Chapter 4: Algebra and group presentations

Matthew Macauley

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

Math 4120, Summer I 2014

Overview

Recall that our informal definition of a group was a collection of actions that obeyed Rules 1–4. This is not the ordinary definition of a group.

In this chapter, we will introduce the standard (and more formal) definition of a group. We will also spend time convincing ourselves that both definitions agree.

Along the way, we will use multiplication tables to better understand groups.

Finally, we will learn about group presentations, an algebraic device to concisely describe groups by their generators and relations.

For example, the following is a presentation for a group that we are familiar with:

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

Do you recognize this group?

More on Cayley diagrams

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

Our choice of generators influenced the resulting Cayley diagram!

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

1. Labeling the nodes with configurations of a thing we are acting on.
2. Leaving the nodes unlabeled (this is the "abstract Cayley diagram").

There is a 3rd thing we can do with the nodes, motivated by the fact that every path in the Cayley diagram represents an action of the group:

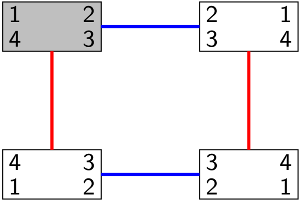
3. Label the nodes with actions (this is called a "diagram of actions").

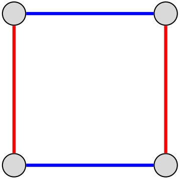
Motivating idea

If we distinguish one node as the "unscrambled" configuration and label that with the identity action, then we can label each remaining node with the action that it takes to reach it from the unscrambled state.

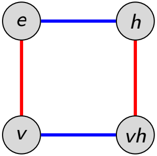
An example: The Klein 4-group

Recall the "rectangle puzzle." If we use horizontal flip (h) and vertical flip (v) as generators, then here is the Cayley diagram labeled by configurations (left), and unlabeled Cayley diagram (right):





Let's apply the steps to the abstract Cayley diagram for V_4, using the upper-left node as the "unscrambled configuration":



Note that we could also have labeled the node in the lower right corner as hv, as well.

How to label nodes with actions

Let's summarize the process that we just did.

Node labeling algorithm

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 "identity 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!

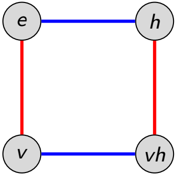
Some authors use the opposite convention, motivated by "function composition."

A "group calculator"

One neat thing about Cayley diagrams with nodes labeled by actions is that they act as a "group calculator".

For example, if we want to know what a particular sequence is equal to, we can just chase the sequence through the Cayley graph, starting at e.

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



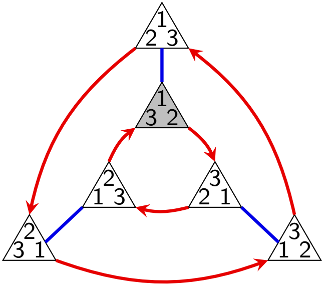
We see that $hhhvhvvhv = h$. A more condensed way to write this is

$$hhhvhvvhv = h^3vhv^2hv = h.$$

A concise way to describe V_4 is by the following group presentation (more on this later):

$$V_4 = \langle v, h \mid v^2 = e, h^2 = e, vh = hv \rangle \,.$$

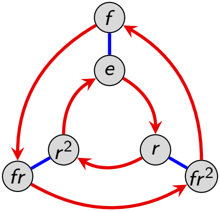
Another familiar example: D_3

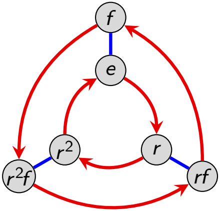


Recall the "triangle puzzle" group $G = \langle r, f \rangle$, generated by a clockwise 120° rotation r, and a horizontal flip f.

Let's take the shaded triangle to be the "unscrambled configuration."

Here are two different ways (of many!) that we can label the nodes with actions:





The following is one (of many!) presentations for this group:

$$D_3 = \langle r, f \mid r^3 = e,\ f^2 = e,\ r^2 f = fr \rangle\,.$$

Group presentations

Initially, we wrote $G = \langle h, v \rangle$ to say that "G is generated by the elements h and v."

All this tells us is that h and v generate G, but not how they generate G.

If we want to be more precise, we use a group presentation of the following form:

$$G = \Big\langle \text{generators} \;\Big|\; \text{relations} \Big\rangle$$

The vertical bar can be thought of as meaning "subject to".

For example, the following is a presentation for V_4:

$$V_4 = \langle a, b \mid a^2 = e,\; b^2 = e,\; ab = ba \rangle\,.$$

Caveat!

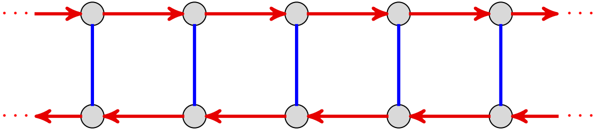
Just because there are elements in a group that "satisfy" the relations above does *not* mean that it is V_4.

For example, the trivial group $G = \{e\}$ satisfies the above presentation; just take $a = e$ and $b = e$.

Loosely speaking, the above presentation tells us that V_4 is the "largest group" that satisfies these relations. (More on this when we study quotients.)

Group presentations

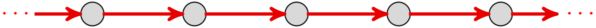
Recall the frieze group from Chapter 3 that had the following Cayley diagram:



One presentation of this group is

$$G = \langle t, f \mid f^2 = e, tft = f \rangle .$$

Here is the Cayley diagram of another frieze group:



It has presentation

$$G = \langle a \mid \quad \rangle .$$

That is, "one generator subject to *no relations*."

Group presentations

Due to the aforementioned caveat, and a few other technicalities, the study of group presentations is a topic usually relegated to graduate-level algebra classes.

However, they are often introduced in an undergraduate algebra class because *they are very useful*, even if the intricate details are harmlessly swept under the rug.

The problem (called the word problem) of determining what a mystery group is from a presentation is actually computationally unsolvable! In fact, it is equivalent to the famous "halting problem" in computer science!

For (mostly) amusement, what group do you think the following presentation describes?

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

Surprisingly, this is the trivial group $G = \{e\}$!

Inverses

If g is a generator in a group G, then following the "g-arrow" backwards is an action that we call its inverse, and denoted by g^{-1}.

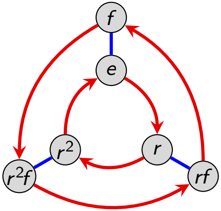
More generally, if g is represented by a path in a Cayley diagram, then g^{-1} is the action achieved by tracing out this path in reverse.

Note that by construction,

$$gg^{-1} = g^{-1}g = e\,,$$

where e is the identity (or "do nothing") action. Sometimes this is denoted by e, 1, 0, or N.

For example, let's use the following Cayley diagram to compute the inverses of a few actions:



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

$f^{-1} = $ _____ because f_____ $= e =$ _____f

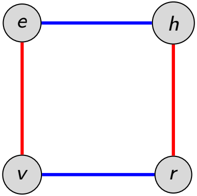
$(rf)^{-1} = $ _____ because (rf)_____ $= e =$ _____(rf)

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

Multiplication tables

Since we can use a Cayley diagram with nodes labeled by actions as a "group calculator," we can create a (group) multiplication table, that shows how every pair of group actions combine.

This is best illustrated by diving in and doing an example. Let's fill out the following multiplication table for V_4.



	e	v	h	r
e	e	v	h	r
v	v	e	r	h
h	h	r	e	v
r	r	h	v	e

Since order of multiplication can matter, let's stick with the convention that the entry in row g and column h is the element gh (rather than hg).

Some remarks on the structure of multiplication tables

Comments

- The 1st column and 1st row repeat themselves. Why? Sometimes these will be omitted (*Group Explorer* does this).
- 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, assigning a unique color to each action of the group. Figure 4.7 (page 47) has examples of a few more tables.
- A group is abelian iff its multiplication table is symmetric about the "main diagonal."
- In each row and each column, each group action occurs exactly once. (This will always happen. . . Why?)

Let's state and prove that last comment as as theorem.

A theorem and proof

Theorem

An element cannot appear twice in the same row or column of a multiplictaion table.

Proof

Suppose that in row a, the element g appears in columns b and c. Algebraically, this means

$$ab = g = ac.$$

Multiplying everything on the left by a^{-1} yields

$$a^{-1}ab = a^{-1}g = a^{-1}ac \qquad \Longrightarrow \qquad b = c.$$

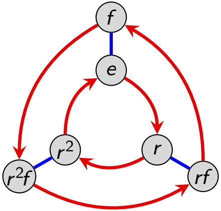
Thus, g (or any element) element cannot appear twice in the same row.

The proof that two elements cannot appear twice in the same column is similar, and will be left as a homework exercise. □

Another example: D_3

Let's fill out the multiplication table for the group D_3; here are several different presentations:

$$\begin{aligned} D_3 &= \langle r, f \mid r^3 = e,\ f^2 = e,\ rf = fr^2 \rangle \\ &= \langle r, f \mid r^3 = e,\ f^2 = e,\ rfr = f \rangle\,. \end{aligned}$$



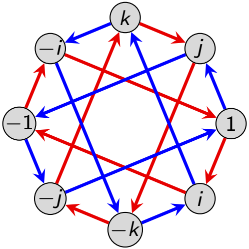
	e	r	r^2	f	rf	r^2f
e	e	r	r^2	f	rf	r^2f
r	r	r^2	e	rf	r^2f	f
r^2	r^2	e	r	r^2f	f	rf
f	f	r^2f	rf	e	r^2	r
rf	rf	f	r^2f	r	e	r^2
r^2f	r^2f	rf	f	r^2	r	e

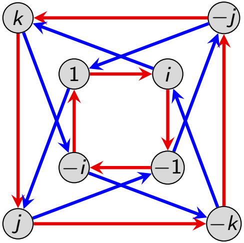
Observations? What patterns do you see?

Just for fun, what group do you get if you remove the "$r^3 = e$" relation from the presentations above? (*Hint*: We've seen it recently!)

Another example: the quaternion group

The following Cayley diagram, laid out two different ways, describes a group of size 8 called the Quaternion group, often denoted $Q_4 = \{\pm 1, \pm i, \pm j, \pm k\}$.





The "numbers" j and k individually act like $i = \sqrt{-1}$, because $i^2 = j^2 = k^2 = -1$.

Multiplication of $\{\pm i, \pm j, \pm k\}$ works like the cross product of unit vectors in $\mathbb{R}^3$:

$$ij = k, \quad jk = i, \quad ki = j, \qquad\qquad ji = -k, \quad kj = -i, \quad ik = -j\,.$$

Here are two possible presentations for this group:

$$\begin{aligned} Q_4 &= \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle \\ &= \langle i, j \mid i^4 = j^4 = 1,\ iji = j \rangle\,. \end{aligned}$$

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 “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 binary operations because they combine two objects into a single object.

Definition

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$. In this case, we say that S is closed under the operation $*$.

Combining, or "multiplying" two group elements (i.e., doing one action followed by the other) is a binary operation. We say that it is a binary operation *on* the group.

Recall that Rule 4 says that any sequence of actions is an action. This ensures that the group is closed under the binary operation of multiplication.

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

However, not every table with symbols in it is going to be the multiplication table for a group.

Associativity

Recall that an operation is associative if parentheses are permitted anywhere, but required nowhere.

For example, ordinary addition and multiplication are associative. However, subtraction of integers is *not* associative:

$$4-(1-2) \neq (4-1)-2.$$

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

Recall D_3, the group of symmetries for the equilateral triangle, generated by r (=rotate) and f (=horizontal flip).

How do the following compare?

$$rfr, \qquad (rf)r, \qquad r(fr)$$

Even though we are associating differently, the end result is that *the actions are applied left to right*.

The moral is that we never need parentheses when working with groups, though we may use them to draw our attention to a particular chunk in a sequence.

Classical definition of a group

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

Definition (official)

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, $e * g = g = g * e$ for all $g \in G$.
4. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Remarks

- Depending on context, the binary operation may be denoted by $*$, $\cdot$, $+$, or $\circ$.
- As with ordinary multiplication, we frequently omit the symbol altogether and write, e.g., xy for $x * y$.
- We generally only use the $+$ symbol if the group is abelian. Thus, $g + h = h + g$ (always), but in general, $gh \neq hg$.
- Uniqueness of the identity and inverses is *not* built into the definition of a group. However, we can without much trouble, prove these properties.

Definitions of a group: Old vs. New

Do our two competing definitions agree? That is, if our informal definition says something is a group, will our official definition agree? Or vice versa?

Since our first definition of a group was informal, it is impossible to answer this question officially and absolutely. An informal definition potentially allows some technicalities and ambiguities.

This aside, our discussion leading up to our official Definition provides an informal argument for why the answer to the first question should be yes. We will answer the second question in the next chapter.

Regardless of whether the definitions agree, we always have $e^{-1} = e$. That is, the inverse of doing nothing is doing nothing.

Even though we haven't officially shown that the two definitions agree (and in some sense, we can't), we shall begin viewing groups from these two different paradigms:

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

A few simple properties

One of the first things we can prove about groups is uniqueness of the identity and inverses.

Theorem

Every element of a group has a *unique* inverse.

Proof

Let g be an element of a group G. By definition, it has at least one inverse.

Suppose that h and k are both inverses of g. This means that $gh = hg = e$ and $gk = kg = e$. It suffices to show that $h = k$. Indeed,

$$h = he = h(gk) = (hg)k = ek = k\,,$$

and the proof is complete. □

The following proof is relegated to the homework; the technique is similar.

Theorem

Every group has a *unique* identity element.