Visual Group Theory

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

Introduction

1. Welcome to VGT Summer 2009!
2. Introductions
3. Discussion of syllabus
4. Expectations and general game plan
5. My web page

   http://oz.plymouth.edu/~dcernst
6. Web page for textbook (including errata)

   http://web.bentley.edu/empl/c/ncarter/vgt/
7. Group Explorer

   http://groupexplorer.sourceforge.net/
8. OK, let's get started!

Chapter 1: What is a group?

Dana C. Ernst

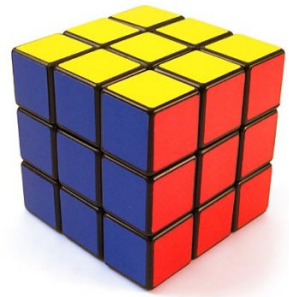
Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

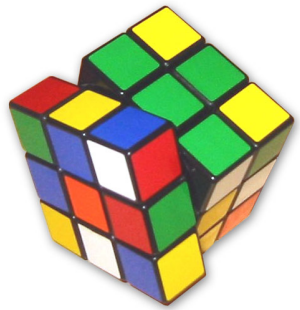
Rubik's Cube

Our introduction to group theory will begin by discussing the famous Rubik's Cube.

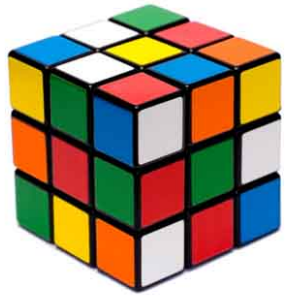
- Invented in 1974 by Ernö Rubik of Budapest, Hungary
- The cube comes out of the box in the solved position:



- But then we can scramble it up by consecutively rotating one of its 6 faces:



- The result might look something like this:



- The goal is to return the cube to its original solved position, again by consecutively rotating one of the 6 faces.

Since Rubik's Cube does not seem to require any skill with numbers to solve it, you may be inclined to think that this puzzle is not mathematical.

Group theory is not primarily about numbers, but rather about patterns and symmetry; something the Rubik's Cube possesses in abundance.

Let's explore the Rubik's Cube in more detail. In particular, let's see if we can identify some key features that will identify the boundaries of our study.

First, some questions to ponder:

- How did we scramble up the cube in the first place? How do we go about unscrambling the cube?
- In particular, what actions do we *need* in order to scramble and unscramble the cube? (There are many correct answers.)
- How is Rubik's Cube different from chess?
- How is Rubik's Cube different from poker?

4 key observations:

Observation 1.1

There is a predefined list of moves that never changes.

Observation 1.2

Every move is reversible.

Observation 1.3

Every move is deterministic.

Observation 1.4

Moves can be combined in any sequence.

We could add more to our list, but as we shall see, these 4 observations encompass the aspects of the mathematical objects that we wish to study.

Group theory studies the mathematical consequences of these 4 observations, which in turn will help us answer interesting questions about symmetrical objects.

Rules of a group

Instead of considering our 4 observations as descriptions of Rubik's Cube, let's rephrase them as rules (axioms) that will define the boundaries of our objects of study.

Advantages of our endeavor:

1. We make it clear what it is we want to explore.
2. Helps us speak the same language, so that we know we are discussing the same objects (trapezoids...).
3. The rules provide the groundwork for making logical deductions, so that we can discover new facts.

Our rules:

Rule 1.5

There is a predefined list of actions that never changes.

Rule 1.6

Every action is reversible.

Rule 1.7

Every action is deterministic.

Rule 1.8

Any sequence of consecutive actions is also an action.

What changes were made in the rephrasing?

Comments

- We swapped the word *move* for *action*.
- The (usually short) list of actions required by Rule 1.5 is our set of building blocks; called the generators.
- Rule 1.8 tells us that any sequence of the generators is also an action.

Finally, here is our unofficial definition of a group. (We'll make things a bit more rigorous later.)

Definition 1.9

A group is a system or collection of actions satisfying Rules 1.5–1.8.

Group Exercises

OK, let's explore a few more examples.

1. Discuss Exercise 1.1 (see Bob = Back of book) as a large group.
2. In groups of 2–3, complete the following exercises (not collected):
   - Exercise 1.3 (see Bob)
   - Exercise 1.4
3. I'd like two groups to volunteer to discuss their answers to the two previous exercises.
4. Now, mix the groups up, so that no group stays the same. In your new groups, complete Exercise 1.8. I want each group to turn in a complete solution.

Potential quiz questions

Here are some potential questions that I may ask you on tomorrow's quiz at the beginning of class:

1. State our unofficial definition of a group by listing the 4 rules.
2. Define generators.
3. Provide 2 examples of a group. In each case, describe a set of generators.

References

I borrowed images from the following web pages:

- http://www.cunymath.cuny.edu/?page=mm
- http://www.math.cornell.edu/~mec/Winter2009/Lipa/Puzzles/lesson2.html

Chapter 2: What do groups look like?

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

A road map for the Rubik's Cube

There are several solution techniques for the Rubik's Cube. If you do a quick Google search, you'll find several methods for solving the puzzle.

These methods describe a sequence of moves to apply relative to some starting position. In many situations, there may be a shorter sequence of moves that would get you to the solution.

Let's pretend for a moment that we were interested in writing a complete solutions manual for the Rubik's Cube. Let me be more specific about what I mean.

We'd like our solutions manual to have the following properties:

1. Given any scrambled configuration of the cube, there is a unique page in the manual corresponding to that configuration.
2. There is a method for looking up any particular configuration. (The details of how to do this are unimportant.)
3. Along with each configuration, a list of available moves is included. In each case, the page number for the outcome of each move is included and information about whether the corresponding move takes us closer to or farther from the solution.

Let's call our solutions manual the *Big Book*. See Figure 2.1 on page 13 for a picture of what a page in the *Big Book* might look like.

We can think of the *Big Book* as a road map for the Rubik's Cube. Each page says, "you are here" and "if you follow this road, you'll end up over there." In addition, you'll know whether "over there" is where you want to go or not.

Pros of the *Big Book*:

- We can solve any scrambled Rubik's Cube.
- In fact, given any configuration, every possible sequence of moves for solving the cube is listed in the book (long sequences and short sequences).
- The *Big Book* contains complete data on the moves in the Rubik's Cube universe and how they combine.

Cons of the *Big Book*:

- We just took all the fun out of the Rubik's Cube.
- If we had such a book, using it would be fairly cumbersome.
- We can't actually make such a book. Rubik's Cube has more than 4×10^{19} configurations. The paper required to write the book would cover the Earth many times over. The book would require over a billion terabytes of data to store electronically, and no computer in existence can store that much data.

Despite the *Big Book*'s apparent shortcomings, it made for a good thought experiment. The most important thing to get out of this discussion is that the *Big Book* is a map of a group.

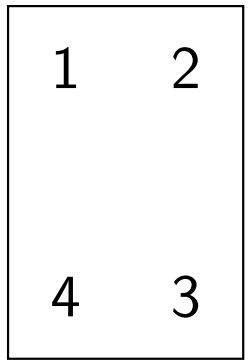
We shall not abandon the mapmaking ideas introduced by our discussion of the *Big Book* simply because the map is too large. We can use the same ideas to map out any group. In fact, we shall frequently do exactly that.

Let's try something simpler...

The Rectangle Puzzle

Here is the Rectangle Puzzle:

- Take a blank sheet of paper (our rectangle) and label as follows:



  This is the solved state of our puzzle.
- The idea of the game is to scramble the puzzle and then find a way to return the rectangle to its solved state.
- We are allowed two moves: horizontal flip and vertical flip, where "horizontal" and "vertical" refer to the motion of your hands, rather than any reference to an axis of reflection.

We'll spend some time in Chapter 3 discussing why these two moves and not some others are the ones that make sense for this game. However, it is worth pointing out that these two moves preserve the orientation of the rectangle. Are there any others that preserve its orientation?

Using only the two valid moves, scramble your rectangle. Any sequence of horizontal and vertical flips will do, but don't do any other types of moves.

Now, again using only our two valid moves, try to return your rectangle to the solved position.

Observations?

Question: do the moves of the Rectangle Puzzle form a group? How can we check?

For reference, here are the rules of a group:

Rule 1.5

There is a predefined list of actions that never changes.

Rule 1.6

Every action is reversible.

Rule 1.7

Every action is deterministic.

Rule 1.8

Any sequence of consecutive actions is also an action.

OK, let's see if we can make a road map for our newly found group.

Using our multiple copies of the rectangle, some colored yarn, and some sticky notes, let's see what we can come up with. (Someone remind me to take a picture when we are done.)

We've just created our first road map of a group! Observations? What sorts of things does the map tell us about the group?

We see that:

- the group has two generators: horizontal flip and vertical flip. Each generator is represented by the two different colors of yarn;
- the group has 4 actions: the "do nothing" action, horizontal flip, vertical flip, and 180° rotation ($r = h \circ v = v \circ h$);
- the map shows us how to get from any one configuration to any other (there may be more than one way to follow the yarn).

It is important to note that how we choose to layout our map is irrelevant. What is important is that the connections between the various states are preserved. However, we will attempt to construct our maps in a pleasing to the eye and symmetrical way.

The official name of the type of group road map that we have just created is Cayley diagram, named after the 19th century British mathematician Arthur Cayley.

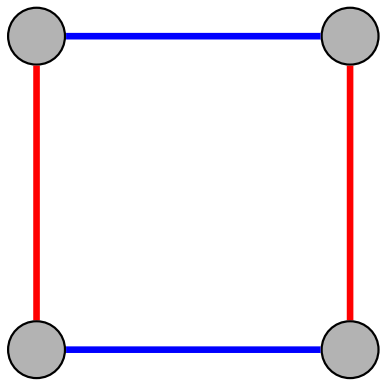
In general, a Cayley diagram consists of nodes that are connected by colored (or labeled) arrows, where

- an arrow of a particular color represents a specific generator;
- each action of the group is represented by a unique node (sometimes we will label nodes by the corresponding action);
- all necessary arrows are present (more on this later).

More on arrows:

- An arrow corresponding to the generator g from node A to node B means that node B is the result of applying the action g to node A.
- If the reverse of applying generator g is the same as g (this happens with horizontal and vertical flips), then we have a 2-way arrow. Our convention will be to drop the tips of the arrows on all 2-way arrows.

Here is one possible representation of the Cayley diagram for our Rectangle Puzzle:



The 2-Light Switch Group

Let's map out another group, which we'll call the 2-Light Switch Group. Here are the details:

- Consider two light switches side by side that both start in the off position.
- We are allowed 2 actions: flip L switch and flip R switch.

Do these actions generate a group?

In small groups, map out the 2-Light Switch Group using paper and yarn just like we did for the Rectangle Puzzle. (I suggest using U and D to denote "light switch up" and "light switch down", respectively.)

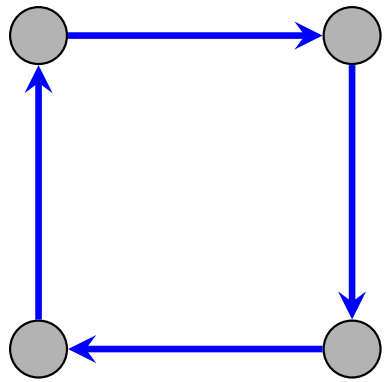
Now, draw the more abstract version of the Cayley diagram. What do you notice?

What we should notice is that the Cayley diagram for the Rectangle Puzzle and the Cayley diagram for the 2-Light Switch Group are essentially the same. The 4 rectangle configurations correspond to the 4 light switch configurations. Horizontal flip and vertical flip correspond to flip L switch and flip R switch.

Although these 2 groups are superficially different, the Cayley diagrams help us see that they have the same structure. (The fancy phrase for this phenomenon is that the "two groups are isomorphic"; more on this later.)

Any group with the same Cayley diagram as the Rectangle Puzzle and the 2-Light Switch Group is called the Klein 4-group, and is denoted by V_4 for *vierergruppe*, "four-group" in German. It is named after the mathematician Felix Christian Klein.

It is important to point out that the number of different types (i.e., colors) of arrows is important. For example, the following Cayley diagram does not represent V_4.



Warning: it is possible for two groups to have different looking Cayley diagrams yet really be the "same." (We'll talk more about what "same" means later.)

More Group Exercises

Let's explore a few more examples.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 2.1 (see Bob)
   - Exercise 2.3 (see Bob)
   - Exercise 2.5
   - Exercise 2.8 (see Bob)
   - Exercise 2.10
   - Exercise 2.13 (see Bob)
2. I'd like each group to present their solution to one of the problems above.
3. Now, complete Exercise 2.18. I want each group to turn in a complete solution.

Potential quiz questions

Here are some potential questions that I may ask you on tomorrow's quiz at the beginning of class:

1. What do the arrows represent in a Cayley diagram?
2. What do the nodes represent in a Cayley diagram?
3. Draw 2 different Cayley diagrams and describe a specific set of actions (i.e., generators) that would yield the corresponding diagrams.

Chapter 3: Why study groups?

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

In the previous 2 chapters, we introduced groups and explored a few basic examples. In this chapter, we shall discuss a few practical (yet not necessarily complicated) applications.

We will see applications of group theory in 3 areas:

1. science
2. art
3. mathematics

Our choice of examples is influenced by how well they illustrate the material rather than how useful they are.

Groups of symmetries

Intuitively, something is symmetrical when it looks the same from more than one point of view. Can you think of an object that you think exhibits symmetry? Have we already seen some?

How does symmetry relate to group? The examples of groups that we've seen so far deal with arrangements of similar things. In chapter 5, we shall uncover the following fact (we'll be more precise later):

Every group can be viewed as a collection of ways to rearrange some set of things.

Groups relate to symmetry because an object's symmetries can be described using arrangements of the object's parts. The following definition provides a technique for finding a group that describes (or measures) a physical object's symmetry (in 3-D).

Definition 3.1

1. Identify all the parts of the object that are similar, and give each such part a different number.
2. Consider the actions that you could perform with your hands that may rearrange the numbered parts, yet leave the object taking up the same physical space it did originally. (This collection of actions forms a group.)
3. (Optional) If you want to visualize the group, explore and map it as we did in Chapter 2 with the rectangle, etc.

Comments

- We'll refer to the physical space that an object occupies as its footprint (this terminology does not appear on the text).
- Step 1 of Definition 3.1 numbers the object's parts so that we can track the manipulations permitted in Step 2. Each new state is a rearrangement of the object's similar parts and allows us to distinguish each of these rearrangements; otherwise we could not tell them apart.
- In this context, not *every* rearrangement of the similar parts is necessarily valid. We are only allowed actions that maintain the physical integrity of the object *and* preserve its footprint. For example, we can't rip two arms off a starfish and then glue them back on in different places.

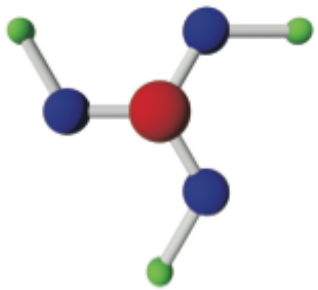
Comments (continued)

- Step 2 requires us to find *all* of the actions that preserve the object's footprint and physical integrity; not just the generators.
- However, if we choose to complete Step 3 (construct Cayley diagram), we must make a choice concerning generators. As we mentioned in the previous chapter, different choices in generators may result in different Cayley diagrams.
- When selecting a set of generators, we would ideally like to select as small a set as possible. We can never choose too many generators, but we can choose too few. But having "extra" generators does nothing but clutter our Cayley diagram.

Shapes of molecules

Because the shape of molecules impacts their behavior, chemists use group theory to classify their shapes. Let's take a look at an example.

The following figure (taken from page 28 of *Visual Group Theory*) depicts a molecule of Boric acid, $B(OH)_3$.

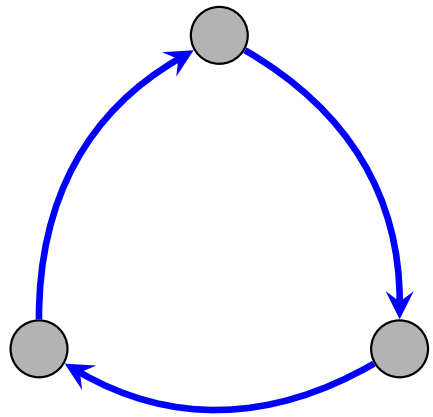


Follow the steps of Definition 3.1 to find the group that describes the symmetry of the molecule and draw a possible Cayley diagram.

What we should have discovered is that the group of symmetries of Boric acid has 3 actions requiring at least one generator. If we choose rotation clockwise 1/3 of a full turn as our generator, then the three actions are:

1. the do nothing action
2. rotation clockwise 1/3 of a full turn
3. rotation clockwise 2/3 of a full turn

The corresponding abstract Cayley diagram is as follows:



This is the cyclic group, C_3. (We'll discuss cyclic groups in Chapter 5.)

Group exercises

Let's explore a few more examples.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 3.5
   - Exercise 3.6 (see Bob)
2. Let's discuss your solutions.
3. Now, complete Exercise 3.7. I want each group to turn in a complete solution.

Crystallography

Solids whose atoms arrange themselves in a regular, repeating pattern are called crystals. The study of crystals is called crystallography.

The wonderful picture in Figure 3.8 (page 30) shows the result of repeating indefinitely the crystal cube from Figure 3.7.

When chemists study such crystals they treat them as patterns that repeat without end. This allows a new manipulation that preserves the infinite footprint of the crystal and its physical integrity: translation.

In this case, the groups describing the symmetry of crystals are infinite. Why?

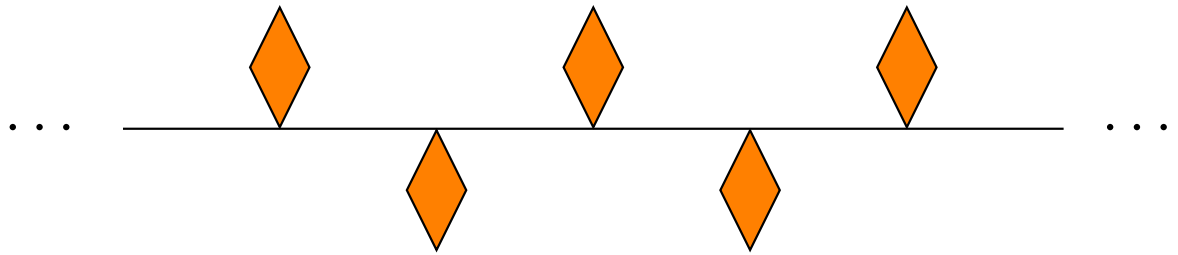
Frieze patterns

Crystals are patterns that repeat in 3 dimensions.

We will discuss simpler patterns that only repeat in one dimension, called frieze patterns. The groups that describe the symmetry of frieze patterns are called frieze groups.

Frieze patterns (or at least finite sections of them) occur throughout art and architecture.

Here is an example of a frieze pattern:



Because this frieze pattern extends infinitely far to the left and right, we are presented with a new type of manipulation that preserves the footprint and the physical integrity of the frieze. This new action is called a glide reflection and consist of a horizontal translation (by the appropriate amount) followed by a vertical flip.

Note that for this pattern, a vertical flip all by itself does not preserve the footprint, and so is not one of the actions of the group of symmetries.

Let's determine the group of symmetries of the frieze pattern on the previous slide and draw a possible Cayley diagram.

The group of symmetries of the frieze pattern on the previous slide turns out to be infinite, but we only needed two generators: horizontal flip and glide reflection. Figure 3.13 (page 33) depicts a possible Cayley diagram.

Comments

- The symmetry of any frieze pattern can be described by one of 7 different infinite groups. It turns out that some of the frieze groups are isomorphic (i.e., have the same structure) even though the visual appearance of the patterns may differ.
- The symmetry of 2-dimensional repeating patterns, called wallpaper patterns, has also been classified. There are 17 different wallpaper groups.

More group exercises

Time to do some more exploring.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 3.11(a)
   - Exercise 3.11(b)
   - Exercise 3.11(d) (Bob may have something to say)
2. Let's discuss your solutions.

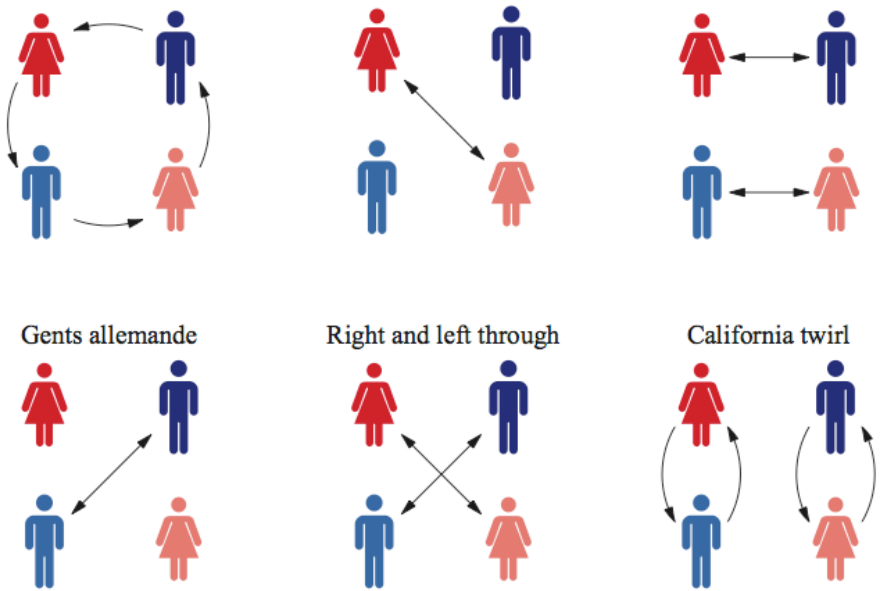
Contra dancing

In square dancing and contra dancing, the dancers follow a sequence of predefined steps called figures. Often dancers learn these steps by name and practice following a caller who orders them to perform specific figures in time with the music.

We'll assume that we have 2 couples standing in the shape of a square, so that individuals of the same sex are on opposite corners. To start, let's assume that one of the women is in the upper left hand corner of the square.

Dancing a figure rearranges the dancers. If they correctly obey the caller, every dance ends with the dancers back in their original positions in the square.

The following figure (taken from page 35 of *Visual Group Theory*) shows the effects of 6 example figures.



Do these 6 actions generate a group? The answer is yes (check the rules). It turns out, perhaps not surprisingly, that the group is isomorphic (i.e., same structure) as the group of symmetries of a square.

Even more group exercises

It's dance time!

1. In a large group, complete the following exercises (not collected):
   - Exercise 3.1
   - Exercise 3.13 (see Bob)
   - Exercise 3.14(a)
2. Let's discuss your solutions.
3. Now, in groups of 2–3, complete Exercise 3.15(a). I want each group to turn in a complete solution.

Potential quiz questions

Here are some potential questions that I may ask you on tomorrow's quiz at the beginning of class:

1. In order for an action to be a member of a group of symmetries for an object in 3-dimensions, what 2 important properties must this action have?
2. What is a glide reflection and to what kinds of objects can we apply them to?
3. Draw a Cayley diagram for a given molecule or frieze pattern.

Chapter 4: Algebra at last

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

Recall that our informal definition of a group was a collection of actions that obeyed Rules 1.5–1.8. This is not the ordinary definition of a group.

In this chapter, we shall introduce the more standard (and more formal) definition of a group. We will also spend some time convincing ourselves that both definitions agree. (They should or we're in trouble!)

Along the way, we will also introduce another powerful visualization technique, called multiplication tables.

More on Cayley diagrams

Recall that the arrows in a Cayley diagram represent the generators of the group. In particular, all the arrows of a particular color correspond to the same unique generator.

Also, don't forget that our choice of generators influenced the resulting Cayley diagram.

By Rule 1.8, we know that any sequence of actions is an action. How are all the non-generator actions represented implicitly in a Cayley diagram?

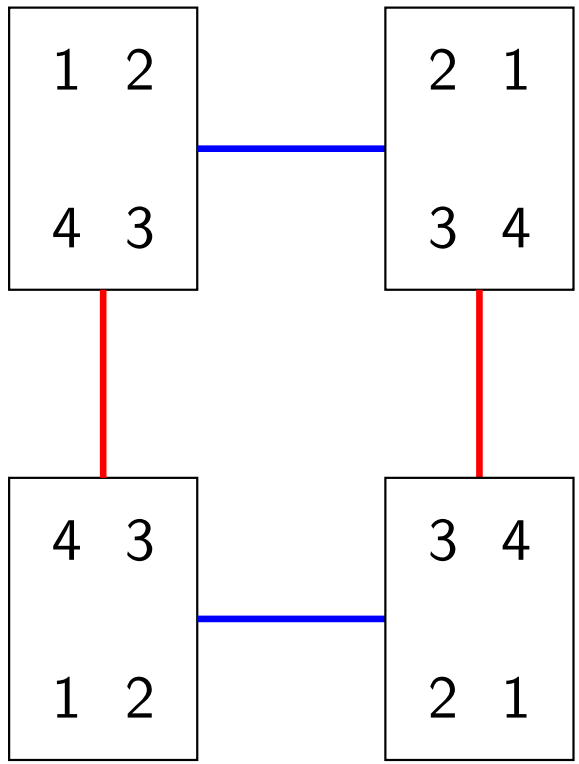
The answer is that every action in the group is represented by a path through the diagram. Our immediate goal is to nail down exactly what this means.

When we have been drawing Cayley diagrams, we have been doing one of two things with the nodes:

1. Labeling a node with a labeled configuration of thing we are acting on, so that the configuration at that node is the result of applying the generator corresponding to the arrow leading into that node.
2. Leaving the nodes unlabeled (I've referred to this as the abstract Cayley diagram).

Let's revisit an example we have already seen to help illustrate the point.

Consider the group of symmetries of a rectangle (alternatively, consider the 2-Lightswitch Group). As we've already discussed, this group has a total of 4 actions and we can use horizontal flip (h) and vertical flip (v) as generators. Here is a possible Cayley diagram, where we have labeled the nodes with configurations of of the rectangle and h is represented by the blue arrows and v is represented by the red arrows.

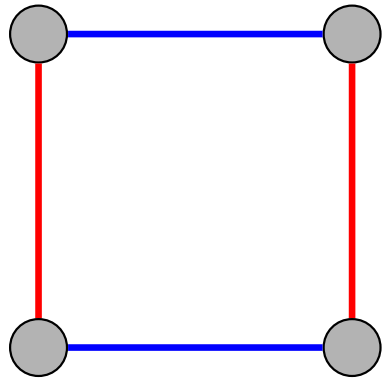


As we can see by looking at the Cayley diagram on the previous slide, following a sequence of arrows from one node to another shows us the result of applying the corresponding generators to the configurations we started with.

For example, if we start with the configuration in the upper left hand corner and then follow the blue edge (h) followed by the red edge (v), we end up at the configuration in the lower right hand corner. This sequence of actions is equivalent to a 180° rotation of the original configuration.

Do you see any other paths that represent this same action?

If we remove all reference to the specific configurations of the rectangle, we end up with an abstract Cayley diagram for V_4:



Now, while abstract Cayley diagrams are nice to look at, we definitely lose some information when we remove reference to the rectangle configurations.

What we'd like to do is strike a balance between these two representations. Since a group is a collection of actions (verbs), this will influence how we proceed.

Definition 4.1

The following steps transform a Cayley diagram into one that focuses on the group's actions.

(i) Choose a node as our initial reference point; label it e. (This will correspond to our "do nothing action.")

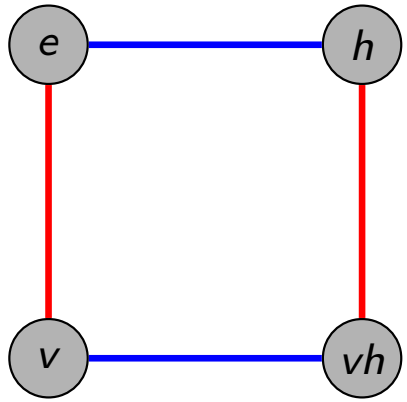
(ii) Relabel each remaining node in the diagram with a path that leads there from node e. (If there is more than one path, pick any one; shorter is better.)

(iii) Distinguish arrows of the same type in some way (color them, label them, dashed vs. solid, etc.)

Our convention will be to label the nodes with sequences of generators, so that reading the sequence from left to right indicates the appropriate path. Warning: different authors often use the opposite convention.

The author calls the resulting diagram a diagram of actions. We will refer to these diagrams of actions as Cayley diagrams with the nodes labeled by actions (instead of configurations).

What do we get if we apply the steps to the abstract Cayley diagram for V_4? Here it is:



Note that we could also have labeled the node in the lower right hand corner as hv, as well. I'll emphasize this again later, but it is important to point out that this phenomenon (i.e., order of generators does not matter) does *not* always happen.

What do you think is a good way to represent the fact that doing a horizontal flip followed by a vertical flip results in the same action as doing a vertical flip followed by a horizontal flip? Yeah, that's right: $hv = vh$.

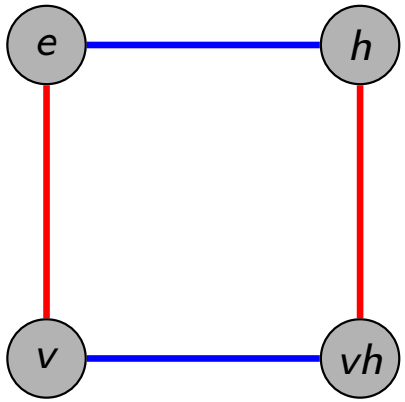
By the way, what if you forget which arrow corresponds to which generator? Just look to see what the label is on the node after following that arrow from e.

One of the really awesome things about Cayley diagrams with nodes labeled by actions is that we can use them as a sort of calculator.

What I mean by this is that if we want to know what a particular sequence (even really long ones!) is equal to, then we can just chase the sequence through the Cayley graph by starting at e.

Let's try one. In V_4, what is the action $hhhvhvvhv$ equal to?

Here is the Cayley diagram for reference:



We see that $hhhvhvvhv = h$. A more condensed way to write this is $h^3vhv^2hv = h$. You might be wondering if we could have just written

$$h^5v^4 \stackrel{?}{=} h^3vhv^2hv = h.$$

Well, check it out! In this case, the answer is yes. Warning: not all groups have this property!!!

Group work

Let's explore a few more examples.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Construct the Cayley diagram with nodes labeled by actions for the group of symmetries of an equilateral triangle (assume one tip of triangle is pointing up) using:
     (i) horizontal flip (h) and 120° rotation clockwise (r) as generators.
     (ii) horizontal flip (h) and the diagonal flip that keeps the lower left corner fixed (d).

     Any observations?
   - Exercise 4.17
   - Exercise 4.4
   - Exercise 4.5(a)
2. Let's discuss your solutions.

Multiplication tables

Since we can use a Cayley diagram with nodes labeled by actions as a calculator for figuring out what any length sequence of generators is equal to, we could create a table that shows how every pair of group actions combine. This type of table is called a (group) multiplication table.

This is best illustrated by diving in and doing an example. Using our Cayley diagram from earlier, let's see if we can complete the following multiplication table for V_4 using our generators h and v.

$*$	e	v	h	vh
e				
v				
h				
vh				

Comments

- The 1st column and 1st row repeat themselves. Why? Sometimes these will be omitted (*Group Explorer* does this).
- In each row and each column, each group action occurred exactly once. (This will always happen.)
- Multiplication tables can visually reveal patterns that may be difficult to see otherwise. To help make these patterns more obvious, we can color the cells of the multiplication table, where we assign a unique color to each action of the group. Figure 4.7 (page 47) has examples of a few such tables.

More group work

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 4.6(a)
   - Exercise 4.6(b)
2. Let's discuss your solutions.
3. Now, complete Exercise 4.19(a)(b)(c). I want each group to turn in a complete solution.

Moving towards the standard definition of a group

We have been calling the members that make up a group "actions" because our definition requires a group to be a collection of actions that satisfy our 4 rules. Since the standard definition of a group is not phrased in terms of actions, we will need more general terminology.

We will call the members of a group elements. In general, a group is a set of elements satisfying some set of properties.

We will also use standard set theory notation. For example, we will write things like

$$h \in V_4$$

to mean "the element h is an element of the group V_4."

Binary operations

Intuitively, an operation is a method for combining objects. For example, $+$, $-$, $\cdot$, and $\div$ are all examples of operations. In fact, these are all examples of binary operations because they combine two objects into a single object.

The combining of group elements is also a binary operation (like composition: do one action and then do another action to the result of the 1st one). We say that it is a binary operation *on* the group.

Binary operations on sets have the following special property.

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$.

The fancy way of saying this is that the set is closed under the binary operation.

Recall that Rule 1.8 says that any sequence of actions is an action. This ensures that the group was closed under the binary operation of combining actions.

Multiplication tables are nice because they depict the group's binary operation in full.

However, it is important to point out that not every table with symbols in it is going to be equal to the multiplication table for a group. Soon we will uncover a couple of features that distinguish those tables that depict groups from those that don't.

Associativity

Does anyone remember what it means for an operation to be associative? An operation is associative if parentheses are permitted anywhere, but required nowhere.

As examples, addition and multiplication of integers is associative. How we group a string together with parentheses has no impact on the outcome.

However, subtraction of integers is not associative. Here is an example:

$$3 - (2 - 4) \neq (3 - 2) - 4.$$

Is the operation of combining actions in a group associative? The answer is yes. We will not prove this fact, but rather illustrate it with an example.

Consider the group of symmetries for the equilateral triangle (called D_3 or S_3) with generators h and r from our group work earlier.

How do the following compare?

$$rhr, \quad (rh)r, \quad r(hr)$$

We see that even though we are associating differently, the end result is that the actions are applied left to right.

The moral of the story is that we do not ever need to use parentheses when working with groups, but sometimes we may use them to draw our attention to a particular chunk in a sequence.

Some more group work

In groups of 2–3, complete the following exercises (not collected):

- Exercise 4.14
- Exercise 4.10(a) (see Bob)

Inverses

Recall that Rule 1.6 requires every action to be reversible. Said another way, given any group element, you can find its opposite action, which we call its inverse.

If g represents some element (action) of a group, then we will use g^{-1} to denote the inverse of g.

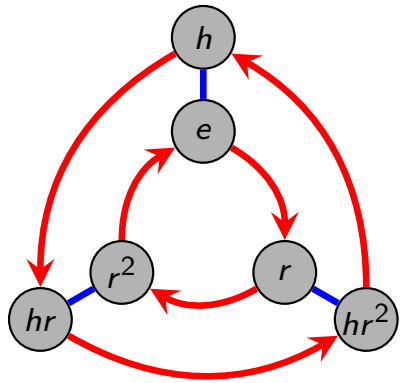
Given any action of a group, what is the result of combining that action and its inverse (in either order)? Yep, we get the "do nothing action."

Our fancy word for the "do nothing action" is identity. We can really use whatever symbol we want to denote the identity of a group, but common choices are e, 1, 0, and N.

Using all of our new fancy notation, we can write expressions like

$$gg^{-1} = e \text{ and } g^{-1}g = e.$$

Let's explore these ideas a little more with one of our common examples. Recall that the Cayley diagram for the group of symmetries of the triangle (S_3 or D_3) is as follows.



Using the Cayley diagram, try to complete the following statements:

$r^{-1} =$ _____ because r_____ $= e =$ _____r

$h^{-1} =$ _____ because h_____ $= e =$ _____h

$(hr)^{-1} =$ _____ because (hr)_____ $= e$_____(hr)

$(hr^2)^{-1} =$ _____ because (hr^2)_____ $= e =$ _____(hr^2).

Some more group exercises

1. In groups of 2–3, complete the following exercises (not collected):
   - Exercise 4.10(b)
   - Exercise 4.11(a)
   - Exercise 4.26(a)
2. Let's discuss your solutions.
3. Now, in groups of 2–3, complete Exercise 4.27(a)(b). I want each group to turn in a complete solution for both parts.

Classical definition of a group

We are now ready to state the standard definition of a group.

Definition 4.2

A set G is a group if the following criteria are satisfied.

1. There is a binary operation $*$ on G.
2. $*$ is associative.
3. There is an identity element $e \in G$. That is, $e * g = g = g * e$.
4. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Do our two competing definitions agree? That is, if Definition 1.9 says something is a group, will Definition 4.2 agree? Or vice versa?

Our discussion leading up to Definition 4.2 provides an informal argument for why the answer to the first question must be yes. We will answer the second question in the next chapter.

Regardless of whether the definitions agree (which they do), we always have $e^{-1} = e$. That is, the reverse of doing nothing is doing nothing.

Even though we haven't officially shown that the two definitions agree, we shall begin viewing groups from these two different paradigms:

- group as a collection of actions
- group as a set with a binary operation

Even more group exercises

In groups of 2–3, complete Exercise 4.32. I want each group to turn in a complete solution.

Potential quiz questions

Here are some potential questions that I may ask you on tomorrow's quiz at the beginning of class:

1. What is a binary operation?
2. What is our second definition of a group?
3. Determine whether a given multiplication table represents a group.
4. State at least two properties that *all* groups share.
5. Find expression for the inverse of a group element.
6. Solve a specified group equation for a particular group.

Chapter 5: Five families

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

In this chapter, we will introduce 5 families of groups.

1. cyclic groups
2. abelian groups
3. dihedral groups
4. symmetric groups
5. alternating groups

Along the way, a variety of new concepts will arise, as well as some new visualization techniques.

The cyclic groups

The cyclic groups describe the symmetry of objects that have *only* rotational symmetry. Here are a couple of examples of objects that only have rotational symmetry (taken from Figure 5.1 of *Visual Group Theory*).

All cyclic groups only require a single generator. An obvious choice would be: single "click" clockwise, where "click" is defined to be rotation by $360^\circ/n$ and n is the number of "arms." (Don't be fooled into thinking that this is the only choice; it's just the natural one.)

Definition

The order of a group is the number of distinct elements in the group.

The cyclic group of order n (n rotations) is denoted C_n (or sometimes by $\mathbb{Z}_n$).

For example, the group of symmetries for the propeller on the previous slide is C_6 and the group of symmetries for the pinwheel is C_8.

One of the most common ways to name the elements in C_n is with the integers $0, 1, 2, \ldots, n-1$, where the identity is 0 and 1 is the single click clockwise.

Comment

The alternate notation $\mathbb{Z}_n$ comes from the fact that the binary operation for C_n is just modular addition. To add two numbers in $\mathbb{Z}_n$, add them as integers, divide by n, and then take the remainder.

For example, in C_6, $3 + 5 \equiv_6 2$. In fact, if the context is clear, we may even write $3 + 5 = 2$.

It is worth mentioning that the set $\{0, 1, \ldots, n-1\}$ is closed under modular addition (mod n). That is, if we add (mod n) any two numbers in this set, the result is another member of the set.

Recall the "generated by" notation introduced in Exercise 4.25 (done for HW). In this case, we can write

$$C_n = \langle 1 \rangle.$$

Here's another natural choice of notation for cyclic groups. If r (rotation!) is a generator for C_n, then we can also denote the n elements of C_n by

$$e, r, r^2, \ldots, r^{n-1}.$$

Note that $r^n = e, r^{n+1} = r, r^{n+2} = r^2$, etc. Can you see modular addition rearing its head again?

Furthermore, we can write

$$C_n = \langle r \rangle.$$

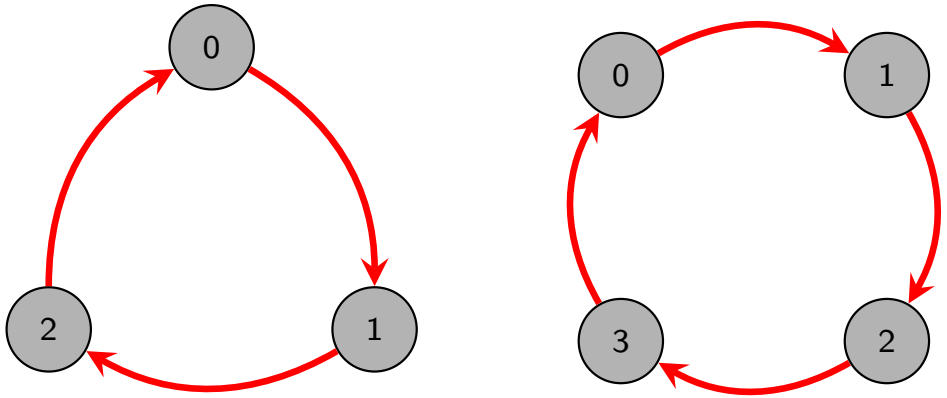
Notice that one of our notations is "additive" and the other is "multiplicative." This presents no problems since we just making a choice about how we denote the action.

The Cayley diagrams for the cyclic groups are all alike. The standard Cayley diagram for C_n consists of a single cycle

$$0 \to 1 \to 2 \to \cdots \to n-1 \to 0$$

with one type of arrow (namely single click clockwise).

Here are the (standard) Cayley diagrams for C_3 and C_4.



Let's go play with the Cayley diagrams of cyclic groups on *Group Explorer*. In particular, let's see if we can conjecture whether there are any other single element generating sets for C_n.

Observations?

Conjecture

Any number from $\{0, 1, \ldots, n-1\}$ that is relatively prime to n will generate C_n.

For example, 1 and 5 generate C_6, while $1, 2, 3$, and 4 all generate C_5.

Important: We have NOT proven this conjecture. We have only witnessed a few instances where it holds.

Modular addition has a nice visual effect on the multiplication tables of cyclic groups. Let's go look at the multiplication tables for some cyclic groups in *Group Explorer* and see if we can figure out what effect this is.

There are probably many things worth commenting on, but one of the most important properties of the multiplication tables for cyclic groups is as follows.

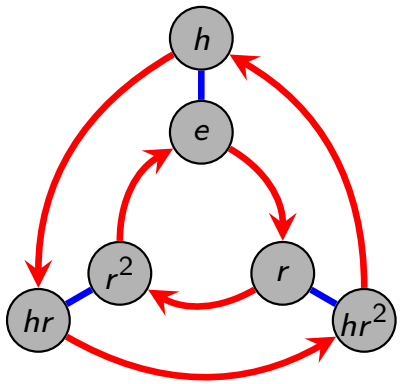
If the headings on the multiplication table are arranged in the natural order, then each row is a cyclic shift to the left of the row above it.

Orbits

We started our discussion with cyclic groups because of their simplicity, but also because they play a fundamental role in other more complicated groups.

Before continuing our exploration into the 5 families, let's see if we can observe how cyclic groups "fit" into other groups.

Consider the Cayley diagram for S_3.



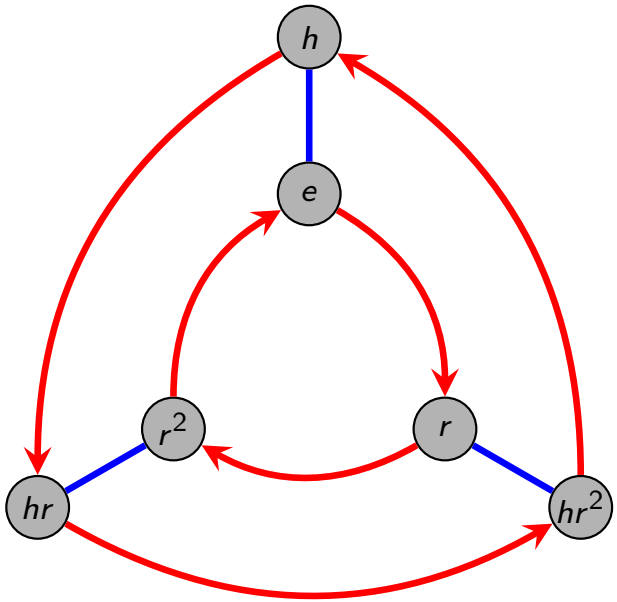
Do you see any copies of the Cayley diagram for any cyclic groups in this picture?

Starting at e, the red arrows lead in a cycle around the inside of the diagram. We refer to this cycle as the orbit of the element r.

Orbits are usually written with braces. In this case, the orbit of r is $\{e, r, r^2\}$.

Every element in a group traces out an orbit. Some of these may not be obvious from the Cayley diagram, but they are there nonetheless.

Let's work out the orbits for the remaining 5 elements of S_3.



element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
h	$\{e, h\}$
hr	$\{e, hr\}$
hr^2	$\{e, hr^2\}$

Note that in the preceding example, there were only 5 distinct orbits. The elements r and r^2 have the same orbit.

Also, for any group, the orbit of e will simply be $\{e\}$.

In general, the orbit of an element g is given by

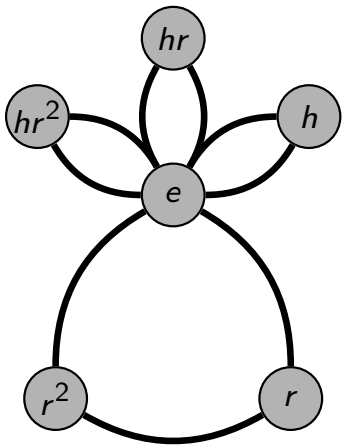
$$\{g^k : k \in \mathbb{Z}\}.$$

This set is not necessarily infinite as we've seen with the finite cyclic groups.

Another way of thinking about this is that the orbit of an element g is the collection of elements in the group that you can get to by doing g or it's inverse any number of times.

Cycle graphs

We can use cycle graphs to visualize the orbits of a group. Here is the cycle graph for S_3.



element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
h	$\{e, h\}$
hr	$\{e, hr\}$
hr^2	$\{e, hr^2\}$

Comments

- For cycle graphs, each cycle in the graph represents an orbit.
- The convention is that orbits that are subsets of larger orbits are only shown within the larger orbit.
- We don't color or put arrows on the edges of the cycles.
- Intersections of cycles show what elements they have in common.
- What do the cycle graphs of cyclic groups look like? There is a single cycle.

See pages 72–73 for more examples.

Group work

Let's explore a few more examples.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 5.2(a)(b)(c)
   - Exercise 5.7
   - Exercise 5.15(a)(b)(c)(d)
   - Exercise 5.6(a)
2. Let's discuss your solutions.
3. Now, complete Exercise 5.13(b). I want each group to turn in a complete solution.

Abelian groups

Definition

A group is called abelian (named after Neils Abel) if the order in which one performs the actions is irrelevant (i.e., the actions commute). That is, a group is abelian iff $ab = ba$ for all a and b in the group.

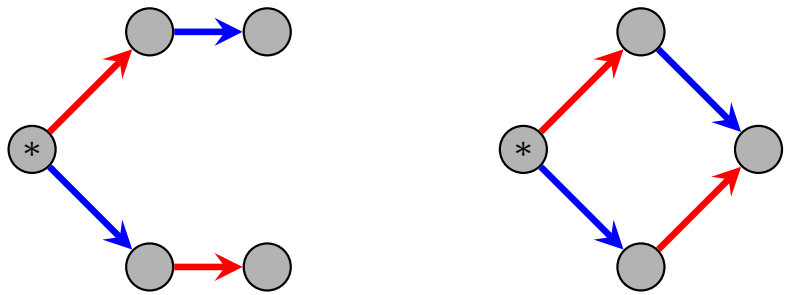
Abelian groups are sometimes referred to as commutative.

The group V_4 is an example of a group that we have seen that is abelian. The group S_3 is not abelian: $rh \neq hr$.

How can we use the Cayley diagram for a group to check to see if the corresponding group is abelian?

It turns out that it is enough to consider the order in which the generators are applied (Why? See Exercise 5.12). Suppose we have a group, where a and b are two of the generators and a and b are represented by red and blue arrows, respectively, in the Cayley diagram.

Commutativity requires $ab = ba$. It terms of arrows, this means that following a red arrow and then a blue arrow should put us at the same node as following a blue arrow and then a red arrow.



The pattern on the left never appears in the Cayley graph for an abelian group, whereas the pattern on the right illustrates the relation $ab = ba$.

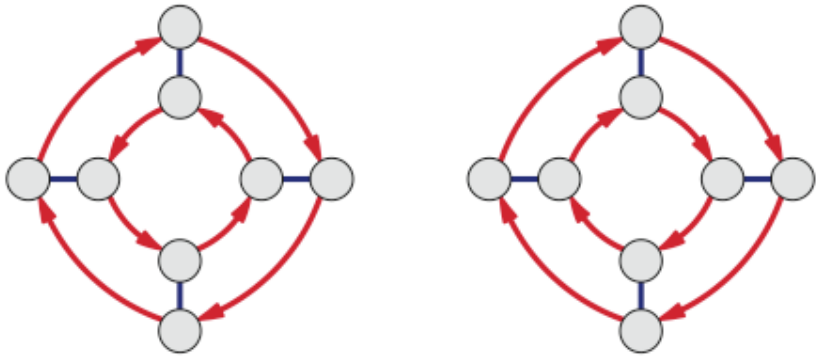
Are cyclic groups abelian? The answer is yes.

One way to see that this is true is to observe that the left configuration on the previous slide can never occur (since there is only one generator).

Here's another way. In a cyclic group with generator r, every element can be written as r^k for some k. Then certainly $r^k r^m = r^m r^k$ for any k and m you like.

How about the converse? That is, if a group is abelian, is it cyclic? The answer is no and the group V_4 provides an easy counterexample.

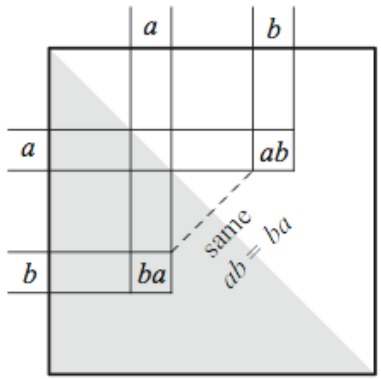
Let's explore a little further. The following diagrams (taken from Figure 5.9 on page 69 of *Visual Group Theory*) represent the Cayley diagrams for the groups D_4 and $C_2 \times C_4$, respectively.



Are either one of these groups abelian?

Abelian groups are easy to spot if you look at their multiplication tables. How does the relation $ab = ba$ manifest itself in the multiplication table for abelian groups?

The table must be symmetric across the diagonal from top-left to bottom-right.



(This is Figure 5.11 on page 70 of *Visual Group Theory*.) Let's check this out in *Group Explorer*.

Dihedral groups

While cyclic groups describe objects that only have rotational symmetry, dihedral groups describe objects that have both rotational symmetry and bilateral symmetry (reflection across a midline).

Regular polygons are examples of objects with rotational and bilateral symmetry. The dihedral group that describes the symmetries of a regular n-gon is written D_n.

All the actions of C_n are also actions of D_n, but there are more actions than that. How many actions does D_n have?

D_n contains $2n$ actions: n rotations and n reflections.

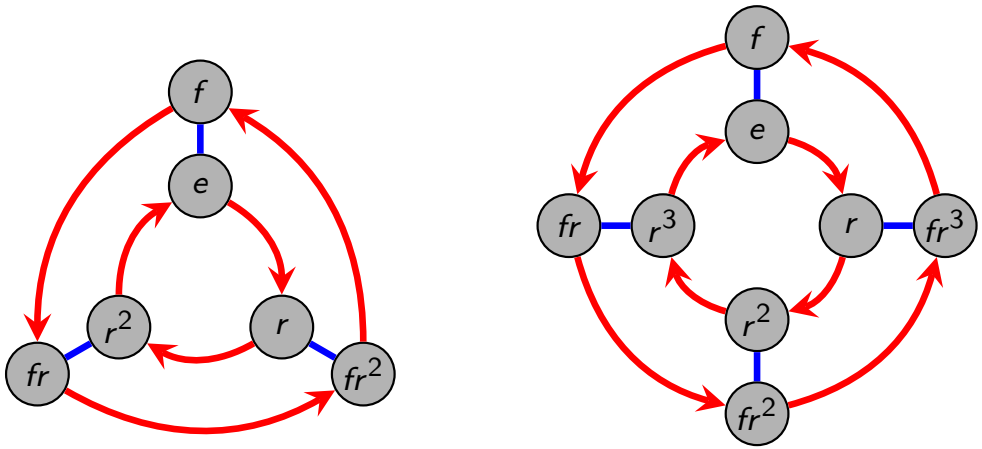
However, we only need two generators:

1. r = rotation clockwise by a single "click" (there are other possible choices)
2. f = horizontal flip (or any other flip will do)

There are many ways to do it, but we can write every one of the $2n$ actions of D_n as a "word" in these two generators. Here is one possibility:

$$\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{f, fr, fr^2, \ldots, fr^{n-1}}_{\text{reflections}}$$

The Cayley diagrams for the dihedral groups all look similar. Here are the (standard) Cayley diagrams for D_3 and D_4, respectively.



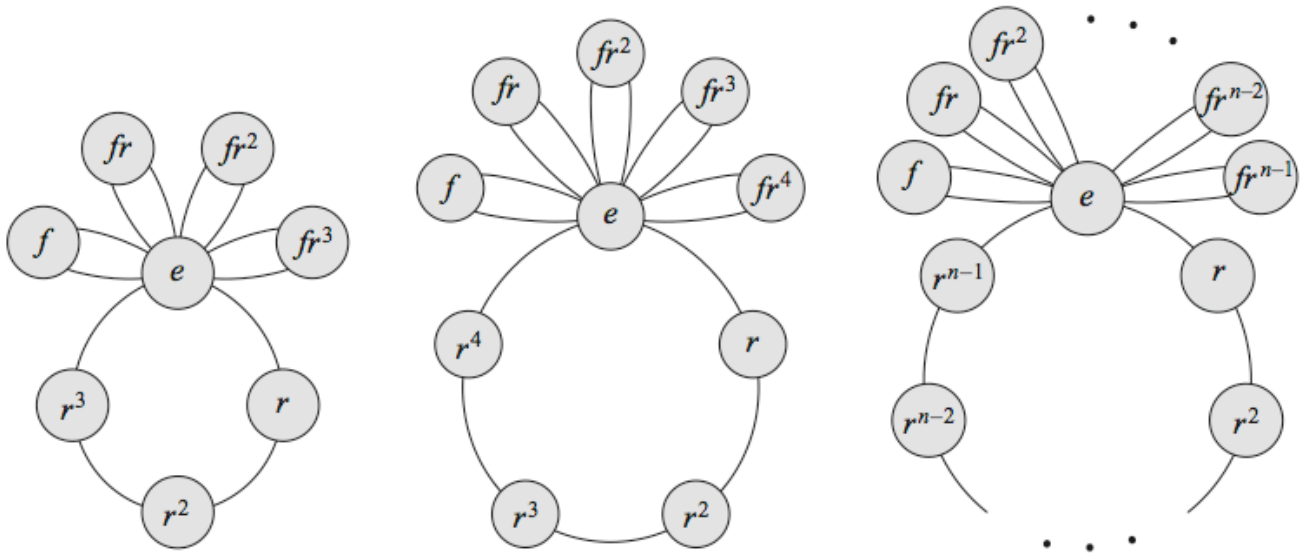
(Note that the author usually switches the inner and outer cycles from how they are drawn here; of course, it doesn't matter.)

In general, the Cayley diagram consists of an inner cycle and an outer cycle of n nodes each, where one cycle is clockwise and the other is counterclockwise. The two cycles are connected by two way arrows representing the flip.

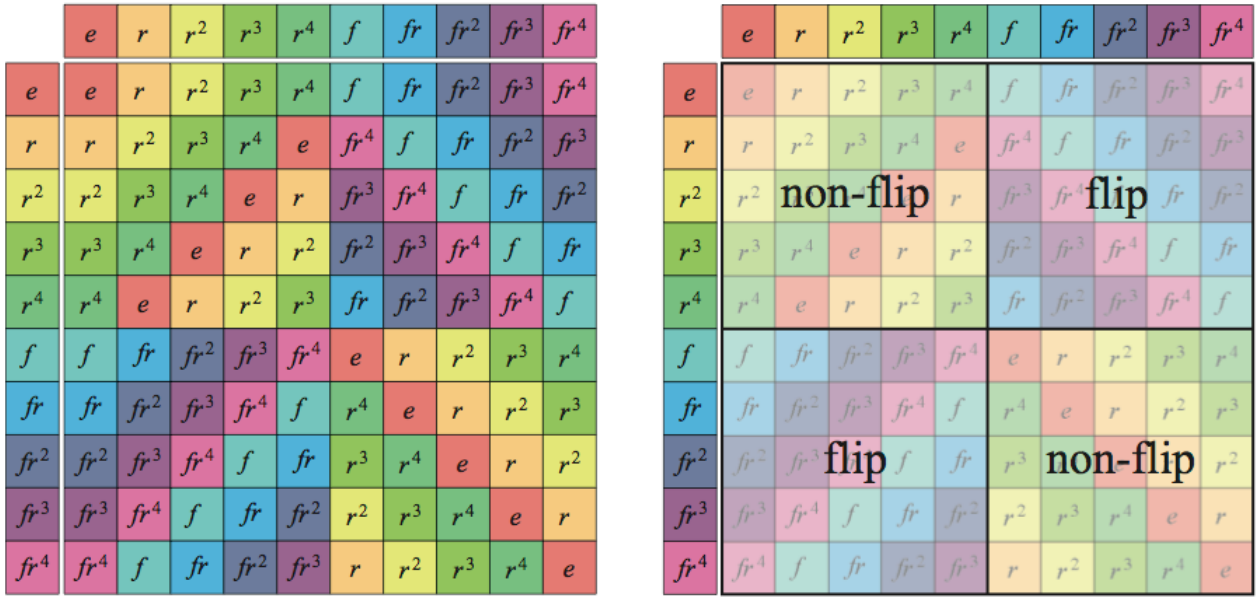
Is D_n (with $n \geq 3$) abelian? Nope: $fr \neq rf = fr^{n-1}$. Why is the last *equality* true?

We can move from e to rf by walking clockwise one click and then moving to the other cycle. This is equivalent to first moving to the other cycle from e followed by $n-1$ clicks counter-clockwise, which puts us at fr^{n-1}. The relation $rf = fr^{n-1}$ will be useful to remember.

D_n consists of an r orbit (with smaller rotation orbit subsets) and n other two element flip orbits. Figure 5.20 on page 78 of *Visual Group Theory* depicts the general pattern of the cycle graphs of the dihedral groups.



The separation of D_n into rotations and reflections is also visible in their multiplication tables.



(Figures 5.18 and 5.19 on pages 76 and 77, respectively, of *Visual Group Theory*.)

As we shall see later in the course, the partition of D_n as depicted above forms the structure of the group C_2. "Shrinking" a group in this way is called taking a quotient.

More group work

Let's explore a few more examples.

1. In groups of 2–3, complete the following exercises (not collected):
   - Exercise 5.16(b)
   - Exercise 5.29(b)(c)
2. Let's discuss your solutions.

Symmetric groups

Most of the groups that we have seen have been collections of ways to rearrange things. Mathematicians have a fancy word to describe rearrangements.

Definition

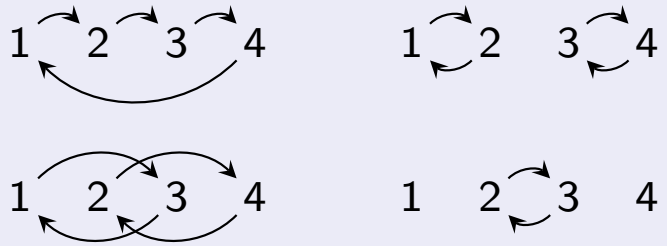
A permutation is an action that rearranges a collection of things.

Because they are easy to write down and deal with, we will usually refer to permutations of positive integers (just like we did when we numbered our rectangle, etc.).

There are many ways to represent permutations, but we will use the notation illustrated by the following example.

Example

Here are some permutations of 4 objects.

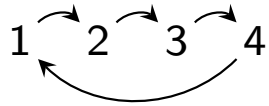


How many permutations of 4 objects are there? The answer is that there are $4! = 24$, which means that there are 24 distinct permutation pictures like above on 4 objects.

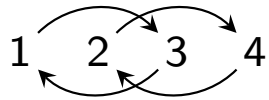
How many permutations of n objects are there? Yep, you guessed it: $n!$.

In order for the collection of permutations of n objects to form a group (which is what we want!), we need to understand how to combine permutations. Let's consider an example.

What should

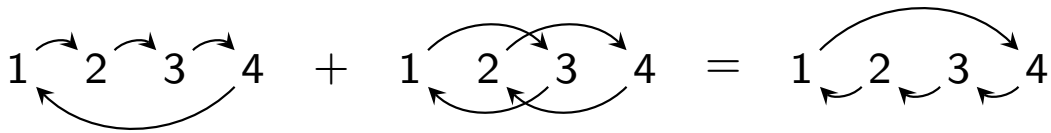


followed by



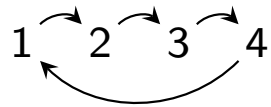
be equal to?

The first permutation rearranges the 4 objects and then we shuffle the result according to the second permutation.

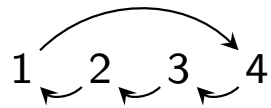


Does the collection of permutations of n items form a group? Yes! To verify this, we just have to check that the appropriate rules of one of our definitions of a group hold true.

How do we find the inverse of a permutation? Just reverse all of the arrows in the permutation picture. For example, the inverse of



is simply



Definition

The group of all permutations of n items is called the symmetric group (on n objects) and is denoted by S_n.

We've already seen the group S_3, which happens to be the same as the dihedral group D_3, but this is the only time the symmetric groups and dihedral groups coincide.

Although the collection of *all* permutations of n items forms a group, creating a groups does not require taking all of the permutations. If we choose carefully, we can form groups by taking a subset of the permutations.

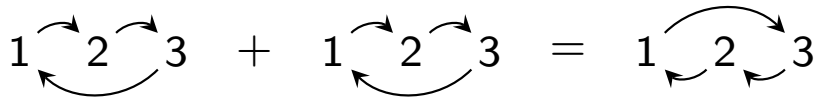
Alternating groups

One way to form a group from a subset of the collection of permutations of n items is to take exactly half of the elements of S_n. But what half? Not just any half will do.

The only major concern is that our "half" must be closed (all other necessary properties are inherited from S_n).That is, we must choose half the elements of S_n such that the combination of any two results in a permutation that is also in our chosen set.

It turns out that the appropriate choice is the set of "squares" in S_n. What we mean by "square" is any element that can be written as an element of S_n times itself.

For example, since



The permutation

is a square in S_3.

Definition

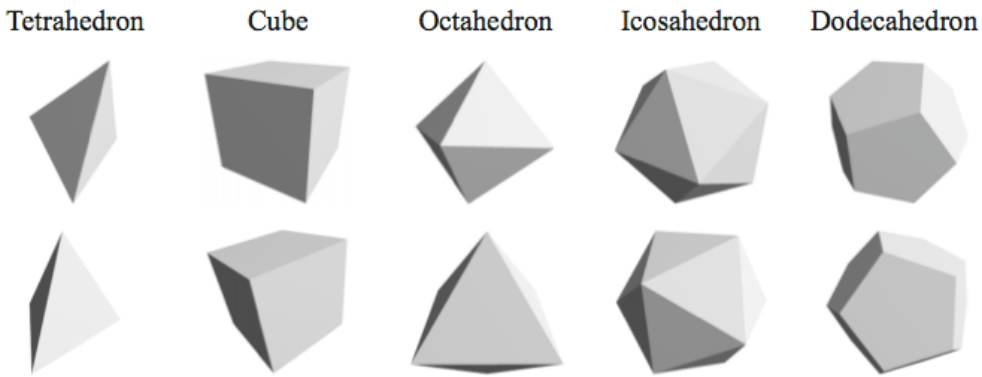
The group of squares from S_n is called the alternating group and is denoted A_n.

We'll see later why we called this group the "alternating" group. Note that A_n has order $n!/2$.

Platonic solids

The symmetric groups and alternating groups turn up all over in group theory. In particular, the groups of symmetries of the 5 Platonic solids turn out to be symmetric and alternating groups.

There are only 5 3-dimensional shapes all of whose faces are regular polygons that meet at equal angles. These 5 shapes are called the Platonic solids:



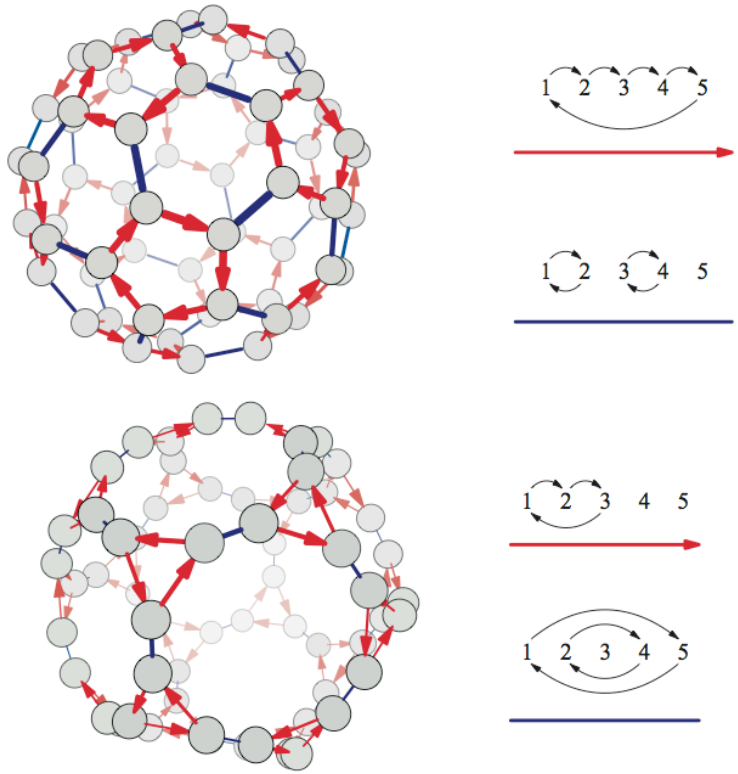
(Figure 5.26 on page 81 of *Visual Group Theory*.)

The groups of symmetries of the Platonic solids are as follows.

shape	group
Tetrahedron	A_4
Cube	S_4
Octahedron	S_4
Icosahedron	A_5
Dodecahedron	A_5

The Cayley diagrams for these 3 groups can be arranged in some very interesting configurations. In particular, the Cayley diagram for Platonic solid "blah" can be arranged on a truncated "blah", where truncated refers to cutting off some corners.

For example, here are two representations for Cayley diagrams of A_5, where the top is a truncated icosahedron and the bottom is a truncated dodecahedron.



(Figure 5.29 on page 83 of *Visual Group Theory*.)

Cayley's theorem

Note that any set of permutations that forms a group is called a permutation group.

Cayley's theorem effectively says that permutations can be used to construct any group. In other words, every group has the same structure as some permutation group.

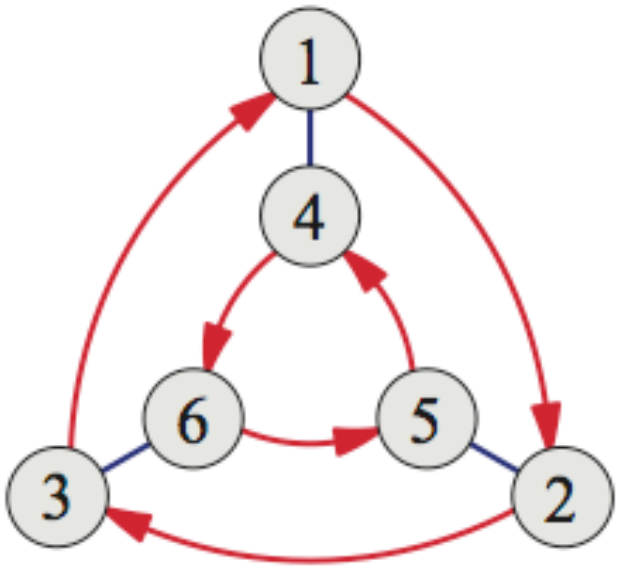
Warning: We are not saying that every group is equal to a symmetric group, but rather that every group can be thought of a subset of some symmetric group, where that subset is a group in it's own right that has the same structure as the original group.

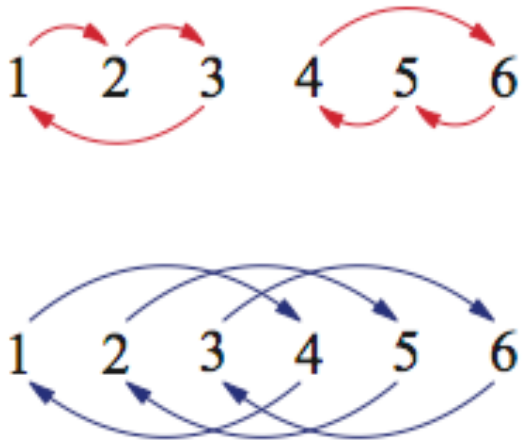
How do we do this?

Here is an algorithm given a Cayley diagram with n nodes:

1. number the nodes 1 through n
2. interpret each arrow type in Cayley diagram as a permutation

The resulting permutations are the generators of the corresponding permutation group. Here is an example (taken from Figure 5.30 on page 84 of *Visual Group Theory*).



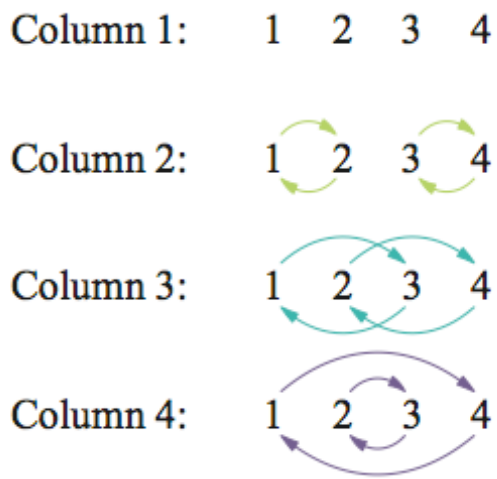


Here is an algorithm given a multiplication table with n elements:

1. replace the table headings with 1 through n
2. make the appropriate replacements throughout the rest of the table
3. interpret each column as a permutation

This results in a 1-1 correspondence between the original group elements (not just the generators) and permutations. Here is an example (taken from Figure 5.31 on page 84 of *Visual Group Theory*).

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1



As we've mentioned before, intuitively, two groups are isomorphic if they have the same structure.

Cayley's Theorem (Theorem 5.1)

Every group is isomorphic to a collection of permutations.

Our algorithms indicate that there is a 1-1 correspondence between the group elements and permutations. However, what we have not shown is that the corresponding permutations form a group or that the resulting permutation group has the same structure as the original.

What needs to be shown is that the permutation from column i followed by the permutation from column j results in the permutation that corresponding to the cell in the ith row and jth column of the original table. See page 85 for a proof.

Some more group work

Let's see Cayley's Theorem in action.

In groups of 2–3, find the permutation group for V_4 guaranteed to exist according to Cayley's theorem. Compare your answer with our original discussion of group of symmetries of the rectangle.

I want each group to turn in a complete solution.

Chapter 6: Subgroups

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

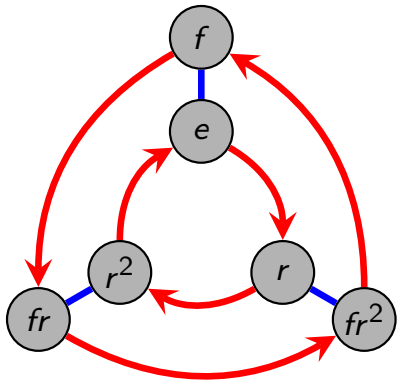
In this chapter we will introduce the concept of subgroup and begin exploring some of the rich mathematical territory that this concept opens up for us. A subgroup is some smaller group living inside a larger group.

Before we embark on this leg of our journey, we must return to a technical feature of Cayley diagrams that we temporarily ignored. This feature, called regularity, will help us visualize the new concepts that we will introduce.

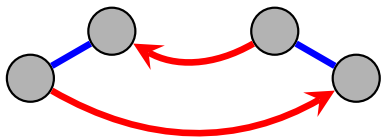
Let's begin with an example.

Regularity

Consider the Cayley diagram for $S_3 = D_3$.



By following the corresponding paths, we see that $frf = r^{-1}$. Notice that this identity manifests itself throughout the diagram regardless of which node we start at. That is, the following fragment permeates throughout the diagram.



There are other patterns that permeate this diagram, as well. Do you see any? Here are a couple: $f^2 = e$, $r^3 = e$.

An algebraic equation, like $frf = r^{-1}$ in S_3, is true not just about one portion of a Cayley diagram, but it is true *across the diagram in the same way*. Cayley diagrams always have a uniform symmetry; every part of the diagram is structured like every other.

Definition 6.1

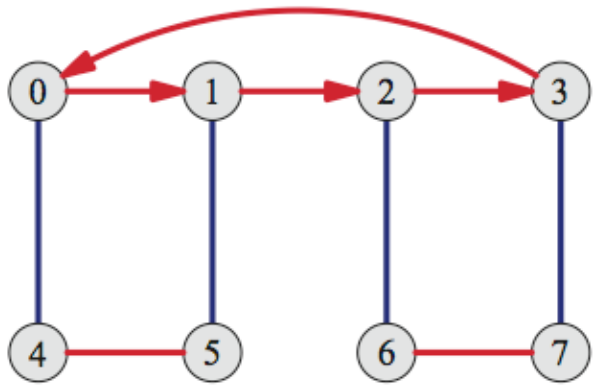
A diagram is called regular if it repeats every one of its interval patterns throughout the whole diagram, in the sense that we just discussed.

Every Cayley diagram is regular. In particular, diagrams lacking regularity do *not* represent groups (and so they are not called Cayley diagrams).

Recall that our original definition (Definition 1.9) of a group was called the "unofficial" definition of a group. One of these reasons that we called it unofficial is that technically regularity needs to be incorporated in the rules that form the definition.

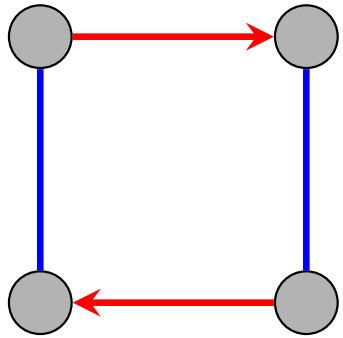
We've been hinting at the regularity property of Cayley diagrams, but we haven't spelled out the details until now.

Is the following diagram a Cayley diagram for some group?



Nope. The diagram is not regular.

How about this one?



This one is tricky. The diagram looks pretty symmetrical, so you might think that it is regular, but it is not. Notice that two of the nodes have a red arrow going in and two of them have a red arrow going out.

What would go "wrong" if we tried to form a group from this diagram? If the red arrow represents action a, then a^2 is not represented in the diagram, which violates Rule 1.8.

Definition 6.2

When one group is completely contained in another, the smaller group is called a subgroup of the larger group. When H is a subgroup of G, we write $H < G$.

All of the orbits that we saw in Chapter 5 are subgroups.

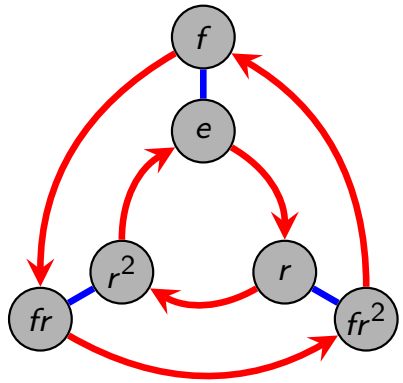
For example, the orbit of r in S_3, $\{e, r, r^2\}$, is a cyclic subgroup of order 3 living inside S_3. We can write

$$\langle r \rangle = \{e, r, r^2\} < S_3.$$

In fact, since $\langle r \rangle$ is really just a copy of C_3, we may be less formal and write

$$C_3 < S_3.$$

There are several other orbits in S_3 and all of them are cyclic subgroups. One of these orbits is staring at us in the Cayley diagram. Which one?

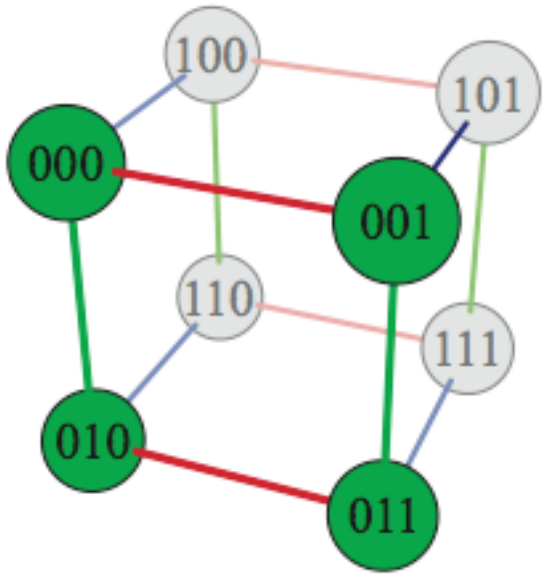


We see that

$$\langle f \rangle = \{e, f\} < S_3.$$

It turns out that all of the subgroups of S_3 are just cyclic orbits, but there are many groups that have subgroups that are not cyclic orbits.

Here is the Cayley diagram for the group $C_2 \times C_2 \times C_2$ with a copy of the subgroup V_4 highlighted (taken from Figure 6.3 on page 100 of *Visual Group Theory*.)



The group V_4 requires at least two generators and hence is not a cyclic subgroup of $C_2 \times C_2 \times C_2$. In this case, we can write

$$\langle 001, 010 \rangle = \{000, 001, 010, 011\} < C_2 \times C_2 \times C_2.$$

Every group has at least two subgroups:

1. the trivial subgroup: $\{e\}$
2. the non-proper subgroup: every group is a subgroup of itself

As we've seen, some subgroups are easy to pick out from a particular arrangement of a Cayley diagram. However, sometimes we may need to create an alternate Cayley diagram with different generators and/or different layouts for the nodes to make subgroups visually obvious.

Let's take a look at $C_6 = \{0, 1, 2, 3, 4, 5\}$ in *Group Explorer* and see if we can discover all of the subgroups by experimenting with different generators for Cayley diagrams and possibly different layouts.

What we should have discovered is that C_6 is equal to $\langle 1 \rangle, \langle 5 \rangle$, and $\langle 2, 3 \rangle$. By looking at the corresponding Cayley diagrams, we found that the subgroups of C_6 are

$$\{e\}, \langle 2 \rangle, \langle 3 \rangle, C_6.$$

Now, let's use *Group Explorer* to search for the subgroups of D_4. There are 10 subgroups (some of which are isomorphic to each other):

$$\{e\}, \underbrace{\langle r^2 \rangle, \langle f \rangle, \langle fr \rangle, \langle fr^2 \rangle, \langle fr^3 \rangle}_{\text{order 2}}, \underbrace{\langle r \rangle, \langle r^2, f \rangle, \langle r^2, fr \rangle}_{\text{order 4}}, D_4.$$

Here is a brute-force method for finding all of the subgroups of a given group G with order n:

1. we always have $\{e\}$ and G as subgroups
2. find all subgroups generated by a single element
3. find all subgroups generated by 2 elements

$\vdots$

n. find all subgroups generated by $n-1$ elements

Along the way, you are likely to duplicate subgroups. Also, this is horribly inefficient!

Note that this algorithm works because every group (and subgroup) has a set of generators.

Group work

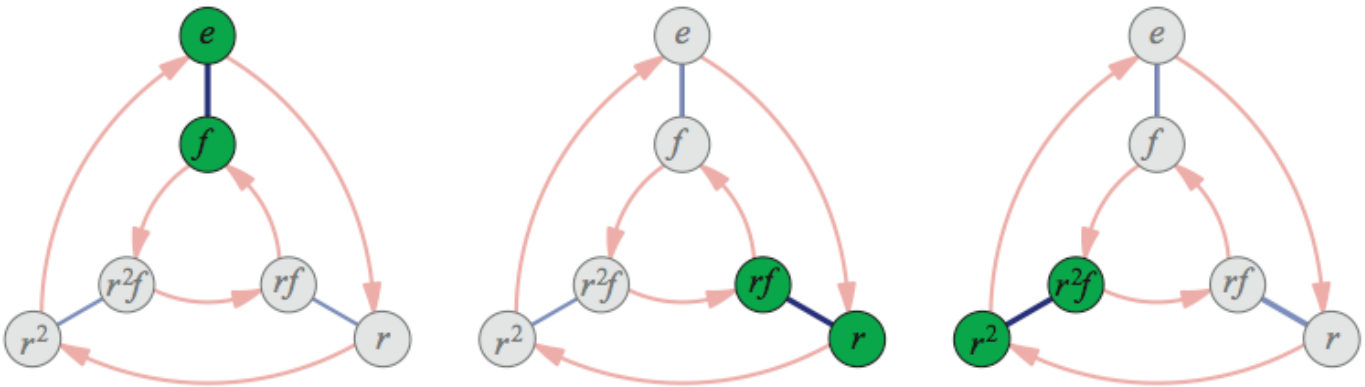
Let's explore a few more examples.

1. In groups of 2–3, complete the following exercises (not collected):
   - Exercise 6.1
   - Exercise 6.2
2. Let's discuss your solutions.
3. Now, complete Exercise 6.5(a) (ignore the part about index). I want each group to turn in a complete solution.

Cosets

The regularity property of Cayley diagrams implies that identical copies of the fragment of the diagram that corresponds to a subgroup appear throughout the rest of the diagram.

For example, the following figure (taken from Figure 6.6 on page 102 of *Visual Group Theory*) highlights the repeated copies of $\langle f \rangle = \{e, f\}$ in S_3.



However, only one of these copies is actually a group! Since the other two copies do *not* contain the identity, they cannot be groups.

The elements that form these repeated copies of the subgroup fragment in the Cayley diagram are called cosets.

To be sure that we understand this concept, let's find all of the cosets of the subgroup $\langle f, r^2 \rangle = \{e, f, r^2, fr^2\}$ of D_4. Using *Group Explorer* will help us pick the right Cayley diagram and layout, so that we can "see" the cosets.

We see that the cosets of $\langle f, r^2 \rangle$ are

$$\underbrace{\{e, f, r^2, fr^2\}}_{\text{original}}, \underbrace{\{r, r^3, fr, fr^3\}}_{\text{copy}}.$$

Now, we will list some observations concerning cosets. We will briefly justify each of these observations.

Obervation 6.3

Every subgroups has cosets, and they cover every node of the group's Cayley diagram.

This follows from the regularity of the Cayley diagram.

Obervation 6.4

Cosets can be described algebraically: we will use aH to denote the copy of H at a.

In this case, we have $aH = \{ah : a \in H\}$.

The meaning of aH: start from the node a and follow *all* paths in H.

For example, for the coset $\{r, fr^2\}$ of $\langle f \rangle$ in D_3 we can write

$$r\langle f \rangle = r\{e, f\} = \{r \cdot e, r \cdot f\} = \{r, fr^2\}.$$

Alternatively, we could have written $fr^2\langle f, r^2 \rangle$ to denote the same coset.

This leads us to the next 2 observations.

Obervation 6.5

Each coset can have more than one name.

Obervation 6.6

If $b \in aH$, then $aH = bH$.

The element that we choose to use to name the coset if called the representative. We refer to the cosets of the form aH as left cosets because we are multiplying the elements of H on the left.

There are also right cosets:

$$Ha = \{ha : h \in H\}.$$

For example, the right cosets of $\langle f \rangle$ in D_3 are

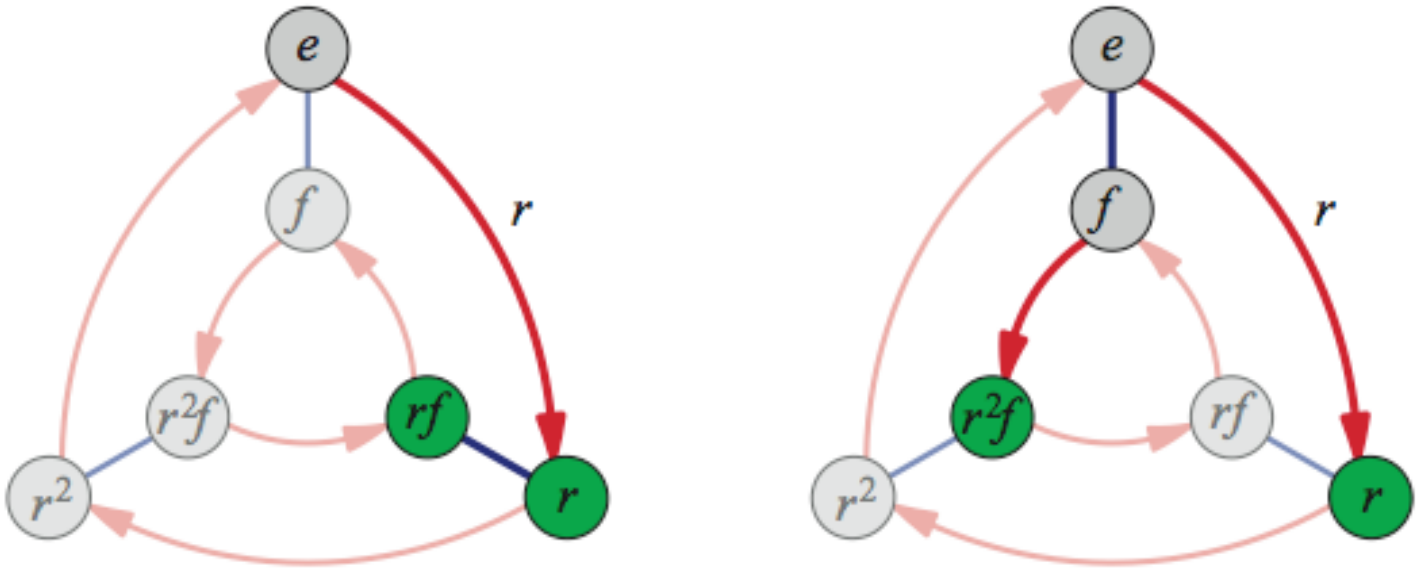
$$\langle f \rangle r = \{e, f\}r = \{e \cdot r, f \cdot r\} = \{r, fr\}$$

and

$$\langle f \rangle r^2 = \{e, f\}r^2 = \{e \cdot r^2, f \cdot r^2\} = \{r^2, fr^2\}.$$

It turns out that in this example, the left cosets for $\langle f \rangle$ were different than the right cosets. Thus, they must look different in the Cayley diagram.

The left diagram below shows the left coset $r\langle f \rangle$ in S_3, the nodes that f arrows can reach after the path to r has been followed. The right diagram shows the right coset $\langle f \rangle r$ in S_3, the nodes that r arrows can reach from teh elements in $\langle f \rangle$.



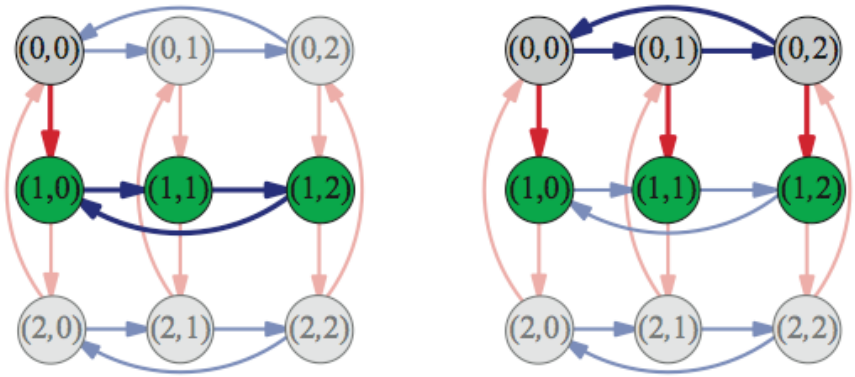
(Taken from Figure 6.7 on page 104 of *Visual Group Theory*.)

The reason that the left cosets look like copies of the subgroup while the elements of right cosets are usually scattered is that we adopted the convention that arrows represent right multiplication.

One of the most important things that we should take away from the last example is that left and right cosets are generally different.

But because they are not always different, it is worth seeing an example where they turn out to be the same.

Consider the subgroup $H = \langle (0,1) \rangle = \{(0,0), (0,1), (0,2)\}$ in the group $C_3 \times C_3$ and take $g = (1,0)$. The following figure (taken from Figure 6.9 on page 104 of *Visual Group Theory*) depicts the equality $gH = Hg$.



In this group, it turns out that $gH = Hg$ for all subgroups H and all elements g (because the group is abelian!) in $C_3 \times C_3$.

Subgroups that satisfy $gH = Hg$ for *all* elements g in the parent group are called normal.

More group work

Let's explore a few more examples.

1. In groups of 2–3 (try to mix the groups up again), complete the following exercises (not collected):
   - Exercise 6.20(a)(b) (ignore index)
   - Exercise 6.6
2. Let's discuss your solutions.

Lagrange's Theorem

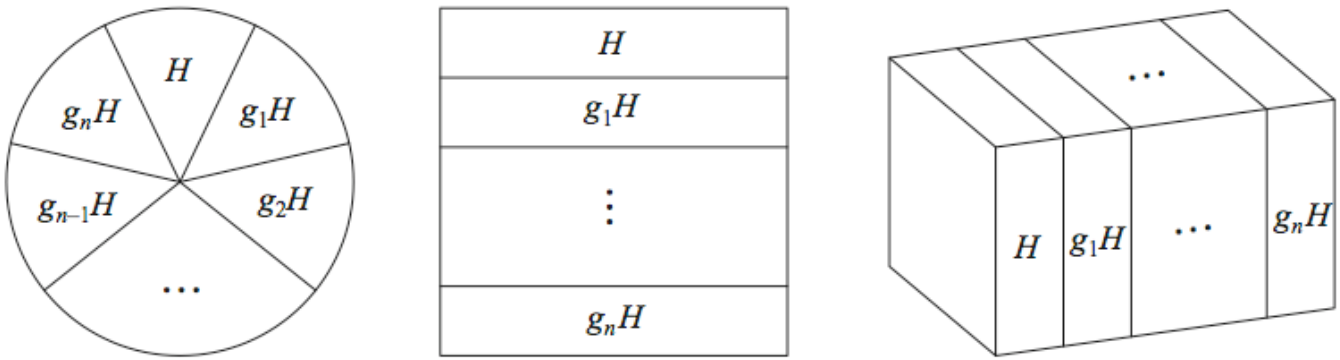
In all the examples that we've seen, not only is every element in one of the cosets of a subgroup H, but each element appears in *exactly one* left or right coset. This is true in general. That is, the left (respectively, right) cosets of a subgroup H form a partition of the parent group.

Theorem 6.7

If $H < G$, then each element of G belongs to exactly one left coset of H.

Proof. Suppose that there exist $g \in G$ such that $g \in aH$ and $g \in bH$. By Observation 6.5, $gH = aH$ and $gH = bH$. But then we must have $aH = bH$, which shows that our arbitrary g lies in a unique coset (with possibly many different names). □

The upshot of Theorem 6.7 is that we can think of a group as being composed exclusively of non-overlapping and equal size copies of any subgroup, namely that subgroup's left cosets. Here are a few visualizations of this idea (taken from Figure 6.12 on page 106 of *VGT*).



We are now ready for one of our first major theorems, which is named after the Italian-born mathematician Joseph Louis Lagrange.

Lagrange's Theorem (Theorem 6.8)

Assume G is finite. If $H < G$, then the order $|H|$ of the subgroup divides the order $|G|$ of the larger group.

Proof. Suppose there are n left cosets of the subgroup H. Since all of the left cosets of H are the same size and these left cosets partition G, we must have

$$|G| = \underbrace{|H| + \cdots |H|}_{n \text{ copies}} = n|H|.$$

This shows that $|H|$ divides $|G|$. □

Definition 6.9

If $H < G$, then the index of H in G, written $[G : H]$, is how many times $|H|$ goes into $|G|$ (which is well-defined because of Lagrange's Theorem).

$$[G : H] = \frac{|G|}{|H|}$$

Note that the index of H in G is equal to the number of left (respectively, right) cosets of H.

One powerful consequence of Lagrange's Theorem is that it significantly narrows down the possibilities for subgroups. How so?

Warning: The converse of Lagrange's Theorem is not generally true. That is, just because the order of G has a divisor does not mean that there is a subgroup of that order.

Even more group work

Let's try this out.

In groups of 2–3 (try to mix the groups up again), complete Exercise 6.4. I want each group to turn in a complete solution.

Chapter 7: Products and quotients

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

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: this process will provide us with a method for making larger groups from smaller groups.
2. quotients: this process will provide us with a method for making smaller groups from larger groups.

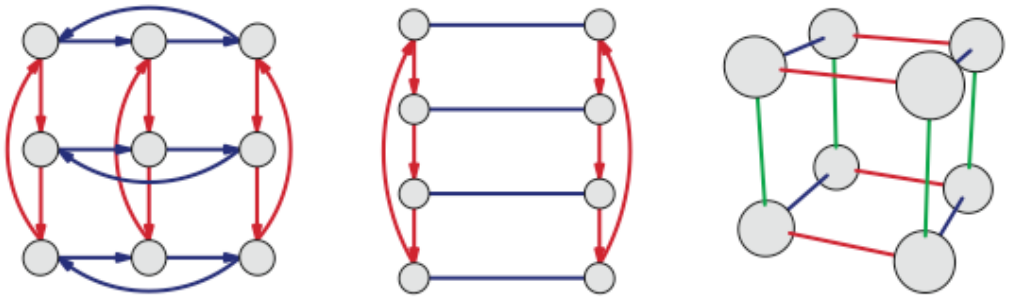
Let me mention straight away before we even describe these processes that we can *always* form a direct product of two groups. However, we cannot always take the quotient of two groups. In fact, quotients are restricted to some pretty specific circumstances as we shall see.

The direct product

Every group whose name contains the symbol $\times$ can be constructed using a process called the direct product.

However, you shouldn't be fooled into thinking that the absence of this symbol means that there isn't some hidden product. As an example, it turns out that V_4 is really just $C_2 \times C_2$.

Here are some examples (take from Figure 7.1 on page 118 of *VGT*).



$C_3 \times C_3$ $C_2 \times C_4$ $C_2 \times C_2 \times C_2$

Do you notice anything about the orders of the product groups above?

Our observation on the previous slide that the order of the direct product is equal to the product of the orders of the smaller groups is true in general. That is, $|A \times B| = |A| \cdot |B|$ for (finite) groups A and B.

But what is $A \times B$?

We will first describe the direct product construction as a process for making a new Cayley diagram from two given Cayley diagrams. Then we will uncover some properties of the corresponding group.

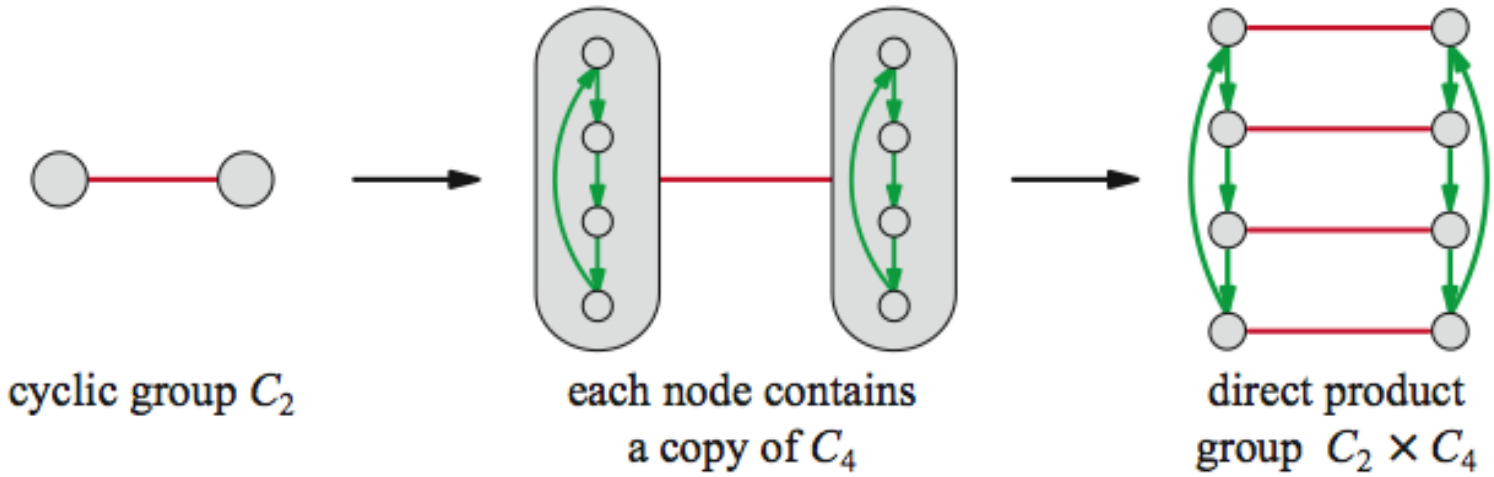
Definition 7.1

To create a Cayley diagram of $A \times B$ from Cayley diagrams of A and B, proceed as follows.

1. Begin with the Cayley diagram for A.
2. Inflate each node in the Cayley diagram of A and place in it a copy of the Cayley diagram for B. (Make sure you are using different colors for the two different 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.

It'll certainly be in our best interest to work through a couple of examples.

Consider the groups C_2 and C_4. Here is an illustration (taken from Figure 7.2 on page 119 of *VGT*) that shows the construction of $C_2 \times C_4$ via Definition 7.1.



It takes quite a bit of skill to pick the right layout for the nodes to get "pretty" representations of the direct product. However, pretty or not, what really matters is the relationships among the nodes, not how they are laid out.

Let's do an example that is a bit more difficult. Create the Cayley diagram for $C_4 \times C_3$.

An important thing to consider here is whether the diagrams that we are ending up with are actually Cayley diagrams. If they aren't, then this process is stupid. Why are the resulting diagrams actually Cayley diagrams?

Definition

The group $A \times B$ whose Cayley diagram results from the procedure in Definition 7.1 is called the direct product of A and B.

We call A and B the factors of the product.

It turns out that $A \times B$ and $B \times A$ always have the same structure (Exercise 8.36 asks you to prove this). The only difference is that the Cayley diagram for one is the other "turned on its side." We say that the direct product operation is commutative.

Our construction of the Cayley diagram for $A \times B$ yielded a diagram with unlabeled nodes. How could we go about labeling the nodes?

In $A \times B$, every element is given a name of the form (a, b), where $a \in A$ and $b \in B$. In particular, a node in the Cayley diagram for $A \times B$ has 1st coordinate a if the node belonged to the inflated node a in the Cayley diagram for A. A node has 2nd coordinate b if the corresponding node inside the inflated A node was labeled b.

Let's see if we can label the nodes of our Cayley diagram for $C_4 \times C_3$.

Group work

Let's explore a few more examples.

1. In groups of 2–3, complete the following exercises (not collected):
    - Create a Cayley diagram with labeled nodes for $C_2 \times C_2$. What familiar group is this?
    - Exercise 7.4(a)
    - Exercise 7.7(a)
    - Exercise 7.2(a)
2. Let's discuss your solutions.

Recall the following definition that we mentioned at the end of the previous chapter.

Definition 7.2

A subgroup $H < G$ is called normal if each left coset of H is also a right coset of H (and vice versa). If H is normal in G, we write $H \lhd G$.

For a direct product $A \times B$ there is always at least two normal subgroups: $A \lhd A \times B$ and $B \lhd A \times B$. You will prove this in Exercise 7.12, but in the meantime, let's at least check that this is true in $C_4 \times C_3$.

Before we do this, I must point out that we are abusing notation here. Technically, A is not even a subset of $A \times B$. $A \times B$ consists of ordered pairs (a, b), whereas, A consists of singletons. We should write $A \times \{e\} \lhd A \times B$.

First, notice that the left cosets of $C_3 = \{(0,0),(0,1),(0,2)\}$ are easy to pick out. The only thing we need to check is that these coincide with the right cosets. Let's check: (I've already thought ahead of time what some good representatives might be.)

$\{(0,0),(0,1),(0,2)\}$ (this is just the original)

$\{(0,0),(0,1),(0,2)\}(1,0) = \{(1,0),(1,1),(1,2)\}$

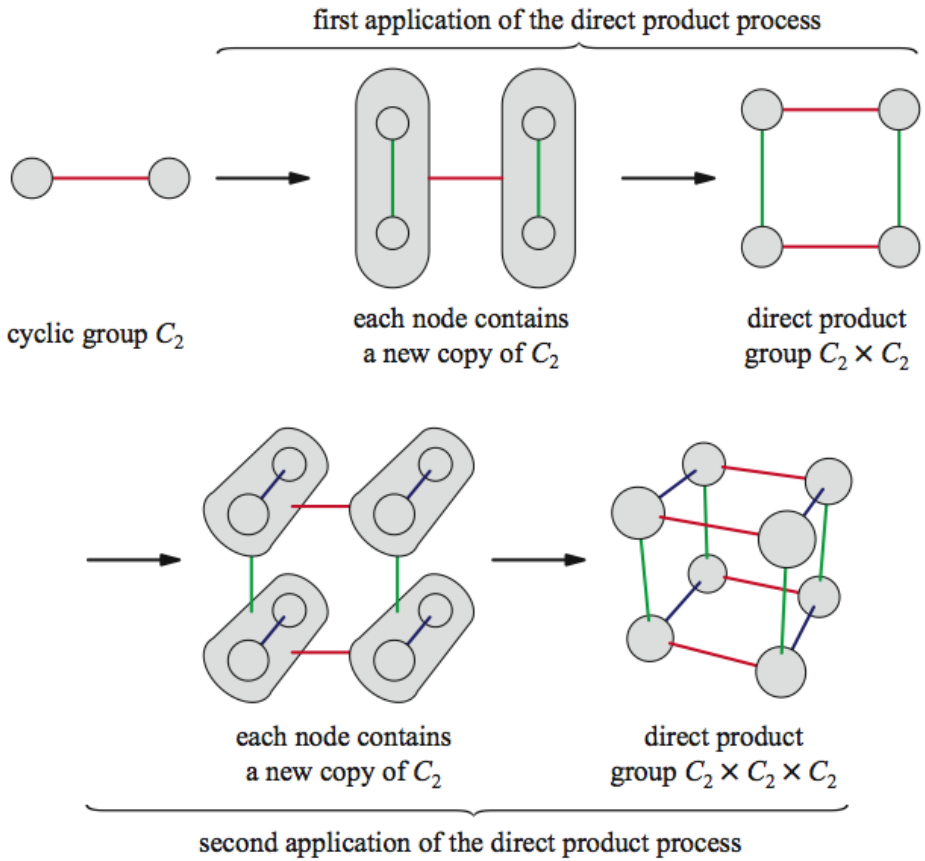
$\{(0,0),(0,1),(0,2)\}(2,0) = \{(2,0),(2,1),(2,2)\}$

$\{(0,0),(0,1),(0,2)\}(3,0) = \{(3,0),(3,1),(3,2)\}$

As we can see, the left and right cosets agree. Therefore, the group in $C_4 \times C_3$ that "is" C_3 is normal.

We can form direct products with more than 2 groups.

If we wanted to form the Cayley diagram for $A \times B \times C$, we could first construct the diagram for $A \times B$ and then construct the diagram for $(A \times B) \times C$. Here is the construction of $C_2 \times C_2 \times C_2$ (taken from Figure 7.6 on page 122 of *VGT*).



In your group work, you learned that V_4 is isomorphic to $C_2 \times C_2$. Also, recall that V_4 is isomorphic to the 2-Light Switch Group. So, we can think of the 2-Light Switch Group as $C_2 \times C_2$ (this should be satisfying!).

One interesting observation is that for the 2 light switches, the action performed on one light switch has no impact on the other and vice versa. This phenomenon occurs in all direct products.

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

Imagine you are at some node (a, b) in the Cayley diagram for $A \times B$. Then we are standing at a node that was at one step in the process contained in an inflated node for A.

Following a B arrow amounts to moving to another node in $A \times B$ that was also contained in the same inflated node of A. This will only change the B coordinate of (a, b).

On the other hand, following an A arrow results in moving to another cluster of nodes that were contained in a different inflated node of A. This will only change the A coordinate of (a, b).

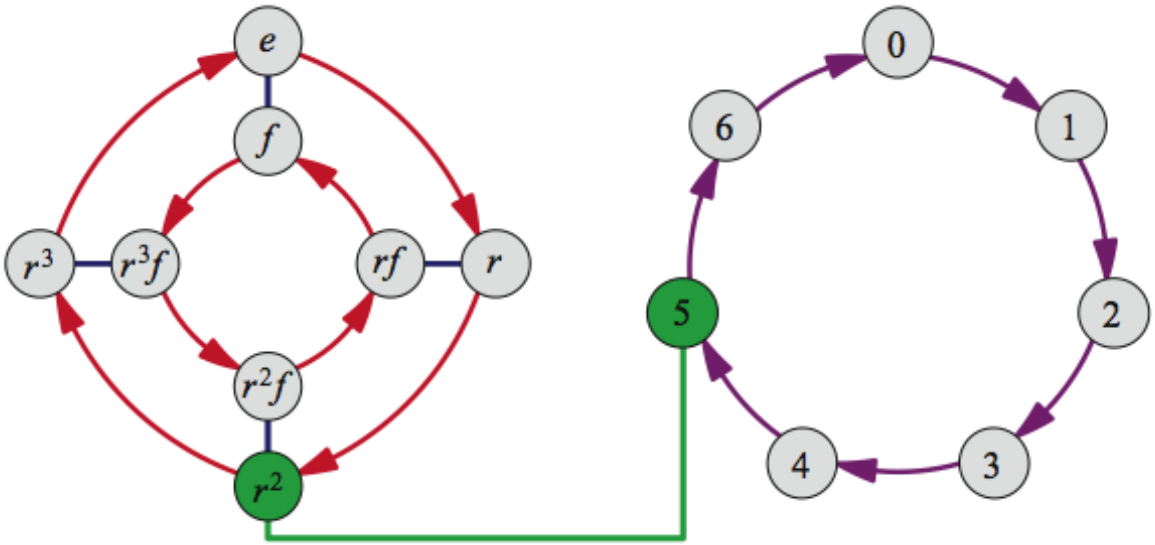
The moral of the story is that the direct product of two groups joins the groups, so that that act independently of each other.

One of the benefits of this revelation is that instead of forming large and complicated Cayley diagrams for $A \times B$, we can think of an action in $A \times B$ as simply instructions for where to go in the Cayley diagram for A and where to go in the Cayley diagram for B.

Here's how I think of the direct product of two cyclic groups, say $C_n \times C_m$: 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 the first wheel and where we end up on the second wheel: say (i, j).

Here is an example of a visual for more general direct products (taken from Figure 7.11 on page 125 of *VGT*) showing the element $(r^2, 5)$ in $D_4 \times C_7$.



One hugely important consequence of the independence of the factors in a direct product is that it tells us that the binary operation in $A \times B$ is simply done coordinate-wise.

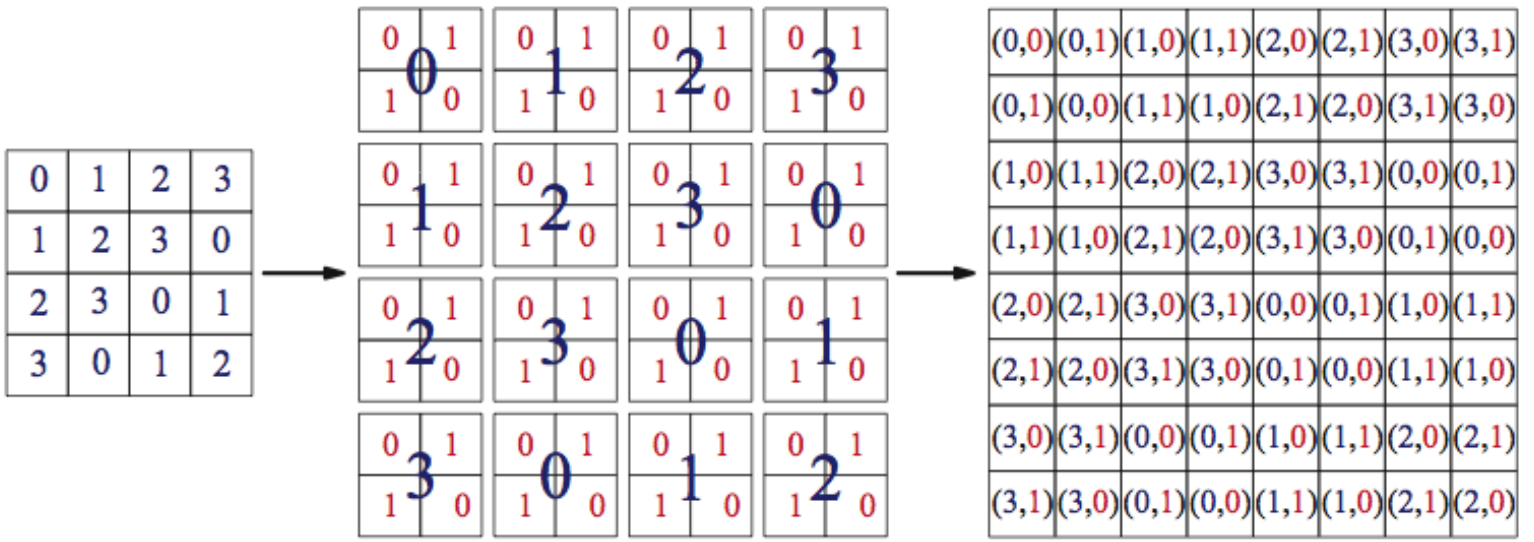
Suppose that $(a, b), (c, d) \in A \times B$. Then

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

It is important to point out that our construction of $A \times B$ along with our method for labeling the nodes respects this binary operation.

As an example, in $D_3 \times C_4$, $(r^2, 1) * (fr, 3) = (fr^2, 0)$.

Direct products can also be visualized using group tables. Definition 7.3 on page 126 gives a detailed list of instructions for creating a multiplication table for $A \times B$ from the multiplication tables for A and B. However, I think you'll understand the general process after discussing this example (taken from Figure 7.12 on page 126 of *VGT*) of $C_4 \times C_2$.



multiplication table for the group C_4

inflate each cell to also contain a copy of the multiplication table for C_2

join the little tables and element names to form the final direct product table

More group work

In groups of 2–3, complete all parts of Exercise 7.3. I want each group to turn in a complete solutions.

Let's discuss your solutions.

Quotients

We saw how we can use direct products to form larger groups from smaller groups. Now, we discuss the opposite procedure, which is called taking a quotient.

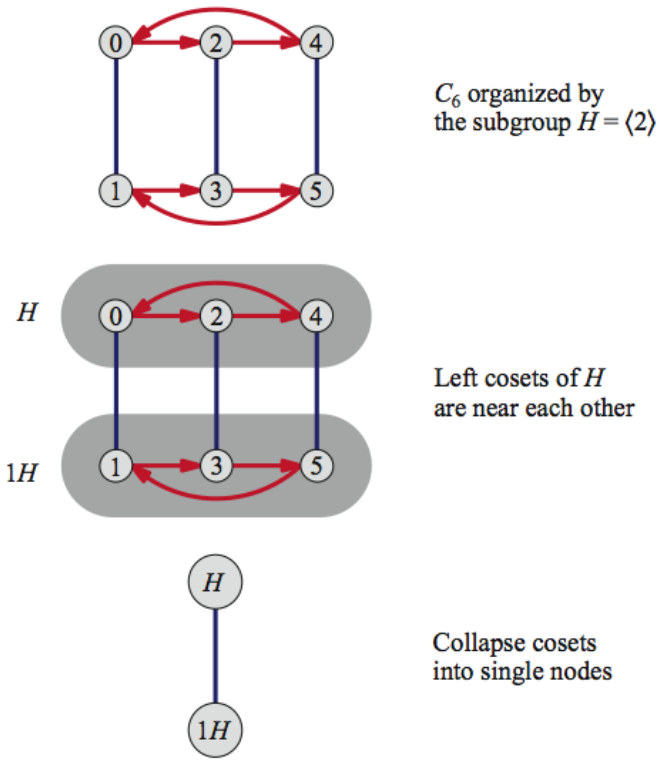
As we did with direct products, we will first describe the quotient operation using Cayley diagrams and then we will explore some properties of the resulting group.

Definition 7.5

To attempt 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 the resulting diagram is a Cayley diagram of a group, then you have obtained the quotient group of G by H, denoted G/H and often read "G mod H." If not, then G cannot be divided by H.

Here is a picture (taken from Figure 7.20 on page 133 of *VGT*) that illustrates the process of Definition 7.5 for the group $G = C_6$ and its subgroup $H = \langle 2 \rangle$.



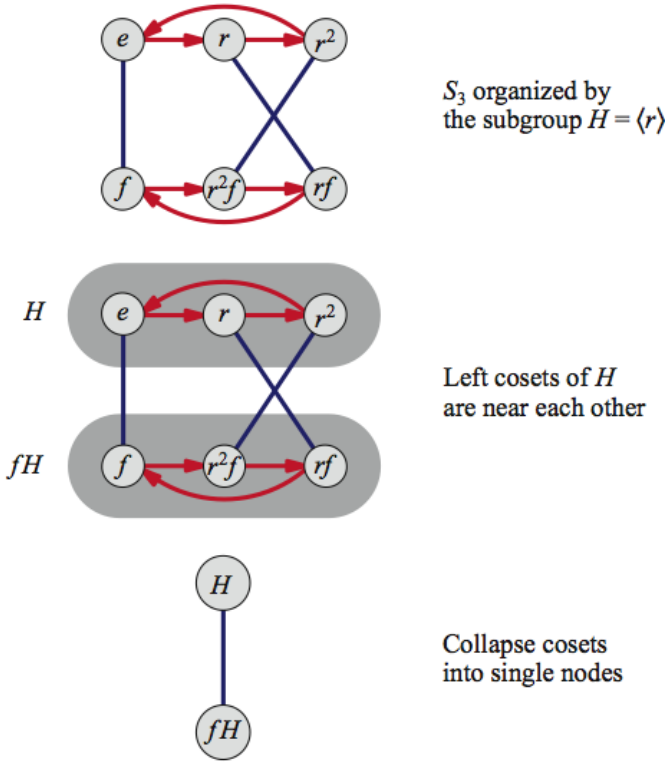
(Labeling of nodes 1, 3, 5 is wrong.)

In this example, the resulting diagram *is* a Cayley diagram. So, we can divide C_6 by $\langle 2 \rangle$. In fact, we see that $C_6/\langle 2 \rangle$ is isomorphic to C_2.

Comments

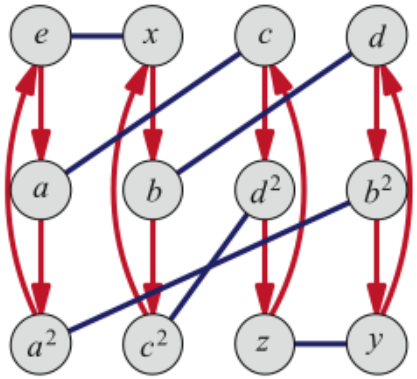
- Step 3 of Definition 7.5 says "If the new diagram is a Cayley diagram ..." It is important to point out that sometimes it won't be, in which case there is no quotient.
- *Important*: The elements of the quotient G/H (if it exists) are the cosets of H. We focus our attention on the teams rather than the individual players.
- As one would expect, if $G = A \times B$ and we divide G by A, then the quotient group is B (it turns out that this always works; we'll see why shortly). However, the converse is not generally true. That is, if we can divide G by H, then that does not necessarily mean that G is equal to a direct product of H and the result of dividing G by H.

Let's take a look at another example. The following picture (taken from Figure 7.21 on page 134 of *VGT*) shows the result of dividing S_3 by $H = \langle r \rangle$.



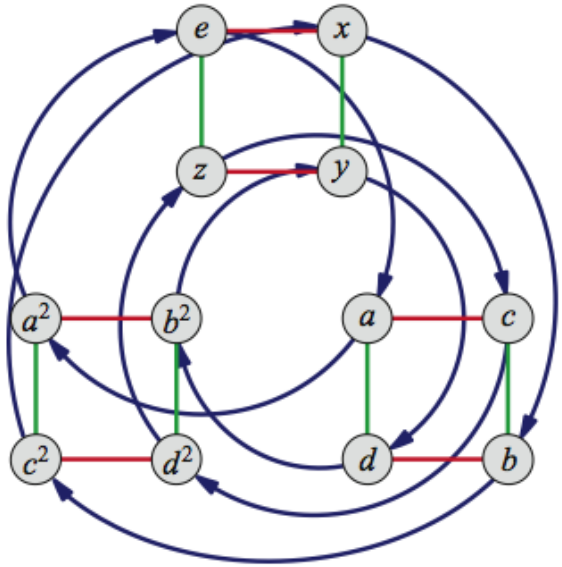
The resulting diagram is a Cayley diagram. So, S_3/C_3 makes sense and is isomorphic to C_2. However, you can tell by the inconsistent wiring of nodes in the middle step that S_3 is not a direct product of C_3 and C_2.

Here's another example. Consider the group A_4 and its subgroup $\langle x, z \rangle$. Recall that one possible Cayley diagram for A_4 (with generators a and x) was the following figure (taken from page 54 of *VGT*).



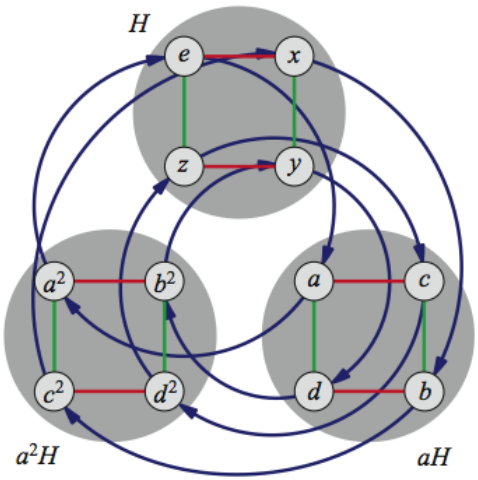
However, the subgroup $H = \langle x, z \rangle$ is not obvious from this diagram. It turns out that $H = \langle x, z \rangle$ is isomorphic to V_4.

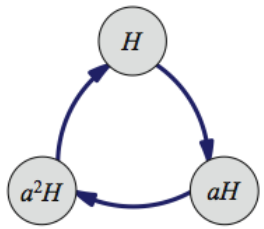
Here is a Cayley diagram for A_4 (with generators x, z, and a) organized by $H = \langle x, z \rangle$.



We can now see the left cosets of H clearly.

The following figure (taken from Figure 7.23 on page 136 of *VGT*) show the steps of Definition 7.5.



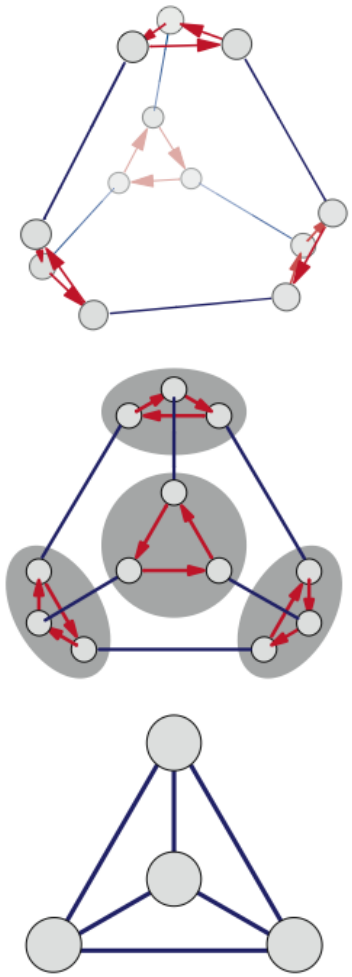


As we can see, the resulting diagram is a Cayley diagram. So, A_4/V_4 is isomorphic to C_3. However, A_4 is not isomorphic to $V_4 \times C_3$.

The last 3 examples may have tricked you into thinking that we can divide G by any H, but as we've already mentioned, we can't. OK, so what can go wrong?

Again, consider the group A_4. But this time, let's try to divide by its subgroup $H = \langle a \rangle$. In this case, H is a cyclic subgroup of order 3.

The figure on the next slide (taken from Figure 7.26 on page 138 of *VGT*) shows the result of trying to divide A_4 by $H = \langle a \rangle$.



OK, so what's wrong? This diagram is *not* a Cayley diagram. It violates Rule 1.7; there is ambiguity about which blue arrow to travel anytime we leave a node.

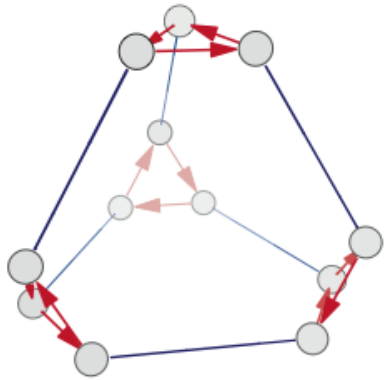
The big question is: when can we divide G by H and when can't we?

It turns out that the answer depends on whether H is normal or not.

This ought to take some convincing.

First, let's determine whether the subgroup in A_4 isomorphic to C_3 is normal or not.

Using the following Cayley diagram for A_4, the left cosets of $H = \langle a \rangle$ are easy to pick out.



Are the right cosets the same as the left cosets? The answer is no. For example, following blue arrows out of any single coset scatters the nodes.

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

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

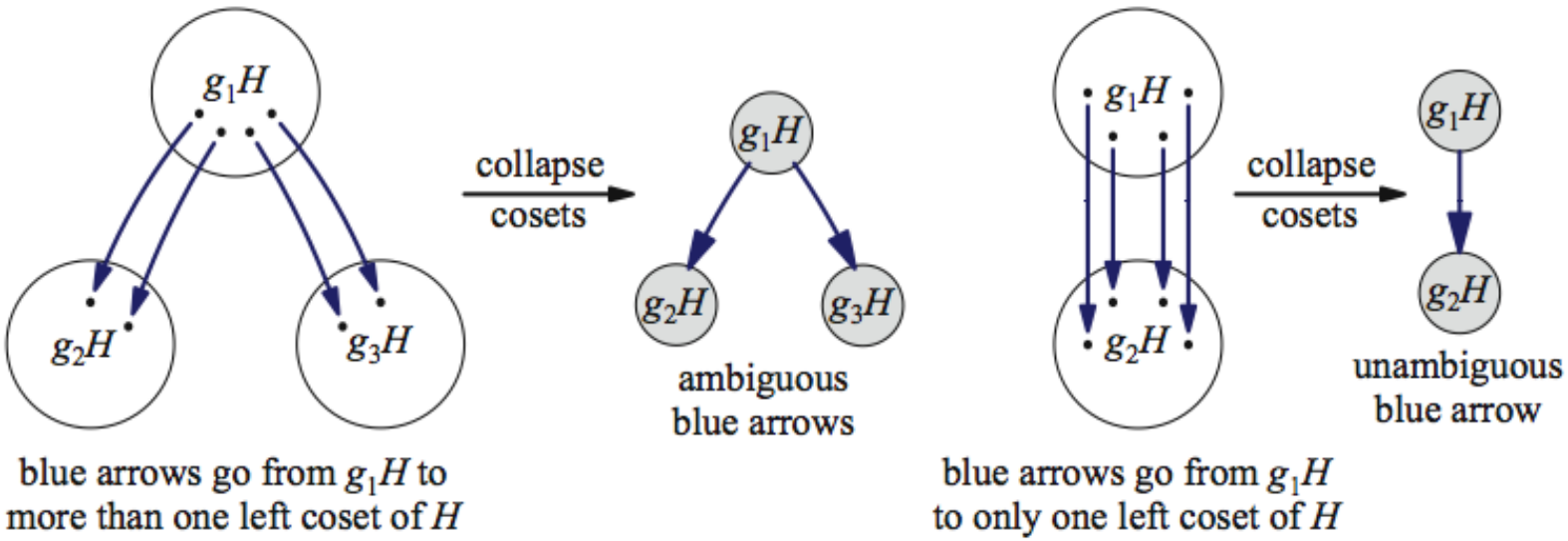
However, these 4 examples do not constitute a proof; they only provide evidence that my claim is true.

Let's see if we can gain some more insight. Consider a group G with subgroup H.

Recall that:

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

The following figure (taken from Figure 7.27 on page 139 of *VGT*) depicts the potential ambiguity that may arise when cosets are collapsed in the sense of Definition 7.5.



Note that the action of the blue arrows above is illustrating multiplication of a left coset on the *right* by some element. That is, the picture is showing us how left and right cosets interact.

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).

Finally, let's state the answer to our original question to when we can take a quotient.

Theorem 7.6

If $H < G$, then a quotient group G/H can be constructed only when $H \lhd G$.

Proof. The quotient process of Definition 7.5 succeeds only when the resulting diagram is a valid Cayley diagram. Nearly all aspects of valid Cayley diagrams are guaranteed by the quotient process.

Because we begin with a diagram that has an arrow of every color exiting every node, our resulting diagram has this property, as well.

Since we begin with a regular diagram and we collapse identically structured sections distributed uniformly throughout the diagram, we end up with a regular diagram.

The only problem that can arise is ambiguity of arrow color at a given node. But we have already argued that this problem is avoided when H is normal. □

Group work

Let's explore a few more examples.

1. In groups of 2–3, complete the following exercises (not collected):
   - Exercise 7.18(a)
   - Exercise 7.18(b)
2. Let's discuss your solutions.
3. Now, complete Exercise 7.18(f). I want each group to turn in a complete solution.

Normalizers

Some subgroups are normal and some are not. An interesting question is: if $H < G$ with H *not* normal, can we measure how far H is from being normal?

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

At a minimum, we know that every $g \in H$ vote in favor of H being normal. Why? Well, since H is closed, if $g \in H$, we must have $gH = H = Hg$.

At a maximum, we would have *all* $g \in G$ voting in favor of H being normal, but this only happens when H really is normal.

There can be levels in 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,

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

Let's explore some possibilities for what the normalizer of a subgroup can be.

First, observe that if some $g \in G$ satisfies $gH = Hg$, then every element of the coset gH does, too. This follows from the fact that any member of gH (respectively, Hg) can be used as a representative of the coset.

So, $N_G(H)$ is made up of whole cosets of H. This implies that the size of $N_G(H)$ must be a multiple of $|H|$.

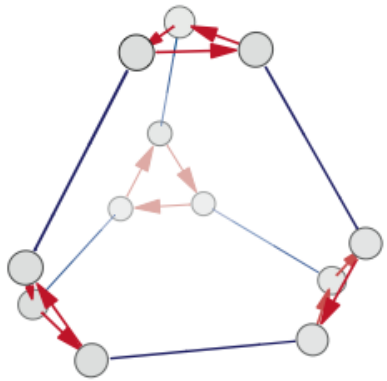
Furthermore, the deciding factor in how a left coset will vote is simply whether it is also a right coset (because gH votes as a block exactly when $gH = Hg$).

Since $N_G(H)$ is composed of left cosets of H that are also right cosets, we can describe the normalizer visually. The normalizer of H in G is made up of those copies of H that are connected to H by unanimous arrows.

We need some examples.

We saw earlier that the subgroup $H = \langle x, z \rangle$ is normal in A_4. So, $N_{A_4}(H) = A_4$.

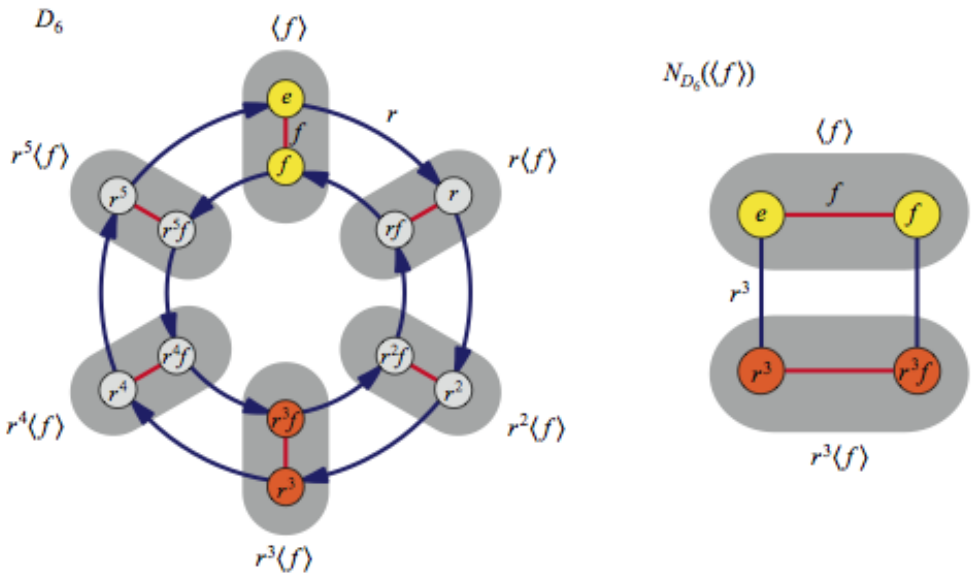
At the other extreme, consider $\langle a \rangle$ in A_4 again.



As we discussed earlier, this subgroup is *not* normal. In fact, it is as far from normal as it can possibly be.

We see that no right coset coincides with a left coset other than $\langle a \rangle$ itself. Thus, $N_{A_4}(\langle a \rangle) = \langle a \rangle$.

For our third example, consider D_6 and its subgroup $\langle f \rangle$. The following figure (taken from Figure 7.29 on page 142 of *VGT*) shows that $\langle f \rangle$ is not normal in D_6, but that its normalizer is something between $\langle f \rangle$ and D_6.



We see that $N_{D_6}(\langle f \rangle) = \{e, f, r^3, r^3 f\}$, which is isomorphic to V_4. What you should notice is that in this example, the normalizer is also a subgroup! It turns out that this is always true.

Theorem 7.7

For any $H < G$, $N_G(H) < G$, as well.

For a proof, see pages 141–142 of *VGT*.

Comments

- We have
$$H \lhd N_G(H) < G.$$
- The closer $N_G(H)$ is to being all of G, the closer H is to being normal.

More group work

Let's explore a few more examples.

1. In groups of 2–3, complete the following exercises (not collected):
    - Exercise 7.25(a)
    - Exercise 7.25(b)
2. Let's discuss your solutions.
3. Now, complete Exercises 7.26(a) and 7.26(b). I want each group to turn in a complete solution for both exercises.

Chapter 8: The power of homomorphisms

Dana C. Ernst

Plymouth State University
Department of Mathematics
http://oz.plymouth.edu/~dcernst

Summer 2009

Throughout the course, we've said things like:

- "This group has the same structure as that group."
- "This group is isomorphic to that group."

However, we've never really spelled out the details about what this means. In this chapter, we'll finally nail down what an isomorphism really is.

In general, we will study special types of functions between groups called homomorphisms, where isomorphisms are a specific type of homomorphism. The Greek roots "homo" and "morph" together mean "same shape."

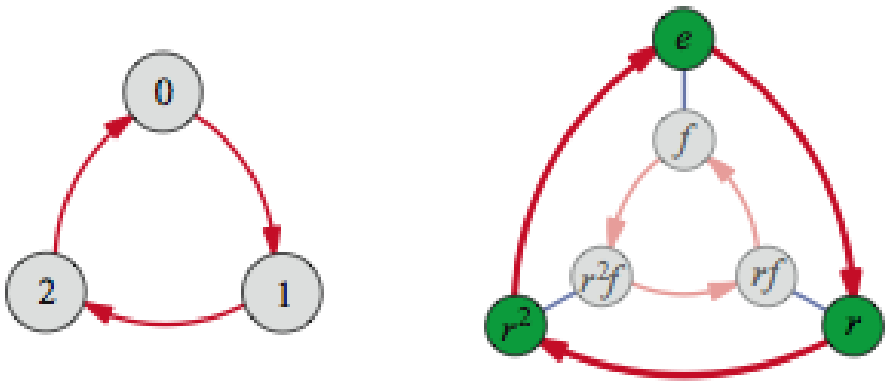
There are two situations (and it turns out that there are only two) where homomorphisms arise:

- when one group is a subgroup of another;
- when one group is a quotient group.

The corresponding homomorphisms are called embeddings and quotient maps.

Embeddings

Let's start off with an example. Consider the statement: $C_3 < S_3$. Here is a visual (taken from Figure 8.1 on page 158 of *VGT*).

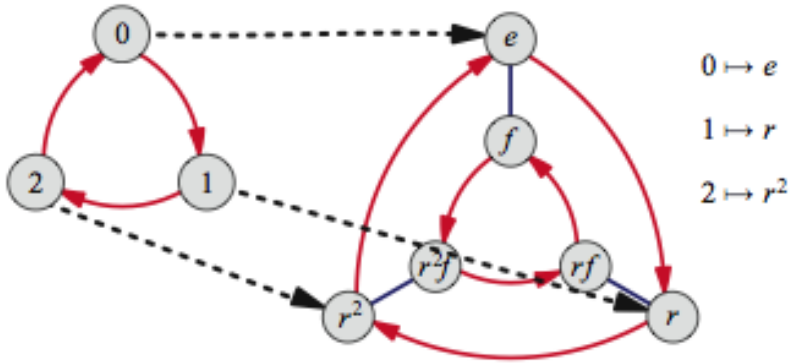


The highlighting in this figure shows that S_3 contains a 3-step cyclic subgroup, which is identical to C_3 in structure only. None of the elements of C_3 (namely 0, 1, 2) are actually in S_3.

When we say $C_3 < S_3$, what we really mean is that the structure of C_3 shows up in S_3.

In particular, there is a 1-1 correspondence between the elements in C_3 and the elements of the 3-step cyclic subgroup in S_3, and furthermore, the relationship between the corresponding nodes is the same.

The following figure (taken from Figure 8.1 on page 158 of *VGT*) illustrates this correspondence.



Homomorphisms are the mathematical tool for succinctly expressing precise structural correspondences. Because homomorphisms describe how elements of one group correspond to elements of another, they are a kind of function.

In the case of our previous example, we say that this function maps elements of C_3 to elements of S_3.

Often Greek letters are used to name maps between groups. For our example, let's use ϕ. We write $\phi : C_3 \to S_3$ to say that ϕ maps C_3 to S_3.

We use standard function notation and terminology. For example, we can write $\phi(1) = r$. In fact, there is a formula for expressing the function in our example: $\phi(n) = r^n$.

The group from which a function originates is called its domain (C_3 in our example) and the group into which the function maps is called the codomain (S_3 in our example).

The particular elements of the codomain that the function maps to are called the image of the function ($\{e, r, r^2\}$ in our example), denoted $Im(\phi)$.

It is important to note that not every function from one group to another is going to be a homomorphism. In our example, the domain and codomain respected each other's structure. We need all homomorphisms to have this same property.

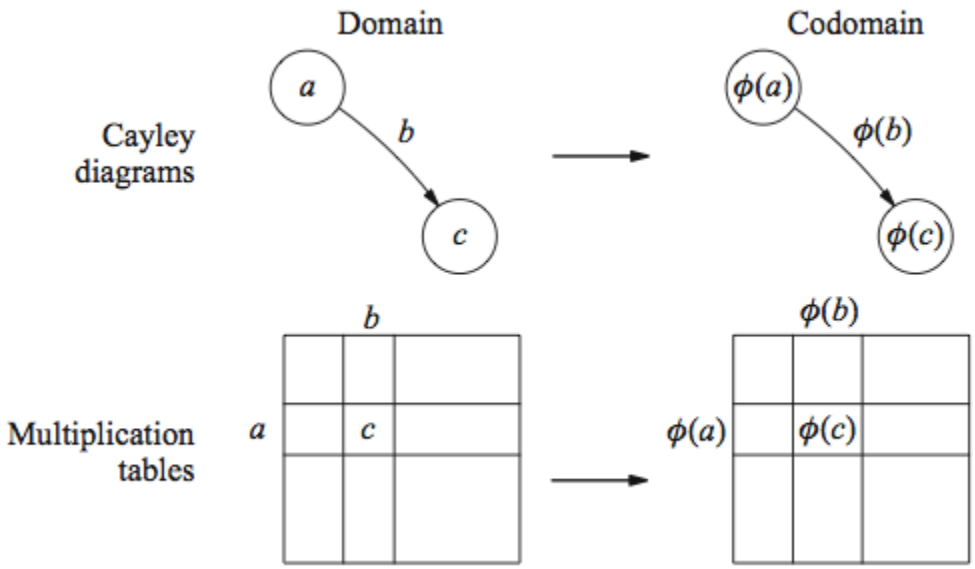
Definition 8.1

A homomorphism is a function between 2 groups that mimics the structure of it domain and codomain. The following condition expressions this requirement (stated in two different ways).

1. Cayley diagrams: If an arrow b in the domain leads from a to c, then the $\phi(b)$ arrow in the codomain must lead from the element $\phi(a)$ to $\phi(c)$.
2. Multiplication tables: If the domain multiplication table says $a \cdot b = c$, then the codomain multiplication table must say that $\phi(a) \cdot \phi(b) = \phi(c)$.

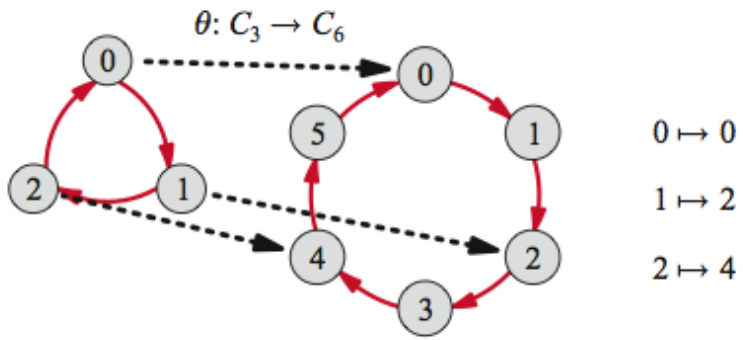
Note that the operation $a \cdot b$ is occurring in the domain while $\phi(a) \cdot \phi(b)$ occurs in the codomain.

The following figure (taken from Figure 8.3 on page 159 of *VGT*) is an illustration of Definition 8.1.

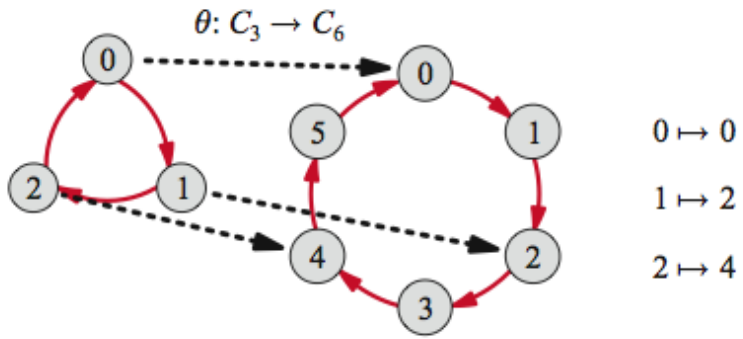


We say that the homomorphism is structure preserving.

Let's walk through another example. We can express $C_3 < C_6$ using the homomorphism $\theta : C_3 \to C_6$ defined by $\theta(n) = 2n$. Here is a visual representation of θ (taken from Figure 8.4 on page 160 of *VGT*).



But is this really a homomorphism? We need to verify that any path from a to b in C_3 corresponds to the path from $\theta(a)$ to $\theta(b)$ in C_6.



θ maps 1 to 2, but it also maps the 1-arrow in C_3 to the 2-step path representing 2 in C_6. The 1 arrow traces the orbit $\{0, 1, 2\}$ in C_3 while the $\theta(1)$ path traces the corresponding orbit $\{\theta(0), \theta(1), \theta(2)\}$ in C_6, which is $\{0, 2, 4\}$.

We can think of the $\theta(1)$ arrow as the path consisting of two red arrows in succession. So, θ doubles both numbers and arrows.

What this last example illustrates to us is that if we know where a homomorphism maps *all* of the domains arrows (i.e., generators), then we know where it maps the rest of the nodes.

For example, suppose there was another homomorphism $\theta' : C_3 \longrightarrow C_6$ different from θ such that $\theta'(1) = 4$. Using this information, we can construct the rest of the homomorphism using the fact that θ' must obey $\theta'(a + b) = \theta'(a) + \theta'(b)$.

We see that

$$\theta'(2) = \theta'(1 + 1) = \theta'(1) + \theta'(1) = 4 + 4 = 2$$

and

$$\theta'(0) = \theta'(1 + 2) = \theta'(1) + \theta'(2) = 4 + 2 = 0.$$

We can use the same general process to determine where a homomorphism maps all the elements of the domain by just knowing where the generators are mapped.

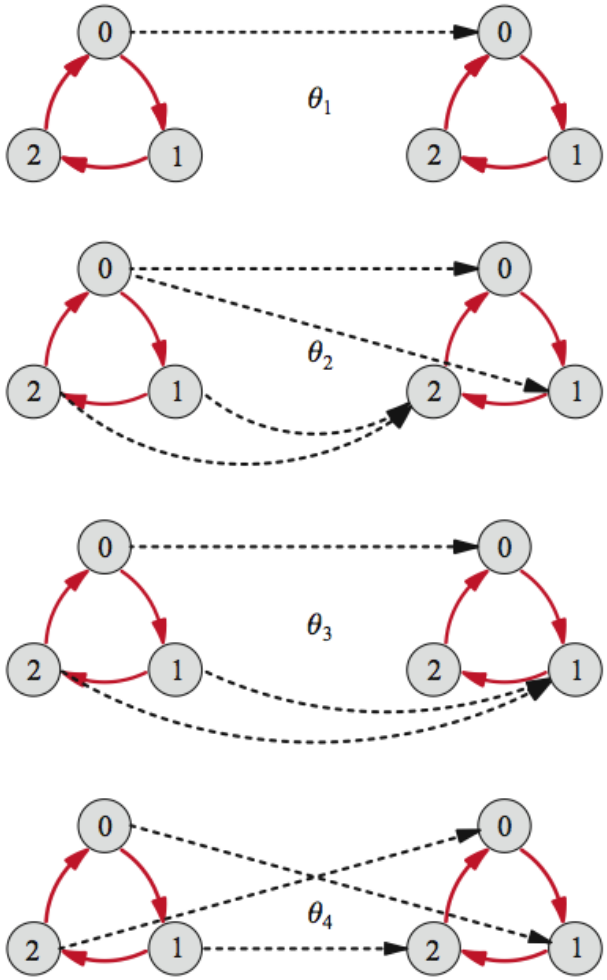
Say $\phi : G \to H$ and assume that $G = \langle a, b \rangle$ and we are give the value of $\phi(a)$ and $\phi(b)$. Using this information we can determine the image of any element in G. For example, for $g = aaabbbab$, we have

$$\phi(aaabbbbab) = \phi(a)\phi(a)\phi(a)\phi(b)\phi(b)\phi(a)\phi(b).$$

Similar reasoning works for any number of generators.

One consequence of this is that the identity of the domain must *always* map to the identity in the codomain (see Exercise 8.7).

The following figure (taken from Figure 8.5 on page 161 of *VGT*) illustrates some non-homomorphisms.



A function maps *each* element of the domain to some element of the codomain. But θ_1 ignores two elements of the domain, and thus is not a function.

A function maps each element of the domain to *one* element of the codomain. But θ_2 maps 0 to two different elements of the domain, and thus is not a function.

Although θ_3 is a function, it is not a homomorphism. In the domain, $1 + 1 = 2$, but in the codomain, $\theta_3(1) + \theta_3(1) \neq \theta_3(2)$.

Although θ_4 is a function, it is not a homomorphism. Although the image is a 3-cycle like the domain, θ_4 does not map the domain identity element to the codomain identity element. For example, $\theta_4(0) + \theta_4(1) \neq \theta_4(1)$.

Any homomorphism that helps us get information about how one group is a subgroup of another is called an embedding.

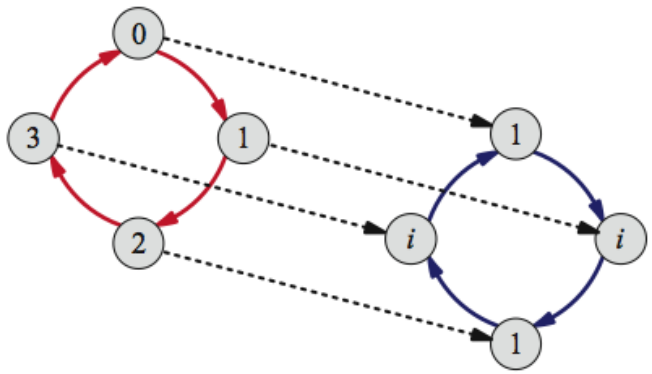
Because any embedding finds a copy of the domain in the codomain, its image is therefore the same size as its domain. So, embeddings never map 2 different elements of the domain to the same element in codomain (i.e., they are 1-1).

An embedding whose image fills the whole codomain shows us that the domain and codomain are actually the same size and have all the same structure. In this case, we say that the function is not just a homomorphism, but an isomorphism.

Two isomorphic groups may name their elements differently and may look different based on the layouts or choice of generators for their Cayley diagrams, but the isomorphism between them guarantees that they have the same structure.

When two groups G and H have an isomorphism between them, we say that "G and H are isomorphic." In this case, we write $G \cong H$.

The following figure equipped with some mislabeling (taken from Figure 8.8 on page 163 of *VGT*) depicts an isomorphism between C_4 and the group of complex numbers $\{1, -1, i, -i\}$.

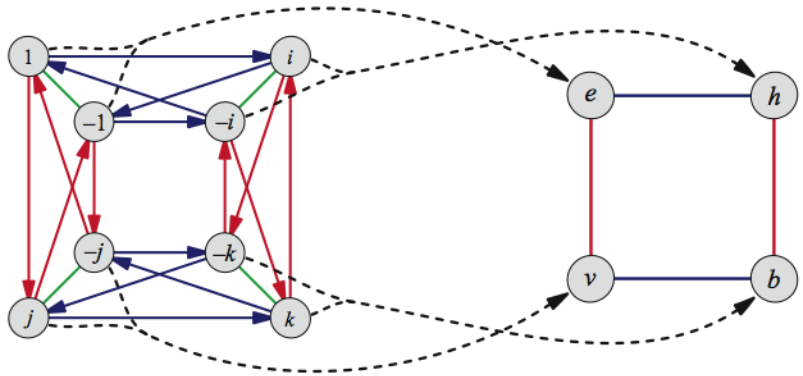


In this case, $C_4 \cong \{i, -1, i, -i\}$.

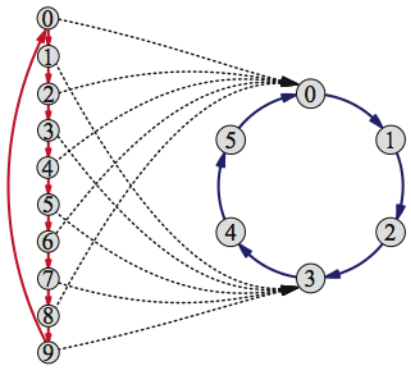
Quotient maps

Well, what happens if more than one element of domain maps to the same element of codomain (i.e., non-embeddings)? Here are some examples (taken from Figure 8.9 on page 164 of *VGT*).

$\tau_1 : Q_4 \to V_4$



$$\tau_2 : C_{10} \to C_6 \text{ by } \tau_2(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases}$$



In the interest of time, we'll skip many of the details of this type of situation. All non-embedding homomorphisms are called quotient maps (because they correspond to our quotient process).

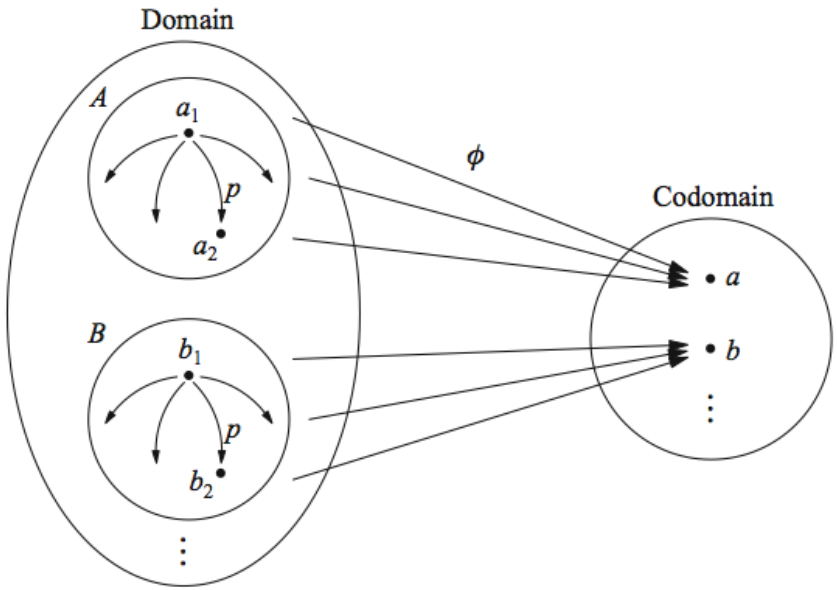
General facts about quotient maps

- Every cluster of domain elements that maps to the same codomain element has the same structure. That is, every non-embedding homomorphism follows a repeating pattern.
- This creates a partition of the domain into identical copies of a structure. (Sound familiar?)
- The clusters of domain elements that map to the same codomain element are actually a subgroup and its cosets.
- The cluster of elements from domain that map to the identity in codomain is the subgroup and the other clusters are the cosets. We call this subgroup the kernel of the homomorphism, denoted $Ker(\phi)$.

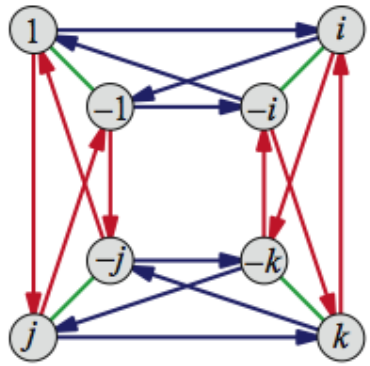
General facts about quotient maps (cont)

- The left cosets of $Ker(\phi)$ are also right cosets. So, $Ker(\phi)$ is a normal subgroup of the domain.
- This means that we can always form the quotient group $G/Ker(\phi)$, where G is the domain of the homomorphism ϕ.

Here is an abstract picture of what quotient maps look like in general (taken from Figure 8.10 on page 165 of *VGT*).



Let's work through an example. Define the homomorphism $\phi : Q_4 \to V_4$ via $\phi(i) = v$ and $\phi(j) = h$. ϕ's "action" on the generators i and j is enough to determine everything else we need to know. Here is the Cayley diagram for Q_4 (taken from Figure 8.12 on page 167 of *VGT*).



Let's determine:

1. the image of the rest of the elements
2. $Ker(\phi)$

What is $Q_4/Ker(\phi)$? Do you notice any relationship between $Q_4/Ker(\phi)$ and $Im(\phi)$?

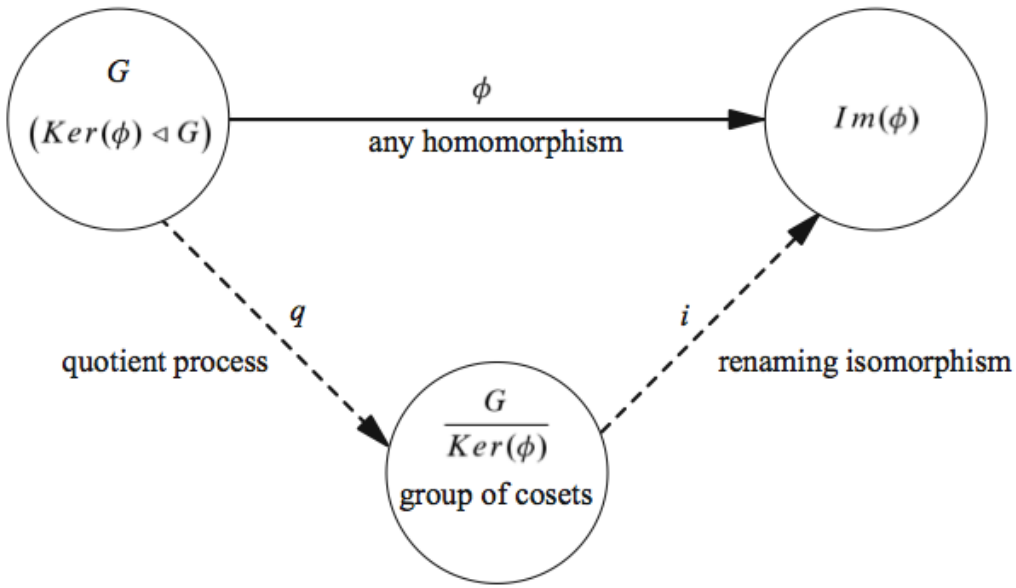
The Fundamental Homomorphism Theorem

Here is one of the crowning achievements of group theory.

Fundamental Homomorphism Theorem

If $\phi : G \to H$ is a homomorphism, then $Im(\phi) \cong G/Ker(\phi)$.

Here is an abstract illustration of the Fundamental Homomorphism Theorem (taken from Figure 8.13 on page 168 of *VGT*).



Unfortunately, we did not have time to prove all of the details leading up to this and we also don't have time to prove this theorem.

Notice that in the special case that ϕ is an embedding, $Ker(\phi) = \{e\}$, in which case the FHT says $Im(\phi) \cong G/\{e\}$. But $G/\{e\}$ is certainly isomorphic to G. So, in the case of an embedding, the FHT simply says that $Im(\phi) \cong G$.

Also, one consequence of the Fundamental Homomorphism Theorem is that $Im(\phi)$ must be a subgroup of the codomain.

Let's take a look at one last example.

The following figure (taken from Figure 8.18 on page 172 of *VGT*) illustrates an isomorphism between C_{12} and $\mathbb{Z}/\langle 12\rangle$.