MAT301

Groups and Symmetries

Gaurav Patil and Shuyang Shen

Fall 2024

Contents

Chapter -1

Introduction

Group theory is the study of symmetry. Broadly speaking, a symmetry is an invertible transformation of some object that preserves the object. In other words, if you can do something to an object and leave it looking the same (or similar), you've found a symmetry.

Nobody's perfect, but if your face was perfectly symmetrical, it would look the same to you in the mirror as it looks to other people who can see you directly. The mirror shows you a reflection of your face and leaves it looking the same—that's a "symmetry" of your face.

Similarly, take a regular pentagon and rotate it about its center by $72°$. The shape of this pentagon remains unchanged because it has rotational symmetry.

In nature, symmetries often manifest as reflectional, rotational, or translational.

Symmetries are...

- Everywhere. Symmetries show up in everything, from the shapes of galaxies all the way down to the arrangements of fundamental particles.

- Pretty. Symmetries are visually pleasing, and we have a lot of art featuring different forms of symmetry.

- Important. Humans use pattern recognition to understand the world, and symmetry is one of those key "patterns". We can study symmetries of objects to better understand those objects and their properties.

... Which brings us back to group theory!

-1.1 Group theory

> *"The theory of groups is a branch of mathematics in which one does something to something and then compares the results with the result of doing the same thing to something else, or [doing] something else to the same thing."*

> —James R. Newman

Before we talk about what groups are, we want to first go over some problems in which group theory shows up, and impress upon you the sheer applicability of group theory.

-1.1.1 Polyhedra

Consider a cube. We cannot easily "reflect" it in three-dimensional space without the aid of a mirror, but we may rotate it in a few different ways while maintaining its shape:

- Rotating by $90°, 180°$, or $270°$ about an axis through the midpoints of two opposing edges.

- Rotating by $180°$ about an axis through the midpoints of two opposing edges.

- Rotating by $120°$ or $240°$ about a "grand diagonal", an axis through two diagonally opposing vertices.

You can see a visualization here. Observe that with each type of rotation, the faces of the cube are permuted in different ways! Something that group theory studies is what these symmetries each *change* and what they *preserve*, as well as how they *interact* with each other.

-1.1.2 Colouring

Suppose we have a bunch of beads of various colors. How many necklaces can be made out of those beads? Basic permutation results aren't enough here: the "starting bead" doesn't matter but the order of the beads matter! This is a type of symmetry—"rotating" the necklace preserves the order of the beads. Similarly, we may also "flip" the necklace and introduce another type of symmetry.

> **Example -1.1.1 —** For a more tractable example, suppose we want to make a necklace out of four beads that are red, yellow, green, and blue respectively. The only distinct necklaces are the following:
>
>

Simply listing the possibilities becomes infeasible when we introduce more colors and/or beads. Group theory to the rescue: Burnside's lemma can be used to count items featuring symmetries like this by counting everything equivalent up to symmetry as the same. We will learn about this sometime in November.

-1.1.3   Polynomial roots

Remember the quadratic formula? If you have a quadratic polynomial $ax^2 + bx + c$, its roots are given by $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Everyone learns this in high school.

Now what if we have a cubic polynomial $ax^3 + bx^2 + cx + d$?

Well, there is also a formula for its roots: they are

$$r_k = -\frac{1}{3a}\left(b + \xi^k C + \frac{b^2 - 3ac}{\xi^k C}\right) \quad (k = 0, 1, 2)$$

where

$$C = \sqrt[3]{\frac{b^2 - 3ac \pm \sqrt{(b^2 - 3ac)^2 - 4(2b^3 - 9abc + 27a^2d)^3}}{2}}$$

and

$$\xi = \frac{-1 + \sqrt{3}i}{2}$$

... you're not expected to know this offhand.

And there is one for quartics as well:

... this is why they don't teach it in high school.

But mathematicians got those formulas in the 1500s, and they started looking at quintics. They got stuck. For two hundred years. The question becomes: is the formula just *really* complicated or is it straight up impossible?

Finally in 1799 Ruffini came up with a partial proof that yes, some quintic polynomials just don't have a solutions in nice formulas like those. Abel finished up the proof some years after. Later Galois and Cayley developed criteria so that we know precisely which polynomials are solvable and which ones aren't. The tools they developed along the way evolved into what we now call Galois theory, which, among other things, is used to investigate the behaviour and relationship of roots of polynomials.

This will be covered in more detail in MAT401, so that's something to look forward to.

-1.1.4 Cryptography

The art of secret messages is another inspiration to the formalization we see in group theory.

The main idea of secret messages is to convert a message to gibberish is a reversible way. The idea is someone who knows the secret, should be able to make sense of the gibberish. But someone who does not know the secret should not be able to decipher the gibberish.

Ideally, you want the ability to have secret communication with many people (often people who don't necessarily know you) without setting up a system of secrets each time. In other words, there have to be many possible secrets. One should be unable to narrow down which secrets a particular person might use. A secret for us is an identifier of the exact process of gibberishizing you re using. You want random person to be unable to try out all secrets on your gibberish and find out your message.

Thus, we take a large 'group' or set of reversible transformations.

> **Example -1.1.2 —** You may have seen the RSA cryptosystem in MAT246 (and a much simpler proof of its mechanism can be had with group theory!). The idea is:
>
> - Take a large modulus m which is a product of two primes p and q. Publish m while keeping p and q secret.
>
> - Choose an encryption key e and give it to the person with whom you wish to communicate.
>
> - Compute the decryption key d using e, p, q and use it to decrypt the messages encrypted with e.
>
> Given a fixed m, we can pick many different encryption keys $e_1, \ldots, e_n$ to give to different people—which improves the safety of communication while keeping decryption nice and simple. These valid encryption keys are derived from the structure of the group behind the RSA cryptosystem, and we will talk about this group in a few weeks.

Exercise 1. What does the set of all valid encryption keys look like here?

Such a system allows for multiple layers of security. For example, healthcare data may be encrypted multiple times while being sent to different agencies, so that identifiable information is obscured and at each step, an agency only knows information essential to their operation. When the processed data is sent all the way back to the hospital, we may apply decryption schemes along the way and retrieve information for each patient.

Chapter 0

Preliminaries

0.1 Sets

A *set* is a collection of things under consideration, and a *subset* is a collection of *some* of those things—including potentially all of them as well as none of them. To write down a set, you can either write down all its elements:

$$\{\text{Buddy}, \text{Rex}, \text{Fido}\}$$

—or you can specify it using *set-builder notation*:

$$\{x : \text{I have a dog named } x\}.$$

The squiggles on either side are called *(curly) braces*.

The *empty set* is the set with no elements. Instead of writing it as $\{\}$, the empty set is denoted

$$\varnothing$$

Some common sets we will be making use of are:

- $\mathbb{N} = \{1, 2, 3, \dots\}$: set of natural numbers (sometimes including 0),
- $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$: set of integers,
- $\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\}$: set of rational numbers,
- $\mathbb{R}$: set of real numbers, and
- $\mathbb{C}$: set of complex numbers.

Given two subsets A and B of a set X, here are the most important ways to form new subsets of X.

The *union* of two sets is the set of elements contained in at least one of them. That is,

$$A \cup B = \{x : x \in A \text{ or } x \in B \text{ (or both!)}\}.$$

The *intersection* of two sets is the set of elements contained in both of them. That is,

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Two sets are *disjoint* if their intersection is empty. Visually, disjoint sets don't overlap.
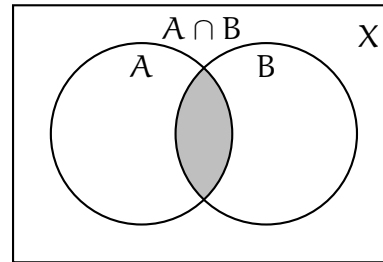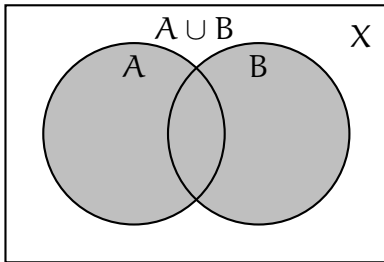
The *complement* of a subset is the set of things *not* in it. More precisely,

$$\overline{A} \text{ or } A^c = \{x \in X : x \notin A\}.$$

The *relative complement* of one set, A, *in* another set, B, is the set of things in B that are not in A. That is,

$$B - A \text{ or } B \setminus A = \{x \in B : x \notin A\}.$$
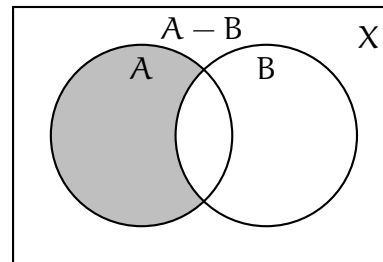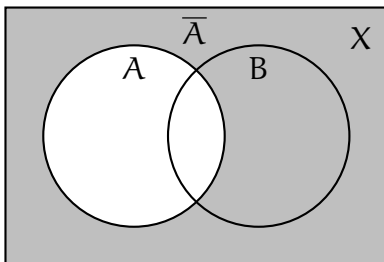
Exercise 2. Write $A \cap A^c = \varnothing$ in plain language (using the word "disjoint"), and then prove it.

Exercise 3. Let $A \subseteq X$. Show that the "complement of A" is the same thing as the "relative complement of A in X".

Exercise 4. Show that $B \setminus A = B \cap A^c$.

A *partition* of a set is a collection of subsets that divide it up. Formally, $A_i \subseteq X$ for all i, and

$$X = \bigcup_i A_i,$$

and $A_i \cap A_j = \varnothing$ for all $i \neq j$, then we say the A_i's *partition* X (also: *form a partition of* X).

> **Example 0.1.1 —** The sets $\{1, 2\}$ and $\{3, 4\}$ partition the set $\{1, 2, 3, 4\}$, but the sets $\{1, 2, 3\}$ and $\{1, 2, 4\}$ do not.

> **Example 0.1.2 —** The intervals $[k, k + 1)$ partition $\mathbb{R}$.
>
>
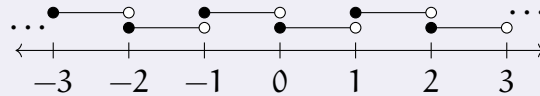
The *Cartesian product* of two sets A and B is the set of ordered pairs (a, b) where a is in A and b is in B. That is,

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

> **Example 0.1.3 —** The "xy-plane" is the Cartesian product of $\mathbb{R}$ with itself.

0.2 Maps a.k.a. Functions

A function is a rule for associating a unique output to every valid input. The set of inputs is the *domain* and the set of outputs (whether or not all are possible) is the *codomain*. If $f(x) = y$ we say y is the *image* of x under f, or the *value* of f at x, depending on what we want to emphasize.

To write down a function, you can describe it in words—

"Let f be the squaring map on $\mathbb{R}$."

—or write down a formula—

$$f : \mathbb{R} \to \mathbb{R},$$
$$f(x) = x^2.$$

A useful "anonymous" shorthand is $x \mapsto x^2$.

When the domain is finite, you can use *two-line notation*: write the elements of the domain in a row and write their images underneath.

> **Example 0.2.1** — The squaring map on the set $\{0, 1, 2, 3\}$ can be written as
> $$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 4 & 9 \end{pmatrix}$$
> in two-line notation.

Given sets X, Y and a map $f : X \rightarrow Y$, here are the most important objects derived from f.

The *image* of a subset $A \subseteq X$ under f is the set of all the values $f(a)$ where a ranges just over A.
$$f(A) = \{y : y = f(a) \text{ for some } a \text{ in } A\}.$$

The *image of* f means the image of X under f, denoted $\operatorname{im} f = f(X)$.

> **Example 0.2.2** — Let $f(x) = x^2 + 1$ from $\mathbb{R}$ to $\mathbb{R}$. Then $\operatorname{im} f = [1, \infty)$ while $f([-2, 1)) = [1, 5]$.

The *graph* of f is the set of pairs $(x, f(x))$ as x ranges over X, formally
$$\Gamma(f) = \{(x, y) \in X \times Y : f(x) = y\}.$$

Exercise 5. Isn't the graph of f just equal to $X \times f(X)$? Explain.

f is *injective* or *one-to-one* (or even just *1-1*) if it doesn't send different inputs to the same output.

Exercise 6. Suppose f is injective, and $f(x) = f(y)$. What can you deduce about x and y?

f is *surjective* or *onto* if the image equals the codomain. Surjectivity only makes sense if you specify a codomain!

Exercise 7. Suppose f is surjective, and y is in Y. What can you deduce about f and X?

f is *bijective* if it is both injective and surjective.

Example 0.2.3 — Injective, surjective, and bijective functions $\mathbb{R} \to \mathbb{R}$.
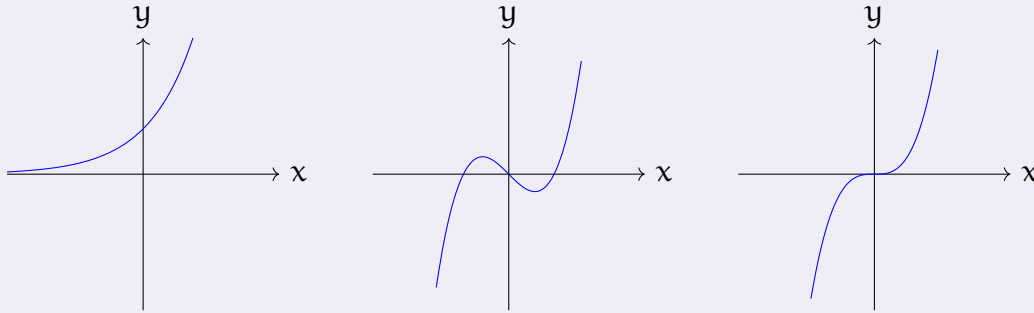
Given another map $g : Y \to Z$, g *composed with* f (or g *after* f) is the map obtained by applying f and then g. That is, $(g \circ f)(x) = g(f(x))$.

Exercise 8.
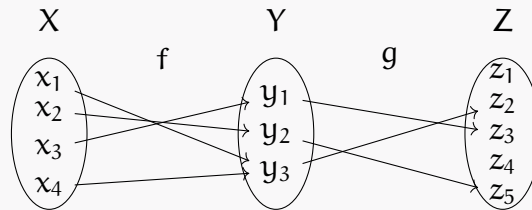
Express the map $g \circ f$ in two-line notation.

Exercise 9. Show that the composition of two injective functions is injective. Do the same with "injective" replaced by "surjective".

An *inverse* of f is a function $g : Y \to X$ such that $g \circ f = \text{id}_X$ and $f \circ g = \text{id}_Y$. f has an inverse if and only if f is bijective, in which case the inverse is denoted f^{-1}. *Be careful* not to confuse this with the *reciprocal* of f—$f^{-1}(x) \neq f(x)^{-1}$!

Let $f : X \longrightarrow Y$ denote a function. For $S \subseteq Y$, we define the *preimage* of S under f to be

$$f^{-1}(S) := \{x \in X : f(x) \in S\}.$$

Take care not to confuse this notation with the *inverse function* f^{-1}: The preimage is a set, while f^{-1} is a function. We may talk about the preimage of sets under any function, but only bijective ones have an inverse.

Exercise 10. What are the preimages of each element in Z under g in the previous example? What about $g \circ f$?

Exercise 11. Let S, T be subsets of Y. Show that if $S \cap T = \emptyset$, then

$$f^{-1}(S) \cap f^{-1}(T) = \emptyset.$$

Exercise 12. Conclude that $\{f^{-1}(\{y\}) : y \in Y\}$ is a partition of X.

f is a *self-map* if $Y = X$. That is, f maps X to it*self*. A bijective self-map is called a *permutation*.
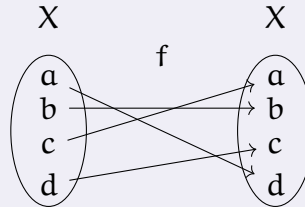
> **Example 0.2.4 —**
>
>
>
> In two-line notation, this map is
>
> $$\begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}.$$

Probably the most important self-map is the *identity map* $x \mapsto x$, sometimes explicitly denoted id or id_X.

Self-maps are interesting because they can be *iterated*. Given $f : X \to X$, the nth *iterate* of f is defined as f composed with itself n times, denoted f^n. For convenience, we set $f^0 = id_X$.

Exercise 13. For the function f in the previous example, write out f^n for $n = 0, \ldots, 6$. What do you notice?

Finally, $f : X \to X$ is an *involution* if it's its own inverse. That is, $f^2(x) = x$.

0.3 Relations

Given a set X, a *relation* on X is, formally, a subset R of $X \times X$ (the set of pairs (x, y) with x and y in X). For any x, y in X, we say x is *related to* y (but not necessarily vice versa) if (x, y) is in R, denoted xRy.

R is *reflexive* if all elements are related to themselves. That is, xRx for all x.

R is *symmetric* if the relation goes both ways. That is, if xRy then yRx as well (for all x and y).

R is *antisymmetric* if *no* two distinct elements are mutually related. That is, if xRy and yRx, then $x = y$.

R is *transitive* if you can "remove the middleman" in a chain of relations. That is, if xRy and yRz, then xRz.

A relation that is reflexive, symmetric, and transitive is called an *equivalence relation*. Equivalence relations are denoted $\sim$ instead of R.

> *"Our human condition is such that [the relation x loves y] is, alas, neither reflexive, symmetric, nor transitive."*

> —Seth Warner, *Modern Algebra*

Exercise 14.

Fill out the properties of the following relations.

x, y are people	R? S? T?
"x loves y"	
"x is aware of y"	
"x and y were married at some point"	
"x is an ancestor of y"	
"x looks like y (Think about the Ship of Theseus paradox!)"	
"x is not younger than y"	
"x has been to the same school as y"	
"x is born in the same year as y"	

Exercise 15. When is a relation possibly symmetric, transitive, but not reflexive?

Given an equivalence relation $\sim$, an *equivalence class* is a complete set of elements that are all related to one another.

The equivalence class of x is denoted $[x] = \{y \in X : x \sim y\}$ and every equivalence class has this form.

Exercise 16. Show that any two elements in $[x]$ are related.

The set of all equivalence classes—a set of sets—is denoted $X/\sim$.

Exercise 17. Show that the equivalence classes partition X.

Exercise 18. Revisit Exercise 12 by showing that the relation "$x \sim y$ if $f(x) = f(y)$" is an equivalence relation. What are the equivalence classes?

0.4 Integers, or: Rem(a)inders from Arithmetic

0.4.1 Division

For any integer a any nonzero integer b, there exist unique integers q and r satisfying

$$a = bq + r \quad \text{and} \quad 0 \le r < |b|.$$

q is called the *quotient* and r is called the *remainder*.

To find q and r, it's easiest to just actually divide a by b. That gives

$$\frac{a}{b} = q + \frac{r}{b}.$$

If $b > 0$, then

$$0 \le \frac{r}{b} < \frac{|b|}{b} = 1.$$

Thus

$$q = \left\lfloor \frac{a}{b} \right\rfloor \tag{1}$$

i.e. q is a/b *rounded down*. Once you know q, finding r is easy.

> **Example 0.4.1** — To divide $a = 42$ by $b = 9$ with remainder, start by observing that $42/9 = 4.666...$ so $q = 4$. But $9 \cdot 4 = 36$, so $r = 6$. In other words,
>
> $$42 = 4 \cdot 9 + 6.$$

When $r = 0$, we say b *divides* a and write $b \mid a$. A number is *prime* if it has just two divisors. Divisibility is a transitive and reflexive relation on $\mathbb{Z}$. It is neither symmetric nor antisymmetric, but if $a \mid b$ and $b \mid a$ then $a = b$ or $a = -b$.

A number is *prime* if it has just two divisors.

A *common divisor* of two numbers is a number dividing them both. The *greatest common divisor* or gcd of two numbers is just that—the biggest of the common divisors. The gcd has the wonderful property that if $c \mid a$ and $c \mid b$ then $c \mid \gcd(a, b)$. Two numbers are *coprime* if $\gcd(a, b) = 1$.

Dually, a *common multiple* of two numbers is a number they both divide. The *least common multiple* or lcm of two numbers is just that—the smallest of the common multiples. Like the gcd, the lcm has the wonderful property that if $a \mid m$ and $b \mid m$ then $\text{lcm}(a, b) \mid m$.

The lcm and the gcd are related by the formula

$$\gcd(a, b) \cdot \text{lcm}(a, b) = |ab|.$$

0.4.2 Congruence

Fix an integer m, called the *modulus*. Say $a \equiv b \pmod{m}$ if and only if $m \mid a - b$. Congruence modulo m is an equivalence relation on $\mathbb{Z}$. [Check this!] When m is clear from context, the equivalence class of a is denoted $[a]$, while the *set* of equivalence classes is variously denoted

$\mathbb{Z}/m$ or $\mathbb{Z}/(m)$ or $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$. In this course, we use $\mathbb{Z}/m\mathbb{Z}$.

The set $\mathbb{Z}/m\mathbb{Z}$ inherits addition, subtraction, and multiplication from $\mathbb{Z}$, meaning that you can add, subtract, and multiply equivalence classes (of the same modulus).

In other words, one *defines*

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab]$$

and then checks that these operations are well-defined.

Example 0.4.2 — $\mathbb{Z}/24\mathbb{Z}$ has twenty-four elements, $[0], [1], [2], \ldots, [23]$.

$$[12] + [15] = [27] = [3]$$

$$[12] - [15] = [-3] = [21]$$

Adding and subtracting modulo 24 is like reckoning with military time.

$$[3] \cdot [10] = [30] = [6]$$

$$[7]^2 = [7] \cdot [7] = [49] = [1]$$

Multiplication doesn't have such a nice interpretation.

0.5 Complex numbers

Complex numbers are numbers of the form $z = x + iy$ where x and y are real numbers and i satisfies $i^2 = -1$.

x and y are called the *real part* and *imaginary part* of z and denoted $\Re z$ and $\Im z$ respectively. Together they are called the *Cartesian* coordinates of z.

Cartesian coordinates are most useful for addition and subtraction, e.g.

$$(a + ib) + (c + id) = (a + c) + i(b + d).$$

They can also be used for multiplication:

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

The set of complex numbers can be visualized as the complex (or Argand) plane:
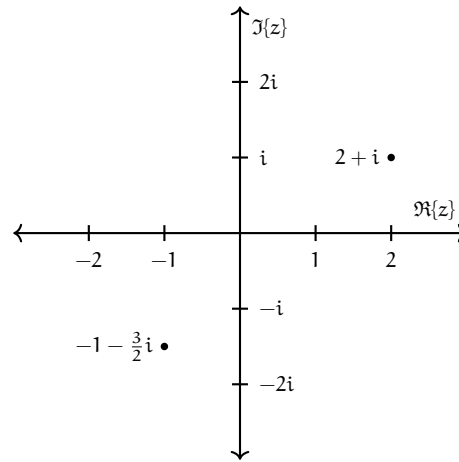
The *(complex) conjugate* of $z = x + iy$ is the number $\bar{z} = x - iy$.

Conjugating twice gets us back where we started:

$$\bar{\bar{z}} = \overline{x - iy} = x + iy = z$$

which means complex conjugation is an *involution*.

Note that

$$z\bar{z} = (x + iy)(x - iy) = x^2 + y^2$$

which gives us a real number.

The *modulus* of z is the distance between z and the origin, that is,

$$|z| = \sqrt{x^2 + y^2}.$$

Exercise 19. If $z \neq 0$, show that $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$.

We can also divide complex numbers by getting rid of the imaginary part in the denominator:

$$\frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + i\frac{bc - ad}{c^2 + d^2}$$

The *argument* of z is the counterclockwise angle, in radians, from the positive real axis to the line segment connecting z and the origin.
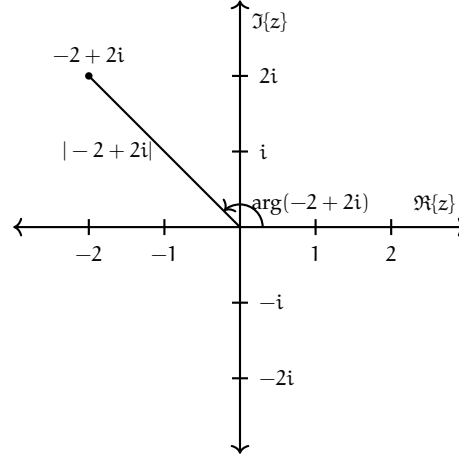
The *polar form* of z is obtained by writing z as

$$z = re^{i\theta}$$

where $r = |z|$ is the modulus and $\theta = \arg z$ is the argument.

We have Euler's famous identity

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

which can be obtained by using the Taylor series for the exponential, and recognizing the Taylor series for sine and cosine.

Euler's identity allows us to easily convert between the polar and Cartesian coordinates.

Polar coordinates are most useful for multiplication, division, and exponentiation owing to identities we know about exponentiation:

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = r_1 r_2 e^{i(\theta_1 + \theta_2)},$$
$$\frac{r_1 e^{i\theta_1}}{r_2 e^{i\theta_2}} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)},$$
$$(re^{i\theta})^n = r^n e^{in\theta}.$$

The *unit circle* is the set of complex numbers with modulus 1. These points form a circle on the complex plane.

16
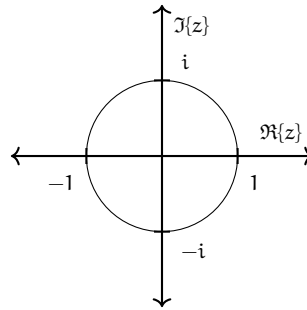
Let n be a natural number. If z is a complex number such that $z^n = 1$, then z is called an nth *root of unity*.

> **Exercise 20.** Show that the nth roots of unity all have the form $e^{2\pi i k/n}$ for some k in $\mathbb{Z}$.

Here is an animation of the nth roots of unity where $n = 3, \ldots, 12$.

0.6 Matrices

An m-by-n *matrix* over $\mathbb{R}$ is an array of real numbers with m rows and n columns.

We typically use capital letters (A, B, C, …) for matrices, and lowercase letters (a, b, c, …) for their entries, subscripted by *row* and then *column*.

The set of all m-by-n matrices is denoted $M_{m \times n}(\mathbb{R})$.

Note, some people write $M_{m \times n}(\mathbb{R})$ as $\mathbb{R}^{m \times n}$. This is fine, but beware—$\mathbb{R}^{2 \times 2} \neq \mathbb{R}^4$!

Given an m-by-n matrix $A = (a_{i,j})$ and an n-by-p matrix $B = (b_{k,l})$, their *product* AB is the m-by-p matrix of dot products of the rows of A with the columns of B. Explicitly,

$$(AB)_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

> **Example 0.6.1** — The product of the 4-by-3 matrix
> $$A = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 5 & 3 \\ 6 & 2 & 4 \\ 4 & 0 & 5 \end{bmatrix}$$

with the 3-by-2 matrix

$$B = \begin{bmatrix} 2 & 1 \\ 3 & 2 \\ 1 & 5 \end{bmatrix}$$

is the 4-by-2 matrix

$$
AB = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 5 & 3 \\ 6 & 2 & 4 \\ 4 & 0 & 5 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 3 & 2 \\ 1 & 5 \end{bmatrix}
$$

$$
= \begin{bmatrix} (1,1,2) \cdot (2,3,1) & (1,1,2) \cdot (1,2,5) \\ (0,5,3) \cdot (2,3,1) & (0,5,3) \cdot (1,2,5) \\ (6,2,4) \cdot (2,3,1) & (6,2,4) \cdot (1,2,5) \\ (4,0,5) \cdot (2,3,1) & (4,0,5) \cdot (1,2,5) \end{bmatrix} = \begin{bmatrix} 7 & 13 \\ 18 & 25 \\ 22 & 30 \\ 13 & 29 \end{bmatrix}.
$$

The *transpose* of an m-by-n matrix A is the n-by-m matrix whose rows are the columns of A. That is, $(A^\mathsf{T})_{i,j} = a_{j,i}$ for all i, j. Just flip it over its diagonal:

$$
\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^\mathsf{T} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}.
$$

A *square matrix* is a matrix with the same number of rows as columns. If A is an n-by-n square matrix, an *inverse* of A is a matrix B such that $AB = BA = I$. Not every matrix has an inverse—just consider

$$
A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}
$$

—but when an inverse exists, it's unique, and we denote it A^{-1}. A matrix whose inverse exists is called *invertible*.

Finally, the *determinant* of a square matrix $A = (a_{ij})$ is defined as follows. For a 1-by-1 matrix,

$$
\det \begin{bmatrix} a \end{bmatrix} = a,
$$

and for a larger matrix,

$$
\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det \tilde{A}_{i,j} \tag{2}
$$

where i is any fixed index between 1 and n, and $\tilde{A}_{i,j}$ is the matrix obtained by removing the ith row and jth column from A. This is known as *row expansion*.

Example 0.6.2 — By expanding along the top row,

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = a \det \begin{bmatrix} d \end{bmatrix} - b \det \begin{bmatrix} c \end{bmatrix} = ad - bc.$$

You're also allowed to expand down any column; the formula for *column expansion* has the same shape as (2) but this time the sum is over i (the rows) and it's j (the column) that's fixed.

Recall that the determinant is *multiplicative*:

$$\det AB = \det A \det B.$$

This fact is fundamental.

Exercise 21. Show that A is invertible if and only if $\det A \neq 0$.

Chapter 1

Groups and subgroups

1.1 Binary operations and groups

> **Definition 1.1.1** — Let S be a set. A *binary operation* on S is a function $\star : S \times S \to S$ written using infix notation, like so: $a \star b$.

In other words, $a \star b$ is the image of the element (a, b) under the function $\star$. In more other words, $a \star b = \star(a, b)$.

> **Example 1.1.2** — Addition on the integers is a binary operation $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. The pair (a, b) is sent to its sum $a + b$.

Recall that the elements of $S \times S$ are *ordered pairs* (a, b) with a and b both in S. A function $\star : S \times S \to S$ has to map each *ordered pair* somewhere. If a and b are distinct, then the ordered pairs (a, b) and (b, a) are distinct, too. There's no reason why $\star$ should send distinct ordered pairs to the same place. Thus, we generally do not have

$$a \star b = b \star a. \tag{1.1}$$

> **Example 1.1.3** — Subtraction on the integers is a binary operation $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. The pair (a, b) is sent to the difference $a - b$. Note that $a - b \neq b - a$ in general.

> **Definition 1.1.4** — A binary operation $\star$ on a set S such that $a \star b = b \star a$ for all a and b in S is called *commutative*.

1.1.1 Visualizing binary operations

Remember your times tables from grade school? A "times table" for a general binary operation is called a *Cayley table*.

> **Example 1.1.5 —** Here is a portion of the Cayley table for subtraction on $\mathbb{Z}$:
>
> | $-$ | -2 | -1 | 0 | 1 | 2 | 3 |
> |---|---|---|---|---|---|---|
> | -2 | 0 | -1 | -2 | -3 | -4 | -5 |
> | -1 | 1 | 0 | -1 | -2 | -3 | -4 |
> | 0 | 2 | 1 | 0 | -1 | -2 | -3 |
> | 1 | 3 | 2 | 1 | 0 | -1 | -2 |
> | 2 | 4 | 3 | 2 | 1 | 0 | -1 |
> | 3 | 5 | 4 | 3 | 2 | 1 | 0 |

As with matrices, Cayley tables are indexed by row and then column. The (a, b)-entry in the Cayley table is $a \star b$.

In any Cayley table, the elements should appear in the same order down the right as across the top. When S is finite, Cayley tables can be used to completely describe (hence define) binary operations.

> **Example 1.1.6 —** Multiplication in $\mathbb{Z}/5\mathbb{Z}$ looks like this:
>
> | $\cdot$ | [0] | [1] | [2] | [3] | [4] |
> |---|---|---|---|---|---|
> | [0] | [0] | [0] | [0] | [0] | [0] |
> | [1] | [0] | [1] | [2] | [3] | [4] |
> | [2] | [0] | [2] | [4] | [1] | [3] |
> | [3] | [0] | [3] | [1] | [4] | [2] |
> | [4] | [0] | [4] | [3] | [2] | [1] |

> **Example 1.1.7** (Rock–Paper–Scissors) **—** Consider the set $M = \{r, p, s\}$, where the elements stand for *r*ock, *p*aper, and *s*cissors. Define $x \star y$ to be the winner of the match if $x \neq y$, and define $x \star x = x$ when it's a tie. Thus, for example, $r \star p = p$ and $p \star s = s$.

Exercise 22. Fill in the Cayley table for Rock–Paper–Scissors.

$\star$	r	p	s
r		p	
p			s
s			

1.1.2   Associativity

Question — In Rock–Paper–Scissors, what is the value of

$$r \star p \star s?$$

On the one hand,

$$(r \star p) \star s = p \star s = s.$$

But on the other hand,

$$r \star (p \star s) = r \star s = r.$$

Perhaps this is an indication that you shouldn't play Rock–Paper–Scissors with three people at once, but the mathematical significance of this ambiguity is due to the failure of $\star$ to be what's called *associative*.

Definition 1.1.8 — A binary operation $\star$ on a set S such that $(a \star b) \star c = a \star (b \star c)$ for all a, b, c in S is called *associative*.

When an operation is associative, everything is wonderful. We're allowed to string together elements freely, unburdened by bothersome brackets, unoppressed by pesky parentheses, without fear of being misapprehended.

Associativity of addition is the reason we (would) never write

$$1 + 2 + 3 + 4 + 5$$

as

$$1 + ((2 + (3 + 4)) + 5).$$

However, non-associativity of subtraction is the reason we (should) never write

$$1 - 2 - 3 - 4 - 5$$

even though, in this case, most people would argue (vehemently and to the death) that it's -13 because they're reading it left to right. But what about

$$1 - ((2 - (3 - 4)) - 5) = 3?!$$

In sum, associativity is about arrangements of *brackets* (i.e. *parentheses*); commutativity is about arrangements of *elements*. Don't confuse

$$a \star (b \star c) = (a \star b) \star c \quad \text{and} \quad a \star (b \star c) = (b \star c) \star a.$$

1.1.3 Operations table

Here is a list of common candidates for binary operations. We may check if they actually are binary operations (that is, they are indeed functions $S \times S \to S$), and if so, decide if they are commutative or associative.

set	candidate	operation?	commutative?	associative?
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	$+$	yes	yes	yes
$\mathbb{N}$	$-$	no	-	-
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	$-$	yes	no	no
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	$\times$	yes	yes	yes
$\mathbb{N}, \mathbb{Z}$	$\div$	no	-	-
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	$\div$	no	-	-
$\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^{\times *}$	$\div$	yes	no	no
$\mathbb{R}$	$\max\{a, b\}$	yes	yes	yes
$\mathbb{R}$	a^b	no	-	-
$\mathbb{R}_{>0}$	a^b	yes	no	no
$\mathbb{R}^3$	cross product	yes	no	no
$\mathbb{R}^n$	dot product	no	-	-
vector space	vector addition	yes	yes	yes
$M_{n \times m}(\mathbb{R})$	$+$	yes	yes	yes
$M_{n \times n}(\mathbb{R})$	$\times$	yes	no	yes
self-maps	composition	yes	no	yes
$\{r, p, s\}$	rock–paper–scissors	yes	yes	no
any set	$(a, b) \mapsto a$	yes	no	yes

Exercise 23. Explain every "no" in the table above. (That is, find a counterexample).

1.1.4 Definition of a group

We are now prepared to define what a group is, once we introduce one additional piece of terminology: Associativity is so *natural* and *desirable* that we'll usually take it for granted

---

*For now, we define them as $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$, and $\mathbb{C}\backslash\{0\}$ respectively. See Section 1.2.1 for the motivation of this definition.

in this course.

> **Definition 1.1.9 —** A *composition law* is an associative binary operation.

> **Definition 1.1.10 —** A *group* is a set G with a composition law $\star$ (called its *group operation*) and a distinguished element e satisfying these two axioms:
>
> **Identity:** $a \star e = e \star a = a$ for all a in G
>
> **Inversion:** for each a in G there exists b in G such that $a \star b = b \star a = e$
>
> We denote this $(G, \star, e)$. Often we simply write $(G, \star)$ or even G and let the rest be implied.

Intuitively, the Identity axiom says "You Can Do Nothing" while the Inversion axiom says "You Can Undo Anything"—these axioms give us the structure of the *invertible symmetries* perspective on groups that we discussed in Week 1.

Any element satisfying the Identity axiom is called an *identity*; any element satisfying the Inversion axiom is called an *inverse*.

> *Aside.* The traditional definition of a group (which you may see in your textbooks) says that a group is a set G with an operation $\star$ satisfying these four axioms:
>
> **Closure:** $a \star b$ is in G for all a, b in G
>
> **Associativity:** $\star$ is associative
>
> **Identity:** there exists e in G such that $a \star e = e \star a = a$ for all a in G
>
> **Inversion:** for each a in G there exists b in G such that $a \star b = b \star a = e$
>
> The traditional definition is unsatisfactory for a few technical reasons. First, the Closure axiom becomes redundant once you ask $\star$ to be a binary operation. Second, the Associativity axiom is moreso a property of the operation than of the elements. Third, the traditional definition doesn't clarify that the 'e' that's asserted to exist in the Identity axiom is the same 'e' that appears in the Inversion axiom.

1.1.5 Immediate consequences

> **Exercise 24.** Show that the identity element e is unique. [That is, show that if e' is another element of G that satisfies the Identity axiom, then $e' = e$.]

Exercise 25. Show that for any a in G, there is a unique element b such that $a \star b = b \star a = e$. [That is, show that if b' is another inverse for a, then $b' = b$.]

Remark 1.1.11. This unique element is called the *inverse* of a and denoted a^{-1}.

Exercise 26. What is the inverse of $a \star b$?

Exercise 27. Show that we can perform *right cancellation*:

$$a \star c = b \star c$$
$$a = b$$

and *left cancellation*:

$$c \star a = c \star b$$
$$a = b$$

for all elements a, b, c in any group.

Note the importance of the *sides* of the expressions we are working with: We *do not* have in general that $c \star a = b \star c$ implies $a = b$ [When do we have this?].

The definition of groups is actually a little stronger than we require. In fact, we can weaken the axioms so that we only check one *side* of the equalities.

Exercise 28. Let G be a set with an associative binary operation $\star$ and a distinguished element e satisfying these two axioms:

- $a \star e = a$ for all a in G (Axiom of Right Identity)

- for each a in G there exists b in G such that $a \star b = e$ (Axiom of Right Inversion)

These are like the group axioms, except they're only required to hold "on one side". In this exercise you will prove that any structure $(G, \star, e)$ satisfying these weaker axioms is actually already a group.

a) Prove that G has the *right-cancellation property*: $a \star c = b \star c$ implies $a = b$.

b) An *idempotent* is an element i such that $i \star i = i$. Show that e is the *only* idempotent in G. How is this related to left-cancellation?

c) Show that every right inverse is a left inverse.

d) Show that e is a left identity.

e) Explain why we are done.

1.1.6   Notation

Composition laws have lots of notations, like $\star$, $*$, $\circ$, $\cdot$, $\times$, $\otimes$, $+$, $\oplus$, ... But when we're dealing with a single group, there's only *one* composition law involved—so we can get away with not writing it at all. (It's also kind of annoying to write $\star$ all the time.) This is called the *multiplicative notation*.

If the composition law is commutative, the group is called *abelian*. Some people write the composition law in abelian groups using a plus sign ($+$), but we'll stick to the multiplicative notation except in very concrete cases, like $\mathbb{Z}/n\mathbb{Z}$ under addition.

Indeed, we will use more notation inspired by those found in multiplication and addition:

> **Definition 1.1.12** — Let G be a group with identity element e and let $g \in G$. For each integer n, define g^n as follows:
>
> if $n > 0$, put
> $$g^n = \underbrace{g \cdot \ldots \cdot g}_{n \text{ times}}$$
>
> if $n < 0$, put
> $$g^n = (g^{-1})^{-n}$$
>
> and if $n = 0$, put
> $$g^0 = e.$$

This notation is extremely useful for simplifying long expressions:

$$aabbbcdddd = a^2 b^3 c d^4.$$

For *abelian* groups written *additively*, "g^n" becomes "ng":

$$a + b + c + b - a = 2b + c.$$

To summarize,

notation	multiplicative	additive
operation	$a \cdot b$ or ab	$a + b$
identity	e or 1	0
inverses	a^{-1}	$-a$
powers	a^n	na

Note in particular that we will use multiplicative notation for function composition.

Multiplicative notation is convenient as it behaves largely the same way multiplication does.

> **Proposition 1.1.13** (Exponent Laws)
>
> For all g in G and all n, m in $\mathbb{Z}$,
>
> 1. $g^n g^m = g^{n+m}$
>
> 2. $(g^n)^m = g^{nm}$
>
> 3. $(g^{-1})^n = (g^n)^{-1} = g^{-n}$

Proof. Exercise. □

Exercise 29. Let G be a group. Suppose $a^2 = e$ for every a in G. Show that G is abelian.

1.2 Examples

1.2.1 Basic groups

Wherever addition is defined, we *may* have a group; the set in question must contain zero (the additive identity) and be closed under negation (to form additive inverses).

Thus $\mathbb{N}$ is not a group under addition, but $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are.

Similarly, wherever multiplication is defined, if the set contains 1 (the multiplicative identity) and is closed under reciprocation (to form multiplicative inverses), then we have a group. Using a superscript $\times$ to denote the set of "multiplicatively invertible" elements, we find that $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ are $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$, and $\mathbb{C}\backslash\{0\}$ respectively, and they are all groups under multiplication.

Exercise 30. What is $\mathbb{Z}^\times$?

1.2.2 Groups of integers

The set $\mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n forms an abelian group under addition: the identity element is $[0]$ and the inverse of $[a]$ is $[-a]$. This is called the *additive group (of integers) modulo* n.

What about multiplication? Sure, we can multiply classes, and $[1]$ is in $\mathbb{Z}/n\mathbb{Z}$, but— inverses?

Actually, not every class has a multiplicative inverse. For example, in $\mathbb{Z}/6\mathbb{Z}$,

$$[3][4] = [12] = [0]$$

so neither [3] nor [4] are invertible. (If they were, say [3][a] = [1], then we'd have

$$[4] = [4][1] = [4][3][a] = [0][a] = [0]$$

which can't happen modulo 6.) However,

$$[5][5] = [25] = [1]$$

so [5] is invertible.

By restricting our attention to *invertible* elements, we obtain:

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

known as the *multiplicative group (of integers) modulo* n, a.k.a. $U(n)$.

Example 1.2.1 — $(\mathbb{Z}/6\mathbb{Z})^\times = \{[1], [5]\}$ and $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}$.

Exercise 31. What are the invertible elements of $\mathbb{Z}/n\mathbb{Z}$? What are the invertible elements of $\mathbb{Z}/p\mathbb{Z}$ if p is a prime?

1.2.3 Matrix groups

The set of invertible $n \times n$ matrices forms a group under matrix multiplication, called the *general linear group*.

$$GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) : \det A \neq 0\}$$

We can also consider matrices with entries in $\mathbb{Z}/m\mathbb{Z}$. However, $\det A \neq [0]$ is no longer enough—we need $\det A$ to be *invertible* modulo m. That is,

$$GL_n(\mathbb{Z}/m\mathbb{Z}) = \{A \in M_{n\times n}(\mathbb{Z}/m\mathbb{Z}) : \det A \in (\mathbb{Z}/m\mathbb{Z})^\times\}$$

Example 1.2.2 — In $\mathbb{Z}/12\mathbb{Z}$, writing $\bar{a}$ instead of $[a]$,

$$\det \begin{bmatrix} \bar{2} & \bar{1} \\ \bar{3} & \bar{4} \end{bmatrix} = \bar{2}\bar{4} - \bar{1}\bar{3} = \bar{8} - \bar{3} = \bar{5}$$

which is invertible because $5^2 = 25 \equiv 1 \pmod{12}$. The inverse matrix is

$$\begin{bmatrix} \bar{2} & \bar{1} \\ \bar{3} & \bar{4} \end{bmatrix}^{-1} = \bar{5}^{-1} \begin{bmatrix} \bar{4} & -\bar{1} \\ -\bar{3} & \bar{2} \end{bmatrix} = \bar{5} \begin{bmatrix} \bar{4} & \bar{11} \\ \bar{9} & \bar{2} \end{bmatrix} = \begin{bmatrix} \bar{20} & \bar{55} \\ \bar{45} & \bar{10} \end{bmatrix} = \begin{bmatrix} \bar{8} & \bar{7} \\ \bar{9} & \bar{10} \end{bmatrix}.$$

1.2.4 Trivial group

Let G be a set with one element, which we'll call e. There is only one possible binary operation on G:

$$G \times G \to G$$
$$(e, e) \mapsto e$$

This yields the *trivial group*.

> **Exercise 32.** Check that the trivial group is a group. What is its Cayley table?

1.2.5 Cyclic groups

A *cyclic group* is a group in which every element is an integer power[*] of a single element, called a *generator*. We write

$$G = \langle g \rangle$$

to mean G is cyclic with generator g.

For example, in the group of integers under addition, every integer is an integer multiple of 1, so

$$\mathbb{Z} = \langle 1 \rangle.$$

Similarly, in the additive group modulo n, every element can be written as a sum of $[1]$'s. Therefore,

$$\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle.$$

The group μ_n is the set of complex nth roots of unity under multiplication. That is,

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\}.$$

Since the nth roots of unity are of the form $e^{2\pi i k/n}$, we may write

$$\mu_n = \langle e^{2\pi i/n} \rangle.$$

1.2.6 Dihedral groups

The dihedral group D_n is the set of reflections and rotations — *SYMMETRIES* — of a regular n-gon, under composition.

---

[*]*multiple* in additive notation

Example 1.2.3 — Consider the regular pentagon with its rotations
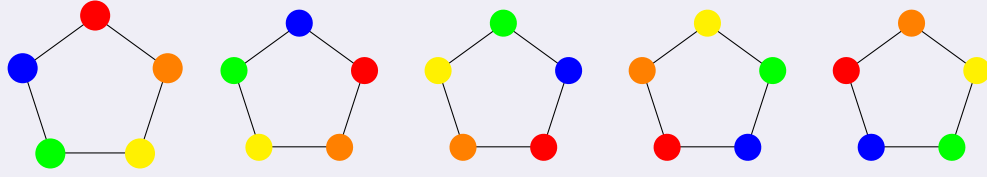
and reflections
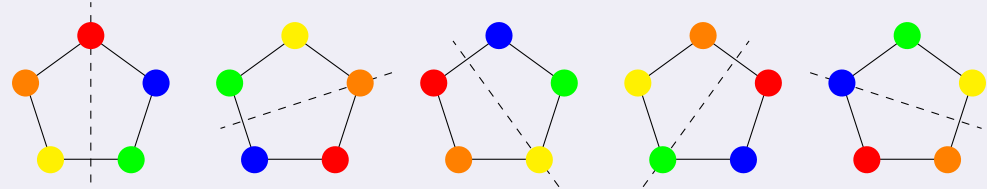
Let r denote the one-fifth clockwise turn and let f denote the flip over the vertical axis. Then *every* rotation is a power of r.

We can also express every reflection in terms of *just* f and r. For example, to produce a flip across the orange axis, first flip across the red axis (f) then turn two-fifths clockwise (r^2), yielding fr^2.
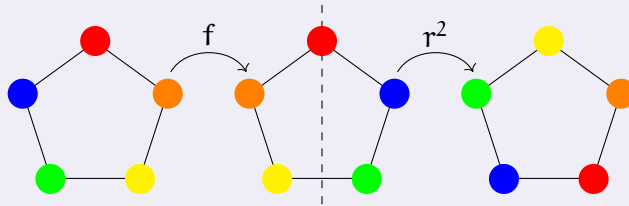
1.2.7 Symmetric groups

Let X be a set. The *symmetric group on* X is the set of all permutations* on X under composition. This group is denoted

$$S_X$$

Special cases: the symmetric group on $\{1, \ldots, n\}$ is denoted S_n while the symmetric group on $\mathbb{N}$ is denoted S_∞.

For example, the only two elements of S_2 are the permutations

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

in two-line notation). The function τ^2 sends $1 \to 2 \to 1$ and $2 \to 1 \to 2$, so $\tau^2 = \mathrm{id}$. Thus $S_2 = \langle \tau \rangle$ is cyclic with 2 elements.

---

*i.e. bijective self-maps

We will explore these groups in more detail in later weeks.

1.3   Subgroups

> **Definition 1.3.1** — A group H is a *subgroup* of a group G if H is a subset of G and the group operation on H is the same as the operation on G. The subgroup relation is written
>
> $$H \leq G$$
>
> meaning "H is a subgroup of G".

To check if a sub*set* H of a group G is a sub*group*, one must show

  (i) $ab \in H$ for all a, b in H (the operation in G restricted to H is still a binary operation)

  (ii) $e \in H$ (the identity element of G is in H)

  (iii) $a^{-1} \in H$ for all a in H (the inverse in G of every element of H is in H)

(i) shows that the group operation in G restricts to a function $H \times H \to H$ while (ii) and (iii) show that H is a group.*

> **Proposition 1.3.2** (Subgroup Criterion)
>
> Let G be a group and let $H \subseteq G$. Then $H \leq G$ if and only if H is non-empty and $ab^{-1} \in H$ for all a, b in H.

Proof. The 'only if' (forward implication) is easy. For the converse, we show that the three properties (i), (ii), and (iii) hold, albeit in a different order.

Start with (ii). Since H is non-empty, there *is* some element a in H. By hypothesis, $aa^{-1} \in H$. But $aa^{-1} = e$, so $e \in H$.

Next, (iii). Let $a \in H$. By (ii) and the hypothesis, $ea^{-1} \in H$. But $ea^{-1} = a^{-1}$, so $a^{-1} \in H$.

Finally, we show (i). Let $a, b \in H$. By (iii) and the hypothesis, $a(b^{-1})^{-1} \in H$. But $(b^{-1})^{-1} = b$, so $ab \in H$. $\square$

> **Exercise 33.** Show that if H_1, H_2 are subgroups of G, then $H_1 \cap H_2$ is a subgroup of G.

Let us now look at some common subgroups of groups.

A priori, H might have its own identity e', but since the operations coincide, $e'e' = e'$ in G, so $e' = e$. Same for inverses.

1.3.1 Basic groups

In additive notation, "ab^{-1}" means $a - b$. Thus, under addition,

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C},$$

because the difference of two integers (resp. rationals, reals) is an integer (resp. rational, real). (Of course, $0 \in \mathbb{Z}$.)

Similarly,

$$\mathbb{Q}^{\times} \leq \mathbb{R}^{\times} \leq \mathbb{C}^{\times},$$

because the quotient of two nonzero rational (resp. real) numbers is rational (resp. real). (Also, $1 \in \mathbb{Q}^{\times}$.)

1.3.2 Matrix groups

A *matrix group* is a subgroup of GL_n for some n. (The definition works the same regardless of what set the entries are in).

The most important matrix groups are the *special linear groups*—matrices that preserve volume ($|\det A| = 1$) and orientation ($\det A > 0$, only relevant when the entries are in $\mathbb{Q}$ or $\mathbb{R}$),

$$SL_n = \{A \in GL_n : \det A = 1\},$$

the *orthogonal groups*—matrices that preserve distance (which necessarily preserves volume [prove it!]),

$$O_n = \{A \in GL_n : A^{-1} = A^{\mathsf{T}}\},$$

and the *special orthogonal groups*—matrices that preserve distance, volume, and orientation,

$$SO_n = \{A \in GL_n : A^{-1} = A^{\mathsf{T}}, \det A = 1\}.$$

To show that $SL_n \leq GL_n$, just note that $I \in SL_n$ because $\det I = 1$, and if $A, B \in SL_n$, then

$$\det AB^{-1} = \det A \cdot \det B^{-1} = 1 \cdot 1^{-1} = 1$$

so $AB^{-1} \in SL_n$.

Exercise 34. Prove that O_n is a matrix group. Conclude that SO_n is a matrix group.

There are many other examples of matrix groups.

Exercise 35. Show that the set of matrices of the form

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \quad (x \in \mathbb{R})$$

is a matrix group.

1.3.3 Cyclic groups

If $G = \langle g \rangle$ is cyclic and k is any fixed integer, it follows from 1.1.13 that the set of integer powers of g^k is a subgroup of G. That is,

$$\langle g^k \rangle \leq G.$$

For example, we saw that $\mathbb{Z}$ under addition forms a cyclic group generated by 1. Thus, $\langle k \rangle \leq \mathbb{Z}$ for every integer k. In particular, the set of *even numbers* is a subgroup of $\mathbb{Z}$.

Exercise 36. Is the set of *odd numbers* a subgroup of $\mathbb{Z}$?

We'll talk more about cyclic groups in Week 4.

1.3.4 Dihedral groups

In D_n, if r is any rotation and f is any flip, then $\langle r \rangle$ and $\langle f \rangle$ are (two of the) subgroups of D_n.

We'll talk more about dihedral groups in Week 4.

1.3.5 Permutation groups

A *permutation group* is a subgroup of a symmetric group. For example, the four permutations

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

constitute a subgroup of S_4 called the Klein four-group[*], denoted V.

Exercise 37. Show that V is a group by completing its Cayley table.

---

[*]Also see Klein Four.

$\circ$	e	ρ	σ	τ
e				
ρ				
σ				
τ				

We'll talk more about symmetric groups and permutation groups in weeks 5 and 6.

1.3.6 Generating new subgroups

Let G be a group and let $S \subseteq G$. The *subgroup generated by* S is the set of all possible combinations of the elements of S (and their inverses) using the composition law in G. It is denoted $\langle S \rangle$. Formally, we have

$$\langle S \rangle = \{g_1^{\pm 1} \ldots g_k^{\pm 1} : k \geq 0 \text{ and } g_i \in S\}.$$

(By allowing $k = 0$ we include the *empty product*, which we always take to be e. In particular, the empty set generates the trivial group!)

> **Proposition 1.3.3**
> Let $S \subseteq G$. Then $\langle S \rangle \leq G$.

Proof. $\langle S \rangle$ is non-empty, because we can always form the empty product to get e. And if $a, b \in S$ then

$$a = g_1^{\epsilon_1} \ldots g_k^{\epsilon_k} \quad \text{and} \quad b = h_1^{\delta_1} \ldots h_l^{\delta_l},$$

where $g_i, h_j \in S$ and $\epsilon_i, \delta_j \in \{1, -1\}$. Thus

$$ab^{-1} = g_1^{\epsilon_1} \ldots g_k^{\epsilon_k} h_l^{-\delta_l} \ldots h_1^{-\delta_1}.$$

All $k + l$ terms are in S and all the exponents are 1 or -1, so $ab^{-1} \in \langle S \rangle$. $\quad\square$

Remark 1.3.4. $\langle S \rangle$ is in fact the *smallest* subgroup containing S—any subgroup containing S must contain all elements of the form $g_1^{\pm 1} \ldots g_k^{\pm 1}$, and so it must contain $\langle S \rangle$.

If S is finite, say $S = \{g_1, \ldots, g_n\}$, then we write

$$\langle g_1, \ldots, g_n \rangle \quad \text{instead of} \quad \langle \{g_1, \ldots, g_n\} \rangle.$$

If S is a singleton (i.e. $n = 1$), say $S = \{g\}$, then $\langle S \rangle = \langle g \rangle$ is called the *cyclic subgroup generated by* g. Of course, the whole group G is cyclic iff $G = \langle g \rangle$ for some g in G.

> **Example 1.3.5** — In the additive group $\mathbb{Q}$,
>
> $$\langle \tfrac{1}{2}, \tfrac{1}{3} \rangle = \{\tfrac{n}{2} + \tfrac{m}{3} : n, m \in \mathbb{Z}\}$$
>
> because $\mathbb{Q}$ is abelian. Putting this expression on a common denominator yields
>
> $$\frac{n}{2} + \frac{m}{3} = \frac{3n + 2m}{6}.$$
>
> Since $3(-3) + 2(5) = 1$, this subgroup is actually cyclic—every element is an integer multiple of $\tfrac{1}{6}$.

> **Example 1.3.6** — In the multiplicative group $\mathbb{Q}^\times$,
>
> $$\langle 2, 3 \rangle = \{2^n 3^m : n, m \in \mathbb{Z}\}$$
>
> is the subgroup of fractions whose numerator and denominator (in lowest terms) are divisible by 2 and 3 only. For example,
>
> $$6, \ \frac{2}{3}, \ \frac{256}{243}, \ \frac{1}{1024} \in \langle 2, 3 \rangle$$
>
> but 5 is not.

Exercise 38. Show that the group in the above example cannot be cyclic. (That is, show that there is no $g \in \mathbb{Q}^\times$ such that $\langle g \rangle = \langle 2, 3 \rangle$.)

1.4   Guises of the same group

We said that there's only one group of one element (the trivial group), so μ_1, S_1, and any trivial subgroup of another group—no matter what the identity element is—must be the trivial group, despite the different names. You may also have noticed that many groups under different names seem to behave in the exact same way—μ_2, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}^\times$, S_2, and D_1, for example, all have two elements, the identity and an involution. Their Cayley tables thus look identical other than the names of the elements. All their group-theoretic properties that we know of are the same. So we are tempted to call them all the same group. But what does it mean, exactly, for two groups to be "the same"?

In general, the answer to this question allows us to export the answer to a specific question to a class of questions.

> **Question —** When are two mathematical objects the same? In other words, when can we interchange one thing with the other in a question?

As it turns out, the answer depends on how we define *sameness*. For example, consider the two sets $S = \{a, b, c, d, e\}$ and $T = \{1, 2, 3, 4, 5\}$. Of course, the elements have different names, so they're different in that manner. However, they do have the same size, and we may view these two sets as interchangeable in set-theoretic contexts.

> **Exercise 39.** Consider the two questions "how many three-letter words can you make from the letters in S (with repeats)?" and "how many functions are there from $\{1, 2, 3\}$ to T?". Why are these two questions in fact the same question?

The notion of "interchangeable" sets allows us to answer questions concerning finite sets by just answering questions about sets $\{1, 2, 3, ..., n\}$.*

When we introduce additional structure on the object in question, the notion of "sameness" also expands to include these structure. For example, if we are to ask questions about a vector space V, we know these questions have the same answers as with the vector space W if there is an invertible linear transformation $T : V \to W$—linear transformations preserve vector addition and scalar multiplication. This allows us to reduce the study of all finite dimensional vector spaces to just the study of F^n, where F is the corresponding field.

Returning to groups, we may ask when two groups are the same. An understanding of this type will allow us to answer questions about groups more easily, by treating many groups as guises of other groups that we've already studied.

> **Definition 1.4.1 —** Given two groups $(G, \star)$ and $(H, \circ)$, we say G and H are *isomorphic* if there is a bijection $\phi : G \to H$ such that for all $a, b \in G$, we have
>
> $$\phi(a \star b) = \phi(a) \circ \phi(b).$$
>
> Such a ϕ is called an *isomorphism*. We denote this $G \cong H$.

Remark 1.4.2. The operation on the left-hand side is done in G (before f is applied) whereas the operation on the right-hand side is done in H (after f is applied). In the future we will drop the operation entirely and write

$$\phi(ab) = \phi(a)\phi(b)$$

if no further information is given.

Note that this immediately gives $\phi(e_G) = e_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$.

---

*The situation for infinite sets is a bit messier, and we will not get into that within this course except to note that two infinite sets may not actually have the same "size" (i.e. cardinality).

Exercise 40. Show that $\cong$ is an equivalence relation.

Exercise 41. Show that $\mathbb{R}^\times$ is isomorphic to $GL_1(\mathbb{R})$. (Is the latter group abelian?)

A visual way to check isomorphisms of small groups is to draw both Cayley tables, colour each element of one group uniquely, and colour the corresponding elements in the other group the same colour. If the resulting patterns match, then the groups are isomorphic.

For example, writing $\omega = e^{2\pi i/3}$, we can consider $\mathbb{Z}/3\mathbb{Z}$ and $\mu_3 = \{1, \omega, \omega^2\}$:

$\mathbb{Z}/3\mathbb{Z}$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

μ_3	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Why does this work? Suppose ▨▨ = ▨ in the group on the left,

By definition of our colouring scheme, f(▨) must be red, f(▨) must be blue, and f(▨▨) = f(▨) must be green. The colour of f(▨)f(▨) is the colour of the cell in the f(▨)-row and the f(▨)-column. This is green if and only if f(▨) = f(▨).

Exercise 42. Show that the groups listed at the beginning of this section are isomorphic.

Exercise 43. Show that $\mathbb{Z}/4\mathbb{Z}$, μ_4, $(\mathbb{Z}/5\mathbb{Z})^\times$, are isomorphic.

Show that V and $(\mathbb{Z}/8\mathbb{Z})^\times$ are isomorphic. Show that they are not isomorphic to the groups above.

1.5 Group Actions

1.5.1 Group actions

"GROUPS, AS MEN, WILL BE KNOWN BY THEIR ACTIONS."

—Guillermo Moreno

Here are all $16 = 2^4$ possible square, non-edge puzzle pieces (idealized).
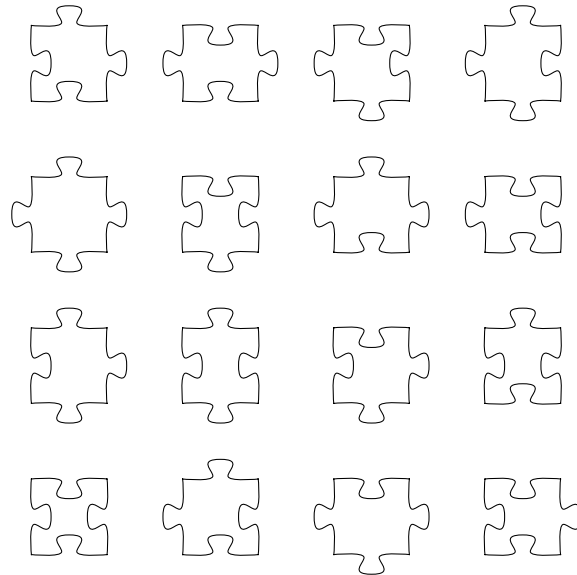
Say two puzzle pieces are rotation-equivalent if you can rotate one so it looks like the other. How many puzzle pieces are there up to rotation-equivalence?
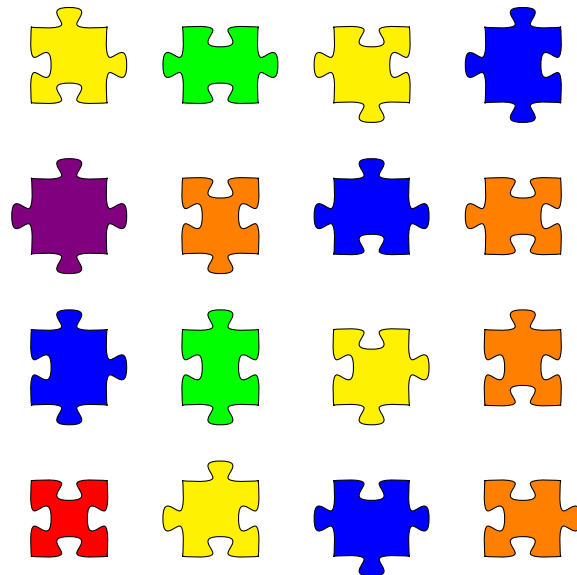
The answer is 6. Each puzzle piece has one of the following shapes:
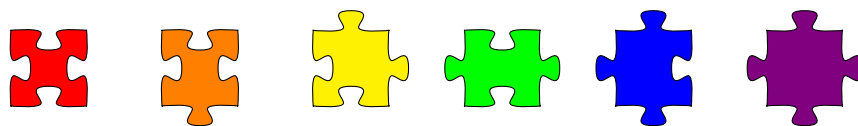
Mathematically, we just determined the *orbits* of the *action* of the group C_4 on the set of puzzle pieces.

Definition 1.5.1 — Let G be a group and X be a set. A *left action of* G *on* X is a function $G \times X \to X$, denoted $(g, x) \mapsto g \, . \, x$, satisfying

1) *identity*: $e \, . \, x = x$ for all x in X

2) *compatibility*: $g \, . \, (h \, . \, x) = gh \, . \, x$ for all x in X and g, h in G

We write $G \curvearrowright X$ to mean G acts on X.

Proposition 1.5.2

Let $G \curvearrowright X$. Then "$x \sim y$ iff $g \, . \, x = y$ for some g in G" is an equivalence relation.

Proof. By the *identity* axiom, $\sim$ is reflexive: $e \, . \, x = x$ so $x \sim x$ for all x in X. By the *compatibility* axiom, $\sim$ is transitive: if $x \sim y$ and $y \sim z$ then $g \, . \, x = y$ and $h \, . \, y = z$ for some g, h in G, so

$$hg \, . \, x = h \, . \, g \, . \, x = h \, . \, y = z.$$

By *both* axioms together, $\sim$ is symmetric: if $x \sim y$ then $g \, . \, x = y$ so

$$g^{-1} \, . \, y = g^{-1} \, . \, g \, . \, x = g^{-1}g \, . \, x = e \, . \, x = x. \qquad \square$$

Definition 1.5.3 — The equivalence classes of the relation above are called *orbits*. The orbit of x is denoted $\mathrm{Orb}_G(x)$ or Gx, and the set of equivalence classes is denoted X/G. That is,

$$\mathrm{Orb}_G(x) = Gx = \{g \, . \, x : g \in G\}$$

and

$$X/G = \{Gx : x \in X\}.$$

Remark 1.5.4. Note that, since orbits are equivalence classes, the set of all orbits form a partition of X.

Exercise 44. Is $gX = \{g \, . \, x : x \in X\}$ interesting?

Example 1.5.5 — Consider again the action of C_4 on the set of puzzle pieces. There are 6 orbits, indicated by colour. Some orbits are small (like those of ✖ and ✦) while others are large (like those of ✖, ✖, and ✦). Note that the total number of puzzle pieces is the sum
$$1 + 4 + 4 + 2 + 4 + 1 = 16$$
because the orbits partition the set.

Remark 1.5.6. A *right group action* is just like a left group action except that the function goes from $X \times G$ to X and is denoted $(x, g) \mapsto x . g$. The difference stems from flipping the compatibility axiom into $(x \curvearrowleft g) \curvearrowleft h = x \curvearrowleft gh$—the action by gh on x is performed g and then h, as opposed to h and then g (as in function composition).

The other notations are flipped as well: we write $X \curvearrowleft G$ to mean G acts on X on the right ("right-acts"), and the orbit space of a right action is denoted $G\backslash X$.

Below we will introduce many types of group actions for future reference.

1.5.2   Concrete examples

Example 1.5.7 — For any X and G, we have the trivial action $g . x = x$ for all x in X, for each g in G. Every orbit is trivial.

Example 1.5.8 — The group μ_2 acts on any group G by inversion: for all x in G,

$$1 . x = x$$
$$-1 . x = x^{-1}$$

Since the identity and involutions are self-inverse, while other elements are not, the orbits are either pairs $\{x, x^{-1}\}$ where $x \neq x^{-1}$ or singletons $\{x\}$ where $x = x^{-1}$ (including $\{e\}$).

Example 1.5.9 — The group $\mathbb{Z}$ does **not** act on an arbitrary group G by $n . g = g^n$, because neither *identity* nor *compatibility* hold:

$$0 . g = g^0 = e \neq g \quad \text{in general, and}$$

$$(n + m) . g = g^{n+m} = g^n g^m \quad \text{whereas} \quad n . m . g = n . (g^m) = g^{mn}.$$

Example 1.5.10 — D_n acts on the n-gon (more precisely, parts of the n-gon) by flips and rotations *on the right*: we agreed that e.g. fr should be interpreted as first flip, then rotate.

Example 1.5.11 — Consider the equilateral triangle with colored vertices. Now we have its rotations
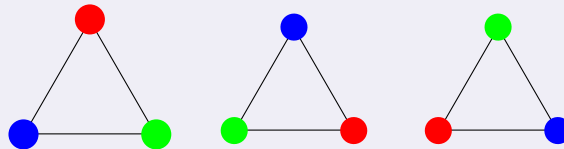
and reflections
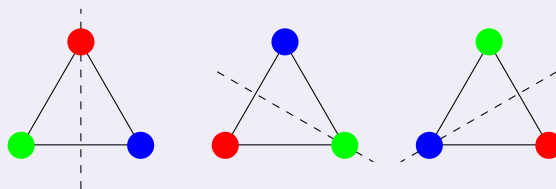
We may say that D_3 acts on the red, green, and blue vertices of the triangle, such that rotation by $120°$ clockwise sends the red vertex to the (original position of the) green vertex. We may also say that D_n acts on the (unlabelled) edges of the triangle. We may even say that D_n acts on the set of six possible configurations of the equilateral triangle.

The orbit of any vertex is the whole set of vertices; the same holds for any edge, *mutatis mutandis*.

Exercise 45. For $n \geq 4$ an n-gon has $\frac{1}{2}n(n-3)$ diagonals. How many orbits of those are there?

Example 1.5.12 — Given a fixed origin, $O_3(\mathbb{R})$ acts on objects in the three-dimensional space by rotations and reflections about that origin. $SO_3(\mathbb{R})$ acts on them by rotations only.

Exercise 46. Show that D_n is a subgroup of $O_2(\mathbb{R})$ using their geometric definitions.

Example 1.5.13 — $S_X \curvearrowright X$ for any set X in the obvious way: $\sigma . x = \sigma(x)$. In particular, S_n acts on $\{1, ..., n\}$.

Example 1.5.14 — The *affine group* $\mathrm{Aff}(\mathbb{R})$ of functions

$$x \mapsto ax + b \qquad (a \neq 0)$$

acts on $\mathbb{R}$ in the obvious way. There is only one orbit—for any two real numbers u and v, the affine map $x \mapsto x + v - u$ sends u to v.

Exercise 47. For which *pairs* of distinct points (u_1, u_2) and (v_1, v_2) does there exist an affine map sending u_i to v_i?

Example 1.5.15 — Assume for simplicity that we can identify musical notes with their fundamental frequencies.

On a standard modern 88-key piano,[*] the A above middle C sounds the frequency 440 Hz, and the ratio between the frequencies $f_0 < f_1$ of two successive keys (white–black, black–white, or white–white) is

$$\frac{f_1}{f_0} = \sqrt[12]{2} = 1.059...$$

Thus the frequencies of the 88 keys (starting four octaves below 440) ranges from 27.5 Hz to just over 4186 Hz.[†]

For reference, the human hearing range is commonly given as 20 Hz to 20000 Hz, which, in musical terms, ranges from a fifth below the bottommost piano-note to two octaves and a minor third above the topmost piano key.

A unifying feature of nearly all musical traditions is the observation that two frequencies sound "the same" when the ratio between them is an integer power of 2. This is called *octave equivalence*.[‡]

So, let
$$X = \{440 \cdot 2^{k/12} : k \in \mathbb{Z}\}$$

be the "idealized" Western musical scale, whose elements we'll refer to as *pitches*, and let $G = \langle 2 \rangle$ be the cyclic subgroup of $\mathbb{R}^\times$ generated by 2. Then $G \curvearrowright X$ by transposition by octaves, and the orbit space X/G has exactly twelve elements (called *pitch classes*):

$$A = \{\ldots, 220, 440, 880, \ldots\} \qquad D^\sharp = \{\ldots, 311, 622, 1244, \ldots\}$$
$$A^\sharp = \{\ldots, 233, 466, 932, \ldots\} \qquad E = \{\ldots, 329, 659, 1318, \ldots\}$$
$$B = \{\ldots, 246, 493, 987, \ldots\} \qquad F = \{\ldots, 349, 698, 1396, \ldots\}$$
$$C = \{\ldots, 261, 523, 1046, \ldots\} \qquad F^\sharp = \{\ldots, 369, 739, 1479, \ldots\}$$
$$C^\sharp = \{\ldots, 277, 554, 1108, \ldots\} \qquad G = \{\ldots, 391, 783, 1567, \ldots\}$$
$$D = \{\ldots, 293, 587, 1174, \ldots\} \qquad G^\sharp = \{\ldots, 415, 830, 1661, \ldots\}$$

---

[*] tuned to concert pitch in equal temperament
[†] $27.5 \cdot 2^{87/12} = 3520 \sqrt[4]{2} = 4186.009...$
[‡] Whether or not human perception of octave equivalence is innate or learned is still unclear, though Jacoby et al. (2019) found evidence for the latter by studying an isolated tribe living in the Bolivian Amazon.

Example 1.5.16 — They say you're supposed to "rotate your mattress" every so often to prevent it from sagging. Certain models can (and therefore must) also be "flipped". Together, these physical manoeuvres give an action of D_2 on the ideal mattress (only

theoretical).

Unfortunately, D_2 is not cyclic. That means you can't "cycle" the mattress through all possible configurations by repeating a single, easy-to-remember action. Consequently, mattress companies have devised complicated mattress-flipping schemes detailing when and how to flip your mattress for maximum performance.

1.5.3 Abstract examples

Example 1.5.17 — Every group G acts on itself by multiplication: $g \cdot x = gx$. There is only one orbit because for any two group elements x, y we can take $g = yx^{-1}$ and get $g \cdot x = y$.

Example 1.5.18 — Every group G acts on itself by *conjugation*—the act of operating on an object by an element on one side and its inverse on the other: $g \cdot x = gxg^{-1}$. The orbits are called *conjugacy classes* and their number is called the *class number* of G, denoted $k(G)$.

Remark 1.5.19. Both these actions have *right* versions: $G \curvearrowright G$ by $x \cdot g = xg$ and $x \cdot g = g^{-1}xg$.

1.5.4 New actions from old

A variety of new actions can be constructed from a given action $G \curvearrowright X$.

Example 1.5.20 (Restricted action) — A subset Y of X is called G-*invariant* if $g \cdot y \in Y$ for all y in Y and all g in G. If $Y \subseteq X$ is G-invariant, then G acts on Y the same way it acts on X.

Exercise 48. Show that orbits are G-invariant, and that every G-invariant subset is a union of (zero or more) orbits.

Example 1.5.21 (Subgroup action) — Let $H \leq G$. Then H acts on X the same way G does.

Example 1.5.22 (Function action) — Let Y be a set and let Y^X denote the collection of all functions $X \to Y$. Then G acts on Y^X on the right by $f \cdot g = (x \mapsto f(g \cdot x))$.

Exercise 49. Show that the function action is indeed an action—that it satisfies the *identity* and *compatibility* axioms.

Exercise 50 (Opposite action)**.** Let $x \cdot g = g^{-1} \cdot x$ for all x in X and all g in G. This turns the left action of G on X into an equivalent right action. In terms of the original (left) action, what is the orbit of x under the opposite (right) action? Show that the opposite of the opposite is the original.

1.6 Orders

1.6.1 Order of a group

With all the structures on G, we would like to *count* it.

Definition 1.6.1 — The *order* of a group G, denoted $o(G)$ or $|G|$, is the number of elements in G. If that number is infinite, we say the group has *infinite order*, and we write $o(G) = \infty$.

Example 1.6.2 — $o(\mathbb{Q}) = \infty$,

$o(\mathbb{Z}/n\mathbb{Z}) = o(\mu_n) = n$,

$o(S_n) = n!$, and

$o(D_n) = 2n$.

Theorem 1.6.3 (Lagrange)

Let G be a finite group and let $H \leq G$. Then $o(H)$ divides $o(G)$.

Proof. Define a *right* group action of H on G by

$$g \cdot h = gh.$$

We may check that this is indeed a group action—$g \cdot e = g$, and $(g \cdot h) \cdot h' = ghh' = g \cdot (hh')$.

Now consider the orbit of some $g \in G$. We claim now that $\text{Orb}_H(g) = \{gh : h \in H\}$, denoted gH. Why? Because:

Take any $g' \in gH$, we know that $g' = gh$ for some h, which immediately tells us $g \cdot h = g'$ and so $g' \in \text{Orb}_H(g)$. On the other hand, for any $g' \in \text{Orb}_H(g)$, we know there is some h such that $g \cdot h = gh = g'$. That is to say, $g' \in gH$.

We also claim that the orbits all have the *same size*. Indeed, given an orbit xH, consider the function $H \to xH$ defined by $h \mapsto xh$. This function is

- injective: if h_1 and h_2 map to the same place, then $xh_1 = xh_2$, so by left-cancellation, $h_1 = h_2$, and

- surjective: if $y \in xH$, then $y \in \mathrm{Orb}_H(x)$, so $y = xh$ for some h in H, so h maps to y.

Thus $h \mapsto xh$ is a bijection, so H and xH have the same size. In particular, every orbit has size $o(H)$.

Since orbits are equivalence classes, they partition G. All the orbits have the same size $o(H)$. Since G is *finite*, $o(G)$ is a multiple of $o(H)$ i.e. $o(H)$ divides $o(G)$. □

During the course of the proof, several very important concepts came up.

- the group action—H acting on G by right multiplication—is called the *right subgroup action of* H *on* G,

- the orbits—the sets of the form xH—are called *left cosets (of* H *(in* G*))*,

- the set of orbits—the set of left cosets of H in G—is denoted G/H, and

- the number of orbits—the size of the set G/H—is called the *index (of* H *(in* G*))*, denoted $[G : H]$.

Remark 1.6.4. Note that only in the end of the proof did we use finiteness of G. The rest of the proof of Lagrange's theorem shows that

$$o(G) = [G : H]o(H)$$

even if any these quantities is ∞. If G is finite, then

$$[G : H] = \frac{o(G)}{o(H)}.$$

Example 1.6.5 — Consider $G = \mathbb{Z}/24\mathbb{Z}$ and $H = \langle [4] \rangle$. The cosets of H, written additively since G is abelian, are

$$H = [0] + H = \{[0], [4], [8], [12], [16], [20]\},$$
$$[1] + H = \{[1], [5], [9], [13], [17], [21]\},$$
$$[2] + H = \{[2], [6], [10], [14], [18], [22]\}, \text{ and}$$
$$[3] + H = \{[3], [7], [11], [15], [19], [23]\}.$$

Clearly, the cosets partition $\mathbb{Z}/24\mathbb{Z}$. Each coset has 6 elements (the order of H) and there are 4 cosets in total (the index of H). And indeed, 6 times 4 is 24.

Exercise 51. Show that if a group G has a finite subgroup of finite index, then G is finite.

Exercise 52. Give an example of an infinite group with an infinite subgroup of infinite index.

Exercise 53. Show that $[\mathbb{Z} : \langle n \rangle] = n$ for each $n > 0$. What is $[\mathbb{Z} : \langle 0 \rangle]$?

Exercise 54. Let $G = \mathbb{Z}$ and let $H = \langle n \rangle$. In the notation from the proof of Lagrange's theorem, show that $a \sim b$ if and only if $a \equiv b \pmod{n}$. What does this prove about the sets $\mathbb{Z}/\langle n \rangle$ and $\mathbb{Z}/n\mathbb{Z}$?

Remark 1.6.6. Note that we often denote the subgroup $H = \langle n \rangle$ by $n\mathbb{Z}$, hence the $\mathbb{Z}/n\mathbb{Z}$ notation.

Remark 1.6.7. Note that in this case, our G/H is itself a group under $gH + g'H = (g + g')H$. This is not true in general—we will explore when G/H is a group in the future when we talk about *normal* subgroups.

Exercise 55. Let $G = S_3$ and $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle$. Can you put a group structure on G/H using the group operation from G?

1.6.2 Order of an element

Definition 1.6.8 — The *order* of an element g, denoted $o(g)$ or $|g|$, is the least positive integer exponent n such that $g^n = e$, or ∞ if no such exponent exists. In symbols,

$$o(g) = \min\{n \geq 1 : g^n = e\}.$$

Example 1.6.9 — The identity element is the only element of order 1. That is, $o(g) = 1$ iff $g = e$.

Example 1.6.10 — $o(g) = 2$ iff g is an involution and not the identity.

Example 1.6.11 — The orders of the elements of $\mathbb{Z}/12\mathbb{Z}$ are

$[a]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$	$[11]$
$o([a])$	1	12	6	4	3	12	2	12	3	4	6	12

> **Lemma 1.6.12** (Division)
> Let G be a group and let $g \in G$ be an element of finite order. Then $g^m = e$ if and only if $o(g) \mid m$.

Proof. Let $n = o(g)$. If $n \mid m$ then

$$g^m = (g^n)^{m/n} = e^{m/n} = e$$

by the exponent laws, since m/n is an integer.

Suppose $g^m = e$. Divide m by n with remainder to get $m = qn + r$ for some integers q and r satisfying $0 \le r < |n| = n$. By the exponent laws,

$$g^m = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

But by hypothesis, $g^m = e$. Thus $g^r = e$. Since n is the *least* positive integer annihilating g, and $r < n$, it must be the case that $r = 0$. Thus $m = qn$ i.e. $n = o(g) \mid m$. $\qquad\square$

> **Exercise 56.** Suppose g has *infinite* order. Show that $g^m = e$ iff $m = 0$.

> **Corollary 1.6.13**
> Let $n = o(g)$ be finite. Then $g^i = g^j$ iff $i \equiv j \pmod n$.

Proof. $g^i = g^j$ iff $g^{j-i} = e$ iff $n \mid j - i$ iff $i \equiv j \pmod n$. $\qquad\square$

The following fundamental Theorem connects the two meanings of the word "order".

> **Theorem 1.6.14**
> The order of an element is equal to the order of the cyclic subgroup it generates.

Proof. Suppose g has infinite order. Then there is no nonzero k such that $g^k = e$, and it follows that $\langle g \rangle$ is infinite.

So, suppose g has finite order n. We want to show two things: first, that

$$\langle g \rangle = \{e, g, g^2, ..., g^{n-1}\}$$

47

and second, that the set on the right-hand side actually has n elements.

First: The elements of $\langle g \rangle$ are, by definition, integer powers of g. Given g^k, let r be the remainder of k when it's divided by n. Then $k \equiv r \pmod{n}$ so, by the Corollary, $g^k = g^r$. Note that $0 \le r < n$, so *every* power of g equals something in this list.

Second: To show that this list has no repeats, suppose $g^i = g^j$ for some $0 \le i \le j < n$. Then $i \equiv j \pmod{n}$, again by the Corollary. But i and j are both less than n, so $i = j$.

Putting it all together, we conclude that the elements of $\langle g \rangle$ are just the n powers $e, g, g^2, \dots, g^{n-1}$. Therefore $o(\langle g \rangle) = n = o(g)$. $\qquad\square$

Exercise 57 (Corollary-Exercise)**.** Let G be a finite group. Show that $o(g)$ divides $o(G)$.

Exercise 58. Show that $\{n \in \mathbb{Z} : g^n = e\}$ is a subgroup of $\mathbb{Z}$ with index $o(\langle g \rangle)$.

Exercise 59. Let $\phi : G \to H$ be an isomorphism of groups. Show that $o(g) = o(\phi(g))$.

The relationship between $o(x)$, $o(y)$, and $o(xy)$ is complicated. One might hope that

$$o(xy) = o(x)o(y)$$

—but that's false in general. For example, $o(xx^{-1}) = 1$ regardless of what $o(x)$ is.

Example 1.6.15 —
$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

has order 4 (because $A^2 = -I$), and

$$B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

has order 3 (because $B^3 = I$), but

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

has infinite order.

Here's a very special case where we *can* say something.

> **Proposition 1.6.16**
> Let g be an element of finite order. Then
> $$o(g^k) = \frac{o(g)}{\gcd(o(g), k)}$$

Proof. Let $n = o(g)$, $m = o(g^k)$, and $d = \gcd(n, k)$.

On the one hand,
$$(g^k)^{n/d} = g^{kn/d} = g^{nk/d} = (g^n)^{k/d} = e,$$

so $m \mid \dfrac{n}{d}$ by the Division Lemma.

On the other hand,
$$g^{km} = (g^k)^m = e,$$

so $n \mid km$, again by the Division Lemma. But that means
$$\frac{n}{d} \mid \frac{km}{d} = \frac{k}{d}m.$$

Since $\dfrac{n}{d}$ and $\dfrac{k}{d}$ are coprime, by the magic of number theory, $\dfrac{n}{d} \mid m$. $\square$

> **Example 1.6.17** — [2] has order 10 in $U(11)$ because
> $$[2]^2 = [4], \ [2]^3 = [8], \ [2]^4 = [5], \ [2]^5 = [10], \ [2]^6 = [9],$$
> $$[2]^7 = [7], \ [2]^8 = [3], \ [2]^9 = [6], \ \text{and} \ [2]^{10} = [1].$$
>
> We can easily compute the order of any other element now. For example,
> $$o([5]) = o([2]^4) = \frac{10}{\gcd(10, 4)} = \frac{10}{2} = 5,$$
> $$o([7]) = o([2]^7) = \frac{10}{\gcd(10, 7)} = \frac{10}{1} = 10,$$
> and
> $$o([10]) = o([2]^5) = \frac{10}{\gcd(10, 5)} = \frac{10}{5} = 2.$$

> **Exercise 60.** Show that $o(g) = o(g^{-1})$ for all g in G.

Here's *another* very special case where we *can* say something.

> **Proposition 1.6.18**
>
> If x and y *commute* (that is, $xy = yx$) and have coprime orders, then $o(xy) = o(x)o(y)$.

Proof. Let $m = o(x)$ and $n = o(y)$. Since x and y commute,

$$(xy)^{mn} = x^{mn}y^{mn} = e.$$

Thus, by the Division lemma, $o(xy) \mid mn$.

To show that $o(xy) = nm$, let $k = o(xy)$. Then

$$e = (xy)^{mk} = x^{mk}y^{mk} = y^{mk}$$

because $(xy)^k = e$ and $x^m = e$. By the Division lemma, $n = o(y) \mid mk$. Since $\gcd(n, m) = 1$, we have $n \mid k$. By symmetry, $m \mid k$.

Now $m = o(x)$ and $n = o(y)$ both divide $k = o(xy)$. Since they're coprime, their product divides $o(xy)$ as well. Therefore $o(xy) = o(x)o(y)$. $\qquad\square$

Exercise 61. Show that $o(xy) = o(yx)$ regardless of whether x and y commute.

Chapter 2

Families of groups

2.1 Congruence groups

2.1.1 $\mathbb{Z}/n\mathbb{Z}$

As we've seen, the additive group of integers modulo n is cyclic:

$$\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle.$$

But $[1]$ is not the only generator! $[-1] = [n-1]$ also works, and in concrete cases we can find many others:

> **Example 2.1.1** — In $\mathbb{Z}/12\mathbb{Z}$ we have
>
> $$\langle [7] \rangle = \{[7], [2], [9], \ldots, [5], [0]\} = \mathbb{Z}/12\mathbb{Z}$$
>
> and
>
> $$\langle [8] \rangle = \{[8], [4], [0]\} \lneq \mathbb{Z}/12\mathbb{Z}$$
>
> so $[7]$ generates $\mathbb{Z}/12\mathbb{Z}$ while $[8]$ does not.

> **Exercise 62.** Can you guess, in general, how to tell whether $[a]$ generates $\mathbb{Z}/n\mathbb{Z}$?

> **Proposition 2.1.2**
> $[a]$ generates $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a, n) = 1$.

Remark 2.1.3. By the Lemma in the handout, $\gcd(a, n)$ is independent of the representative—if $[a] = [b]$, then $\gcd(a, n) = \gcd(b, n)$.

Proof. First of all, $[a]$ generates $\mathbb{Z}/n\mathbb{Z}$ iff $o([a]) = n$. [Why?] In particular, since $\mathbb{Z}/n\mathbb{Z} = \langle[1]\rangle$, we have $o([1]) = n$. Expressing $[a] = a[1]$ as a "power" of the generator, we can appeal to the order formula:

$$o([a]) = \frac{o([1])}{\gcd(o([1]), a)} = \frac{n}{\gcd(n, a)}.$$

It follows that $o([a]) = n$ iff $\gcd(n, a) = 1$. $\qquad\square$

> **Example 2.1.4** — The generators of $\mathbb{Z}/12\mathbb{Z}$ are $[1]$, $[5]$, $[7]$, and $[11]$. The other classes('s representatives) are divisible by 2 or 3.

The number of generators of $\mathbb{Z}/n\mathbb{Z}$ is therefore $\varphi(n)$, as defined in the GCD and φ handout.

2.1.2 $U(n)$

Aside from cyclic groups (like the additive groups $\mathbb{Z}/n\mathbb{Z}$) the most important finite abelian groups are the multiplicative groups $U(n)$. In some sense, studying these particular groups tells you everything you need to know about finite abelian groups.

Recall that $U(n)$ a.k.a. $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is the set of invertible residue classes modulo n. As promised, we're going to explain

1. how to tell if a given class is invertible, and

2. how to find the inverse of an invertible class.

> **Definition 2.1.5** — Fix an integer n. A residue class $[a]$ is *invertible* if there exists $[b]$ such that $[a][b] = [1]$.

The inverse of $[a]$ is unique if it exists, and we denote it $[a]^{-1}$.

> **Example 2.1.6** — In $\mathbb{Z}/16\mathbb{Z}$, $[5]$ and $[11]$ are invertible because $[5][13] = [65] = [1]$ and $[11][3] = [33] = [1]$. We have $[5]^{-1} = [13]$ and $[11]^{-1} = [3]$.

How do we tell apart invertible and non-invertible classes? Let's start with a simple criterion for the latter.

> **Lemma 2.1.7**
>
> If $[a][b] = [0]$ but $[a], [b] \neq [0]$, then neither $[a]$ nor $[b]$ is invertible modulo n.

Proof. Suppose $[b]$ had an inverse, say $[c]$. Then $[b][c] = [1]$. But $[a][b] = [0]$ by hypothesis. Since multiplication is associative,

$$[a][b][c] = [a] \quad \text{and} \quad [a][b][c] = [0],$$

contradicting the assumption that $[a]$ was nonzero. $\qquad\square$

> **Example 2.1.8** — Continuing in $\mathbb{Z}/16\mathbb{Z}$, neither $[4]$ nor $[8]$ are invertible because $[4][8] = [32] = [0]$.

As you may have guessed from the last two examples, coprimality with n has something to do with invertibility.

> **Lemma 2.1.9**
>
> If $\gcd(a, n) > 1$ then $[a]$ is not invertible modulo n.

Proof. Let d be a nontrivial common divisor of a and n. Then the integer $b = n/d$ is *not* divisible by n. However, $ab = an/d$ *is* divisible by n, because the quotient ab/n is the integer a/d. Thus,

$$[a][b] = [ab] = [0]$$

so $[a]$ is not invertible. $\qquad\square$

> **Theorem 2.1.10**
>
> If $\gcd(a, n) = 1$ then $[a]$ is invertible modulo n.

Proof. Consider the multiplication-by-$[a]$ map,

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$[x] \mapsto [a][x].$$

If $[a][x] = [a][y]$, then n divides $ax - ay = a(x - y)$. But since n and a are coprime, that means n divides $x - y$, and so $[x] = [y]$. Thus f is injective.

But! An injection from a finite set to itself must be bijective (by the pigeonhole principle). In particular, $[1]$ is in the image of f. In other words, there exists some $[b]$ in $\mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = [1]$. That means $[a]$ is invertible! $\qquad\square$

This fulfills our first promise—$[a]$ is invertible iff $\gcd(a, n) = 1$.

For the second promise—we need a second proof!

Second proof of the Theorem. Since a and n are coprime, by "Bézout's Euclidean algorithm," there exist integers s and t such that

$$as + nt = 1.$$

Reducing this equation modulo n, we obtain

$$as \equiv 1 \pmod{n}$$

or, what is equivalent,

$$[a][s] = [1].$$

That means $[a]$ is invertible! $\qquad\square$

Example 2.1.11 — Let's compute the inverse of $[123]$ modulo 1024, if it exists. First, we run the Euclidean algorithm to compute $\gcd(1024, 123)$.

$$1024 = 8 \cdot 123 + 40$$
$$123 = 3 \cdot 40 + 3$$
$$40 = 13 \cdot 3 + 1$$

Thus $\gcd(1024, 123) = 1$, so $[123]$ is invertible modulo 1024. To find its inverse, we work backwards:

$$1 = 40 - 13 \cdot 3$$
$$= 40 - 13 \cdot (123 - 3 \cdot 40) = 40 \cdot 40 - 13 \cdot 123$$
$$= 40 \cdot (1024 - 8 \cdot 123) - 13 \cdot 123 = 40 \cdot 1024 - 333 \cdot 123$$

Thus $40 \cdot 1024 - 333 \cdot 123 = 1$, so $[-333][123] = [1]$, meaning that $[123]^{-1} = [-333] = [691]$.

With these theorems in hand, it's now clear that the order of the multiplicative group of integers modulo n is the totient of n:

$$o(U(n)) = \varphi(n).$$

(Yes, so few symbols mean so many words!)

Example 2.1.12 —
$$U(7) = \{[1], [2], [3], [4], [5], [6]\}$$

and

$$U(12) = \{[1], [5], [7], [11]\}.$$

More generally, for p prime,

$$U(p) = \{[1], \ldots, [p-1]\}.$$

Remark 2.1.13. This result tells us that $\mathbb{Z}/p\mathbb{Z}$ is actually a field!

We are also in a position to derive a fundamental result in number theory, concerning the multiplicative orders of invertible residue classes.

Theorem 2.1.14 (Euler–Fermat)

If a and n are coprime, then
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. By Exercise 57, $a^{o(G)} = e$ in any group G. Thus $[a]^{\varphi(n)} = [1]$ in $U(n)$. □

Remark 2.1.15. Compare this proof with the very long proofs you may have seen in MAT246 or MAT315!

2.2 Cyclic groups

2.2.1 Definitions

Recall that a *cyclic group* is a group in which every element is an integer power* of a single element, called a *generator*. We write

$$G = \langle g \rangle$$

to mean G is cyclic with generator g.

Example 2.2.1 —

The trivial group is cyclic.

$\mathbb{Z} = \langle 1 \rangle$ is infinite cyclic.

$\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$ is finite cyclic of order n.

$\mu_n = \langle e^{2\pi i/n} \rangle$ is also finite cyclic of order n.

Let G be any group and let $h \in G$. Then $H = \langle h \rangle$ is a cyclic subgroup of G of order $o(g)$.

$\langle 2 \rangle \leq \mathbb{Q}^\times$ is the subgroup of powers of 2:

$$\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots$$

---

*multiple in additive notation

$\langle 1 + \sqrt{2} \rangle \leq \mathbb{R}^{\times}$ is the subgroup of powers of $1 + \sqrt{2}$:

$$\ldots, \; 3 - 2\sqrt{2}, \; -1 + \sqrt{2}, \; 1, \; 1 + \sqrt{2}, \; 3 + 2\sqrt{2}, \; \ldots$$

Exercise 63. Prove that every integer power of $1 + \sqrt{2}$ has the form $a + b\sqrt{2}$ for some integers a and b.

In certain contexts, the generator of a cyclic group has a special name.

Definition 2.2.2 — A generator for μ_n is called *primitive nth root of unity*, while a (representative of a) generator for $U(n)$ is called a *primitive root modulo n*.

Example 2.2.3 — Consider some "small" groups of roots of unity. In particular, let $\zeta = e^{(2\pi i)/8} = \frac{1}{\sqrt{2}}(1 + i)$ and $\xi = e^{(2\pi i)/12} = \frac{1}{2}(\sqrt{3} + i)$. Then

$$\mu_8 = \langle \zeta \rangle = \{1, \, \zeta, \, \zeta^2, \, \zeta^3, \, \zeta^4, \, \zeta^5, \, \zeta^6, \, \zeta^7\}$$
$$= \{1, \, \zeta, \, i, \, \zeta^3, \, -1, \, \zeta^5, \, -i, \, \zeta^7\}$$

and

$$\mu_{12} = \langle \xi \rangle = \{1, \, \xi, \, \xi^2, \, \xi^3, \, \xi^4, \, \xi^5, \, \xi^6, \, \xi^7, \, \xi^8, \, \xi^9, \, \xi^{10}, \, \xi^{11}\}$$
$$= \{1, \, \xi, \, \xi^2, \, i, \, \xi^4, \, \xi^5, \, -1, \, \xi^7, \, \xi^8, \, -i, \, \xi^{10}, \, \xi^{11}\}$$
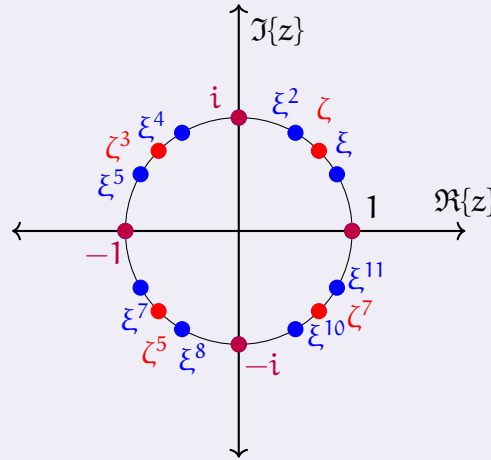
The only nontrivial proper subgroups of μ_8 are $\mu_4 = \{1, i, -1, -i\}$ and *its* subgroup $\mu_2 = \{1, -1\}$. On the other hand, μ_{12} has several additional subgroups aside from these, like $\mu_3 = \{1, \xi^4, \xi^8\}$ and $\mu_6 = \{1, \xi^2, \xi^4, \xi^6, \xi^8, \xi^{10}\}$. However,

$$\mu_8 \not\leq \mu_{12}.$$

Observe that *all* these subgroups are cyclic.

Exercise 64. Show that a complex number ζ can be a primitive nth root of unity for at most *one* positive integer n. What is n in terms of ζ?

Here's the most basic criterion for determining whether a finite group is cyclic.

Proposition 2.2.4

A finite group of order n is cyclic iff it has an element of order n.

Proof. Exercise. □

Exercise 65. In the Proposition, why is it necessary that the group be finite?

Example 2.2.5 (A non-cyclic group) — $U(8) = \{[1], [3], [5], [7]\}$ is not cyclic, as every element squares to the identity.

Example 2.2.6 (Another non-cyclic group) — The dihedral group D_n has order $2n$, but no element has such large order, because rotations have order at most n, and flips are involutions. Thus D_n is not cyclic.

Example 2.2.7 (Yet another non-cyclic group) — Fix $n > 1$. Let G be the set of subsets of $\{1, \ldots, n\}$ under the $\triangle$ operation. In Homework 1, you proved G is a group. Today, we prove G is not cyclic. We have

$$A^2 = A \triangle A = (A \setminus A) \cup (A \setminus A) = \varnothing \cup \varnothing = \varnothing$$

for all A in G, so no element has order 2^n.

There is always at least *one* group of any given finite order n, namely C_n, the cyclic group of order n. We say "the", because...

Proposition 2.2.8

Any two cyclic groups of the same order are isomorphic.

Proof. Let $G = \langle g \rangle$ and $H = \langle h \rangle$ be cyclic groups of order n and define $f : G \to H$ by $f(g^i) = h^i$.

Before we can say anything about f, we have to check that it's actually well-defined—that the proposed value on an element is independent of the exponent. So, if $g^i = g^j$ then $i \equiv j$ $(\bmod\ n)$, so $j = i + mn$. Thus

$$h^j = h^{i+mn} = h^i(h^n)^m = h^i$$

because $o(h) = n$. Thus f is well-defined.

Now, f preserves group structure by the exponent laws:

$$f(g^i g^j) = f(g^{i+j}) = h^{i+j} = h^i h^j = f(g^i)f(g^j).$$

Moreover, f is injective because if $f(g^i) = f(g^j)$ then $h^i = h^j$, so $n \mid i - j$; but $o(h) = o(g)$, so $g^{i-j} = e$. Since G and H have the same size, f is bijective, hence an isomorphism. Thus $G \cong H$. $\qquad\square$

> **Exercise 66.** Show that any two infinite cyclic groups are isomorphic.

2.2.2 Fundamental Theorem of Cyclic Groups

What do subgroups of cyclic groups look like? If $G = \langle g \rangle$ then certainly, for each integer k, the cyclic subgroup generated by g^k is a subgroup of G, i.e. $\langle g^k \rangle \leq G$.

You'd be hard-pressed to find a subgroup that *isn't* cyclic, because...

<p style="text-align:center">Every subgroup of a cyclic group is cyclic.</p>

> **Lemma 2.2.9**
>
> Let $G = \langle g \rangle$ be a cyclic group and let $H \leq G$ have finite index k. Then $H = \langle g^k \rangle$.

Proof. First, we prove there exists *some* positive integer d such that $g^d \in H$.

- If H is trivial, then G must be finite, so we may take $d = o(G)$.

- If H is nontrivial, then H contains some nonidentity element g^m (as every element of G looks like this), so we may take $d = |m|$.

Next, let d be the *least* positive integer such that $g^d \in H$. We claim $g^m \in H$ iff $d \mid m$ (cf. Division Lemma).

($\Leftarrow$) If $d \mid m$, then $g^m = (g^d)^{m/d} \in H$ because $g^d \in H$.

($\Rightarrow$) If $g^m \in H$, then $m = qd + r$ for some $0 \leq r < d$, and $g^r = g^m(g^d)^{-q} \in H$. Since d was least, we get $r = 0$, so $d \mid m$.

It follows immediately that $H = \langle g^d \rangle$.

Finally, we prove that $d = k$. Since k is the index and G may be infinite, we use cosets. The cosets of

$$H = \{\ldots, g^{-d}, e, g^d, g^{2d}, g^{3d}, \ldots\}$$

are just

$$g^r H = \{\ldots, g^{r-d}, g^r, g^{r+d}, g^{r+2d}, g^{r+3d}, \ldots\}$$

for $0 \le r < d$. Since $g^r H \ne g^s H$ for $r \ne s$ in this range (lest g^{r-s} be in H and d divide $r - s$) there are exactly d cosets. $\qquad\square$

Exercise 67. Exactly one situation is not covered by the Lemma. What is it?

To complete this remaining case, we consider a digression back into indices.

Exercise 68. Let G be a group and K, H be subgroups of G satisfying $K \le H \le G$. Prove that

$$[G : K] = [G : H][H : K].$$

Corollary 2.2.10

Let $G = \langle g \rangle$ be cyclic. If H_1 and H_2 have the same index in G, then $H_1 = H_2$.

Proof. Let $k = [G : H_1] = [G : H_2]$. If $k < \infty$, we are done.

If $k = \infty$, suppose $g^n \in H_1$ for $n \ne 0$. Then $\langle g^n \rangle \le H_1$ and so $[G : H_1] \le [G : \langle g^n \rangle] = n$. We must have instead $H_1 = \{e\}$. Similarly, $H_2 = \{e\}$. $\qquad\square$

Remark 2.2.11. Note that this accounts for when the index is ∞.

Example 2.2.12 — Suppose $G = \langle g \rangle$ has order n. For each $d \mid n$, the subgroup $\langle g^d \rangle$ has order n/d and index d, because

$$o(\langle g^d \rangle) = o(g^d) = \frac{n}{\gcd(n, d)} = \frac{n}{d}$$

and

$$[G : \langle g^d \rangle] = \frac{o(G)}{o(\langle g^d \rangle)} = \frac{n}{n/d} = d.$$

Example 2.2.13 — Suppose $G = \langle g \rangle$ has order ∞. For each $d \ne 0$, the subgroup $\langle g^d \rangle$ has order ∞ and index d. What about $d = 0$?

The Lemma, its Corollary, and the two Examples show that a cyclic group has exactly one subgroup of every possible index.* What's interesting is that the *converse* is true (at least in the finite case). In fact:

Theorem 2.2.14

Let G be a finite group. If G has at most one subgroup of each index (equivalently, order), then G is cyclic.

We will leave the proof for later. In the meantime, let's see an application of the FToCG.

Example 2.2.15 — Recall Bézout's theorem: if $\gcd(a, b) = d$ then there exist integers s and t such that
$$as + bt = d.$$

We proved Bézout's theorem by way of the Extended Euclidean algorithm. Using the fact that every subgroup of $\mathbb{Z}$ is cyclic, we can give another proof of Bézout's theorem.

Consider $\langle a, b \rangle$ which is the subgroup of $\mathbb{Z}$ generated by a and b; its elements are integer combinations of a and b.

Since $\mathbb{Z} = \langle 1 \rangle$ is cyclic, its subgroup $\langle a, b \rangle$ must be cyclic as well, so

$$\langle a, b \rangle = \langle d \rangle$$

for some integer d (a "power" of the generator 1). Since $\langle d \rangle = \langle -d \rangle$, we may take d to be positive.

Now, since $a, b \in \langle d \rangle$ we have $d \mid a$ and $d \mid b$. To prove that $d = \gcd(a, b)$ we use the other inclusion: $d \in \langle a, b \rangle$ so there exist integers n and m such that $d = an + bm$. Then if $c \mid a$ and $c \mid b$ then $c \mid an + bm$. In (other) words, if c divides a and b then c divides every integer combination of a and b. In particular, every common divisor of a and b divides d. Since d divides a and b, d is the greatest common divisor of a and b.

Exercise 69. What happens in the most degenerate case $a = b = 0$?

2.2.3 Cyclicity of *U(n)*

Theorem 2.2.16

$U(n)$ is cyclic iff $n = 2, 4, p^k$, or $2p^k$ for some odd prime p and positive integer k.

---

*Gallian calls this result the *Fundamental Theorem of Cyclic Groups*, but he only proves it for finite cyclic groups, and states it in terms of orders instead of indices.

Remark 2.2.17. We will prove only the "if" direction, leaving the "only if" for PS3.

Proof. $U(2)$ is the trivial group, which is cyclic; and $U(4) = \{[1], [3]\} = \langle [3] \rangle$ is cyclic, too.

Let p be an odd prime. We will postpone the cyclicity of $U(p)$ to a homework problem. For now, let's assume this fact.

Next up, let $k > 1$. To show $U(p^k)$ is cyclic, we will take the product of two elements of orders p^{k-1} and $p - 1$ to obtain an element of order $p^{k-1}(p - 1) = o(U(p^k))$.

The first element is $[p + 1]$. Observe that, for any $n \geq 1$, the binomial theorem says

$$(p + 1)^n = p^n + \binom{n}{1} p^{n-1} + \binom{n}{2} p^{n-2} \cdots + \binom{n}{n-1} p + 1 \tag{*}$$

where

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} = \frac{n(n-1)(n-2)\ldots(n-i+1)}{i(i-1)(i-2)\ldots 1}.$$

Choosing $n = p^{k-1}$, we see that each term in (*)—except the last one—is divisible by p^k [because $\binom{p^m}{i} = \frac{p^m}{i}\binom{p^m-1}{i-1}$.] Thus

$$[p + 1]^{p^{k-1}} = [1] \text{ in } U(p^k)$$

so $o([p + 1]) \mid p^{k-1}$.

On the other hand, choosing $n = p^{k-2}$ in (*), every term—except the last *two*—is divisible by p^k. Thus

$$[p + 1]^{p^{k-2}} = [p^{k-1} + 1] \neq [1] \text{ in } U(p^k)$$

so $o([p + 1]) > p^{k-2}$. Therefore $o([p + 1]) = p^{k-1}$. [If $p = 2$, then the last *three* terms remain, and we cannot make this conclusion; that is why we require p to be odd.]

The second element is obtained in a different manner. Let g be a primitive root modulo p [This is where we assume the cyclicity of $U(p)$.] and let m be the order of $[g]$ in $U(p^k)$. Then

$$g^m \equiv 1 \pmod{p}$$

because $p \mid p^k$, so $p - 1$ divides m. If we let $h \equiv g^{\frac{m}{p-1}} \pmod{p^k}$, it follows from the order formula that $[h]$ has order $p - 1$ in $U(p^k)$.

Putting these together, we deduce that $U(p^k)$ is generated by $[p + 1][h]$.

Finally, for $U(2p^k)$, let g be an *odd* primitive root modulo p^k. [This is possible precisely because p is odd—the class of g modulo p^k therefore contains representatives of both parities.] We claim $U(2p^k) = \langle [g] \rangle$. Indeed, $\gcd(g, 2p^k) = 1$ because $\gcd(g, p^k) = 1$ and $\gcd(g, 2) = 1$, so $[g]$ is invertible. Note that the elements of $\langle [g] \rangle$ are distinct modulo $2p^k$ because the same is true modulo p^k. Since $\varphi(2p^k) = \varphi(p^k)$, we have $\langle [g] \rangle = U(2p^k)$. $\square$

Exercise 70. Show that $U(2^k)$ is not cyclic for $k \geq 3$ by exhibiting "too many" subgroups of order 2.

2.3 Dihedral groups

2.3.1 Definitions

Definition 2.3.1 — A group is called *dihedral* if it's generated by a pair of nontrivial (identity) involutions.

Compare this with the definition of cyclic: generated by a single element.

When we introduced dihedral groups way back, we said they were symmetries of n-gons under composition. Well, those groups actually *are* dihedral in this new sense!

To see why, let r be the one-nth clockwise rotation, and let f be the flip over the vertical axis. Then fr is an involution, because, geometrically, fr is a flip (over the axis through the bottommost left-side vertex, to be precise). Moreover, f and fr generate every other symmetry, because $f(fr) = r$ is the minimal rotation. And as we saw previously, a flip and a minimal rotation are all you need to express *every* possible flip and rotation.
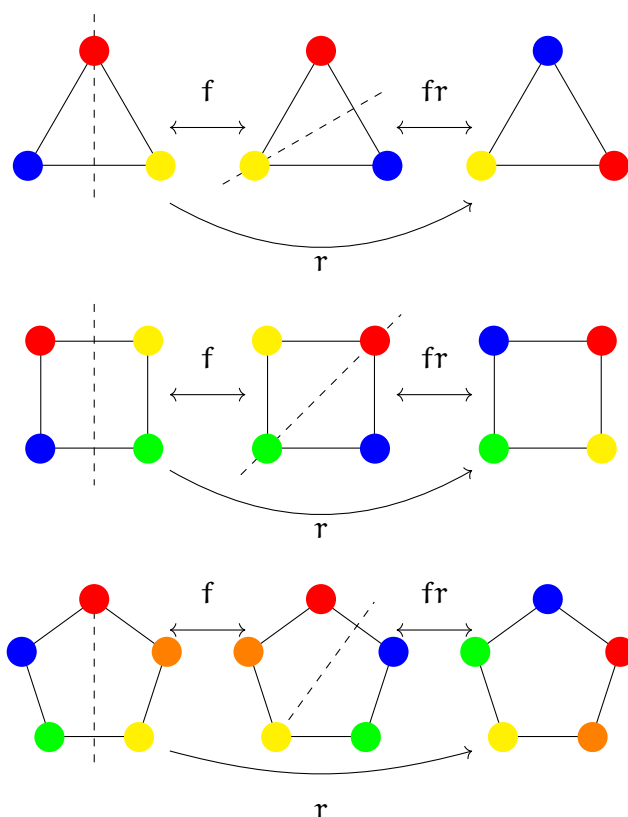
Exercise 71. Is the trivial group dihedral?

Equivalent definition

While the "two-involutions" definition is very useful theoretically, the "geometric" definition is very useful in practice. The following Proposition describes how to canonically switch back and forth between these two perspectives.

> **Proposition 2.3.2**
>
> Let G be a dihedral group with generating involutions a and b. Then G is generated by the *flip* $f = a$ and the *rotation* $r = fb$, which are distinct and satisfy $frf = r^{-1}$.
>
> Conversely, if a group G is generated by two distinct elements f and r such that $o(f) = 2$ and $frf = r^{-1}$, then G is dihedral with generating involutions f and fr.
>
> Moreover, passing from one description the another and back again leaves us where we started.

Proof. We just showed the backward direction. For the forward, we have to show that if $f = a$ and $r = ab$ then $G = \langle f, r \rangle$ and $f \neq r$ and $frf = r^{-1}$.

Plainly,
$$\langle a, ab \rangle \leq \langle a, b \rangle;$$
and since $a(ab) = b$, we have $b \in \langle a, ab \rangle$, so
$$\langle a, b \rangle \leq \langle a, ab \rangle.$$

Thus $\langle a, b \rangle = \langle a, ab \rangle$ i.e. $G = \langle f, r \rangle$.

Next, $f = r$ iff $a = ab$ iff $b = e$, but b must have order 2. So $f \neq r$.

Finally, we show that $frf = r^{-1}$. By our definitions of f and r, we have
$$frf = a(ab)a = a^2ba = ba.$$

On the other hand, since a and b are self-inverse,
$$r^{-1} = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Thus $frf = r^{-1}$.

To show that these descriptions are equivalent, just note that
$$(a, b) \longrightarrow (a, ab) \longrightarrow (a, aab) = (a, b)$$
and
$$(f, r) \longrightarrow (f, fr) \longrightarrow (f, ffr) = (f, r). \qquad \square$$

The identity
$$frf = r^{-1}$$
is called the *fundamental relation between flip and rotation*.
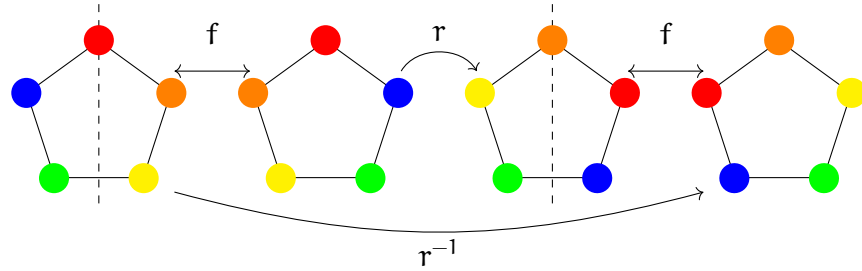
Since f is self-inverse, we can rewrite this identity as
$$rf = fr^{-1}.$$

It follows that
$$r^k f = fr^{-k}$$

for all integers k. This enables us to simplify long strings of r's and f's—we can move any rotation past f, at the cost of inverting it.

Exercise 72. Which of the following are trivial for any D_n?

a) `frffrf`

b) `rffrfrrfr`

c) `rrrrrfr`

d) `rfrrfr`

e) `frfrfrfrf`

2.3.2 Order of a dihedral group

Let $G = \langle r, f \rangle$ be a dihedral group with flip f and rotation r. Then the order of f is 2, but the order of r could be anything!

Theorem 2.3.3

If $o(r)$ is finite, then $o(G) = 2o(r)$.

Proof. Let $n = o(r)$. The fundamental relation between flip and rotation allows us to write every element of G as either r^k (a rotation) or fr^k (a flip) for some integer k. Thus

$$G = \{e, r, r^2, \ldots, r^{n-1}, f, fr, fr^2, \ldots, fr^{n-1}\}$$

which means $o(G) \leq 2n$. (We don't know if these are all distinct—the list could contain repeats.)

For i, j between 0 and $n - 1$, we have

$$fr^i = fr^j \iff r^i = r^j \iff i \equiv j \pmod{n}$$

which can only happen if $i = j$ (since $0 \leq i, j < n$). Thus, in our list above, the flips are distinct from each other, and the rotations are distinct from each other.

Yet are flips and rotations distinct from each other? We know that $f \neq r$, but what about fr^i and r^j? We have

$$fr^i = r^j \iff f = r^{j-i} \iff f \in \langle r \rangle.$$

So to prove that $fr^i \neq r^j$, we just have to show that $f \notin \langle r \rangle$.

Suppose to the contrary that $f \in \langle r \rangle$. Then f commutes with r, so $rf = fr$. But, by the fundamental relation, $rf = fr^{-1}$. Together, these imply $r = r^{-1}$, so $r^2 = e$. Thus r has order 1 or 2. Since $f \in \langle r \rangle$ has order 2, r must have order 2. However, the 2-element cyclic group $\langle r \rangle$ can only have *one* element of order 2. Therefore $f = r$, a contradiction. $\square$

We use the notation D_n to denote the dihedral group with a rotation of order n. By the theorem, $o(D_n) = 2n$.

> **Example 2.3.4 —** The symmetry group of an equilateral triangle has 6 elements.

Just like with cyclic groups, we also speak of D_n as *the* dihedral group of order $2n$, because there is only ever one such group:

> **Proposition 2.3.5**
> Any two dihedral groups of the same order are isomorphic.

Proof. Omitted (straightforward, but tedious). $\square$

Not-really-dihedral groups

While it's difficult to draw regular n-gons for $n = 1$ and 2, that hasn't stopped ~~crazy mathematicians~~ group theorists from talking about their symmetry groups, D_1 and D_2.

> **Exercise 73.** What are D_1 and D_2? [Use the theorem.]

> **Proposition 2.3.6**
> D_n is abelian iff $n = 1$ or 2.

Proof. If D_n is abelian, then r and f commute; conversely, if r and f commute, then so does every pair of elements in the group they generate.

As we saw at the end of the proof of Theorem 2.3.3, $fr = rf$ is equivalent to $r^2 = e$, which is equivalent to $n = 1$ or 2. $\square$

These two "smallest" dihedral groups are so boring and so unlike their non-abelian bigger siblings that for the rest of this class we will assume $n \geq 3$.

2.3.3 Subgroups of dihedral groups

Last lecture, we proved that cyclicity is a hereditary property: subgroups of cyclic groups are cyclic. The analogous assertion for dihedral groups is:

> Subgroups of dihedral groups are dihedral—or cyclic.

(Doesn't sound as nice, does it?)

> **Theorem 2.3.7**
>
> Let G be a dihedral group and let $H \leq G$. Then H is either
>
> c) cyclic: $\langle r^k \rangle$ where $k = \frac{1}{2}[G : H]$, or
>
> d) dihedral: $\langle r^k, fr^i \rangle$ where $k = [G : H]$ and $0 \leq i < k$.

We will explore the proof of this (at least in the finite dihedral case) in Problem Set 3.

> **Example 2.3.8 —** The subgroup of all rotations in D_n is $\langle r \rangle$. Its order is n, so its index is 2. Subgroups of the rotation subgroup are cyclic subgroups of the whole group.

> **Example 2.3.9 —** Consider D_8. By inscribing a square in an octagon* we can give an example of a dihedral subgroup of D_8. If r is the one-eighth turn, then r^2 is a quarter turn. We have $fr^2f = r^{-2} = (r^2)^{-1}$, so the subgroup $\langle r^2, f \rangle$ is dihedral. Writing out its elements,
> $$\langle r^2, f \rangle = \{e, r^2, r^4, r^6, f, fr^2, fr^4, fr^6\}.$$
> Its index is 2.
>
> ---
> *or an octagon in a square!

> **Exercise 74.** How many distinct subgroups does D_n have?

2.3.4 The center of a group

When G is abelian, all its elements commute with each other, and life is easy.

What about when G is not abelian? Do we still have any such nice elements?

The groups D_n for $n \geq 3$ are the first non-abelian groups that we're studying systematically.

One way to measure the "non-abelianness" of a group is to ask which elements commute with everything. Such elements are called *central* and their union is called the *center*.

> **Definition 2.3.10** — Let G be a group. The *center* of G is the set
> $$Z(G) = \{g \in G : gh = hg \text{ for all } h \text{ in } G\}.$$

> **Exercise 75.** Show that $Z(G) \leq G$, with equality if and only if G is abelian.

> **Example 2.3.11** ($Z(D_n)$) — Let r^i be a rotation. Since rotations commute with rotations, let fr^j be a flip. Then
> $$(r^i)(fr^j) = fr^{j-i}$$
> whereas
> $$(fr^j)(r^i) = fr^{j+i}.$$
> These are equal if and only if $r^{-i} = r^i$, i.e. r^i is an involution. Geometrically, the only involutive rotation is the 180-degree turn, possibly only when n is even. Algebraically, $r^{-i} = r^i$ implies $i \equiv -i \pmod{n}$, and if $n \mid 2i$ then n must be even and i must be $n/2$. Either way, $r^{n/2}$ is the only rotation that commutes with a flip. In particular, no flip commutes with r when $n > 2$, so we conclude
> $$Z(D_n) = \begin{cases} \langle e \rangle & \text{if } n \text{ is odd} \\ \langle r^{n/2} \rangle & \text{if } n \text{ is even.} \end{cases}$$

When a group's center is trivial—like D_n's is when n is odd—we say the group is *centerless*.

> **Example 2.3.12** ($Z(GL_2(\mathbb{R}))$) — Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL_2(\mathbb{R}))$. Since A commutes with *every* invertible matrix, A must commute with the particular matrix $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

(which is invertible). We have

$$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$$

and

$$BA = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

so if $AB = BA$ then $a = d$ and $b = c$.

Next, consider the non-invertible matrix $N = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. We have

$$AN = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}$$

and

$$NA = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}.$$

As we mentioned, N is not invertible so it is not an element of $GL_2(\mathbb{R})$—but $I + N = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ is! If $A(I + N) = (I + N)A$ then $AI + AN = IA + NA$. Since $AI = IA$, we have $AN = NA$. Therefore $b = c = 0$.

Putting these together, we conclude that an invertible matrix A that commutes with every other invertible matrix must be of the form

$$A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = aI$$

with $a \neq 0$. After verifying that these so-called "scalar matrices" *do* commute with everything else, we conclude that $Z(GL_2(\mathbb{R})) = \{aI : a \neq 0\}$.

Exercise 76. Generalize this example to GL_n.

2.3.5   Generators and relations

The dihedral group D_n is generated by an involution f and another element r of order n, satisfying the fundamental relation $frf = r^{-1}$.

A convenient way to encode this information about D_n is to write down its *presentation*:

$$D_n = \langle r, f \mid r^n = e, \; f^2 = e, \; frf = r^{-1} \rangle.$$

In general, a presentation of a group G takes the form

$$G = \langle S \mid R \rangle$$

where S is a set of generators for G and R is a list of *relations* they satisfy.*

Implicit in every presentation is the assumption that the relations are "complete" in the sense that the generators satisfy *no other relations* except for those that you can prove from R. Thus, when we write D_n using the presentation above, the relations $r^n = e$ and $f^2 = e$ encode that $o(r) = n$ and $o(f) = 2$. Moreover, it can be shown that you *cannot derive* the identity $f = r$ using only the relations $f^2 = e$, $r^n = e$, $frf = r^{-1}$.

> **Exercise 77.** Suppose G is generated by the involutions a and b. Write down a presentation for G.

> **Exercise 78.** Suppose $G = \langle g \rangle$ is cyclic of order n. Write down a presentation for G.

2.3.6   Infinite dihedral group

You might be tempted to wonder what happens if we let $n = \infty$ in the presentation of D_n,

$$D_n = \langle r, f \mid r^n = e, \; f^2 = e, \; frf = r^{-1} \rangle.$$

Well, it doesn't quite make sense to say "$r^\infty = e$". But it *does* make sense to say $o(r) = \infty$, which means r satisfies *no* nontrivial relation of the form $r^n = e$. The other relations—$f^2 = e$ and $frf = r^{-1}$—have no dependence on n, so they remain. It seems reasonable, therefore, to define the *infinite dihedral group* as

$$D_\infty = \langle r, f \mid f^2 = e, \; frf = r^{-1} \rangle.$$

To justify the name, we prove:

> **Proposition 2.3.13**
>
> The group D_∞ is a dihedral group of infinite order.

Proof. D_∞ is generated by the involutions f and fr. $\square$

---

*In this context, a *relation* is an equality between two expressions formed using products of elements of S and their inverses.

To interpret D_∞ geometrically, consider this sequence of nested n-gons, depicted here for $3 \le n \le 12$:
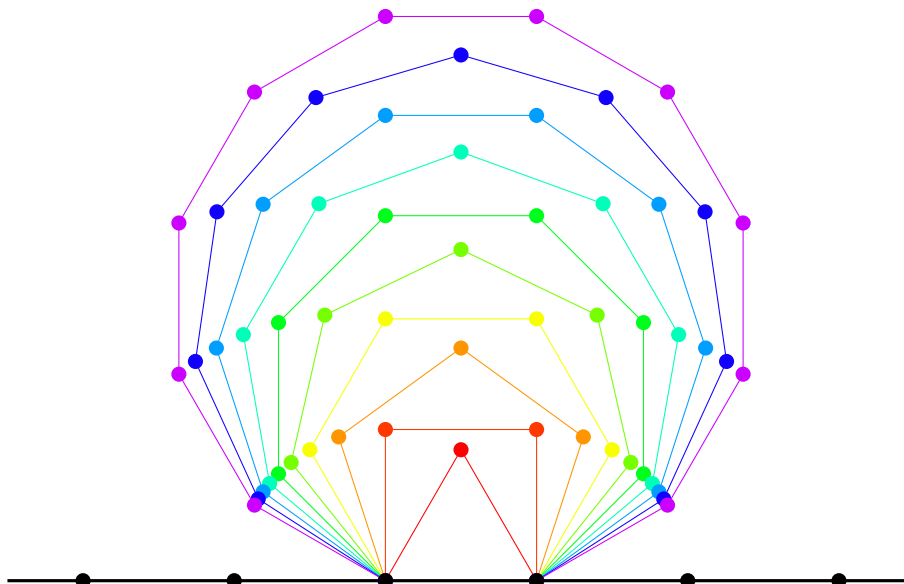
Pointwise, as $n \to \infty$, the sides of the n-gons converge to the black line, and the vertices converge to the black dots. The rotational symmetry becomes a *translational* symmetry—we can shift the black line, left or right, any integer number of side-lengths. The vertical reflection symmetry remains present all the while—we can flip the "∞-gon" across the middle, or indeed across the perpendicular to any vertex or midpoint.
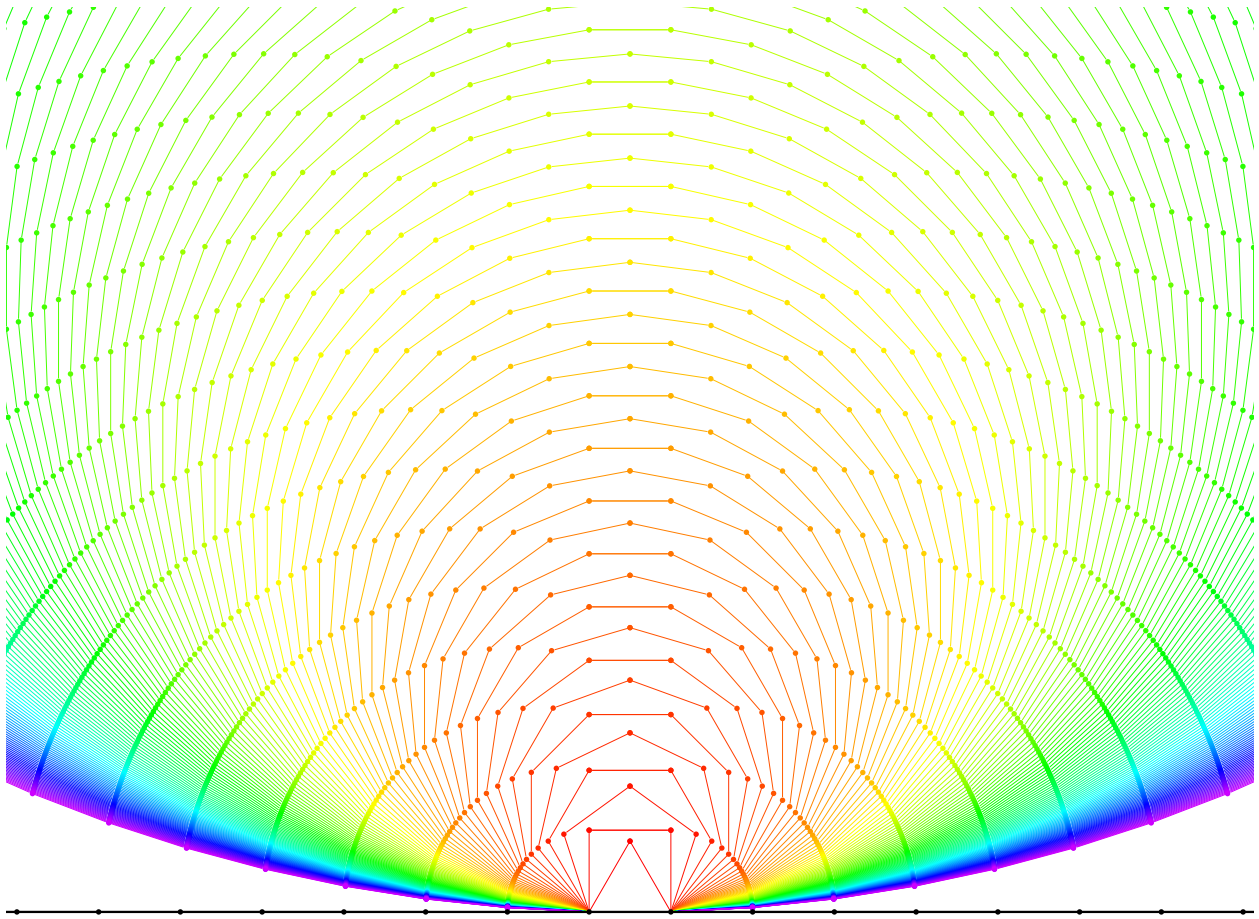
Exercise 79. Show that

$$\mathrm{Aff}(\mathbb{Z}) = \{x \mapsto ax + b : a, b \in \mathbb{Z} \text{ and the map has an inverse with coefficients in } \mathbb{Z}\}$$

is infinite dihedral.

2.4 Symmetric groups

2.4.1 Fundamentals

Recall from Lecture 4:

Definition 2.4.1 — Let X be a set. The *symmetric group on* X is the set of all permutations* on X under composition. This group is denoted

$$S_X.$$

_____
*i.e. bijective self-maps

Remark 2.4.2. Other notations you might encounter include

$$\text{Sym}(X) \quad \text{and} \quad \mathfrak{S}_X.$$

The symmetric group on $\{1, \ldots, n\}$ is denoted S_n while the symmetric group on $\mathbb{N}$ is denoted S_∞.

The elements of a symmetric group are usually denoted by Greek letters: σ [SIGMA], τ [TAU], α, β, γ, etc. The elements of the underlying set X are sometimes called *letters* due to the fact that, historically, arbitrary sets were written like

$$a, b, c, \ldots$$

i.e. using letters, literally. Consequently you may hear people refer to S_n as "the symmetric group on n *letters*" and to its elements as "*substitutions*".

> **Definition 2.4.3** — Let σ be a permutation. A letter i is said to be *moved* if $\sigma(i) \neq i$ and *fixed* if $\sigma(i) = i$. A *transposition* is a permutation that moves just two points.

> **Example 2.4.4** — The identity map ϵ fixes everything, and is the only element in any symmetric group to do so.

We may regard S_X as a group action acting on X by function evaluation:

> **Example** (Example 1.5.13) — $S_X \curvearrowright X$ for any set X in the obvious way: $\sigma . x = \sigma(x)$. In particular, S_n acts on $\{1, ..., n\}$.
>
> What are the orbits of this action?

2.4.2 Order of the symmetric group

> **Proposition 2.4.5**
>
> If X has n elements, then S_X has $n!$ elements.

Proof. Let $X = \{x_1, \ldots, x_n\}$. To write down a permutation of X, we just have to fill in the bottom row of

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ & & & & \end{pmatrix}$$

in such a way that each x_i appears exactly once (here, $n = 5$ for concreteness).

Clearly, there are n possible things to put in the first column (under x_1). Write something down, like x_3:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & & & & \end{pmatrix}$$

and move on to the next column.

Since our map must be a permutation, we can't send x_2 to the same place we sent x_1 (here, x_3). But the remaining possibilities (here, x_1, x_2, x_4, and x_5) are all available, so there are $n-1$ possible things we can put in the second column (under x_2). Pick one, say x_5:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_5 \end{pmatrix}$$

and move on.

Continuing in this manner, by the time we get to x_n, there'll only be *one* unused element—so write it in:

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_5 & x_4 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_5 & x_4 & x_1 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_5 & x_4 & x_1 & x_2 \end{pmatrix}.$$

Every permutation of X can be obtained this way. At each stage, the number of choices decreases by 1, from n at the start to 1 at the end, so there are $n(n-1)\ldots 1 = n!$ permutations altogether. $\qquad\square$

n	1	2	3	4	5	6	7	8	9	10
$n!$	1	2	6	24	120	720	5040	40320	362880	3628800

Exercise 80. Let X be an infinite set. Show that $\mathrm{Sym}(X)$ is infinite. [Hint: Let $x_1, x_2, x_3, \ldots$ be infinitely many distinct elements of X and let x_0 be another; define $\sigma_i : X \to X$ to do nothing except swap x_0 and x_i.]

2.4.3 Composing and inverting permutations

Permutations, like any functions, are composed *right-to-left*: $\sigma\tau$ sends x to $\sigma(\tau(x))$, **not** $\tau(\sigma(x))$. When written in two-line notation, function composition can be denoted by juxtaposition, as in

$$\begin{pmatrix} \bar1 & \bar2 & \bar3 & \bar4 & \bar5 & \bar6 \\ \bar2 & \bar4 & \bar6 & \bar1 & \bar3 & \bar5 \end{pmatrix} \begin{pmatrix} \bar1 & \bar2 & \bar3 & \bar4 & \bar5 & \bar6 \\ \bar3 & \bar6 & \bar2 & \bar5 & \bar1 & \bar4 \end{pmatrix} = \begin{pmatrix} \bar1 & \bar2 & \bar3 & \bar4 & \bar5 & \bar6 \\ \bar6 & \bar5 & \bar4 & \bar3 & \bar2 & \bar1 \end{pmatrix}$$

Perhaps a more intuitive way to compose permutations in two-line notation is to (i) stack them vertically and (ii) rearrange the columns so that the top one's bottom line matches the bottom one's top line; then (iii) the composite permutation is just the mapping defined

by the outermost lines.

$$
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \\ 1 & 5 & 4 & 3 & 2 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}
$$

The inverse of a permutation in two-line notation is obtained by just (i) interchanging the lines and (ii) sorting the columns so the top line matches the original.

$$
\begin{pmatrix} a & b & c & x & y & z \\ c & x & a & y & z & b \end{pmatrix}^{-1} = \begin{pmatrix} c & x & a & y & z & b \\ a & b & c & x & y & z \end{pmatrix} = \begin{pmatrix} a & b & c & x & y & z \\ c & z & a & b & x & y \end{pmatrix}
$$

The *order* of a permutation is its order as an element of the symmetric group it lives in.

2.4.4   Examples

Example 2.4.6 — Let $X = \{1, 2, 3, 4\}$. The functions σ, τ, and ϵ, defined for all i by $\sigma(i) = 5 - i$, $\tau(i) \equiv i - 1 \pmod 4$, and $\epsilon(i) = i$, are permutations of X, hence elements of S_4. In two-line notation, they are written

$$
\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}
$$

$$
\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}
$$

The orders of σ, τ, and ϵ are 2, 4, and 1.

Example 2.4.7 — The permutation $f : \mathbb{N} \to \mathbb{N}$ defined by

$$
f(n) = \begin{cases} n + 1 & n \text{ is odd} \\ n - 1 & n \text{ is even} \end{cases}
$$

can be written in two-line notation as

$$
f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \dots \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & \dots \end{pmatrix}
$$

Similarly, the permutation $g : \mathbb{Z} \to \mathbb{Z}$ defined by

$$g(n) = \begin{cases} n+2 & n \text{ is odd} \\ n-2 & n \text{ is even} \end{cases}$$

can be expressed as

$$g = \begin{pmatrix} \dots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ \dots & -4 & 1 & -2 & 3 & 0 & 5 & 2 & 7 & \dots \end{pmatrix}$$

f is an involution while g has infinite order.

Example 2.4.8 — Label the vertices of a pentagon like so:
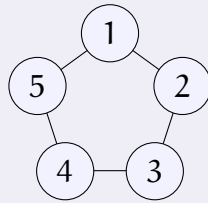
Each symmetry of the pentagon defines a permutation of its vertices, namely by $i \mapsto j$ iff the vertex labelled i goes where the vertex labelled j was. Thus r defines the permutation

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

while f defines the permutation

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

ρ has order 5 while ϕ has order 2.

Example 2.4.9 — Let G be a group. Then every g in G defines a permutation in $\mathrm{Sym}(G)$ by $x \mapsto gx$, which can be visualized using the Cayley table of G. We showed in Tutorial 3 Question 2b that this is a bijection.

For example, if $G = U(7)$, writing $\bar{a}$ instead of $[a]$, we have

·	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Each row can be interpreted as a permutation of the first row, so that e.g. $\bar{2}$ and $\bar{3}$ define the permutations

$$\begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{2} & \bar{4} & \bar{6} & \bar{1} & \bar{3} & \bar{5} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{3} & \bar{6} & \bar{2} & \bar{5} & \bar{1} & \bar{4} \end{pmatrix}$$

respectively. What are their orders?

2.4.5 Cayley's Theorem

Before we go on and talk more about the elements of the symmetric group, the last example already hints at something important about its subgroups.

The *Fundamental Theorems of Cyclic and Dihedral Groups* provide complete descriptions of all these groups' possible subgroups.

So it's natural to ask next: what are all the possible subgroups of symmetric groups?

<div style="text-align:center">Subgroups of symmetric groups are…every group!</div>

If any theorem deserves to be called the *Fundamental Theorem of Symmetric Groups*, it's the following.

> **Theorem 2.4.10** (Cayley)
> Every group is isomorphic to some permutation group*.
> ——————
> *Recall that a *permutation group* is any subgroup of a symmetric group.

Proof. [This was previously covered in Tutorial 3 Question 2, but we include the proof for completeness' sake.]

Fix a group G. For every $g \in G$, we call the map in Example 2.4.9

$$f_g : G \to G, f_g(x) = gx.$$

Tutorial 3 Question 2b gives a proof this is a bijection, but knowing G is a group, the proof could be simplified greatly:

- $f_g(x) = f_g(y)$ iff $gx = gy$ iff $x = y$, so f_g is injective.

- For any $y \in G$, $f_g(g^{-1}y) = gg^{-1}y = y$, so f_g is surjective.

Now consider the map

$$F : G \to \text{Sym}(G), g \mapsto f_g.$$

This is an injection because $f_g = f_h$ only if $f_g(e) = g = h = f_h(e)$. Thus we may restrict the codomain to $F(G)$, and automatically get that F is a bijection $G \to F(G)$.

Now for any $g, h, x \in G$, we also have

$$F(gh)(x) = f_{gh}(x) = ghx = f_g(hx) = f_g(f_h(x)) = (F(g) \circ F(h))(x).$$

Which tells us $F(gh) = F(g) \circ F(h)$, and so F is an isomorphism. $\qquad\square$

Example 2.4.11 — Consider $G = D_2$. Let g_1, g_2, g_3, g_4 be e, r, f, fr respectively.

To quickly determine the corresponding permutations $\sigma_1, \sigma_2, \sigma_3$, and σ_4, we write the Cayley table of G in terms of the g_i's:

$\cdot$	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_1	g_4	g_3
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_3	g_2	g_1

Then our four permutations are

$$\sigma_1 = \epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

which form the order-4 dihedral subgroup $\langle \sigma_2, \sigma_3 \rangle$ in S_4.

2.4.6 Cycles

What do the following permutations (from above) have in common?

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \quad \text{and "}\overline{3}\text{"} = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\ \overline{3} & \overline{6} & \overline{2} & \overline{5} & \overline{1} & \overline{4} \end{pmatrix}$$

If we write $i \to j$ to mean $\sigma(i) = j$ then we can visualize the action of each of these permutations on their respective letter-sets:

$$\tau: 1 \to 4 \to 3 \to 2 \to 1 \to \dots$$

$$\rho: 1 \to 2 \to 3 \to 4 \to 5 \to 1 \to \dots$$

$$\text{``}\bar{3}\text{''}: \bar{1} \to \bar{3} \to \bar{2} \to \bar{6} \to \bar{4} \to \bar{5} \to \bar{1} \to \dots$$

All the elements are in one loop! Permutations which act cyclically like this have a special name.

> **Definition 2.4.12** — Let $k \geq 2$. A k-*cycle*, denoted $(a_1\ a_2\ \dots\ a_k)$ where the a_i's are distinct, is a permutation that moves a_i to a_{i+1} for $1 \leq i < k$, moves a_k to a_1, and fixes everything else.
>
> An *infinite cycle* is a permutation denoted
>
> $$(\dots a_{-1}\ a_0\ a_1\ a_2\ \dots)$$
>
> that moves a_i to a_{i+1} for all $i \in \mathbb{Z}$, and fixes everything else.
>
> A *cycle* is a k-cycle for some k or an infinite cycle.

The three cyclic permutations above can be expressed in *cycle notation* as

$$\tau = (1\ 4\ 3\ 2)$$

$$\rho = (1\ 2\ 3\ 4\ 5)$$

$$\text{``}\bar{3}\text{''} = (\bar{1}\ \bar{3}\ \bar{2}\ \bar{6}\ \bar{4}\ \bar{5})$$

Remark 2.4.13. Cycles can be written in multiple ways, namely by "rotating" their innards:

$$(a_1\ a_2\ \dots\ a_k) = (a_2\ a_3\ \dots\ a_k\ a_1) = \dots = (a_k\ a_1\ \dots\ a_{k-1}).$$

These are all equally valid, but if it makes sense to do so, we prefer to write the smallest letter first.

> **Exercise 81.** Show that σ is a transposition iff σ is a 2-cycle.

> **Theorem 2.4.14**
>
> k-cycles have order k.

Proof. Let $\sigma = (a_1\ a_2\ \dots\ a_k)$ be a k-cycle. Then σ^k is the identity map, because it "moves" each a_i to a_i and fixes everything else. But if $1 < i < k$, then σ^i moves a_1 to a_{i+1}, so σ^i is not the identity map. Thus $o(\sigma) = k$. $\qquad \square$

Example 2.4.15 — All nontrivial elements in S_3 are cycles:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3), \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2).$$

Exercise 82. If $\sigma = (a_1\, a_2\, \ldots\, a_k)$ is a k-cycle in S_X, the cyclic group H generated by σ has order k.

We may consider the group action of H acting on X by restricting the natural action of S_X to its subgroup H. What are the orbits of this action?

2.4.7 Inverting and composing cycles

Cycles are permutations, so anything you can do to permutations, you can do to cycles. The catch is you're not always guaranteed to end up with a cycle.

The inverse of a cycle is obtained by writing it backwards:

$$(a\,b\,c\,d\,e)^{-1} = (e\,d\,c\,b\,a) = (a\,e\,d\,c\,b).$$

The inverse of a cycle is **always** a cycle.

The product of two cycles is their composition—remember, right-to-left!

$$(1\,2)(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$$

The product of two cycles **need not** be a cycle.

Example 2.4.16 — The composition of any cycle with its inverse is the identity map, which is not a cycle.

Example 2.4.17 — The product of transpositions

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

is the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

> which is not a cycle.

> **Example 2.4.18** — The product of cycles
>
> $$(1\,2\,3)(2\,3\,4\,5)$$
>
> is the permutation
>
> $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$
>
> which is not a cycle.

So, what's the point of cycles?

2.4.8   Permutations in terms of cycles

Let's revisit why the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

is not a cycle. We see that σ swaps 1 and 2 and permutes 3, 4, and 5 cyclically. A cycle is supposed to move things in *one* loop, but σ moves things in *two* loops. So although σ isn't a cycle, it *is* a product of the cycles

$$(1\,2) \quad \text{and} \quad (3\,4\,5)$$

in the sense that

$$\sigma = (1\,2)(3\,4\,5) = (3\,4\,5)(1\,2).$$

Let's look at another example. The permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 8 & 6 & 2 & 5 \end{pmatrix}$$

moves 1 to 4, 4 to 3, and 3 to 1, so there's a 3-cycle $(1\,4\,3)$; it moves 2 to 7 and 7 to 2, so there's a 2-cycle $(2\,7)$; similarly, it swaps 5 and 8, so there's another 2-cycle $(5\,8)$; and 6 isn't in any cycle, so we ignore it. Thus

$$\tau = (1\,4\,3)(2\,7)(5\,8).$$

Can every permutation be written as a product of cycles? Well, yes...

$$(1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5) = (1\,5)(1\,4)(1\,3)(1\,2) = (1\,4\,5)(1\,2\,3)$$

...but that's probably not what you were expecting.

Without any further restrictions, there is no end to the number of possible "cycle decompositions" of a given permutation. What's special about *our* decompositions of σ and τ above is that the constituent cycles *do not interact*.

> **Definition 2.4.19** — Two permutations are *disjoint* if they do not move any of the same elements. In other words, σ and τ are disjoint if for all x in X, $\sigma(x) \neq x$ implies $\tau(x) = x$.

> **Example 2.4.20** — The permutations $(1\ 2)$ and $(3\ 4)$ are disjoint, while the permutations $(1\ 2)$ and $(2\ 3)$ are not.

Observe that $(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$ are the same permutation. On the other hand,

$$(1\ 2)(2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

while

$$(2\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

so $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$ are not the same permutation.

> **Lemma 2.4.21**
>
> Disjoint permutations commute.

Proof. We want to show that $\sigma\tau = \tau\sigma$ or, equivalently, that

$$\sigma(\tau(x)) = \tau(\sigma(x))$$

for all x in X. So, let $x \in X$. There are four cases to consider.

Case 1: $\sigma(x) = x$ *and* $\tau(x) = x$. This is easy:

$$\sigma(\tau(x)) = \sigma(x) = x \quad \text{and} \quad \tau(\sigma(x)) = \tau(x) = x.$$

Case 2: $\sigma(x) \neq x$ *and* $\tau(x) = x$. Here,

$$\sigma(\tau(x)) = \sigma(x)$$

but what about $\tau(\sigma(x))$? Since $\sigma(x) \neq x$ and σ is injective, $\sigma(\sigma(x)) \neq \sigma(x)$! Thus σ moves $\sigma(x)$. Since σ and τ are disjoint, τ fixes $\sigma(x)$. In other words,

$$\tau(\sigma(x)) = \sigma(x).$$

Case 3: $\sigma(x) = x$ *and* $\tau(x) \neq x$. This is just Case 2 with the roles of σ and τ reversed.

Case 4: $\sigma(x) \neq x$ *and* $\tau(x) \neq x$. Impossible, because σ and τ are disjoint! $\qquad\square$

Exercise 83. Can non-disjoint permutations commute?

With this terminology in hand, we can now state the most important theorem on permutations:

2.4.9 Cycle Decomposition Theorem

Theorem 2.4.22 (Cycle Decomposition Theorem)

Every permutation can be written as a product of disjoint cycles. Moreover, the decomposition is unique up to reordering of factors.

Before we prove this theorem, let's consider what permutations do to elements in X to provide some intuition for this idea.

For any $\sigma \in S_X$, consider the following relation:

Proposition 2.4.23

Let X be a set and let $\sigma \in S_X$. Define $x \sim y$ iff $\sigma^k(x) = y$ for some integer k. Then $\sim$ is an equivalence relation on X.

Proof. We give two proofs of this fact:

Firstly, this directly follows from the fact that $\langle \sigma \rangle$ is a subgroup of S_X and hence the action of $H = \langle \sigma \rangle$ acting on X (by restricting the natural action of S_X to its subgroup H) yields

$$\sigma^k . x = \sigma^k(x).$$

Which yields precisely this equivalence relation as per Proposition 1.5.2.

Secondly, we also explored a relation similar to this relation in Problem Set 1 Q2:

Problem (PS1Q2). Let f be a self-map on a set X. For $x, y \in X$, define $x \sim_0 y$ if and only if there are some integers $n, m \geq 0$, such that $f^n(x) = f^m(y)$. Then $\sim_0$ is an equivalence relation.

Now when σ is a permutation, we claim that $\sim$ and $\sim_0$ define the same relation.

If $x \sim y$, we have $\sigma^k(x) = y = \sigma^0(y)$, so $x \sim_0 y$.

If $x \sim_0 y$, we have $\sigma^n(x) = \sigma^m(y)$. Without loss of generality, assume $m < n$ and $n - m = k$. Then $\sigma^m(\sigma^k(x)) = \sigma^m(y)$. Since σ is injective, we conclude that $\sigma^k(x) = y$, so $x \sim y$. We again conclude that $\sim$ is an equivalence relation. $\square$

The orbit of a particular $x \in X$ under this action is denoted $\langle \sigma \rangle x$. We call this *the orbit of x under σ^**, and the set of all orbits *the orbits of σ*.

Lemma 2.4.24

Let $\sigma \in S_X$ and let $x \in X$. Then

$$\langle \sigma \rangle x = \{\sigma^k(x) : k \in \mathbb{Z}\}.$$

Proof. Exercise. [This should be very short.] $\square$

Example 2.4.25 — The identity permutation ϵ is the empty product. It generates the trivial group, which acts on X by
$$\epsilon \cdot x = x.$$
The orbits of ϵ are the singleton subsets $\langle \epsilon \rangle x = \{x\}$.

Example 2.4.26 — Let $X = \{1, \ldots, 7\}$. The cycle $\sigma = (1\,2\,3\,4\,5)$ in S_7 generates a cyclic subgroup of order 5. $H = \langle \sigma \rangle$ acts on X by

$$1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1, 6 \mapsto 6, 7 \mapsto 7.$$

The orbits of σ are

$$\langle \sigma \rangle 1 = \{1, 2, 3, 4, 5\}, \langle \sigma \rangle 6 = \{6\}, \text{ and } \langle \sigma \rangle 7 = \{7\}.$$

Example 2.4.27 — Let $X = \{1, \ldots, 8\}$ and let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 3 & 8 & 7 & 4 & 1 & 6 \end{pmatrix} = (1\,2\,5\,7)(4\,8\,6)(3).$$

Then the orbits of τ are

$$\langle \tau \rangle 1 = \{1, 2, 5, 7\}, \langle \tau \rangle 4 = \{4, 6, 8\}, \text{ and } \langle \tau \rangle 3 = \{3\}.$$

[Isn't this a lot shorter than the solution we had in PS1Q2c)?]

---

*Instead of "$\langle \sigma \rangle$".

Example 2.4.28 — Multiplication by $\bar{2}$ on $U(7)$ effects the non-cyclic permutation

$$(\bar{1}\ \bar{2}\ \bar{4})(\bar{3}\ \bar{6}\ \bar{5})$$

(a pair of 3-cycles), while multiplication by $\bar{3}$ there is the 6-cycle

$$(\bar{1}\ \bar{3}\ \bar{2}\ \bar{6}\ \bar{4}\ \bar{5}).$$

Example 2.4.29 — On $\mathbb{N}$,

$$f(n) = \begin{cases} n+1 & n \text{ is odd} \\ n-1 & n \text{ is even} \end{cases}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \dots \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & \dots \end{pmatrix}$$

$$= (1\ 2)(3\ 4)(5\ 6)(7\ 8)\dots$$

is the product of infinitely many 2-cycles (transpositions), while on $\mathbb{Z}$,

$$g(n) = \begin{cases} n+2 & n \text{ is odd} \\ n-2 & n \text{ is even} \end{cases}$$

$$= \begin{pmatrix} \dots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ \dots & -4 & 1 & -2 & 3 & 0 & 5 & 2 & 7 & \dots \end{pmatrix}$$

$$= (\dots 4\ 2\ 0 -2 -4 \dots)(\dots -1\ 1\ 3\ 5\ 7 \dots)$$

is the product of two ∞-cycles ("chains").

Example 2.4.30 — Let

$$\mu_{2^\infty} = \bigcup_{n \geq 0} \mu_{2^n} = \mu_1 \cup \mu_2 \cup \mu_4 \cup \mu_8 \cup \dots$$

be the set of all 2^nth roots of unity, i.e. ζ in $\mathbb{C}$ such that $\zeta^{2^n} = 1$ for some $n \geq 0$. Then $\kappa(z) = z^3$ is a permutation of μ_{2^∞}. [Exercise.] Let $\zeta = e^{2\pi i/8}$ and $\xi = e^{2\pi i/16}$ be primitive 8th and 16th roots of unity, respectively. Then

$$\kappa = \begin{pmatrix} 1 & -1 & i & -i & \zeta & \zeta^3 & \zeta^5 & \zeta^7 & \xi & \dots \\ 1 & -1 & -i & i & \zeta^3 & \zeta & \zeta^7 & \zeta^5 & \xi^3 & \dots \end{pmatrix}$$

$$= (i\ {-i})(\zeta\ \zeta^3)(\zeta^5\ \zeta^7)(\xi\ \xi^3\ \xi^9\ \xi^{11})(\xi^5\ \xi^{15}\ \xi^{13}\ \xi^7)\dots$$

is the product of infinitely many finite cycles of increasing length. [The precise cycle structure of κ is related to the order of $[3]$ in $U(2^n)$.]

Exercise 84. Show that σ fixes x iff $\langle\sigma\rangle x = \{x\}$. Such orbits are called *trivial*.

Exercise 85. If $\langle\sigma\rangle x$ has l elements, then

$$\langle\sigma\rangle x = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{l-1}(x)\}.$$

We may re-define cycles using orbit language now:

Definition 2.4.31 — A *cycle* is a permutation with just one nontrivial orbit. If that orbit has size l, the cycle is called an l-*cycle* and l is called the *length*.

Remark 2.4.32. ∞-cycles are also called *chains* because they aren't really "cycles" in the literal sense.*

Remark 2.4.33. Trivial orbits, i.e. orbits of size 1, a.k.a. fixed points, are also called "1-cycles" (another oxymoron).

Exercise 86. Let $\sigma \in S_n$ be an l-cycle. How many letters does σ fix?

We now have everything we need to properly state and prove the Cycle Decomposition Theorem.

Theorem 2.4.34 (Cycle Decomposition Theorem – Final Form)

Let X be a set and let $\sigma \in S_X$. Then there exists pairwise-disjoint cycles $\sigma_i \in S_X$ such that

$$\sigma = \prod_i \sigma_i.$$

Moreover, this decomposition into cycles is unique up to reordering. That is, if $\tau_j \in S_X$ are any other pairwise-disjoint cycles whose product is σ, then there exists a bijection φ such that $\tau_j = \sigma_{\varphi(j)}$ for all j.

Remark 2.4.35. Note that the product notation makes sense because disjoint cycles commute.

---

*But if we're being picky, isn't the term "infinite cyclic group" literal nonsense as well?

Proof. Pick one x_i from each nontrivial orbit of σ and define $\sigma_i : X \to X$ by the formula

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in \langle\sigma\rangle x_i \\ x & \text{otherwise.} \end{cases}$$

You should check that each σ_i is a bijection (one-to-one and onto). In fact, each σ_i is a *cycle*, because $\langle\sigma\rangle x_i$ is its only nontrivial orbit.

This identity also shows that σ_i and σ_j are *disjoint* when i and j are distinct, because

$$i \neq j \iff x_i \neq x_j \iff x_i \not\sim x_j \iff \langle\sigma\rangle x_i \cap \langle\sigma\rangle x_j = \varnothing.$$

To prove that

$$\prod_i \sigma_i = \sigma$$

we evaluate both sides at an arbitrary x in X. So, let $x \in X$.

- If σ fixes x, then the σ-orbit of x is trivial, so $x \not\sim x_i$ for any i. Thus $\sigma_i(x) = x$ for all i, and we have

$$\Big(\prod_i \sigma_i\Big)(x) = x = \sigma(x).$$

- If σ moves x, then the σ-orbit of x is *non*trivial, so $x \sim x_{i_0}$ for some i_0. Since the x_i's are one per orbit, $x \not\sim x_i$ for any other $i \neq i_0$. Thus $\sigma_{i_0}(x) = \sigma(x)$, while $\sigma_i(x) = x$. Since disjoint permutations commute [and since composition is associative], we have

$$\Big(\prod_i \sigma_i\Big)(x) = \sigma_{i_0}\Big(\Big(\prod_{i \neq i_0} \sigma_i\Big)(x)\Big) = \sigma_{i_0}(x) = \sigma(x).$$

Thus $\sigma = \prod_i \sigma_i$ is the desired decomposition of σ as a product of disjoint cycles.

To show uniqueness, suppose $\sigma = \prod_j \tau_j$ where $\tau_j \in S_X$ are pairwise disjoint cycles. Since $\sigma(x_i) \neq x_i$, there must exist a unique $j = \psi(i)$ such that $\tau_j(x_i) \neq x_i$. [Exists because $\prod_j \tau_j = \sigma$; unique because τ_j are disjoint.] Since τ_j is a *cycle*, it has only *one* nontrivial class, which must be $\langle\tau_j\rangle x_i$. Since $\prod_j \tau_j = \sigma$, it follows that $\tau_j(x) = \sigma(x)$ for all $x \sim x_i$. But $\sigma(x) = \sigma_i(x)$ for these same x! Therefore, $\tau_j = \sigma_i$. The desired bijection is then $\varphi = \psi^{-1}$. $\quad\square$

2.4.10 Cycle type

Now's as good a time as any to make the following definition.

Definition 2.4.36 — Let $\sigma \in S_X$. For each $l = 1, 2, \ldots, \infty$ let c_l be the number of orbits of size l. The *cycle type* of σ is the ordered list of the c_l's.

Remark 2.4.37. When X is finite, say of order n, cycle types are written as n-tuples $(c_1, c_2, c_3, \ldots, c_n)$. When X is infinite, we separate c_∞ from the rest of the list with a semicolon: $(c_1, c_2, c_3, \ldots; c_\infty)$.

Example 2.4.38 — The cycle type of ϵ in S_n is $(n, 0, \ldots, 0)$.

Example 2.4.39 — The cycle types of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (1\,2)(3\,4\,5) \in S_5 \quad \text{and}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 8 & 6 & 2 & 5 \end{pmatrix} = (1\,4\,3)(2\,7)(5\,8) \in S_8$$

are $(0, 1, 1, 0, 0)$ and $(1, 2, 1, 0, 0, 0, 0, 0)$.

Example 2.4.40 — The cycle types of

$$\text{``}\bar{2}\text{''} = (\bar{1}\,\bar{2}\,\bar{4})(\bar{3}\,\bar{6}\,\bar{5})$$

and

$$\text{``}\bar{3}\text{''} = (\bar{1}\,\bar{3}\,\bar{2}\,\bar{6}\,\bar{4}\,\bar{5})$$

in $\mathrm{Sym}(U(7))$ are $(0, 0, 2, 0, 0, 0)$ and $(0, 0, 0, 0, 0, 1)$, respectively.

Example 2.4.41 — The cycle type of

$$f(n) = \begin{cases} n+1 & n \text{ is odd} \\ n-1 & n \text{ is even} \end{cases}$$

$$= (1\,2)(3\,4)(5\,6)(7\,8)\ldots$$

on $\mathbb{N}$ is $(0, \infty, 0, \ldots; 0)$. On the other hand, the cycle type of

$$g(n) = \begin{cases} n+2 & n \text{ is odd} \\ n-2 & n \text{ is even} \end{cases}$$

$$= (\ldots 4\,2\,0\,-2\,-4\ldots)(\ldots-1\,1\,3\,5\,7\ldots)$$

on $\mathbb{Z}$ is $(0, 0, 0, \ldots; 2)$.

Exercise 87. What's the cycle type of $\kappa(z) = z^3$ on μ_{2^∞}?

Exercise 88. What's the cycle type of a general cycle?

Proposition 2.4.42

When X is finite, then so is every orbit, and we have

$$\sum_{l \geq 1} l c_l = n.$$

Proof. The orbits partition X. $\qquad\square$

2.4.11 The order of a permutation

We first give a generalization of Proposition 1.6.18:

Proposition 2.4.43

Let G be a group and let $a, b \in G$. If a and b commute and have finite order, then

$$o(ab) \mid \text{lcm}(o(a), o(b)).$$

Proof. Write $n = o(a)$ and $m = o(b)$. Since a and b commute,

$$(ab)^{\text{lcm}(n,m)} = a^{\text{lcm}(n,m)} b^{\text{lcm}(n,m)} = e.$$

Thus, by the Division Lemma, $o(ab) \mid \text{lcm}(n, m)$. $\qquad\square$

Remark 2.4.44. Note that this proof is identical to the first half of Proposition 1.6.18, except with $\text{lcm}(n, m)$ in place of mn.

Note that $\gcd(n, m) = 1$ implies $\text{lcm}(n, m) = nm$.

When G is a symmetric group and a and b are disjoint permutations, the Proposition gets an upgrade:

Theorem 2.4.45

If σ and τ are disjoint permutations of finite order, then

$$o(\sigma\tau) = \text{lcm}(o(\sigma), o(\tau))$$

Proof. Write $n = o(\sigma)$ and $m = o(\tau)$. By the Proposition, we just have to prove that $\text{lcm}(n, m) \leq o(\sigma\tau)$.

Let $k = o(\sigma\tau)$. Then
$$\sigma^k\tau^k = (\sigma\tau)^k = \epsilon$$
because σ and τ commute. Now, since σ and τ are disjoint, it follows that every power of σ is disjoint from every power of τ. [Why?]

In particular, σ^k and τ^k are disjoint! And if σ^k moves an element, then τ^k cannot move it back; therefore σ^k and τ^k must both equal ϵ. By the Division Lemma, $n = o(\sigma) \mid k$ and $m = o(\tau) \mid k$. That is, $k = o(\sigma\tau)$ is a common multiple of m and n, and so $\mathrm{lcm}(n, m) \leq k$. $\qquad\square$

Exercise 89. Show that the hypothesis of disjointness is necessary.

Corollary 2.4.46

Suppose σ has cycle type $(c_1, c_2, \ldots; c_\infty)$. If $c_\infty = 0$ and $c_l = 0$ for all but finitely many l, then
$$o(\sigma) = \mathrm{lcm}\{l : c_l > 0\}.$$

Proof. By the CDT,
$$\sigma = \prod_{l \geq 1}\prod_{i=1}^{c_l} \sigma_{l,i}$$
where the $\sigma_{l,i}$ are pairwise disjoint cycles of lengths l. By the preceding Theorem, the order of σ is
$$o(\sigma) = \mathrm{lcm}\{o(\sigma_{l,i}) : l \geq 1 \text{ and } 1 \leq i \leq c_l\}$$
$$= \mathrm{lcm}\{\underbrace{1,\ldots,1}_{c_1}, \underbrace{2,\ldots,2}_{c_2}, \underbrace{3,\ldots,3}_{c_3}, \ldots\}$$
$$= \mathrm{lcm}\{l : c_l > 0\}. \qquad\square$$

Example 2.4.47 —
$$o\big((1\,2)(3\,4\,5)\big) = \mathrm{lcm}(2,3) = 6$$
and
$$o\big((1\,4\,3)(2\,7)(5\,8)\big) = \mathrm{lcm}\{3,2,2\} = 6.$$

Example 2.4.48 —
$$o\big((1\,2)(3\,4)(5\,6)(7\,8)\ldots\big) = \mathrm{lcm}\{2,2,2,2,\ldots\} = 2.$$

Exercise 90. Suppose σ has cycle type $(c_1, c_2, \ldots; c_\infty)$. Show that $o(\sigma) = \infty$ iff $c_\infty > 0$ or $c_l \neq 0$ for infinitely many l.

2.4.12 What generates S_n?

We've seen the generating sets of C_n and D_n. What about S_n? [We restrict our attention to finite symmetric groups because the infinite group is much more complicated.]

> **Proposition 2.4.49**
>
> Any k-cycle $(a_1 \ \ldots \ a_k)$ can be written as a product of transpositions
>
> $$(a_1 \ \ldots \ a_k) = (a_1 \ a_2) \ldots (a_{k-1} \ a_k).$$

Proof. It suffices to check the right hand side: If $i \neq a_j$ for some j, the right hand fixes i. If $i = a_j$ for $j \neq k$, then the right hand side sends it to

$$a_j \mapsto a_{j+1}.$$

If $i = a_k$, the right hand side sends it to

$$a_k \mapsto a_{k-1} \mapsto \cdots \mapsto a_1.$$

So the right hand side evaluates to the cycle $(a_1 \ \ldots \ a_k)$. $\qquad \square$

> **Corollary 2.4.50**
>
> Any permutation in S_n can be written as a product of transpositions. That is, S_n is generated by the transpositions in S_n.

Proof. Exercise. $\qquad \square$

> **Proposition 2.4.51**
>
> S_n is generated by the transpositions
>
> $$(1 \ 2), (2 \ 3), \ldots, (n-1 \ n).$$

Proof. For any transposition $(i \ j) \in S_n$ with $i < j$, we observe that
$$(i \ j) = (i \ i+1 \ \ldots \ j-1 \ j)(j-1 \ j-2 \ \ldots \ i+1 \ i).$$
Proposition 2.4.49 decomposes the cycles into transpositions swapping adjacent numbers.

$\qquad \square$

> **Theorem 2.4.52**
> S_n is generated by the n-cycle $\sigma = (1\ 2\ \ldots\ n)$ and the transposition $\tau = (1\ 2)$.

Proof. We claim that
$$(k\ k+1) = \sigma^{k-1}\tau\sigma^{1-k}.$$
To prove this, we proceed via induction. For $k = 1$, we are done. Suppose the claim holds for $k = K$, then

$$\sigma^{(K+1)-1}\tau\sigma^{1-(K+1)} = \sigma(\sigma^{k-1}\tau\sigma^{1-k})\sigma^{-1}$$
$$= (1\ 2\ \ldots\ n)(K\ K+1)(1\ 2\ \ldots\ n)^{-1}$$
$$= (K+1\ K+2).$$

Induction tells us σ and τ generate all transpositions in Proposition 2.4.51, so they together generate S_n. $\square$

> **Exercise 91.** Give an example of an n-cycle and a transposition that do *not* together generate S_n.

You can find a number of other generating sets of S_n, but these—the set of all transpositions, the set of *adjacent* transpositions, and the set $\{(1\ 2\ \ldots\ n), (1\ 2)\}$—are the most commonly seen.

> **Exercise 92.** Show that S_n must be generated by at least two elements. [That is, S_n is not cyclic.]