Section 2: Examples of groups

Matthew Macauley

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

Math 4120, Modern Algebra

Overview

In this section, 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.

We will study permutations, how to write them concisely in cycle notation.

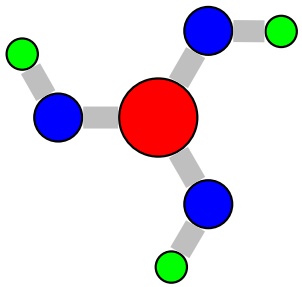
Cayley's theorem tells us that every finite group is isomorphic to a collection of permutations (i.e., a subgroup of a symmetric group).

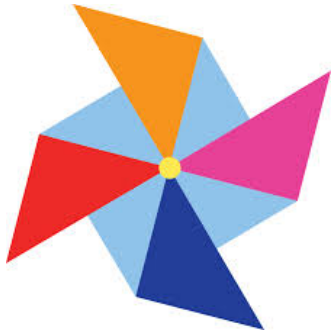
Cyclic groups

Definition

A group is cyclic if it can be generated by a single element.

Finite cyclic groups describe the symmetry of objects that have *only* rotational symmetry. Here are some examples of such objects.





An obvious choice of generator would be: *counterclockwise rotation by* $2\pi/n$ (called a "click"), where n is the number of "arms." This leads to the following presentation:

$$C_n = \langle r \mid r^n = e \rangle .$$

Remark

This is not the only choice of generator; but it's a natural one. Can you think of another choice of generator? Would this change the group presentation?

Cyclic groups

Definition

The order of a group G is the number of distinct elements in G, denoted by $|G|$.

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

For example, the group of symmetries for the objects on the previous slide are C_3 (boric acid), C_4 (pinwheel), and C_{10} (chilies).

Comment

The alternative 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 take the remainder.

For example, in $\mathbb{Z}_6$: $3 + 5 \equiv_6 2$. "3 clicks + 5 clicks = 2 clicks". (If the context is clear, we may even write $3 + 5 = 2$.)

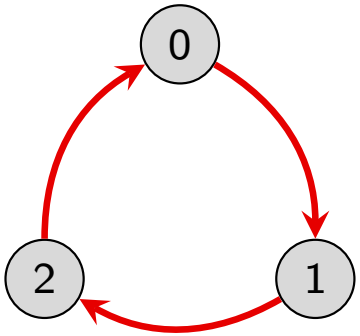
Cyclic groups, additively

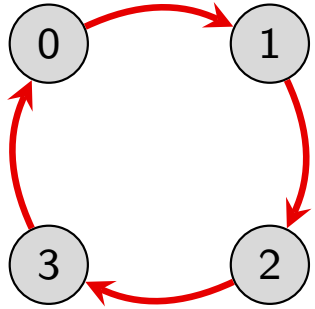
A common way to write elements in a cyclic group is with the integers $0, 1, 2, \ldots, n-1$, where

- 0 is the identity
- 1 is the single counterclockwise "click".

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

Here are some Cayley diagrams of cyclic groups, using the canonical generator of 1.





Summary

In this setting, the cyclic group consists of the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under the binary operation of $+$ (modulo n). The (additive) identity is 0.

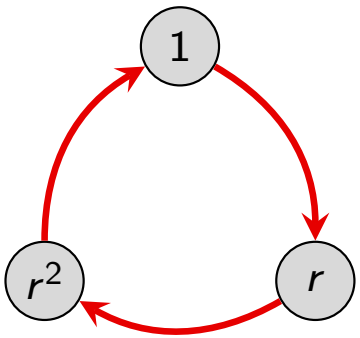
Cyclic groups, multiplicatively

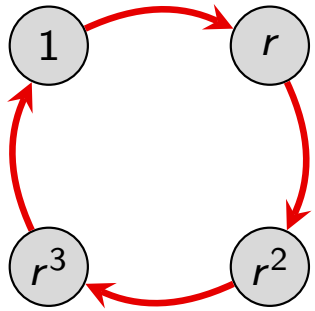
Here's another natural choice of *notation* for cyclic groups. If r is a generator (e.g., a rotation by $2\pi/n$), then we can denote the n elements by

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

Think of r as the complex number $e^{2\pi i/n}$, with the group operation being *multiplication!*

Note that $r^n = 1$, $r^{n+1} = r$, $r^{n+2} = r^2$, etc. Can you see modular addition rearing its head again? Here are some Cayley diagrams, using the canonical generator of r.





Summary

In this setting, the cyclic group can be thought of as the set $C_n = \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\}$ under the binary operation of $\times$. The (multiplicative) identity is 1.

More on cyclic groups

One of our notations for cyclic groups is "additive" and the other is "multiplicative." This doesn't change the actual group; only our choice of notation.

Remark

The (unique) infinite cyclic group (additively) is $(\mathbb{Z}, +)$, the integers under addition. Using multiplicative notation, the infinite cyclic group is

$$G = \langle r \mid \quad \rangle = \{r^k : k \in \mathbb{Z}\}.$$

For the infinite cyclic group $(\mathbb{Z}, +)$, only 1 or -1 can be generators. (Unless we use multiple generators, which is usually pointless.)

Proposition

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

For example, 1 and 5 generate $\mathbb{Z}_6$, while $1, 2, 3$, and 4 all generate $\mathbb{Z}_5$. i.e.,

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle, \qquad \mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle.$$

Recall that the above notation isn't a presentation, it just means "generated by."

More on cyclic groups

Modular addition has a nice visual appearance in the multiplication tables of cyclic groups.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

There are many things worth commenting on, but one of the most important properties of the multiplication tables for cyclic groups is the following:

Observation

If the headings on the multiplication table are arranged in the "natural" order $(0, 1, 2, \ldots, n-1)$ or $(e, r, r^2, \ldots, r^{n-1})$, then each row is a cyclic shift to the left of the row above it.

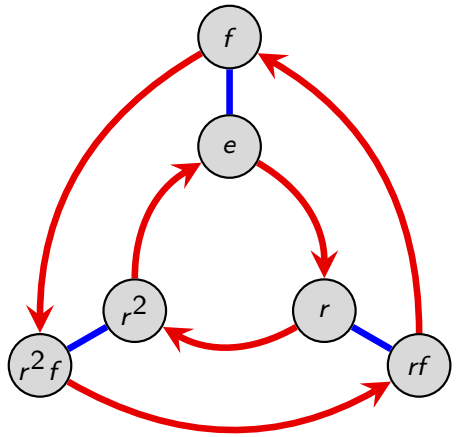
Do you see *why* this happens?

Orbits

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

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

Consider the Cayley diagram for D_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 length-3 cycle around the inside of the diagram. We refer to this cycle as the orbit of the element r.

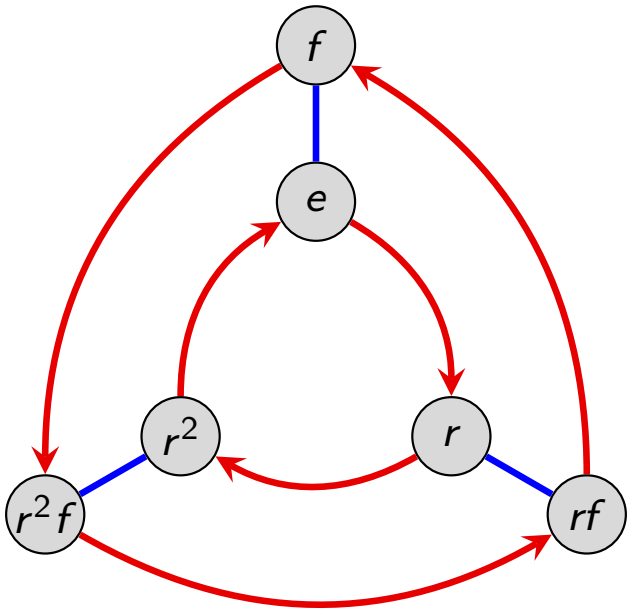
The blue arrows lead in a length-2 cycle – the orbit of f.

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

Orbits

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 elements of D_3.



element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
f	$\{e, f\}$
rf	$\{e, rf\}$
r^2f	$\{e, r^2f\}$

Note that there are 5 *distinct* orbits. The elements r and r^2 have the same orbit.

Orbits

Definition

The order of an element $g \in G$, denoted $|g|$, is the size of its orbit. That is, $|g| := |\langle g \rangle|$. (Recall that the order of G is defined to be $|G|$.)

Note that in any group, the orbit of e will simply be $\{e\}$.

In general, the orbit of an element g is the set

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

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

We allow negative exponents, though this only matters in infinite groups.

One way of thinking about this is that the orbit of an element g is the collection of elements that you can get to by doing g or its inverse any number of times.

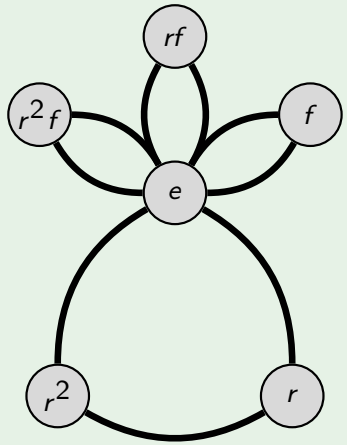
Remark

In *any* group G, the orbit of an element $g \in G$ is a cyclic group that "sits inside" G. This is an example of a subgroup, which we will study in more detail later.

Visualizing the orbits of a group using "cycle graphs"

Example: Cycle graph of D_3

element	orbit
e	$\{e\}$
r	$\{e, r, r^2\}$
r^2	$\{e, r^2, r\}$
f	$\{e, f\}$
rf	$\{e, rf\}$
r^2f	$\{e, r^2f\}$



Comments

- In a cycle graph (also called an orbit graph), each cycle 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, because one orbit could have multiple generators.
- Intersections of cycles show what elements they have in common.
- What do the cycle graphs of cyclic groups look like? (*Answer*: a single cycle.)

Abelian groups

Recall that a group is abelian (named after Neils Abel) if the order of actions is irrelevant (i.e., the actions *commute*). Here is the formal mathematical definition.

Definition

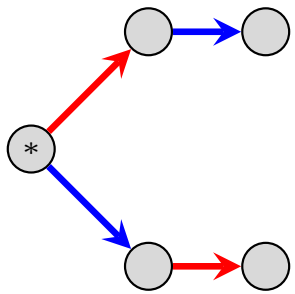
A group G is abelian if $ab = ba$ for all $a, b \in G$.

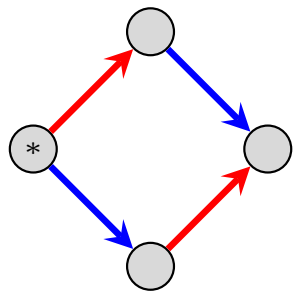
Abelian groups are sometimes referred to as commutative.

Remark

To check that a group G is abelian, it suffices to only check that $ab = ba$ for all pairs of generators of G. (*Why?*)

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





Examples

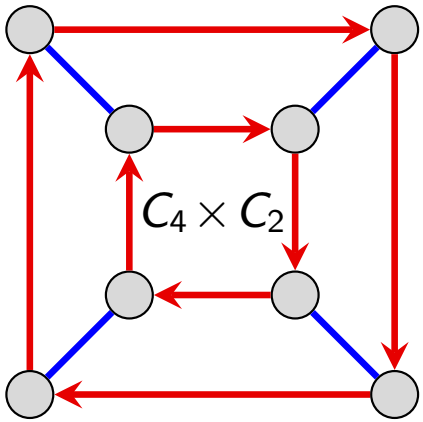
Cyclic groups are abelian.

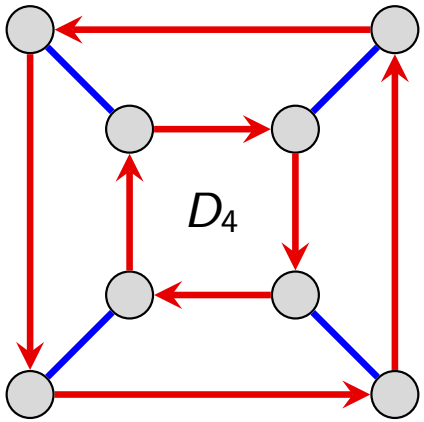
Reason 1: The left configuration on the previous slide can never occur (since there is only one generator).

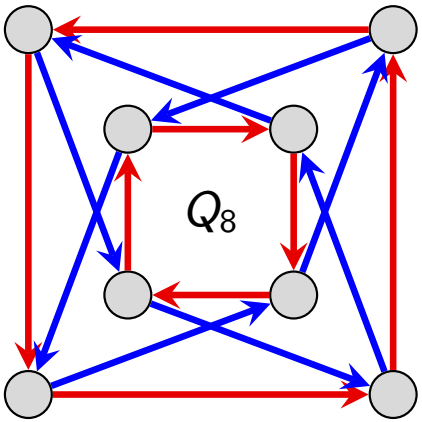
Reason 2: In the cyclic group $\langle r \rangle$, every element can be written as r^k for some k. Clearly, $r^k r^m = r^m r^k$ for all k and m.

Note that the converse fails: if a group is abelian, it need not be cyclic. (Take V_4 as an example.)

Let's explore a little further. The following are Cayley diagrams for three groups of order 8.





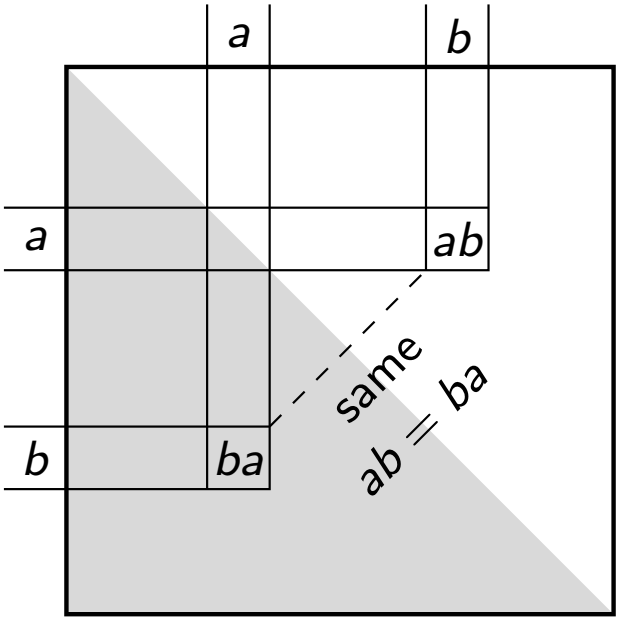


Are any of these groups abelian?

Multiplication tables of abelian groups

Abelian groups are easy to spot if you look at their multiplication tables.

The property "$ab = ba$ for all a and b" means that the table must be symmetric across the main diagonal.



	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Dihedral groups

While cyclic groups describe 2D objects that only have rotational symmetry, dihedral groups describe 2D objects that have rotational *and* reflective symmetry.

Regular polygons have rotational and reflective symmetry. The dihedral group that describes the symmetries of a regular n-gon is written D_n.

All actions in C_n are also actions of D_n, but there are more than that. The group D_n contains $2n$ actions:

- n rotations
- n reflections.

However, we only need two generators. Here is one possible choice:

1. r = counterclockwise rotation by $2\pi/n$ radians. (A single "click.")
2. f = flip (fix an axis of symmetry).

Here is one of (of many) ways to write the $2n$ actions of D_n:

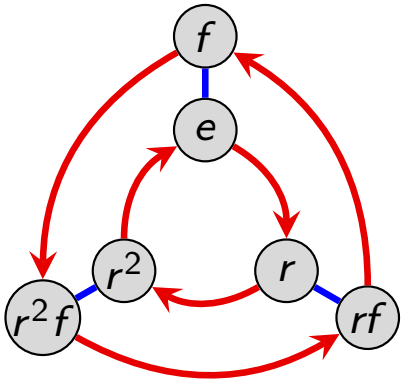
$$D_n = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{f, rf, r^2 f, \ldots, r^{n-1} f}_{\text{reflections}}\}.$$

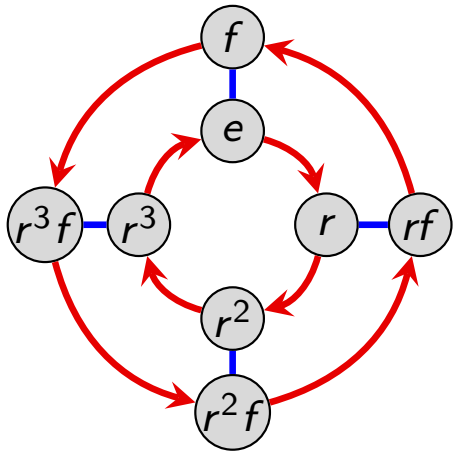
Cayley diagrams of dihedral groups

Here is one possible presentation of D_n:

$$D_n = \langle r, f \mid r^n = e,\ f^2 = e,\ rfr = f \rangle.$$

Using this generating set, the Cayley diagrams for the dihedral groups all look similar. Here they are for D_3 and D_4, respectively.

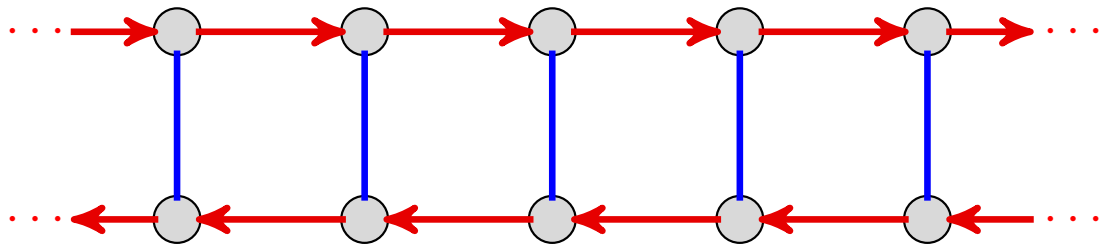




There is a related infinite dihedral group D_∞, with presentation

$$D_\infty = \langle r, f \mid f^2 = e,\ rfr = f \rangle.$$

We have already seen its Cayley diagram:



Cayley diagrams of dihedral groups

If s and t are two reflections of an n-gon across adjacent axes of symmetry (i.e., axes incident at π/n radians), then st is a rotation by $2\pi/n$.

To see an explicit example, take $s = rf$ and $t = f$ in D_n; obviously $st = (rf)f = r$.

Thus, D_n can be generated by two reflections. This has group presentation

$$\begin{aligned} D_n &= \langle s, t \mid s^2 = e,\ t^2 = e,\ (st)^n = e \rangle \\ &= \{\underbrace{e, st, ts, (st)^2, (ts)^2, \ldots,}_{\text{rotations}}\ \underbrace{s, t, sts, tst, \ldots}_{\text{reflections}}\}. \end{aligned}$$

What would the Cayley diagram corresponding to this generating set look like?

Remark

If $n \geq 3$, then D_n is nonabelian, because $rf \neq fr$. However, the following relations are very useful:

$$rf = fr^{n-1}, \qquad fr = r^{n-1}f.$$

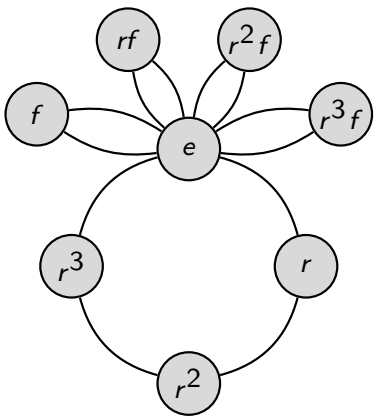
Looking at the Cayley graph should make these relations visually obvious.

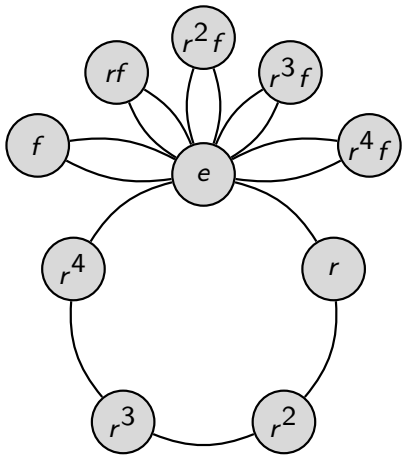
Cycle graphs of dihedral groups

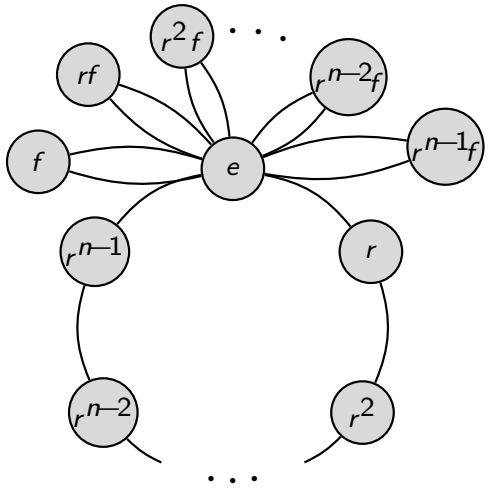
The (maximal) orbits of D_n consist of

- 1 orbit of size n consisting of $\{e, r, \ldots, r^{n-1}\}$;
- n orbits of size 2 consisting of $\{e, r^k f\}$ for $k = 0, 1, \ldots, n-1$.

Here is the general pattern of the cycle graphs of the dihedral groups:





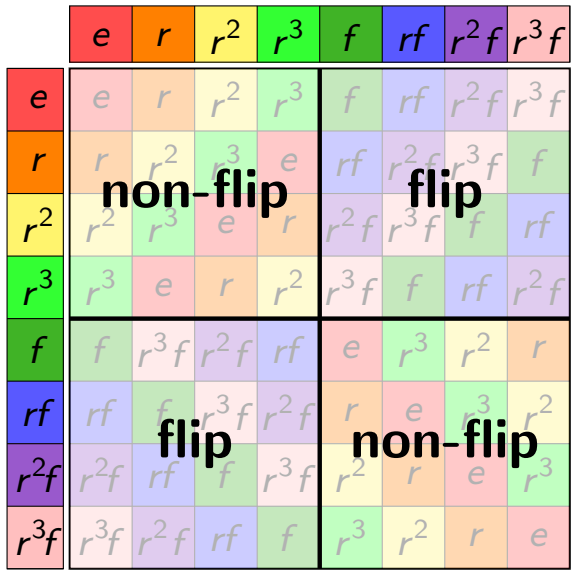


Note that the size-n orbit may have smaller subsets that are orbits. For example, $\{e, r^2, r^4, \ldots, r^{n-2}\}$ and $\{e, r^{n/2}\}$ are orbits if n is even.

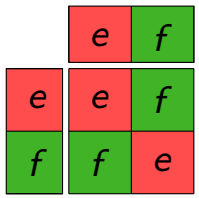
Multiplication tables of dihedral groups

The separation of D_n into rotations and reflections is also visible in their multiplication tables. For example, here is D_4:

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



As we shall see later, 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.



It yields a group of order 2 with the following Cayley diagram:

Symmetric groups

Most groups we have seen have been collections of ways to rearrange things. This can be formalized.

Definition

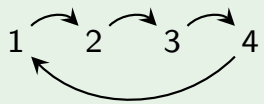
A permutation is an action that rearranges a collection of things.

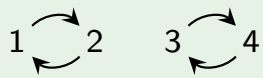
For convenience, we will usually refer to permutations of positive integers (just like we did when we numbered our rectangle, etc.).

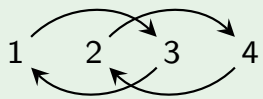
There are many ways to represent permutations, but we will start with the notation illustrated by the following example.

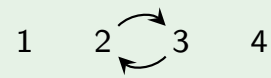
Example

Here are some permutations of 4 objects.





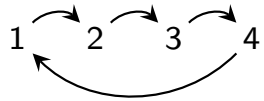




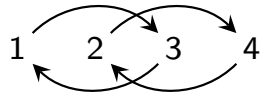
Combining permutations

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

What should

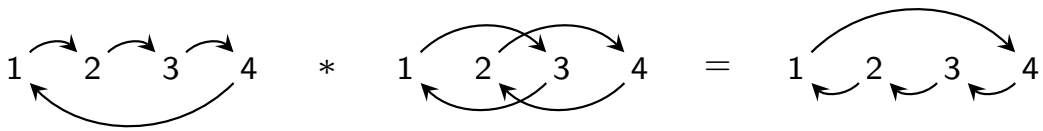


followed by



be equal to?

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



Groups of permutations

Fact

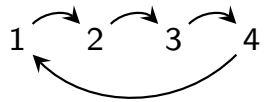
There are $n! = n(n-1)\cdots 3\cdot 2\cdot 1$ permutations of n items.

For example, there are $4! = 24$ "permutation pictures" on 4 objects.

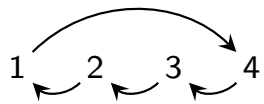
The collection of permutations of n items forms a group!

To verify this, we just have to check that the appropriate rules of *one* of our definitions of a group hold.

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



The symmetric group

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. (*Why?*)

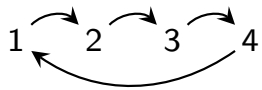
Although the set of *all* permutations of n items forms a group, creating a group does not require taking all permutations.

If we choose carefully, we can form groups by taking a subset of the permutations.

For example, the cyclic group C_n and the dihedral group D_n can both be thought of groups of certain permutations of $\{1, \ldots, n\}$. (*Why?* Do you see *which* permutations they represent?)

Cycle notation for S_n

We can concisely describe the permutation



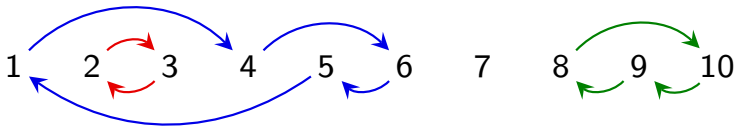
as $(1\ 2\ 3\ 4)$.

This is called cycle notation.

Observation 1

Every permutation can be decomposed into a product of disjoint cycles.

For example, in S_{10}, we can write



as $(1\ 4\ 6\ 5)\,(2\ 3)\,(8\ 10\ 9)$.

Observation 2

Disjoint cycles commute.

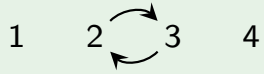
For example: $(1\ 4\ 6\ 5)\,(2\ 3)\,(8\ 10\ 9) = (2\ 3)\,(8\ 10\ 9)\,(1\ 4\ 6\ 5)$.

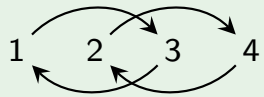
Cycle notation for S_n

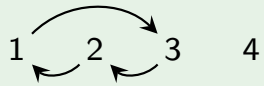
Example

Consider the following permutations in S_4:

- 

is $(1\ 2)\,(3\ 4)$
- 

is $(2\ 3)$
- 

is $(1\ 3)\ (2\ 4)$
- 

is $(1\ 3\ 2)$

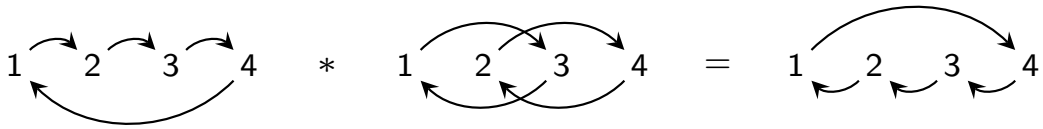
Remark

It doesn't matter "where we start" when writing the cycle. In the last example above,

$$(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3) = (1\ 2)\,(2\ 3) = (1\ 2)\,(2\ 3)\,(2\ 3)\,(2\ 3)\,.$$

Composing permutations in cycle notation

Recall how we combined permutations:



In cycle notation, this is

$$(1\ 2\ 3\ 4) * (1\ 3)(2\ 4) = (1\ 4\ 3\ 2)\,.$$

We read left-to-right. (*Caveat*: some books use the right-to-left convention as in function composition.)

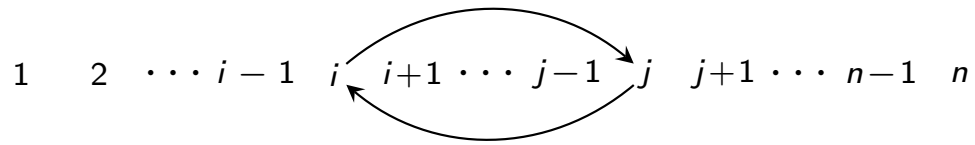
Do you see how to combine permutations in cycle notation? In the example above, we start with 1 and then read off:

- "1 goes to 2, then 2 goes to 4"; Write: (1 4
- "4 goes to 1, then 1 goes to 3"; Write: (1 4 3
- "3 goes to 4, then 4 goes to 2"; Write: (1 4 3 2
- "2 goes to 3, then 3 goes to 1"; Write: (1 4 3 2)

In this case, we've used up each number in $\{1, \ldots, n\}$. If we hadn't, we'd take the the smallest unused number and continue the process with a new (disjoint) cycle.

Transpositions

A transposition is a permutation that swaps two objects and fixes the rest, e.g.:



In cycle notation, a transposition is just a 2-cycle, e.g., $(i \;\; j)$.

Theorem

The group S_n is generated by transpositions.

Intuitively, this means that every permutation can be constructed by successively exchanging pairs of objects.

In other words, if n people are standing in a row, and we want to rearrange them in some other order, we can always do this by successively having pairs of people swap places.

In fact, we only need adjacent transpositions to generate S_n:

$$S_n = \langle (1\ 2),\ (2\ 3),\ \ldots,\ (n-1\ \ n) \rangle.$$

Transpositions and the alternating groups

Remark

Even though every permutation in S_n can be written as a product of transpositions, there may be many ways to do this.

For example:

$$(1\ 3\ 2) = (1\ 2)\,(2\ 3) = (1\ 2)\,(2\ 3)\,(2\ 3)\,(2\ 3) = (1\ 2)\,(2\ 3)\,(1\ 2)\,(1\ 2).$$

Theorem

The parity of the number of transpositions of a fixed permutation is unique.

That is, a fixed permutation can either be written with an even number of transpositions, or an odd number of transpositions, but *not both*!

We thus have a notion of even permutations and odd permutations.

Theorem

Exactly half of the permutations in S_n are even, and they form a group called the alternating group, denoted A_n.

Practice

At this point, it helps to "get your hands dirty" and try a few examples. Here are some good exercises.

1. Write the following products of permutations into a product of *disjoint cycles*:
   - $(1\ 2\ 3)\,(1\ 2\ 3\ 4)$ in S_4
   - $(1\ 6)\,(1\ 2\ 4\ 5)\,(1\ 6\ 4\ 2\ 5\ 3)$ in S_6.

Let $G = S_3$, the symmetric group on three objects. This group has six elements.

2. Do the following for each element in S_3:
   - Draw its "permutation picture."
   - Write it as a product of disjoint transpositions (that is, using only $(1\ 2)$, $(2\ 3)$, and $(1\ 3)$).
   - Write it as a product of disjoint *adjacent* transpositions (that is, using only $(1\ 2)$ and $(2\ 3)$).
   - Determine whether it is even or odd.

3. Now, write down the alternating group A_3. This is the group consisting of only the *even* permutations. What familiar group is this isomorphic to?

Alternating groups

How can we verify that A_n a group?

The only major concern is it must be closed under combining permutations (all other necessary properties are inherited from S_n).

Do you see why combining two even permutations yields an even permutation?

Interesting fact

For $n \leq 5$, the group A_n consists precisely of the set of "squares" in S_n. By "square," we mean an element that can be written as an element of S_n times itself.

For example, the permutation  is a square in S_3, because:

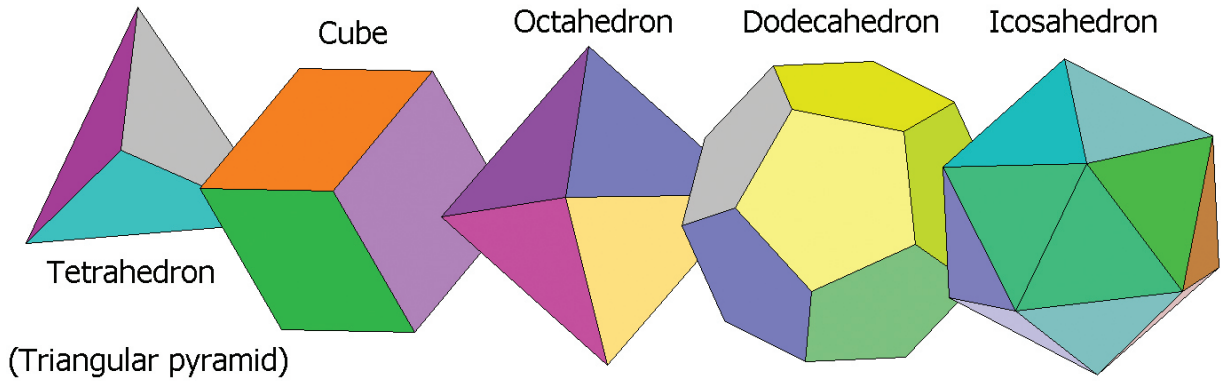
In cycle notation, this is $(1\ 3\ 2) = (1\ 2\ 3)\,(1\ 2\ 3)$.

Note that A_n has order $\dfrac{n!}{2}$.

Platonic solids

The symmetric groups and alternating groups arise throughout group theory. In particular, the groups of symmetries of the 5 Platonic solids are symmetric and alternating groups.

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



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

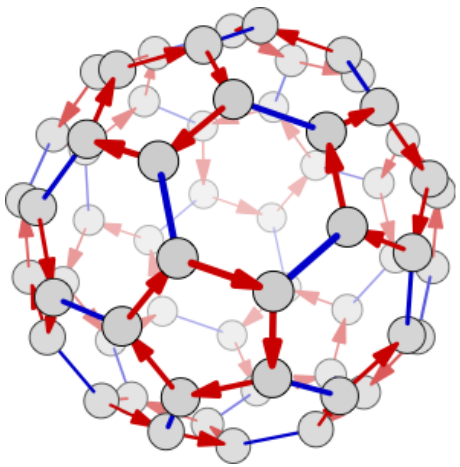
shape	group
Tetrahedron	A_4
Cube	S_4
Octahedron	S_4
Icosahedron	A_5
Dodecahedron	A_5

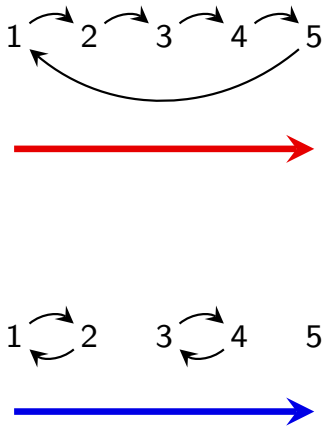
Platonic solids

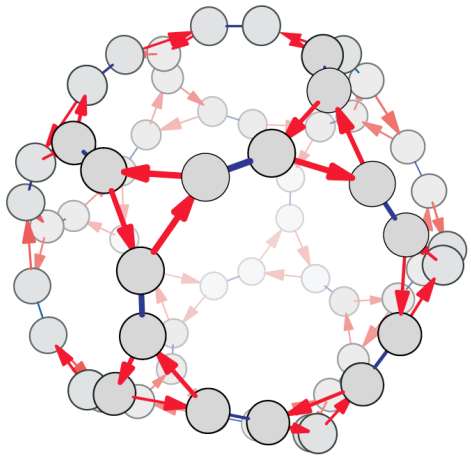
The Cayley diagrams for these 3 groups can be arranged in some very interesting configurations.

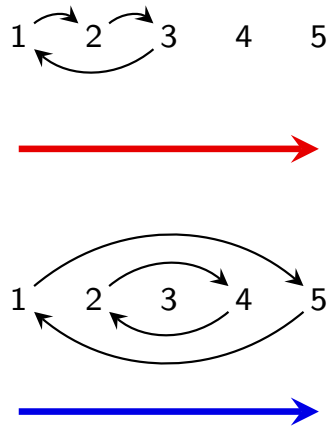
In particular, the Cayley diagram for Platonic solid 'X' can be arranged on a truncated 'X', where truncated refers to cutting off some corners.

For example, here are two representations for Cayley diagrams of A_5. At left is a truncated icosahedron and at right is a truncated dodecahedron.









Cayley's theorem

Any set of permutations that forms a group is called a permutation group.

Cayley's theorem says that permutations can be used to construct any finite group.

In other words, every group has the same structure as (we say "*is isomorphic to*") some permutation group.

Warning! We are *not* saying that every group is isomorphic to some symmetric group, S_n. Rather, every group is isomorphic to a subgroup of some symmetric group S_n – i.e., a subset of S_n that is *also* a group in its own right.

Question

Given a group, how do we associate it with a set of permutations?

Cayley's theorem; how to construct permutations

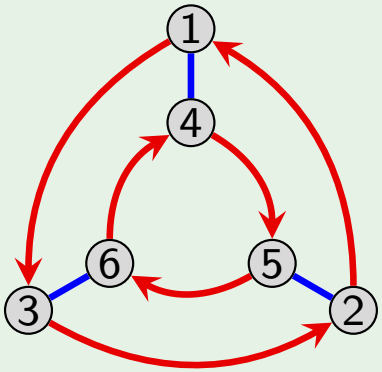
Here is an algorithm given a Cayley diagram with n nodes:

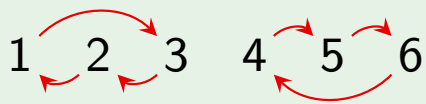
1. number the nodes 1 through n,
2. interpret each arrow type in the Cayley diagram as a permutation.

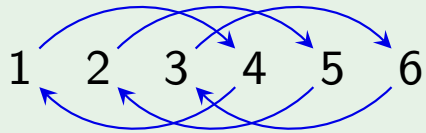
The resulting permutations are the generators of the corresponding permutation group.

Example

Let's try this with $D_3 = \langle r, f \rangle$.







We see that D_3 is isomorphic to the subgroup $\langle (132)(456),\ (14)(25)(36) \rangle$ of S_6.

Cayley's theorem; how to construct permutations

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.

Example

Let's try this with the multiplication table for $V_4 = \langle v, h \rangle$.

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

Column 1: 1 2 3 4

Column 2: (1 2)(3 4)

Column 3: (1 3)(2 4)

Column 4: (1 4)(2 3)

We see that V_4 is isomorphic to the subgroup $\langle (12)(34),\ (13)(24) \rangle$ of S_4.

Cayley's theorem

Intuitively, two groups are isomorphic if they have the same structure.

Two groups are *isomorphic* if we can construct Cayley diagrams for each that look identical.

Cayley's Theorem

Every finite group is isomorphic to a collection of permutations.

Our algorithms exhibit a 1-1 correspondence between group elements and permutations.

However, we have *not* shown 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 the i^{th} row followed by the permutation from the j^{th} column, results in the permutation that corresponding to the cell in the i^{th} row and j^{th} column of the original table (Exercise.)