

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

-1	Introduction	1
-1.1	Group theory	2
-1.1.1	Polyhedra	2
-1.1.2	Colouring	2
-1.1.3	Polynomial roots	3
-1.1.4	Cryptography	4
0	Preliminaries	6
0.1	Sets	6
0.2	Maps a.k.a. Functions	8
0.3	Relations	11
0.4	Integers, or: Rem(a)inders from Arithmetic	13
0.4.1	Division	13
0.4.2	Congruence	14
0.5	Complex numbers	14
0.6	Matrices	17
1	Groups and subgroups	20
1.1	Binary operations and groups	20
1.1.1	Visualizing binary operations	21
1.1.2	Associativity	22
1.1.3	Operations table	23
1.1.4	Definition of a group	23
1.1.5	Immediate consequences	24
1.1.6	Notation	26
1.2	Examples	27
1.2.1	Basic groups	27
1.2.2	Groups of integers	27
1.2.3	Matrix groups	28
1.2.4	Trivial group	29
1.2.5	Cyclic groups	29
1.2.6	Dihedral groups	29
1.2.7	Symmetric groups	30

1.3	Subgroups	31
1.3.1	Basic groups	32
1.3.2	Matrix groups	32
1.3.3	Cyclic groups	33
1.3.4	Dihedral groups	33
1.3.5	Permutation groups	33
1.3.6	Generating new subgroups	34

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

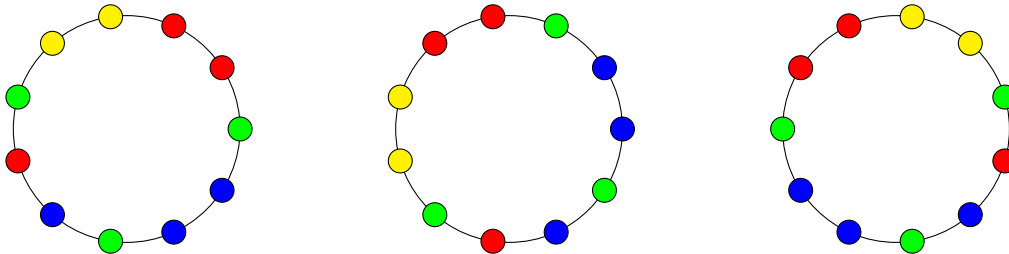
Consider a cube. We cannot easily “reflect” it in three-dimensional space without the aid of a mirror, but we may rotate it in a few different ways while maintaining its shape:

- 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.

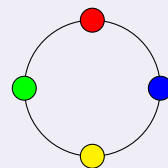
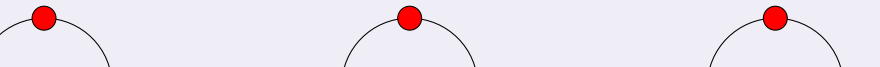
You can see a visualization here. Observe that with each type of rotation, the faces of the cube are permuted in different ways! Something that group theory studies is what these symmetries each *change* and what they *preserve*, as well as how they *interact* with each other.

-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

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

and

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

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

And there is one for quartics as well:

[illegible]

...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 in 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, \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



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 .

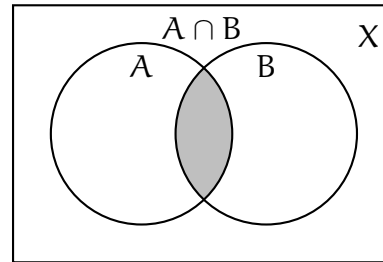
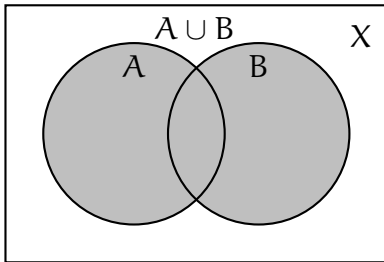
The *union* of two sets is the set of elements contained in at least one of them. That is,

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

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.

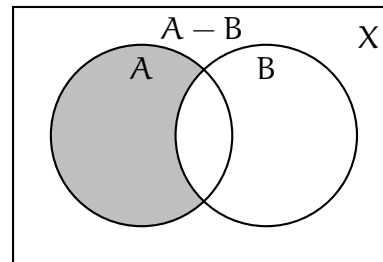
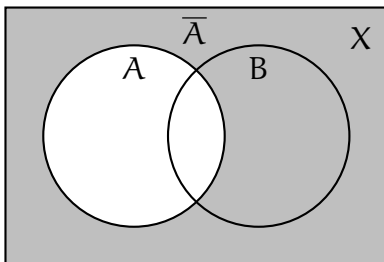


The *complement* of a subset is the set of things *not* in it. More precisely,

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

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

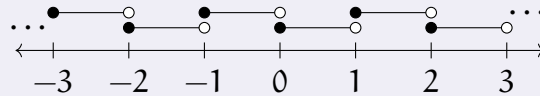
A *partition* of a set is a collection of subsets that divide it up. Formally, $A_i \subseteq X$ for all i , and

$$X = \bigcup_i A_i,$$

and $A_i \cap A_j = \emptyset$ 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—

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R}, \\ f(x) &= x^2. \end{aligned}$$

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 $\text{im } f = f(X)$.

Example 0.2.2 — Let $f(x) = x^2 + 1$ from \mathbb{R} to \mathbb{R} . Then $\text{im } f = [1, \infty)$ 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.

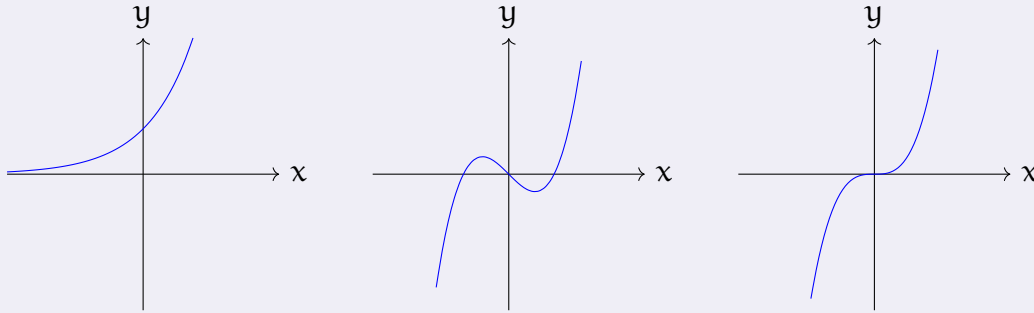
f is *injective* or *one-to-one* (or even just *1-1*) if it doesn't send different inputs to the same output.

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

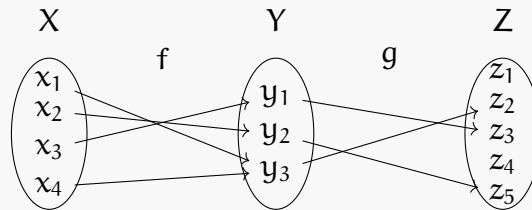
f is *surjective* or *onto* if the image equals the codomain. Surjectivity only makes sense if you specify a codomain!

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 $\mathbb{R} \rightarrow \mathbb{R}$.

Given another map $g : Y \rightarrow Z$, 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 $g : Y \rightarrow X$ 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 $f : X \rightarrow Y$ 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 $g \circ f$?

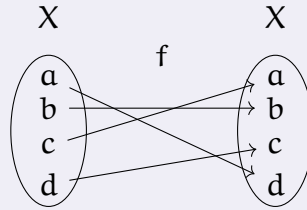
Exercise 11. Let S, T be subsets of Y . Show that if $S \cap T = \emptyset$, then

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

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 itself. 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 $f : X \rightarrow X$, the n th *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 $n = 0, \dots, 6$. What do you notice?

Finally, $f : X \rightarrow X$ 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

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

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

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

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 $42/9 = 4.666\dots$ 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, $[0], [1], [2], \dots, [23]$.

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

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

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 .

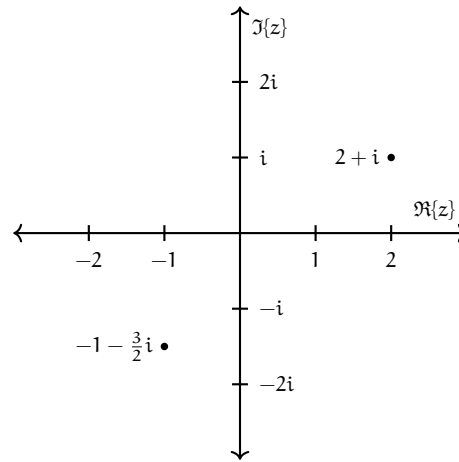
Cartesian coordinates are most useful for addition and subtraction, e.g.

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

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,

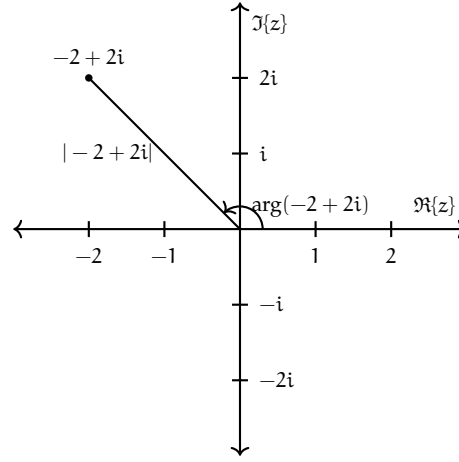
$$|z| = \sqrt{x^2 + y^2}.$$

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

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

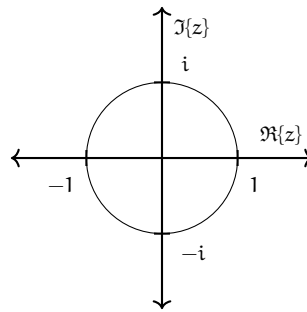
which can be obtained by using the Taylor series for the exponential, and recognizing the Taylor series for sine and cosine.

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:

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

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 *n th root of unity*.

Exercise 20. Show that the n th 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 n th 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,

$$\det [a] = a,$$

and for a larger matrix,

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

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

Example 0.6.2 — By expanding along the top row,

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

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 $\star : S \times S \rightarrow S$ 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 $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. 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 $\star : S \times S \rightarrow S$ 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 $- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. 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:

·	[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 *rock*, *paper*, and *scissors*. 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 $S \times S \rightarrow S$), 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 $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ 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*:

$$\begin{aligned} a \star c &= b \star c \\ a &= b \end{aligned}$$

and *left cancellation*:

$$\begin{aligned} c \star a &= c \star b \\ a &= b \end{aligned}$$

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

$$g^n = \underbrace{g \cdot \dots \cdot g}_{n \text{ times}}$$

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:

$$aabbcbcd\ddots = a^2b^3cd^4.$$

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 $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$ 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. $U(n)$.

For example, $(\mathbb{Z}/6\mathbb{Z})^\times = \{[1], [5]\}$ 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,

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

For example, 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 :

$$\begin{aligned} G \times G &\rightarrow G \\ (e, e) &\mapsto e \end{aligned}$$

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 n th roots of unity under multiplication. That is,

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

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

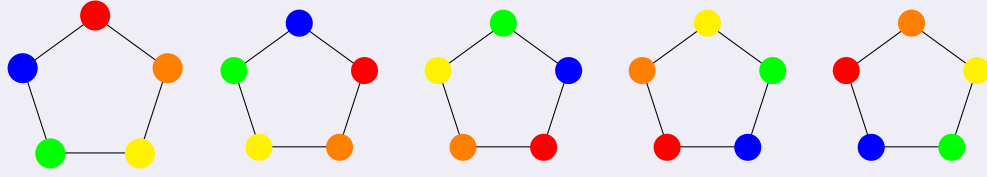
$$\mu_n = \langle e^{2\pi i/n} \rangle.$$

1.2.6 Dihedral groups

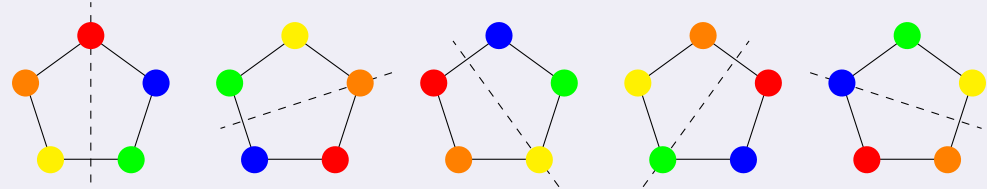
The dihedral group D_n is the set of reflections and rotations — *SYMMETRIES* — of a regular n -gon, under composition.

*multiple in additive notation

Example 1.2.1 — Consider the regular pentagon with its rotations

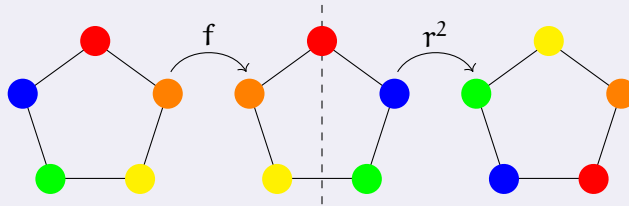


and reflections



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 $\{1, \dots, n\}$ 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

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

in two-line notation). The function τ^2 sends $1 \rightarrow 2 \rightarrow 1$ and $2 \rightarrow 1 \rightarrow 2$, so $\tau^2 = \text{id}$. Thus $S_2 = \langle \tau \rangle$ is cyclic of order 2.

*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 subset H of a group G is a *subgroup*, 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 $H \times H \rightarrow H$ 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 ($\det A > 0$),

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

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

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

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

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

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

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

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

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

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

(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 $S \subseteq G$. Show that $\langle S \rangle \leq G$.

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

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

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

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

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

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

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

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 1.3.4 — In the additive group \mathbb{Q} ,

$$\langle \frac{1}{2}, \frac{1}{3} \rangle = \{ \frac{n}{2} + \frac{m}{3} : n, m \in \mathbb{Z} \}$$

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 $\frac{1}{6}$.

Example 1.3.5 — 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 $\langle g \rangle = \langle 2, 3 \rangle$.)