Chapter 5: Five families

Dana C. Ernst

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

Summer 2009

Notes

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.

Notes

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.)

Notes

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.

Notes

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

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

Notes

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

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

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.

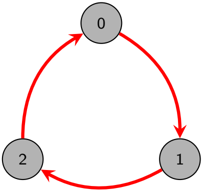
Notes

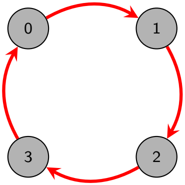
The Cayley diagrams for the cyclic groups are all alike. The standard Cayley diagram for C_n consists of a single cycle

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

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

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





Notes

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.

Notes

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.

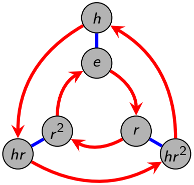
Notes

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?

Notes

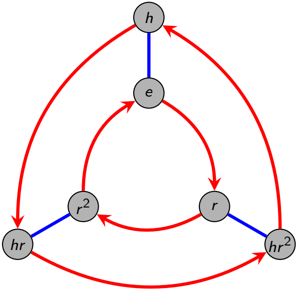
Starting at e, the red arrows lead in a cycle around the inside of the diagram. We refer to this cycle as the orbit of the element r.

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.

Notes



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

Notes

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

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

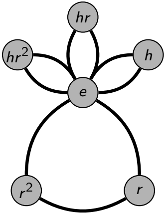
This set is not necessarily infinite as we've seen with the finite cyclic groups.

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.

Notes

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	$\{e, hr^2\}$

Notes

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.

Notes

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.

Notes

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.

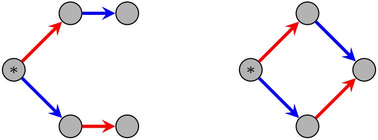
The group V_4 is an example of a group that we have seen that is abelian. The group S_3 is not abelian: $rh \neq hr$.

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

Notes

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 $ab = ba$.

Notes

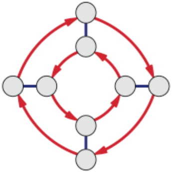
Are cyclic groups abelian? The answer is yes.

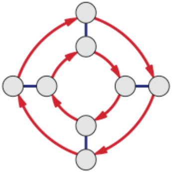
One way to see that this is true is to observe that the left configuration on the previous slide can never occur (since there is only one generator).

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.



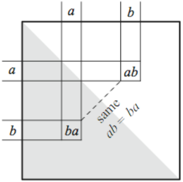


Are either one of these groups abelian?

Notes

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*.

Notes

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?

Notes

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

However, we only need two generators:

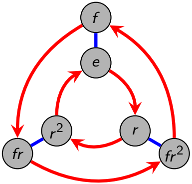
1. $r =$ rotation clockwise by a single "click" (there are other possible choices)
2. $f =$ horizontal flip (or any other flip will do)

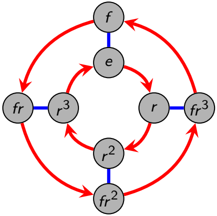
There are many ways to do it, but we can write every one of the $2n$ actions of D_n as a "word" in these two generators. Here is one possibility:

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

Notes

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.

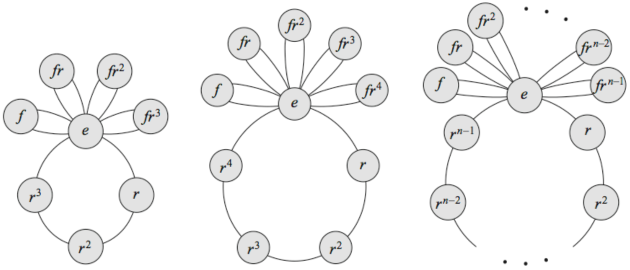
Notes

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.

Notes

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.



Notes

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

	e	r	r^2	r^3	r^4	f	fr	fr^2	fr^3	fr^4
e	e	r	r^2	r^3	r^4	f	fr	fr^2	fr^3	fr^4
r	r	r^2	r^3	r^4	e	fr^4	f	fr	fr^2	fr^3
r^2	r^2	r^3	r^4	e	r	fr^3	fr^4	f	fr	fr^2
r^3	r^3	r^4	e	r	r^2	fr^2	fr^3	fr^4	f	fr
r^4	r^4	e	r	r^2	r^3	fr	fr^2	fr^3	fr^4	f
f	f	fr	fr^2	fr^3	fr^4	e	r	r^2	r^3	r^4
fr	fr	fr^2	fr^3	fr^4	f	r^4	e	r	r^2	r^3
fr^2	fr^2	fr^3	fr^4	f	fr	r^3	r^4	e	r	r^2
fr^3	fr^3	fr^4	f	fr	fr^2	r^2	r^3	r^4	e	r
fr^4	fr^4	f	fr	fr^2	fr^3	r	r^2	r^3	r^4	e

	e	r	r^2	r^3	r^4	f	fr	fr^2	fr^3	fr^4
e	e	r	r^2	r^3	r^4	f	fr	fr^2	fr^3	fr^4
r	r	r^2	r^3	r^4	e	fr^4	f	fr	fr^2	fr^3
r^2	r^2	non-flip			r	fr^3	fr^4	flip	fr	fr^2
r^3	r^3	r^4	e	r	r^2	fr^2	fr^3	fr^4	f	fr
r^4	r^4	e	r	r^2	r^3	fr	fr^2	fr^3	fr^4	f
f	f	fr	fr^2	fr^3	fr^4	e	r	r^2	r^3	r^4
fr	fr	fr^2	fr^3	fr^4	f	r^4	e	r	r^2	r^3
fr^2	fr^2	fr^3	flip	f	fr	r^3	non-flip			r^2
fr^3	fr^3	fr^4	f	fr	fr^2	r^2	r^3	r^4	e	r
fr^4	fr^4	f	fr	fr^2	fr^3	r	r^2	r^3	r^4	e

(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.

Notes

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.

Notes

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.

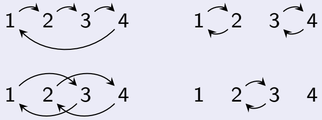
Because they are easy to write down and deal with, we will usually refer to permutations of positive integers (just like we did when we numbered our rectangle, etc.).

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

Notes

Example

Here are some permutations of 4 objects.

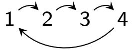


How many permutations of 4 objects are there? The answer is that there are $4! = 24$, which means that there are 24 distinct permutation pictures like above on 4 objects.

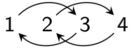
How many permutations of n objects are there? Yep, you guessed it: $n!$.

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

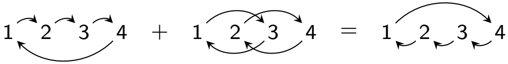


followed by



be equal to?

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



Notes

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

$$\begin{tikzcd} 1 \arrow[r, bend left] & 2 \arrow[r, bend left] & 3 \arrow[r, bend left] & 4 \arrow[lll, bend left] \end{tikzcd}$$

is simply

$$\begin{tikzcd} 1 \arrow[rrr, bend left] & 2 \arrow[l, bend left] & 3 \arrow[l, bend left] & 4 \arrow[l, bend left] \end{tikzcd}$$

Notes

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.

Notes

Alternating groups

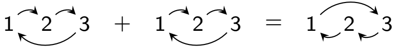
One way to form a group from a subset of the collection of permutations of n items is to take exactly half of the elements of S_n. But what half? Not just any half will do.

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.

Notes

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.

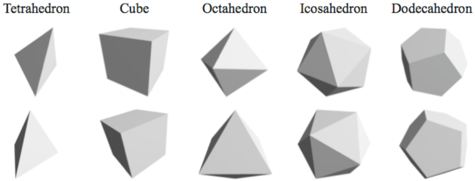
We'll see later why we called this group the "alternating" group. Note that A_n has order $n!/2$.

Notes

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*.)

Notes

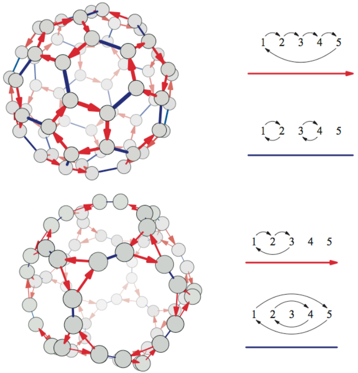
The groups of symmetries of the Platonic solids are as follows.

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.

Notes

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*.)

Notes

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.

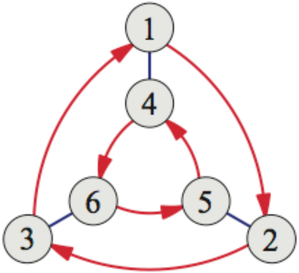
How do we do this?

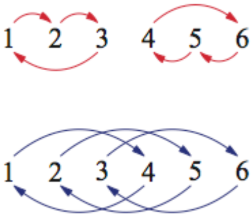
Notes

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*).





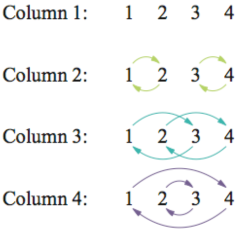
Notes

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



Notes

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.

Notes

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.

Notes