A zoo of examples of groups!

Spencer Bagley

With many thanks to Matthew Macauley,
`http://www.math.clemson.edu/~macaule/`

29 Jan 2025

Families of groups

So far we've seen some examples of *individual* groups, but here we're going to see some examples of *families* of groups, because they'll be nice go-to examples:

1. **cyclic groups**: rotational symmetries
   - (Side quest: orbits and cycle graphs)
2. **dihedral groups**: rotational *and* reflective symmetries
3. **abelian groups**: where $ab = ba$ (always)
4. **permutation groups**: collections of rearrangements.

We'll show that *every* finite group is "isomorphic" to a permutation group.

Then, we'll see how to combine groups into bigger groups using

6. **direct products** and
7. **semidirect products** of groups.

I'm also kicking a couple of things to the homework for you to think about on your own:

8. **matrix groups**
9. the **quaternion group** Q_8

Some definitions

Definition

A subgroup of G is a subset $H \subseteq G$ that is also a group. We denote this by $H \leq G$.

(More on this soon.)

Definition

The order of a group G is its size as a set (how many distinct elements are in it), denoted by $|G|$.

Example

$|\mathbf{Sq}| = 8$, and $|\mathbb{Z}| = \infty$.

Definition

The order of an element $g \in G$ is $|g| := \big|\langle g\rangle\big|$, i.e., either

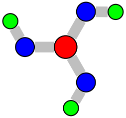
- the minimal $k \geq 1$ such that $g^k = e$, or
- ∞, if there is no such k.

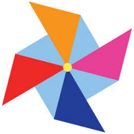
Cyclic groups

Definition

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

Finite cyclic groups describe the symmetries of objects that have *only* rotational symmetry.





Remark

You can make a cyclic group of any order you want.

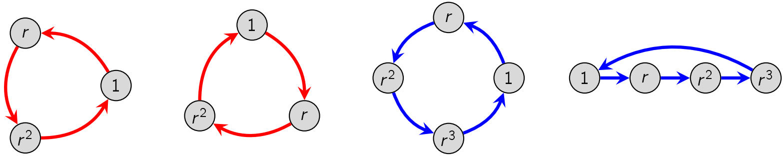
Cyclic groups, multiplicatively

Definition

For $n \geq 1$, the multiplicative cyclic group C_n is the set

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

where $r^i r^j = r^{i+j}$, and the exponents are taken modulo n. The identity is $r^0 = r^n = 1$.



It is clear that a presentation for this is

$$C_n = \langle r \mid r^n = 1 \rangle.$$

Note that r^2 generates C_5:

$$(r^2)^0 = 1, \quad (r^2)^1 = r^2, \quad (r^2)^2 = r^4, \quad (r^2)^3 = r^6 = r, \quad (r^2)^4 = r^8 = r^3.$$

Do you have a conjecture about for which k does $C_n = \langle r^k \rangle$?

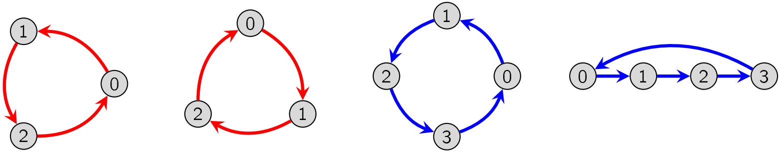
Cyclic groups, additively

Definition

For $n \geq 1$, the additive cyclic group $\mathbb{Z}_n$ is the set

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

where the binary operation is addition modulo n. The identity is 0.



We can write a group presentation additvely:

$$\mathbb{Z}_n = \langle 1 \mid n \cdot 1 = 0 \rangle.$$

What else generates $\mathbb{Z}_5$?

Remark

It is wrong to write $C_n = \mathbb{Z}_n$. (Why?)
Instead, we say C_n is isomorphic to $\mathbb{Z}_n$, and we write $C_n \cong \mathbb{Z}_n$.

Cayley tables of cyclic groups

Modular addition has a nice visual appearance in the Cayley tables for cyclic groups, if we order the elements $0, 1, \ldots, n-1$.

Here are two different ways to write the Cayley table for $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

	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

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

(Hey, this looks kind of familiar, like the hilt of a sword)

Exercise

Draw the Cayley table for C_2.

Infinite cyclic groups

Definition

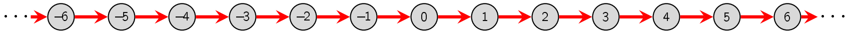
The additive infinite cyclic group is

$$\mathbb{Z} = \langle 1 \mid \quad \rangle,$$

the integers under addition. The multiplicative infinite cyclic group is

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

What does a Cayley graph of $\mathbb{Z}$ look like?



Orbits and cycle graphs

Definition

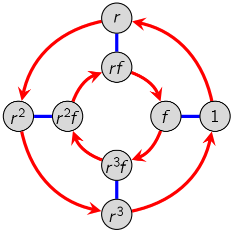
The orbit of an element $g \in G$ is the cyclic subgroup that it generates,

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\},$$

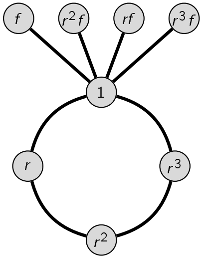
and its order is $|g| := \big|\langle g \rangle\big|$.

We can visualize the orbits by the (undirected) orbit graph, or cycle graph.

Let's think about this in the example of **Sq**. Use your Cayley graph to write down the orbits of each element.



element	orbit
1	$\{1\}$
r^2	$\{1, r^2\}$
r	$\{1, r, r^2, r^3\}$
r^3	
f	$\{1, f\}$
rf	$\{1, rf\}$
r^2f	$\{1, r^2f\}$
r^3f	$\{1, r^3f\}$



By convention, we typically only draw maximal orbits.

Dihedral groups

Definition

The dihedral group D_n or $\mathbf{Dih}_n$ is the group of symmetries of a regular n-gon.

Examples

$\mathbf{Tri} = D_3$ and $\mathbf{Sq} = D_4$. :)

Conjecture time:

- What is the order of a generic D_n?
- What does the Cayley graph of a generic D_n look like?
- Do you immediately see any subgroups of a generic D_n?
- What do you think is a presentation for a generic D_n?

Dihedral groups

Definition

The dihedral group D_n is the group of symmetries of a regular n-gon. It has order $2n$.

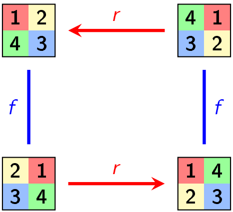
One possible choice of generators is

1. r = counterclockwise rotation by $2\pi/n$ radians,
2. f = flip across a fixed axis of symmetry.

Using these generators, one (of many) ways to write the elements of $D_n = \langle r, f \rangle$ is

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

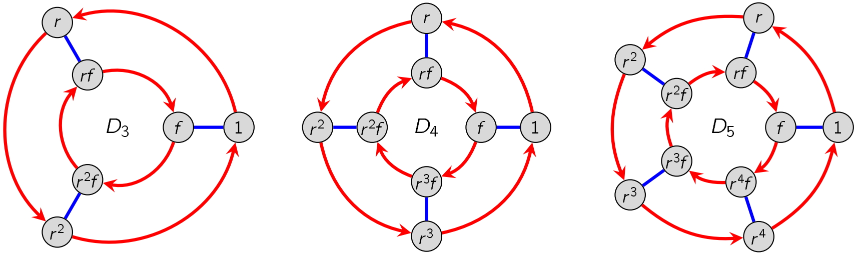
It is easy to check that $rf = fr^{-1}$:



Dihedral groups

Several different presentations for D_n are:

$$D_n = \left\langle r, f \mid r^n = 1,\ f^2 = 1,\ rfr = f \right\rangle = \left\langle r, f \mid r^n = 1,\ f^2 = 1,\ rf = fr^{n-1} \right\rangle.$$



Warning!

Many books denote the symmetries of the n-gon as D_{2n}.

A strong advantage to our convention is that we can write

$$C_n = \langle r \rangle = \left\{1, r, r^2, \ldots, r^{n-1}\right\} \leq \langle r, f \rangle = D_n.$$

(In the other convention, for instance, $C_3 \leq D_6$, which I find annoying.)

Dihedral groups

Observation

When we were first playing with **Sq** and **Tri**, we identified lots of different reflections, but lately we've been pinning it down to just one specific one.

Question

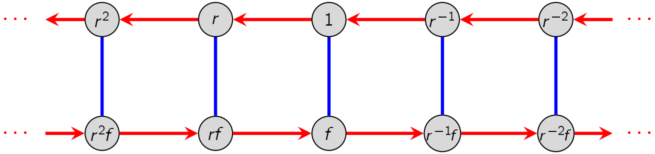
Can you generate D_n using only reflections?

Dihedral groups

Definition

The infinite dihedral group, denoted D_∞, has presentation

$$D_\infty = \langle r, f \mid f^2 = 1,\ rfr = f \rangle.$$



Question

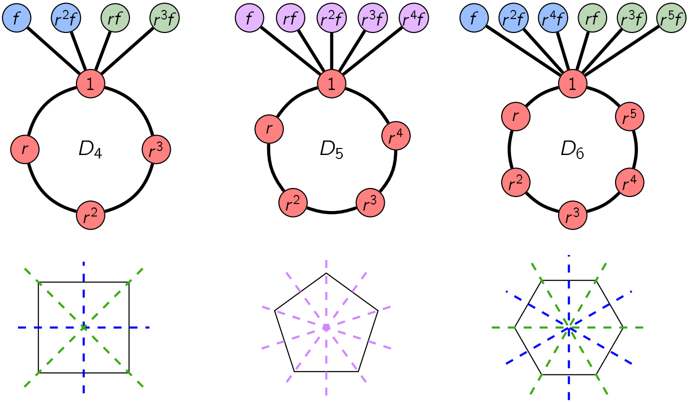
Can we generate D_∞ with two reflections?

Cycle graphs of dihedral groups

The maximal orbits of D_n consist of

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

Unless n is prime, the size-n orbit will have smaller subsets that are orbits.



Cayley tables of dihedral groups

The separation of D_n into rotations and reflections is visible in its Cayley tables.

	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	r^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	r^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

rotation **reflection**

reflection **rotation**

The partition of D_n as depicted above has the structure of group C_2.

"Shrinking" a group in this way is called a quotient.

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

	1	f
1	1	f
f	f	1

Abelian groups

Definition

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

Claim

Every cyclic group is abelian.

Remark

To check that G is abelian, it suffices to only check that $ab = ba$ for all pairs of generators.

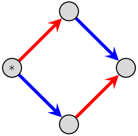
Jokes

- What's purple and commutes?
- What's warm, nourishing, delicious, and commutative?

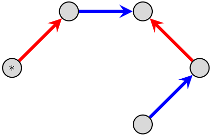
Abelian groups

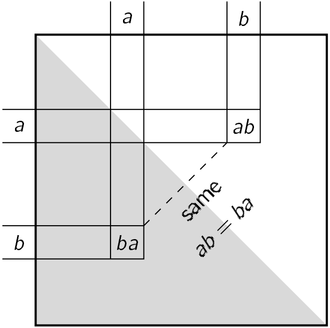
It is easy to check whether a group is abelian from either its Cayley graph or Cayley table.

$ab = ba$



$ab \neq ba$





Abelian groups

One way to build abelian groups is to "glue together" cyclic groups using direct products.

Fundamental Theorem of Finite Abelian Groups

Every finite abelian group A is isomorphic to a direct product of cyclic groups

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}, \qquad \text{for some } k_1, k_2, \ldots, k_m \in \mathbb{N}.$$

(More on this later.)

What *infinite* abelian groups might there be?

- The *rational numbers*, $\mathbb{Q}$, under addition
- The *real numbers*, $\mathbb{R}$, under addition
- The *complex numbers*, $\mathbb{C}$, under addition
- all of these (with 0 removed) under multiplication: $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$.
- the positive versions of these under multiplication: $\mathbb{Q}^+$, $\mathbb{R}^+$ (but not $\mathbb{C}^+$).

Other abelian groups

It is clear that $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. However, there are many more subgroups of $\mathbb{C}$ than these.

Most of the following are actually rings: additive groups also closed under multiplication. We'll study these more later.

Definition

The Gaussian integers are the complex numbers of the form

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

We'll see $\mathbb{Z}[\sqrt{-m}]$ and others when we encounter rings of algebraic integers.

The set of polynomials in x "*over the integers*" is a group under addition, denoted

$$\mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}\}.$$

We can also look at certain subgroups, like the polynomials of degree $\leq n$.

Polynomials can be defined in multiple variables, like

$$\mathbb{Z}[x, y] = \Big\{ \sum a_{ij} x^i y^j \mid a_{ij} \in \mathbb{Z}, \ \text{ all but finitely many } a_{ij} = 0 \Big\},$$

or over a finite ring such as $\mathbb{Z}_n$.

Groups of permutations

Loosely speaking, a permutation is an action that rearranges a set of objects.

Definition

Let X be a set. A permutation of X is a bijection $\pi \colon X \to X$.

Definition

The permutations of a set X form a group that we denote S_X. The special case when $X = \{1, \ldots, n\}$ is called the symmetric group, and denoted S_n.

If $|X| = |Y|$, then $S_X \cong S_Y$, so we'll usually work with S_n, which has order $n! = n(n-1)\cdots 2 \cdot 1$.

There are several notations for permutations, each with their strengths and weaknesses.

This is best seen with an example:

i	1	2	3	4	5	6
$\pi(i)$	2	3	1	6	5	4

"*one-line notation*"

"*permutation diagram*"

$$\pi = (1\,2\,3)\,(4\,6)$$

"*cycle notation*"

Permutation notations

One-line notation: $\pi = 231654, \qquad \sigma = 564123$

Pros:

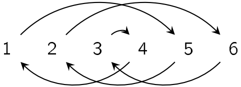
- concise
- nice visualization of rearrangement

Cons:

- bad for combining permutations
- not clear where elements get mapped
- hard to compute the inverse

Permutation diagram: π:

σ:



Pros:

- can see where elements get mapped
- easy to compute inverses
- convenient for combining permutations

Cons:

- cumbersome to write
- can get tangled

Cycle notation: $\pi = (1\,2\,3)\,(4\,6), \qquad \sigma = (1\,5\,2\,6\,3\,4)$;

Pros:

- short and concise
- easy to see the disjoint cycles
- convenient for combining permutations

Cons:

- representation isn't unique
- not clear what n is

Cycle notation

The cycle $(1\,4\,6\,5)$ means

"*1 goes to 4, which goes to 6, which does to 5, which goes back to 1.*"

Thus, we can write $(1\,4\,6\,5) = (4\,6\,5\,1) = (6\,5\,1\,4) = (5\,1\,4\,6)$.

To find the inverse of a cycle, write it backwards:

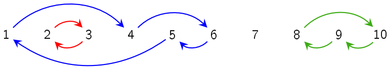
$$(1\,4\,6\,5)^{-1} = (5\,6\,4\,1) = (1\,5\,6\,4) = \cdots$$

Though it's not necessary, we usually prefer to begin a cycle with its smallest number.

Remark

Every permutation in S_n can be written in cycle notation as a product of disjoint cycles, and this is unique up to commuting and cyclically shifting cycles.

For example, consider the following permutation in S_{10}:



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

This is a product of four disjoint cycles. Since they are disjoint, they commute:

$$(1465)\,(23)\,(8\;10\;9) = (23)\,(8\;10\;9)\,(1465) = (23)\,(8\;10\;9)\,(1465) = \cdots$$

Composing permutations

Remark

The order of a permutation is the least common multiple of the sizes of its disjoint cycles.

For example, $(1\ 3\ 8\ 6)(2\ 9\ 7\ 4\ 10\ 5) \in S_{10}$ has order 12; this should be intuitive.

When cycles are not disjoint, order matters.

Many books compose permutations from right-to-left, due to function composition.

Since we have been using right Cayley graphs, we will compose them from left-to-right.

Notational convention

Composition of permutations will be done left-to-right. That is, given $\pi, \sigma \in S_n$,

$$\pi\sigma \quad \text{means "}\textit{do } \pi\textit{, then do } \sigma\text{"}.$$

The main drawback about our convention is that it does not work well with function notation applied to elements, like $\pi(i)$.

For example, notice that

$$(\pi\sigma)(i) = \sigma(\pi(i)) \neq \pi(\sigma(i)).$$

However, we will hardly ever use this notation, so that drawback is minimal.

Composing permutations

Here are two ways illustrating how permutations are composed, with the example

First do

i	1	2	3	4	5	6
$\pi(i)$	4	3	1	2	6	5

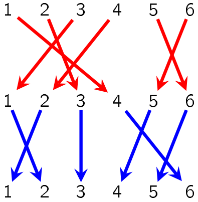
then do

i	1	2	3	4	5	6
$\sigma(i)$	2	1	3	6	4	5

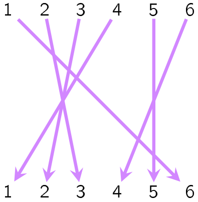
- "By stacking:"

first (1423)(56)

then (12)(465)

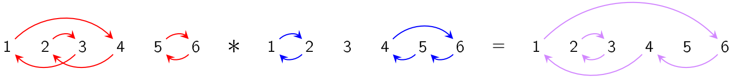


=



(164)(23)

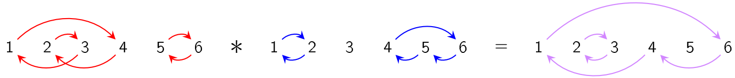
- "By cycles:"



first (1423)(56) *then* (12)(465) (164)(23)

Composing permutations in cycle notation

Let's practice composing two permutations:



first (1423)(56) *then* (12)(465) (164)(23)

Let's now do that in slow motion.

In the example above, we start with 1 and then read off:

- "**1** goes to 4, then 4 goes to 6"; Write: (1 6
- "6 goes to 5, then 5 goes to 4"; Write: (1 6 4
- "4 goes to 2, then 2 goes to **1**"; Write: (1 6 4), and start a new cycle.
- "**2** goes to 3, then 3 is fixed"; Write: (1 6 4) (2 3
- "3 goes to 1, then 1 goes to **2**"; Write: (1 6 4) (2 3), and start a new cycle.
- "**5** goes to 6, then 6 goes to **5**"; Write: (1 6 4) (2 3) (5); now we're done.

We typically omit 1-cycles (fixed points), so the permutation above is just (1 6 4) (2 3).

Cayley's theorem

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

A fundamental theorem by British mathematician Arthur Cayley (1821–1895) says that every finite group can be thought of as a collection of permutations.

This is clear for groups of symmetries like V_4, C_n, or D_n, but less so for groups like Q_8.

Cayley's theorem

Every finite group is "isomorphic to" a collection of permutations, i.e., some subgroup of S_n.

We don't have the mathematical tools to prove this formally, but we'll get a 1-line proof when we study group actions.

Let's make an intuitive argument, though.

Constructing permutations from a Cayley graph

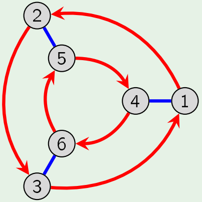
Here is an algorithm given a Cayley graph with n nodes:

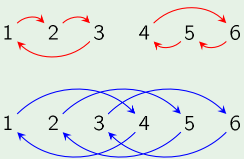
1. number the nodes 1 through n,
2. interpret each arrow type in the Cayley graph as a permutation.

Take the permutations corresponding to the generators.

Example

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





We see that D_3 is isomorphic to the subgroup $\langle (123)(456),\ (14)(25)(36) \rangle$ of S_6.

Question:

Would this have worked if we had chosen a different numbering?

Constructing permutations from a Cayley table

Here is an algorithm given a Cayley 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 row (or column) as a permutation.

Take the permutations corresponding to *any* generating set.

Example

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

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

Row 1 (1): 1 2 3 4 5 6

Row 2 (r): 1 2 3 4 5 6

Row 3 (r^2): 1 2 3 4 5 6

Row 4 (f): 1 2 3 4 5 6

Row 5 (rf): 1 2 3 4 5 6

Row 6 $(r^2 f)$: 1 2 3 4 5 6

We see that D_3 is isomorphic to the subgroup $\langle (123)(456), (14)(26)(35) \rangle$ of S_6.