}_{D_4}(f)$, we don't need to check e, r^2, f, or $r^2 f$, since these all commute with f:

$$rfr^{-1} = r^2 f, \qquad r^3 f (r^3)^{-1} = r^2 f, \qquad (rf)f(rf)^{-1} = r^2 f, \qquad (r^3 f)f(r^3 f)^{-1} = r^2 f\,.$$

Therefore, $\mathrm{cl}_{D_4}(f) = \{f, r^2 f\}$.

What is $\mathrm{cl}_{D_4}(rf)$? Note that it has size greater than 1 because rf does not commute with everything in D_4.

It also *cannot* contain elements from the other conjugacy classes. The only element left is $r^3 f$, so $\mathrm{cl}_{D_4}(rf) = \{rf, r^3 f\}$.

The "Class Equation", visually:
Partition of D_4 by its
conjugacy classes

e	r	f	$r^2 f$
r^2	r^3	rf	$r^3 f$

We can write $D_4 = \underbrace{\{e\} \cup \{r^2\}}_{\text{these commute with everything in } D_4} \cup \{r, r^3\} \cup \{f, r^2 f\} \cup \{r, r^3 f\}$.

The class equation

Definition

The center of G is the set $Z(G) = \{z \in G \mid gz = zg, \ \forall g \in G\}$.

Observation

$\text{cl}_G(x) = \{x\}$ if and only if $x \in Z(G)$.

Proof

Suppose x is in its own conjugacy class. This means that

$$\text{cl}_G(x) = \{x\} \iff gxg^{-1} = x, \ \forall g \in G \iff gx = xg, \ \forall g \in G \iff x \in Z(G).$$

$\square$

The Class Equation

For any finite group G,

$$|G| = |Z(G)| + \sum |\text{cl}_G(x_i)|$$

where the sum is taken over distinct conjugacy classes of size greater than 1.

More on conjugacy classes

Proposition

Every normal subgroup is the union of conjugacy classes.

Proof

Suppose $n \in N \lhd G$. Then $gng^{-1} \in gNg^{-1} = N$, thus if $n \in N$, its entire conjugacy class $\mathrm{cl}_G(n)$ is contained in N as well. $\square$

Proposition

Conjugate elements have the same order.

Proof

Consider x and $y = gxg^{-1}$.

If $x^n = e$, then $(gxg^{-1})^n = (gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1}) = gx^ng^{-1} = geg^{-1} = e$. Therefore, $|x| \geq |gxg^{-1}|$.

Conversely, if $(gxg^{-1})^n = e$, then $gx^ng^{-1} = e$, and it must follow that $x^n = e$. Therefore, $|x| \leq |gxg^{-1}|$. $\square$

Conjugacy classes in D_6

Let's determine the conjugacy classes of $D_6 = \langle r, f \mid r^6 = e,\ f^2 = e,\ r^i f = f r^{-i} \rangle$.

The center of D_6 is $Z(D_6) = \{e, r^3\}$; these are the *only* elements in size-1 conjugacy classes.

The only two elements of order 6 are r and r^5; so we must have $\mathrm{cl}_{D_6}(r) = \{r, r^5\}$.

The only two elements of order 3 are r^2 and r^4; so we must have $\mathrm{cl}_{D_6}(r^2) = \{r^2, r^4\}$.

Let's compute the conjugacy class of a reflection $r^i f$. We need to consider two cases; conjugating by r^j and by $r^j f$:

- $r^j (r^i f) r^{-j} = r^j r^i r^j f = r^{i+2j} f$
- $(r^j f)(r^i f)(r^j f)^{-1} = (r^j f)(r^i f) f r^{-j} = r^j f r^{i-j} = r^j r^{j-i} f = r^{2j-i} f$.

Thus, $r^i f$ and $r^k f$ are conjugate iff i and k are both even, or both odd.

The Class Equation, visually:
Partition of D_6 by its
conjugacy classes

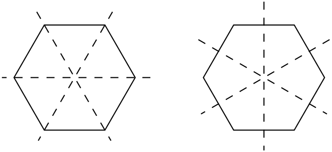
e	r	r^2	f	$r^2 f$	$r^4 f$
r^3	r^5	r^4	rf	$r^3 f$	$r^5 f$

Conjugacy "preserves structure"

Think back to linear algebra. Two matrices A and B are *similar* (=conjugate) if $A = PBP^{-1}$.

Conjugate matrices have the same eigenvalues, eigenvectors, and determinant. In fact, they represent the *same linear map*, but under a change of basis.

If n is even, then there are two "types" of reflections of an n-gon: the axis goes through two corners, or it bisects a pair of sides.



Notice how in D_n, conjugate reflections had the same "type." Do you have a guess of what the conjugacy classes of reflections are in D_n when n is odd?

Also, conjugate rotations in D_n had the same rotating angle, but in the opposite direction (e.g., r^k and r^{n-k}).

Next, we will look at conjugacy classes in the symmetric group S_n. We will see that conjugate permutations have "the same structure."

Cycle type and conjugacy

Definition

Two elements in S_n have the same cycle type if when written as a product of disjoint cycles, there are the same number of length-k cycles for each k.

We can write the cycle type of a permutation $\sigma \in S_n$ as a list $c_1, c_2, \dots, c_n$, where c_i is the number of cycles of length i in σ.

Here is an example of some elements in S_9 and their cycle types.

- $(1\ 8)\,(5)\,(2\ 3)\,(4\ 9\ 6\ 7)$ has cycle type 1,2,0,1.
- $(1\ 8\ 4\ 2\ 3\ 4\ 9\ 6\ 7)$ has cycle type 0,0,0,0,0,0,0,0,1.
- $e = (1)(2)(3)(4)(5)(6)(7)(8)(9)$ has cycle type 9.

Theorem

Two elements $g, h \in S_n$ are conjugate if and only if they have the same cycle type.

Big idea

Conjugate permutations have the same structure. Such permutations are *the same up to renumbering*.

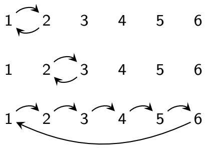
An example

Consider the following permutations in $G = S_6$:

$g = (1\ 2)$

$h = (2\ 3)$

$r = (1\ 2\ 3\ 4\ 5\ 6)$



Since g and h have the same cycle type, they are conjugate:

$$(1\ 2\ 3\ 4\ 5\ 6)\,(2\ 3)\,(1\ 6\ 5\ 4\ 3\ 2) = (1\ 2)\,.$$

Here is a visual interpretation of $g = rhr^{-1}$: