MAT301
Groups and Symmetries

Gaurav Patil and Shuyang Shen

Fall 2024

These lecture notes were written and edited over iterations of group theory courses, including MAT301 in Summer 2020 (Matt Olechnowicz and Shuyang Shen) and MAT301 in Fall 2024 (Gaurav Patil and Shuyang Shen).

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

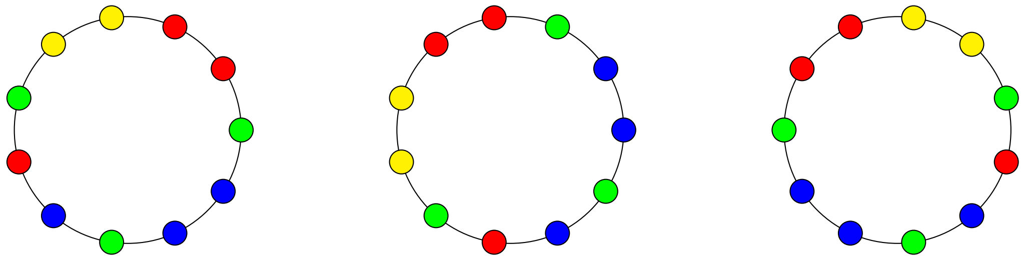
Consider a cube. We cannot easily "reflect" it in three-dimensional space without the aid of a mirror, but we may rotate it in a few different ways while maintaining its shape:

- 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.

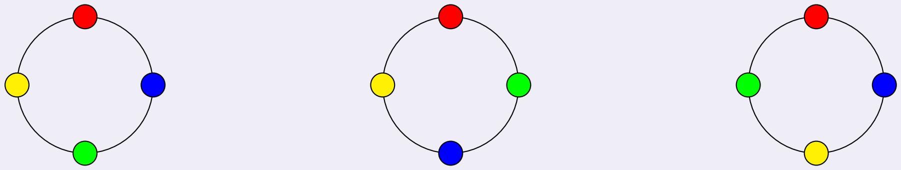
You can see a visualization here. Observe that with each type of rotation, the faces of the cube are permuted in different ways! Something that group theory studies is what these symmetries each *change* and what they *preserve*, as well as how they *interact* with each other.

-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 $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. 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

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

and

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

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

And there is one for quartics as well:

$$\begin{aligned}
r_1 &= \frac{-a}{4} - \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}} - \frac{1}{2}\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} - \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}} - \frac{-a^3+4ab-8c}{4\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}}}} \\
r_2 &= \frac{-a}{4} - \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}} + \frac{1}{2}\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} - \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}} - \frac{-a^3+4ab-8c}{4\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}}}} \\
r_3 &= \frac{-a}{4} + \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}} - \frac{1}{2}\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} - \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}} + \frac{-a^3+4ab-8c}{4\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}}}} \\
r_4 &= \frac{-a}{4} + \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}} + \frac{1}{2}\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} - \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}} + \frac{-a^3+4ab-8c}{4\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2-3ac+12d)}{3\left(2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}\right)^{\frac{1}{3}}} + \left(\frac{2b^3-9abc+27c^2+27a^2d-72bd+\sqrt{-4(b^2-3ac+12d)^3+(2b^3-9abc+27c^2+27a^2d-72bd)^2}}{54}\right)^{\frac{1}{3}}}}}
\end{aligned}$$

... 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 secret.

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 $e_1, \dots, e_n$ 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.

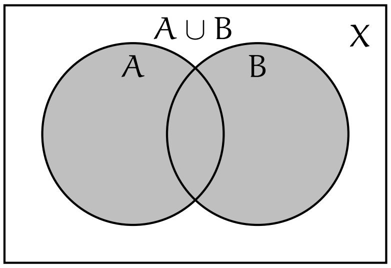
The *union* of two sets is the set of elements contained in at least one of them. That is,

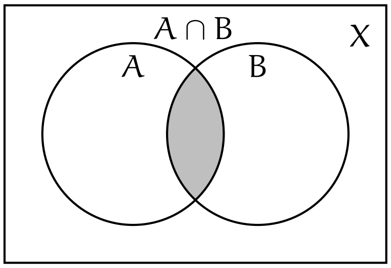
$$A \cup B = \{x : x \in A \text{ or } x \in B \text{ (or both!)}\}.$$

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.



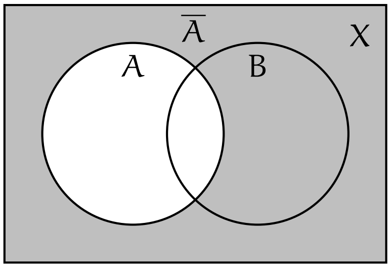


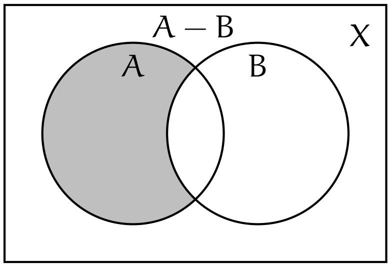
The *complement* of a subset is the set of things *not* in it. More precisely,

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

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 $B \setminus A = B \cap A^c$.

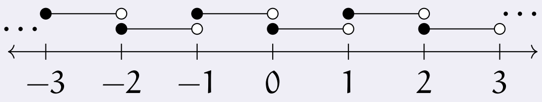
A *partition* of a set is a collection of subsets that divide it up. Formally, $A_i \subseteq X$ for all i, and

$$X = \bigcup_i A_i,$$

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 $f : X \to Y$, 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.

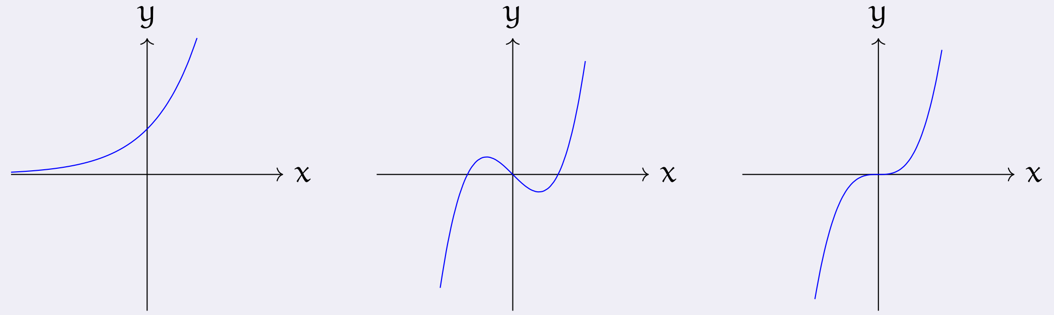
Exercise 6. Suppose f is injective, and $f(x) = f(y)$. What can you deduce about x and y?

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?

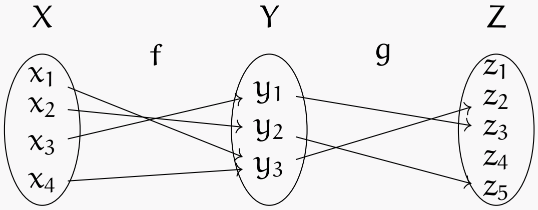
f is *bijective* if it is both injective and surjective.

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 $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. 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 $g \circ f$?

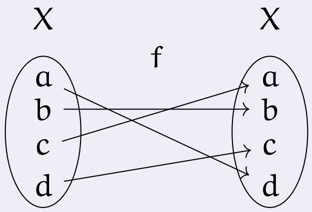
Exercise 11. Show that if $S \cap T = \phi$, then

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

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 $f^0 = \text{id}_X$.

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"	

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

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

Exercise 16. Show that the equivalence classes partition X.

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 $\operatorname{lcm}(a, b) \mid m$.

The lcm and the gcd are related by the formula

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

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 order 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], . . . , [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.

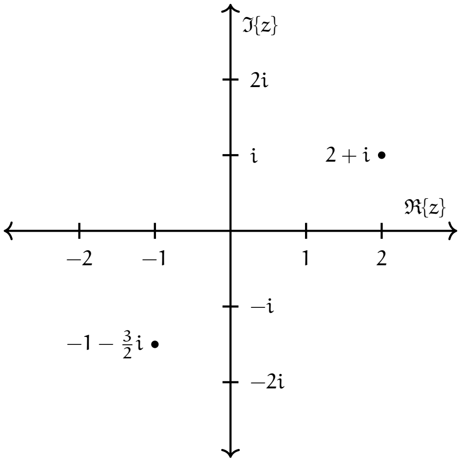
Cartesian coordinates are most useful for addition and subtraction, e.g.

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

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,

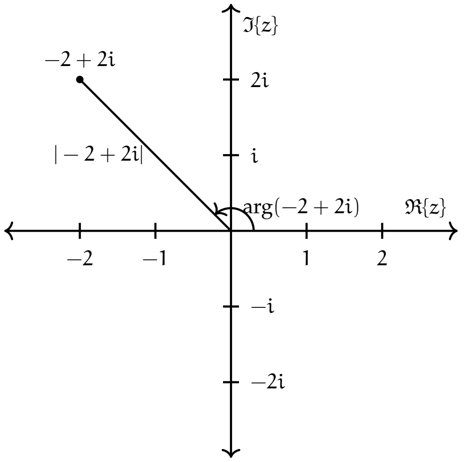
$$|z| = \sqrt{x^2 + y^2}.$$

> **Exercise 17.** 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

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

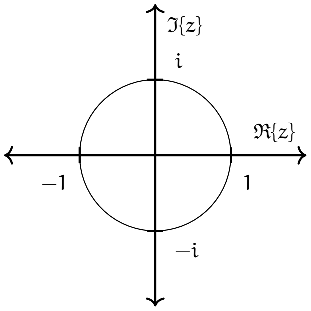
which can be obtained by using the Taylor series for the exponential, and recognizing the Taylor series for sine and cosine.

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:

$$\begin{aligned}(r_1e^{i\theta_1})(r_2e^{i\theta_2}) &= r_1r_2e^{i(\theta_1+\theta_2)},\\ \frac{r_1e^{i\theta_1}}{r_2e^{i\theta_2}} &= \frac{r_1}{r_2}e^{i(\theta_1-\theta_2)},\\ (re^{i\theta})^n &= r^ne^{in\theta}.\end{aligned}$$

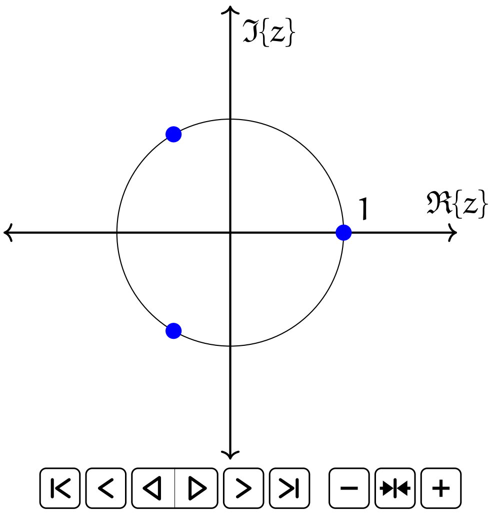
The *unit circle* is the set of complex numbers with modulus 1. These points form a circle on the complex plane.



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 18.** 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 $n = 3, \dots, 12$.



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 $(A, B, C, \dots)$ for matrices, and lowercase letters $(a, b, c, \dots)$ 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

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

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

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

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