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).

We would like to thank the many students who suggested corrections to the text, especially Khizer Ahmad, Callum Cassidy-Nolan, Paola Driza, Rachel Leggett, Wenda Li, Michael Luan, Amy Mann, Bayan Mehr, Kelly Qiu, and Bohan Xuan.

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.

3

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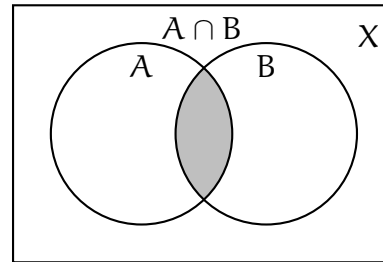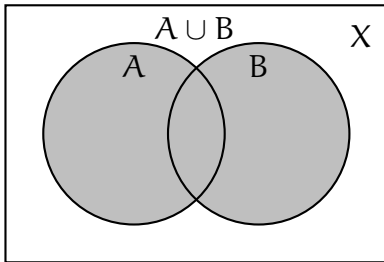
The *complement* of a subset is the set of things *not* in it. More precisely,

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

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,

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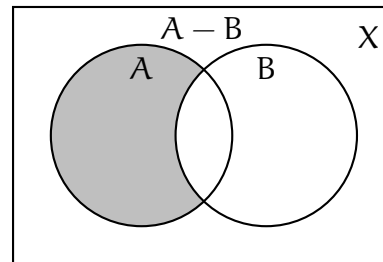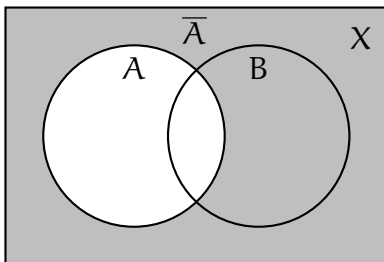
Exercise 2. Write $A \cap A^c = \varnothing$ in plain language (using the word "disjoint"), and then prove it.

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

7

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 $\mathbb{R}$.
>
>
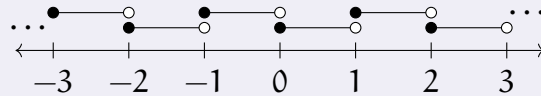
The *Cartesian product* of two sets A and B is the set of ordered pairs (a, b) where a is in A and b is in B. That is,

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

> **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 $\mathbb{R} \to \mathbb{R}$.
>
>
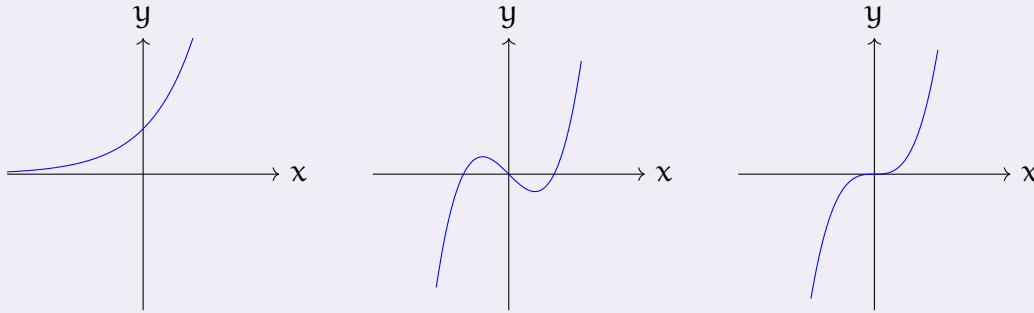
Given another map $g : Y \to Z$, g *composed with* f (or g *after* f) is the map obtained by applying f and then g. That is, $(g \circ f)(x) = g(f(x))$.
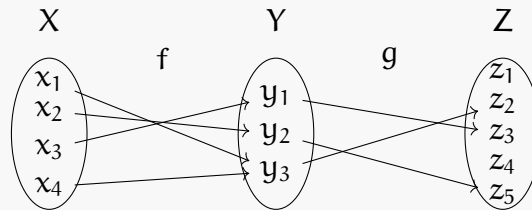
> **Exercise 8.**
>
>
>
> Express the map $g \circ f$ in two-line notation.

> **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. 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*.
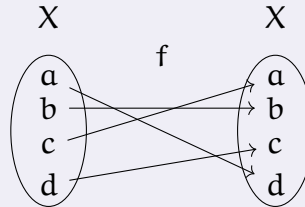
> **Example 0.2.4 —**
>
>
>
> In two-line notation, this map is
>
> $$\begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}.$$

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

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 $x R y$ and $y R x$, then $x = y$.

R is *transitive* if you can "remove the middleman" in a chain of relations. That is, if $x R y$ and $y R z$, then $x R z$.

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 $42/9 = 4.666...$ 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 $\mathfrak{R}z$ and $\mathfrak{I}z$ 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:
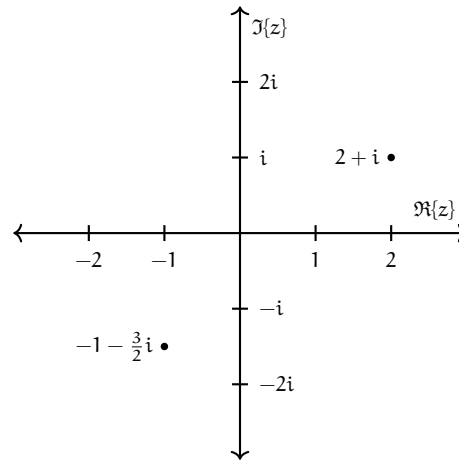
The *(complex) conjugate* of $z = x + iy$ is the number $\bar{z} = x - iy$.

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.

15
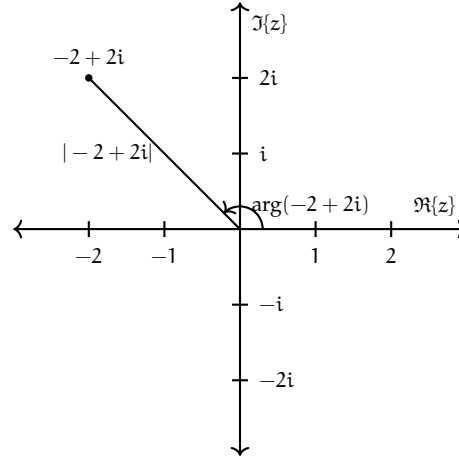
The *polar form* of z is obtained by writing z as

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

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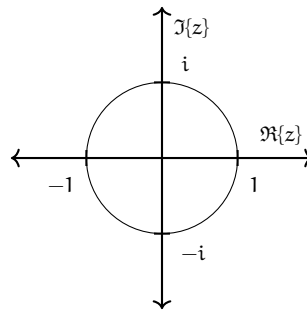
Let n be a natural number. If z is a complex number such that $z^n = 1$, then z is called an nth *root of unity*.

> **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,

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

where i is any fixed index between 1 and n, and $\widetilde{A}_{i,j}$ 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*.

20

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 *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

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

22

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 $\overline{a}$ instead of $[a]$,
>
> $$\det \begin{bmatrix} \overline{2} & \overline{1} \\ \overline{3} & \overline{4} \end{bmatrix} = \overline{2 \cdot 4} - \overline{1 \cdot 3} = \overline{8} - \overline{3} = \overline{5}$$
>
> which is invertible because $5^2 = 25 \equiv 1 \pmod{12}$. The inverse matrix is
>
> $$\begin{bmatrix} \overline{2} & \overline{1} \\ \overline{3} & \overline{4} \end{bmatrix}^{-1} = \overline{5}^{-1} \begin{bmatrix} \overline{4} & \overline{-1} \\ \overline{-3} & \overline{2} \end{bmatrix} = \overline{5} \begin{bmatrix} \overline{4} & \overline{11} \\ \overline{9} & \overline{2} \end{bmatrix} = \begin{bmatrix} \overline{20} & \overline{55} \\ \overline{45} & \overline{10} \end{bmatrix} = \begin{bmatrix} \overline{8} & \overline{7} \\ \overline{9} & \overline{10} \end{bmatrix}.$$

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.
>
>
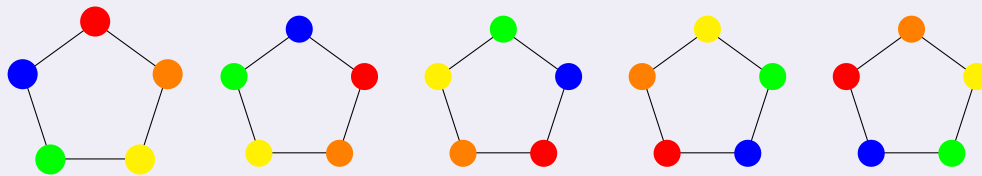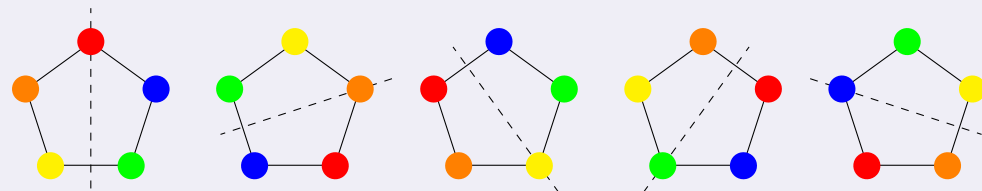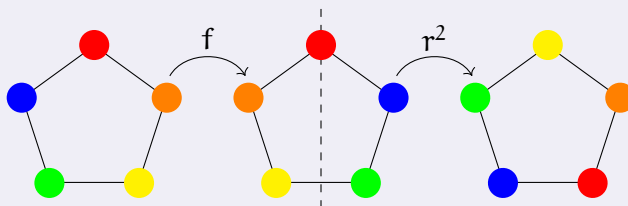
1.2.7 Symmetric groups

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

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

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 $ab \in H$. □

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 $ab^{-1} \in \langle S \rangle$. $\qquad\square$

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).
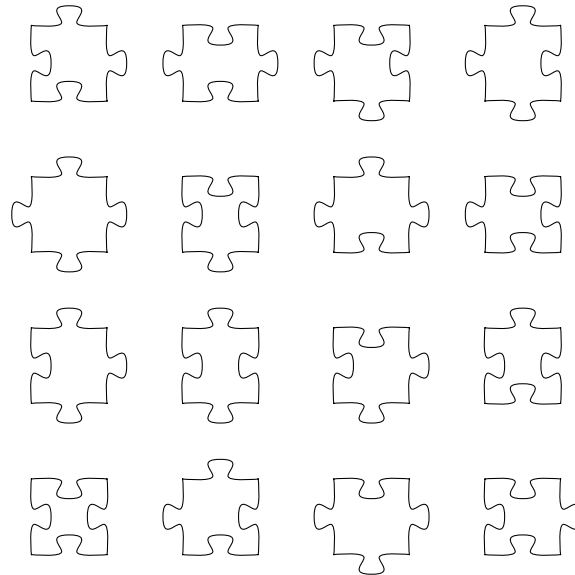
Say two puzzle pieces are rotation-equivalent if you can rotate one so it looks like the other. How many puzzle pieces are there up to rotation-equivalence?
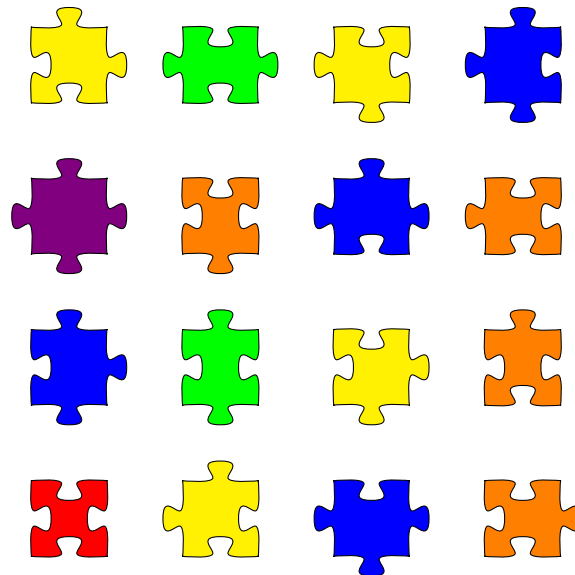
The answer is 6. Each puzzle piece has one of the following shapes:
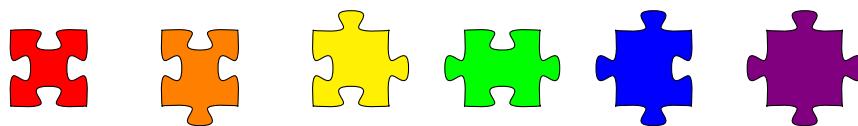
Mathematically, we just determined the *orbits* of the *action* of the group C_4 on the set of puzzle pieces.

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 $(g, x) \mapsto g \cdot x$, satisfying

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

2) *compatibility*: $g \cdot (h \cdot x) = gh \cdot x$ 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 $g \cdot x = y$ for some g in G" is an equivalence relation.

Proof. By the *identity* axiom, $\sim$ is reflexive: $e \cdot x = x$ 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 $g \cdot x = y$ and $h \cdot y = z$ for some g, h in G, so

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

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

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

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,

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

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 $gX = \{g \cdot x : x \in X\}$ 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
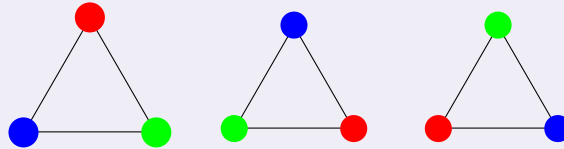
and reflections
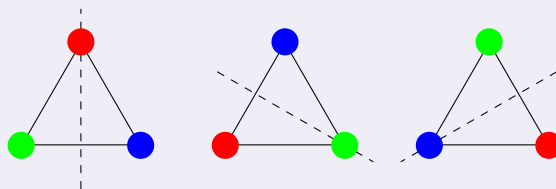
We may say that D_3 acts on the red, green, and blue vertices of the triangle, such that rotation by $120°$ clockwise sends the red vertex to the (original position of the) green vertex. We may also say that D_n acts on the (unlabelled) edges of the triangle. We may even say that D_n acts on the set 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* $\text{Aff}(\mathbb{R})$ 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 $\mathrm{Orb}_H(g) = \{gh : h \in H\}$, 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 $g' \in \mathrm{Orb}_H(g)$. On the other hand, for any $g' \in \mathrm{Orb}_H(g)$, 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 $o(G)$. $\qquad\square$

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. $n = o(g) \mid m$. $\square$

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 $i \equiv j \pmod n$. $\square$

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 $e, g, g^2, \ldots,$ 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, $\dfrac{n}{d} \mid m$. $\qquad\square$

> **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
> $$\langle [8] \rangle = \{[8], [4], [0]\} \lneqq \mathbb{Z}/12\mathbb{Z}$$
>
> 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. $\quad\square$

> **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. $\quad\square$

> **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! $\quad\square$

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! □

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 $o(h)$.

$\langle 2 \rangle \leq \mathbb{Q}^\times$ 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

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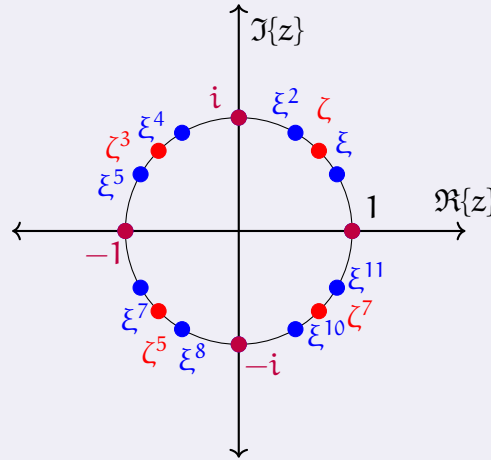
The only nontrivial proper subgroups of μ_8 are $\mu_4 = \{1, i, -1, -i\}$ and *its* subgroup $\mu_2 = \{1, -1\}$. On the other hand, μ_{12} has several additional subgroups aside from these, like $\mu_3 = \{1, \xi^4, \xi^8\}$ and $\mu_6 = \{1, \xi^2, \xi^4, \xi^6, \xi^8, \xi^{10}\}$. However,

$$\mu_8 \nleq \mu_{12}.$$

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 $i \equiv j$ (mod 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:

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

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

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

<div align="center">Every subgroup of a cyclic group is cyclic.</div>

Lemma 2.2.9

Let $G = \langle g \rangle$ be a cyclic group and let $H \le G$ 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 $0 \le r < d$, 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.
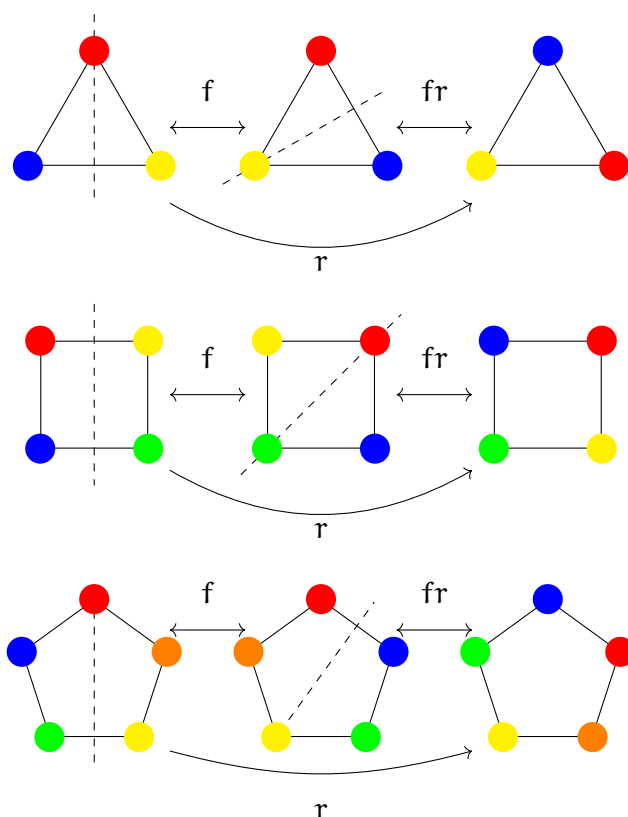
Exercise 71. Is the trivial group dihedral?

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*.
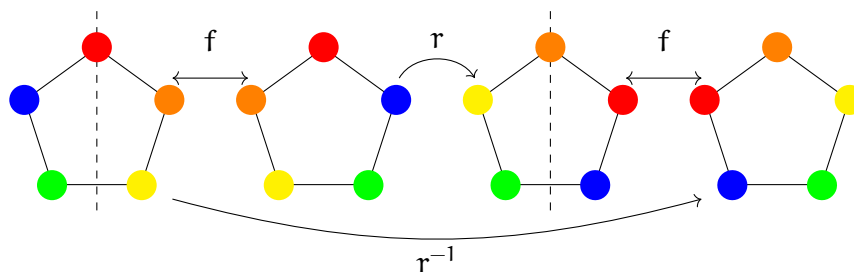
Since f is self-inverse, we can rewrite this identity as

$$rf = fr^{-1}.$$

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 $o(G) \le 2n$. (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 $0 \le i, j < n$). 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 $f \ne r$, 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 $fr^i \ne r^j$, 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. $\qquad\square$

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. □

---

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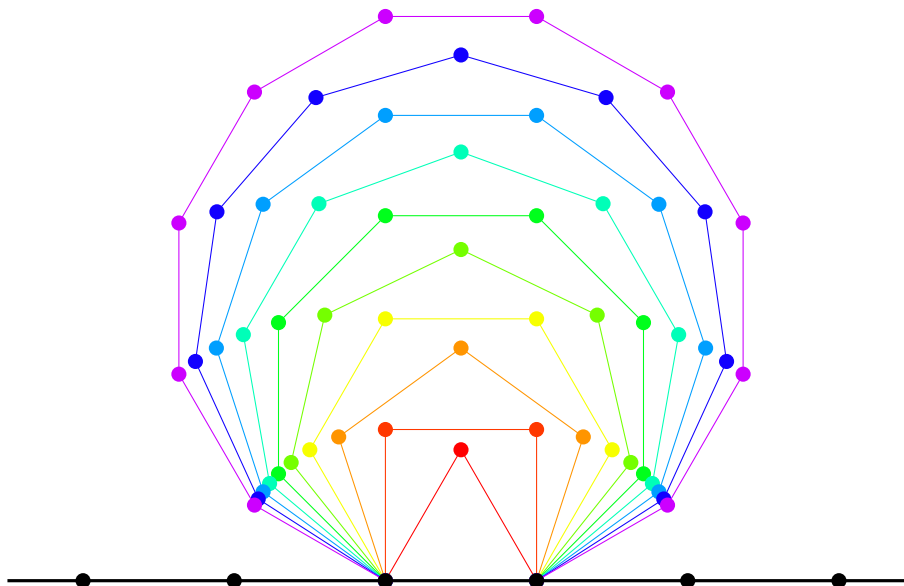
Pointwise, as $n \to \infty$, the sides of the n-gons converge to the black line, and the vertices converge to the black dots. The rotational symmetry becomes a *translational* symmetry—we can shift the black line, left or right, any integer number of side-lengths. The vertical reflection symmetry remains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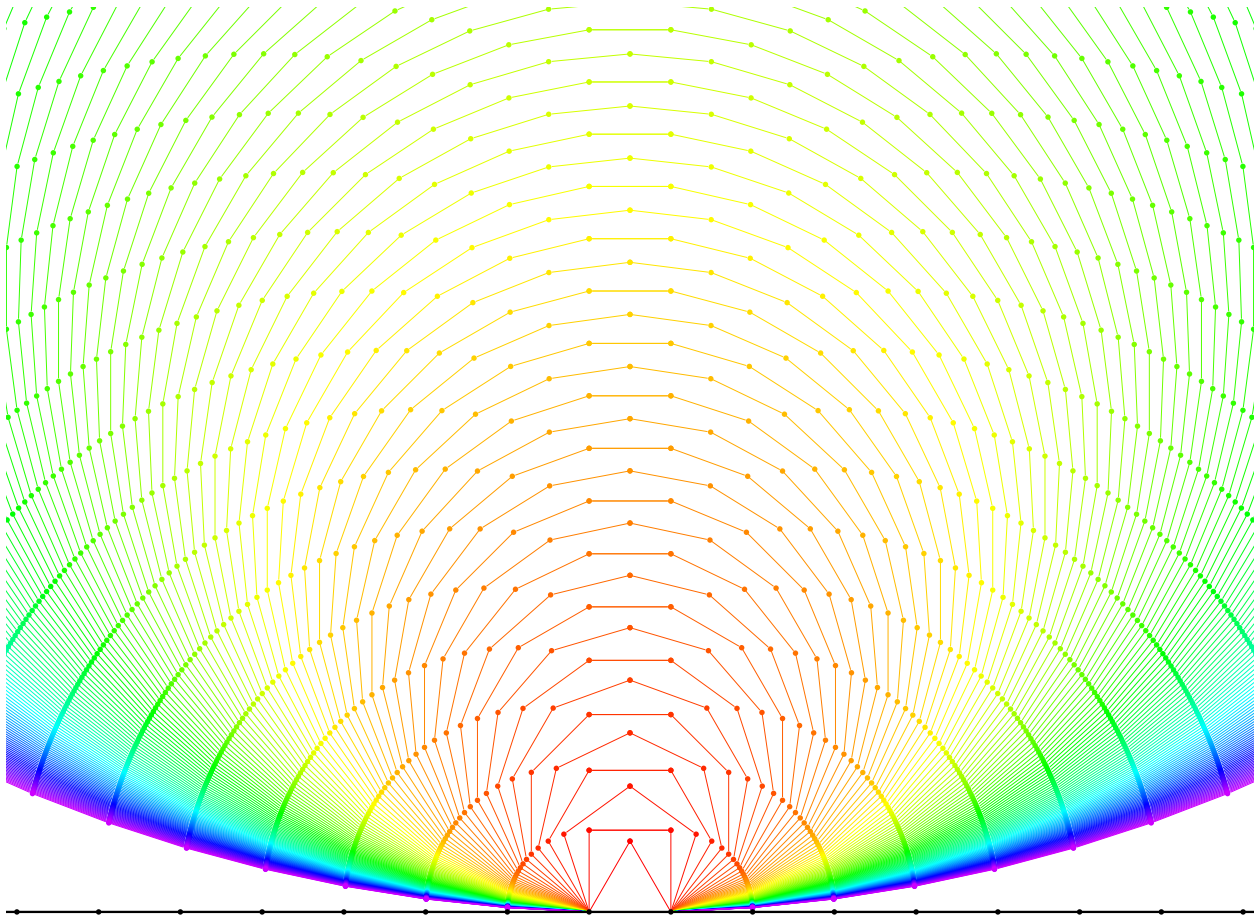
Exercise 79. Show that

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

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

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

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

$$\begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{2} & \bar{4} & \bar{6} & \bar{1} & \bar{3} & \bar{5} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{3} & \bar{6} & \bar{2} & \bar{5} & \bar{1} & \bar{4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{6} & \bar{5} & \bar{4} & \bar{3} & \bar{2} & \bar{1} \end{pmatrix}$$

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

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

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

$$g = \begin{pmatrix} \cdots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \cdots \\ \cdots & -4 & 1 & -2 & 3 & 0 & 5 & 2 & 7 & \cdots \end{pmatrix}$$

f is an involution while g has infinite order.

Example 2.4.8 — Label the vertices of a pentagon like so:
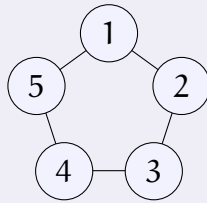
Each symmetry of the pentagon defines a permutation of its vertices, namely by $i \mapsto j$ iff the vertex labelled i goes where the vertex labelled j was. Thus r defines the permutation

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

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

$$\begin{array}{c|cccccc}
\cdot & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\
\hline
\bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\
\bar{2} & \bar{2} & \bar{4} & \bar{6} & \bar{1} & \bar{3} & \bar{5} \\
\bar{3} & \bar{3} & \bar{6} & \bar{2} & \bar{5} & \bar{1} & \bar{4} \\
\bar{4} & \bar{4} & \bar{1} & \bar{5} & \bar{2} & \bar{6} & \bar{3} \\
\bar{5} & \bar{5} & \bar{3} & \bar{1} & \bar{6} & \bar{4} & \bar{2} \\
\bar{6} & \bar{6} & \bar{5} & \bar{4} & \bar{3} & \bar{2} & \bar{1} \\
\end{array}$$

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 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

$$F : G \to \mathrm{Sym}(G), g \mapsto f_g.$$

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. □

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?

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \quad \text{and ``3''} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{3} & \bar{6} & \bar{2} & \bar{5} & \bar{1} & \bar{4} \end{pmatrix}$$

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:

$$\tau: 1 \to 4 \to 3 \to 2 \to 1 \to \ldots$$

$$\rho: 1 \to 2 \to 3 \to 4 \to 5 \to 1 \to \ldots$$

$$\text{``}\overline{3}\text{''}: \overline{1} \to \overline{3} \to \overline{2} \to \overline{6} \to \overline{4} \to \overline{5} \to \overline{1} \to \ldots$$

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 $(a_1 \, a_2 \, \ldots \, a_k)$ 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
>
> $$(\ldots a_{-1} \, a_0 \, a_1 \, a_2 \, \ldots)$$
>
> 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

$$\tau = (1 \, 4 \, 3 \, 2)$$

$$\rho = (1 \, 2 \, 3 \, 4 \, 5)$$

$$\text{``}\overline{3}\text{''} = (\overline{1} \, \overline{3} \, \overline{2} \, \overline{6} \, \overline{4} \, \overline{5})$$

Remark 2.4.13. Cycles can be written in multiple ways, namely by "rotating" their innards:

$$(a_1 \, a_2 \, \ldots \, a_k) = (a_2 \, a_3 \, \ldots \, a_k \, a_1) = \ldots = (a_k \, a_1 \, \ldots \, a_{k-1}).$$

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 $\sigma = (a_1 \, a_2 \, \ldots \, a_k)$ 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 $o(\sigma) = k$. $\square$

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! □

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. $\qquad\square$

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.] $\qquad\square$

Example 2.4.25 — The identity permutation ϵ is the empty product. It generates the trivial group, which acts on X by
$$\epsilon . x = x.$$
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 $\mathbb{N}$,

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

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

$$= (1\,2)(3\,4)(5\,6)(7\,8)\ldots$$

is the product of infinitely many 2-cycles (transpositions), while on $\mathbb{Z}$,

$$g(n) = \begin{cases} n+2 & n \text{ is odd} \\ n-2 & n \text{ is even} \end{cases}$$

$$= \begin{pmatrix} \ldots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \ldots \\ \ldots & -4 & 1 & -2 & 3 & 0 & 5 & 2 & 7 & \ldots \end{pmatrix}$$

$$= (\ldots 4\,2\,0\,{-2}\,{-4}\ldots)(\ldots {-1}\,1\,3\,5\,7\ldots)$$

is the product of two ∞-cycles ("chains").

Example 2.4.30 — Let

$$\mu_{2^\infty} = \bigcup_{n \geq 0} \mu_{2^n} = \mu_1 \cup \mu_2 \cup \mu_4 \cup \mu_8 \cup \ldots$$

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

$$\kappa = \begin{pmatrix} 1 & -1 & i & -i & \zeta & \zeta^3 & \zeta^5 & \zeta^7 & \xi & \ldots \\ 1 & -1 & -i & i & \zeta^3 & \zeta & \zeta^7 & \zeta^5 & \xi^3 & \ldots \end{pmatrix}$$

$$= (i\,-i)(\zeta\,\zeta^3)(\zeta^5\,\zeta^7)(\xi\,\xi^3\,\xi^9\,\xi^{11})(\xi^5\,\xi^{15}\,\xi^{13}\,\xi^7)\dots$$

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

$$\langle\sigma\rangle x = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{l-1}(x)\}.$$

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 $\varphi = \psi^{-1}$. $\square$

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

$$\text{``}\overline{2}\text{''} = (\overline{1}\,\overline{2}\,\overline{4})(\overline{3}\,\overline{6}\,\overline{5})$$

and

$$\text{``}\overline{3}\text{''} = (\overline{1}\,\overline{3}\,\overline{2}\,\overline{6}\,\overline{4}\,\overline{5})$$

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. □

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

$$o(ab) \mid \mathrm{lcm}(o(a), o(b)).$$

Proof. Write $n = o(a)$ and $m = o(b)$. Since a and b commute,

$$(ab)^{\mathrm{lcm}(n,m)} = a^{\mathrm{lcm}(n,m)} b^{\mathrm{lcm}(n,m)} = e.$$

Thus, by the Division Lemma, $o(ab) \mid \mathrm{lcm}(n, m)$. □

Remark 2.4.44. Note that this proof is identical to the first half of Proposition 1.6.18, except with $\mathrm{lcm}(n, m)$ in place of mn.

Note that $\gcd(n, m) = 1$ implies $\mathrm{lcm}(n, m) = nm$.

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

$$o(\sigma\tau) = \mathrm{lcm}(o(\sigma), o(\tau))$$

Proof. Write $n = o(\sigma)$ and $m = o(\tau)$. By the Proposition, we just have to prove that $\mathrm{lcm}(n, m) \leq o(\sigma\tau)$.

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. $\qquad\square$

> **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.** For $n \geq 3$, show that S_n must be generated by at least two elements. [That is, S_n is not cyclic.]

Chapter 3

Quotients and Morphisms

3.1 Normality and Quotients

We spent a lot of time in the first half of the course talking about groups in their own right, with a sharp focus on their elements and their subgroups.

In the second part, we turn our attention to how groups are related to other groups, how new groups are constructed from old ones, and how groups interact with other mathematical objects.

3.1.1 Recall...

Let H be a subgroup of G.

A *left coset* of H in G is a subset of the form

$$aH = \{ah : h \in H\}$$

where $a \in G$.

A *right coset* of H in G is a subset of the form

$$Ha = \{ha : h \in H\}$$

where $a \in G$.

Left cosets are precisely the equivalence classes of the *left coset relation*[†]: $a \sim b$ iff $b^{-1}a \in H$ iff $aH = bH$. The set of equivalence classes (a.k.a. left cosets) is denoted G/H.

> **Exercise 93.** The space of *right* cosets of H in G is denoted $H\backslash G$. What is the analogous equivalence relation, $Ha = Hb$ iff $... \in H$?

Remark 3.1.1. When we talk about "cosets" without specifying left or right, we always mean left cosets.

The significance of these relations being *equivalence* relations is that two cosets (of the same type) are either identical or disjoint—cosets cannot *partially* overlap.

[†]Originating from the orbits of the *right action of* H *on* G *by left multiplication.*

Finally, we record the trivial but highly useful observation that $aH = H$ if (and only if) $a \in H$. In particular, $eH = H$.

The notation for the coset space sometimes produces familiar objects.

> **Example 3.1.2** — Let $G = \mathbb{Z}$, $H = n\mathbb{Z}$, then G/H can be written as...
>
> $$\mathbb{Z}/n\mathbb{Z}!$$

> **Question** — Let $H \leq G$. When is the coset space G/H itself a group?

3.1.2 First examples

How do we put a group structure on G/H?

The elements of G/H are cosets. Although we could, in theory, put any old composition law on G/H, the operation on G/H *ought* to be *somehow* related to (or derived from) the operation on G.

How should we combine aH and bH? Well, the most naive way to interpret $(aH)(bH)$ is to view it as the set of all pairwise products of elements of aH with elements of bH, namely $\{ah_1bh_2 : h_1, h_2 \in H\}$.*

Let's see if that works.

> **Example 3.1.3** — Let $G = \mathbb{Z}$ and $H = 10\mathbb{Z}$. Consider the cosets $2 + 10\mathbb{Z}$ and $3 + 10\mathbb{Z}$. We have
>
> $$\begin{aligned}(2 + 10\mathbb{Z}) + (3 + 10\mathbb{Z}) &= \{\ldots, -8, 2, 12, \ldots\} + \{\ldots, -7, 3, 13, \ldots\} \\ &= \{\ldots, -15, -5, 5, 15, 25, \ldots\} \\ &= 5 + 10\mathbb{Z}\end{aligned}$$
>
> which looks just like the addition $[2] + [3] = [5]$ in $\mathbb{Z}/10\mathbb{Z}$.

> **Example 3.1.4** — Let $G = \mathbb{R}$ and $H = \mathbb{Z}$. Consider the cosets $-0.7 + \mathbb{Z}$ and $2.5 + \mathbb{Z}$. We have
>
> $$\begin{aligned}(-0.7 + \mathbb{Z}) + (2.5 + \mathbb{Z}) &= \{\ldots, -0.7, 0.3, 1.3, \ldots\} + \{\ldots, -0.5, 0.5, 1.5, \ldots\} \\ &= \{\ldots, -1.2, -0.2, 0.8, 1.8, 2.8, \ldots\} \\ &= 1.8 + \mathbb{Z}\end{aligned}$$

---

*After all, we already interpret aH that way.

which looks just like the addition $\{-0.7\} + \{2.5\} = \{1.8\}$ in $\mathbb{R}/\mathbb{Z}$.

Notice that, in both examples, the sum of two cosets is again a coset: the "coset of the sum".

Example 3.1.5 — Let $G = \mathbb{R}^\times$ and $H = \langle -1 \rangle$. Consider the cosets $\pi H = \{\pi, -\pi\}$ and $\sqrt{2}H = \{\sqrt{2}, -\sqrt{2}\}$. We have

$$(\pi H)(\sqrt{2}H) = \{\pi, -\pi\}\{\sqrt{2}, -\sqrt{2}\}$$
$$= \{\pi\sqrt{2}, -\pi\sqrt{2}\}$$
$$= \pi\sqrt{2}H.$$

Example 3.1.6 — Let $G = \mathbb{R}^\times$ and $H = (0, \infty)$. Consider the cosets $1H = H$ and $-1H = (-\infty, 0)$. We have

$$(1H)(-1H) = \{xy : x > 0, y < 0\} = \{z : z < 0\} = -1H$$

while

$$(-1H)(-1H) = \{xy : x < 0, y < 0\} = \{z : z > 0\} = 1H.$$

Notice that, in both examples, the product of two cosets is again a coset—the "coset of the product".

How about a non-abelian example?

Example 3.1.7 — Let $G = D_6$ and $H = \langle r^2 \rangle = \{e, r^2, r^4\}$. Consider the cosets $fH = \{f, fr^2, fr^4\}$ and $rH = \{r, r^3, r^5\}$. We have

$$(fH)(rH) = \{f, fr^2, fr^4\}\{r, r^3, r^5\}$$
$$= \{fr, fr^3, fr^5,$$
$$fr^3, fr^5, fr^7,$$
$$fr^5, fr^7, fr^9\}$$
$$= \{fr, fr^3, fr^5\}$$
$$= frH$$

and *again* we see that the product of cosets is the "coset of the product".

Our next and final example serves to dispel the hasty conclusion that multiplying cosets *always* works out.

> **Example 3.1.8** — Let $G = D_n$ for $n > 2$ and $H = \langle f \rangle = \{e, f\}$. Consider the cosets $rH = \{r, rf\} = \{r, fr^{-1}\}$ and $frH = \{fr, frf\} = \{fr, r^{-1}\}$. We have
>
> $$(rH)(frH) = \{r, fr^{-1}\}\{fr, r^{-1}\}$$
> $$= \{rfr, rr^{-1},$$
> $$fr^{-1}fr, fr^{-1}r^{-1}\}$$
> $$= \{f, e, r^2, fr^{-2}\}$$
>
> but this is *not* a coset of $H = \{e, f\}$—it's too big!

Exercise 94. Suppose $m = o(H)$. Show that $m \leq |(aH)(bH)| \leq m^2$.

3.1.3 When is $(aH)(bH)$ a coset of H?

In general, $(aH)(bH) = cH$ iff

$\subseteq$: for all h_1, h_2 in H there exists h_3 in H such that $ah_1 bh_2 = ch_3$,

and

$\supseteq$: for all h_3 in H there exist h_1, h_2 in H such that $ch_3 = ah_1 bh_2$.

If the product of cosets *is* a coset, which coset is it?

> **Lemma 3.1.9**
> Suppose $(aH)(bH) = cH$. Then $c \sim ab$, i.e., $cH = abH$.

Proof. Certainly $a \in aH$ and $b \in bH$, so $ab \in (aH)(bH)$. But if $(aH)(bH) = cH$, then there exists h in H such that $ab = ch$, in which case $cH = chH = abH$. $\qquad\square$

In other words, if the product of cosets, $(aH)(bH)$, *is* a coset of H, then it must be the "coset of the product", abH. So, when *do* we have the equality $(aH)(bH) = abH$?

> **Lemma 3.1.10**
> If $b^{-1}hb \in H$ for all h in H, then $(aH)(bH) = abH$.

Proof. We always have $(aH)(bH) \supseteq abH$ because $abh = (ae)(bh)$ for all $h \in H$. Therefore, the equality $(aH)(bH) = abH$ holds if and only if

$$(aH)(bH) \subseteq abH. \tag{1}$$

On the level of elements, (1) is equivalent to

$$\text{For all } h_1, h_2 \text{ in } H \text{ there exists } h_3 \text{ in } H \text{ such that } ah_1bh_2 = abh_3. \tag{2}$$

So, suppose it's true that $b^{-1}hb \in H$ for all h in H. Then, for all h_1, h_2 in H, we have

$$ah_1bh_2 = abb^{-1}h_1bh_2 = ab\underbrace{(b^{-1}h_1b)(h_2)}_{h_3}$$

so (2) holds, proving the Lemma. □

Remark 3.1.11. The expression $b^{-1}hb$ is an instance of *conjugation*, the act of operating on an object by an element on one side and its inverse on the other. If two objects are related by conjugation, then they are called *conjugates* (of each other).

Remember, our goal is to put a binary operation on the set G/H such that it becomes a group.

We've been attempting to use the most naive operation possible—$(aH)(bH) = \{ah_1bh_2 : h_1, h_2 \in H\}$—to achieve our goal.

The above Lemmas show that in order for coset multiplication to work for *all* cosets of H in G, we'd better have $b^{-1}Hb \subseteq H$ for all b in G.

> **Definition 3.1.12** — A subgroup H of a group G is called *normal* if $b^{-1}Hb \subseteq H$ for all b in G, in which case we write $H \trianglelefteq G$.[*]
>
> ———————
> [*]`\trianglelefteq`

We summarize the above investigations in the following Theorem.

> **Theorem 3.1.13**
> Let $H \trianglelefteq G$. Then G/H is a group under coset multiplication, called *the quotient group of G by H*.

Proof. By the Lemmas, coset multiplication is a binary operation on G/H. It's associative because

$$\big((aH)(bH)\big)(cH) = (abH)(cH) = (ab)cH$$
$$= a(bc)H = (aH)(bcH) = (aH)\big((bH)(cH)\big)$$

so it's a composition law. The identity is H itself: for all aH in G/H,

$$(aH)H = aH;$$

and the inverse of aH is $a^{-1}H$, because

$$(aH)(a^{-1}H) = aa^{-1}H = eH = H. \qquad \square$$

Exercise 95. The order of the group G/H is ...

Since H is always clear from context* it's common to write $\bar{a}$, instead of aH, for a typical element of the quotient group G/H.

> **Example 3.1.14 —** Every subgroup H of an abelian group G is normal, because $g^{-1}hg = hg^{-1}g = h$ for all h in H and g in G. In particular,
>
> 3.1.3 $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ for all n in $\mathbb{Z}$
>
> 3.1.4 $\mathbb{Z} \trianglelefteq \mathbb{R}$.
>
> 3.1.5 $\langle -1 \rangle \trianglelefteq \mathbb{R}^{\times}$.
>
> 3.1.6 $(0, \infty) \trianglelefteq \mathbb{R}^{\times}$.
>
> The corresponding quotient groups are
>
> 3.1.3 $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n ($\cong C_n$)
>
> 3.1.4 $\mathbb{R}/\mathbb{Z} = \mathbb{T}$, the "reals modulo 1" (Problem Set 1 Extra Problem 3a)
>
> 3.1.5 $\mathbb{R}^{\times}/\langle -1 \rangle$, the "unsigned" reals under multiplication ($\cong (0, \infty)$)
>
> 3.1.6 $\mathbb{R}^{\times}/(0, \infty) = \{(0, \infty), (-\infty, 0)\}$, the "group of signs" ($\cong C_2$)

Taking a quotient is kind of like ignoring the information encoded by the subgroup. In $\mathbb{Z}/10\mathbb{Z}$, we're ignoring everything but the ones digits. In $\mathbb{R}/\mathbb{Z}$, we're ignoring the integer parts and just focusing on the fractional parts. In $\mathbb{R}^{\times}/\langle -1 \rangle$, we're ignoring *signs*: $-\bar{x} = \bar{x}$ for all x. And in $\mathbb{R}^{\times}/(0, \infty)$, we're ignoring *magnitude*: $\overline{10^{100}} = \overline{10^{-100}} = \bar{1}$.

> **Example 3.1.15 —** Subgroups of *non*abelian groups are not necessarily normal:
>
> 3.1.7 $\langle r^2 \rangle \trianglelefteq D_6$ because $(fr^k)^{-1}r^2(fr^k) = r^{-2}$ for all $k \in \mathbb{Z}$, but
>
> 3.1.8 $\langle f \rangle \ntrianglelefteq D_n$ for $n > 2$ because $r^{-1}fr = fr^2 \notin \langle f \rangle$.
>
> The corresponding quotient group $D_6/\langle r^2 \rangle$ is isomorphic to D_2, because its order is 4—
>
> $$o(D_6/\langle r^2 \rangle) = [D_6 : \langle r^2 \rangle] = \frac{o(D_6)}{o(\langle r^2 \rangle)} = \frac{12}{3} = 4$$
>
> —and it's not cyclic—every element squares to the identity:
>
> $$\left(g\langle r^2 \rangle\right)^2 = g^2\langle r^2 \rangle = \langle r^2 \rangle$$

---

*It's right there in the notation G/H!

because $g^2 \in \langle r^2 \rangle$ whether g is a flip ($g^2 = e$) or a rotation ($g^2 = r^{2k}$).

Explicitly, we may write out the elements of $D_6/\langle r^2 \rangle$ in full as

$$\bar{e} = \langle r^2 \rangle = \{e, r^2, r^4\} \qquad \bar{r} = r\langle r^2 \rangle = \{r, r^3, r^5\}$$
$$\bar{f} = f\langle r^2 \rangle = \{f, fr^2, fr^4\} \qquad \overline{fr} = fr\langle r^2 \rangle = \{fr, fr^3, fr^5\}$$

Taking the quotient of a finite group by a (proper) nontrivial normal subgroup always yields a smaller (nontrivial) group. Although quotients may be "slippery" to work with, they are, in a certain sense, *simpler*.

3.1.4 Examples of normal subgroups

Example 3.1.16 — For any group G, the trivial subgroup 1 and the group G itself are always normal subgroups of G. If these are the *only* two normal subgroups of G, then G is called *simple*.[*] The quotients are $G/1 \cong G$ and $G/G \cong 1$ respectively. These are called the *trivial* normal subgroups of G, even though only 1 is called the *trivial* group!

---

[*]Alas, the trivial group (which is the *simplest* group) is not considered a *simple* group—for the same reason that 1 (which is the *first* number) is not considered a *prime* number.

Example 3.1.17 — Subgroups of abelian groups are normal.

Exercise 96. Are abelian subgroups of nonabelian groups normal?

Exercise 97. Are normal subgroups abelian?

Proposition 3.1.18

The normal subgroups of D_n are D_n, every subgroup of $\langle r \rangle$, and, just when n is even, $\langle r^2, f \rangle$ and $\langle r^2, fr \rangle$. The corresponding quotients are $D_n/D_n \cong 1$, $D_n/\langle r^k \rangle \cong D_k$ for each $k \mid n$, and $D_n/\langle r^2, f \rangle \cong D_n/\langle r^2, fr \rangle \cong C_2$.

Since $C_2 \cong D_1$, the Proposition may be summarized as saying "quotients of dihedral groups are dihedral". We omit the proof for now.

Exercise 98. Show that quotients of cyclic groups are cyclic.

> **Example 3.1.19 —**
>
> $$V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle = \{\epsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
>
> is a normal subgroup of S_4 because conjugation preserves cycle type, and V contains all possible double-transpositions in S_4. The quotient S_4/V has order $4!/4 = 6$, so it's either D_3 or C_6. It cannot be cyclic because S_4 has no elements of order 6, so it must be D_3.

> **Exercise 99** (PS1XQ3b)**.** Show that every proper subgroup of the quaternion subgroup $Q = \langle i, j, k \rangle$ is normal in Q.* What are the possible quotients of Q?
>
> ---
>
> *Recall that i, j, k are the unit quaternions satisfying $i^2 = j^2 = k^2 = ijk = -1$.

> **Exercise 100.** Show that subgroups of index 2 are normal.

> **Example 3.1.20 —** $Z(G)$ is a normal subgroups of G.

> **Example 3.1.21 —** Automorphisms of the form $c_g(x) = gxg^{-1}$ are called *inner*; automorphisms *not* of this form are called *outer*.* Inner automorphisms constitute a normal subgroup of $\mathrm{Aut}(G)$ [Why?]; the quotient is denoted $\mathrm{Out}(G)$.
>
> ---
>
> *Some jokesters like to abbreviate "outer automorphism" to "outermorphism".

> **Exercise 101.** What's an outer automorphism of $\mathbb{Z}$? Of $\mathbb{Z}/n\mathbb{Z}$?

3.1.5 Lingering questions

Let $H \leq G$. We tried to put a natural group structure on G/H (the set of left cosets of H in G), and it *worked*—but only after making the additional assumption that H was *normal* in G, i.e.,

$$g^{-1}hg \in H \text{ for all } h \text{ in } H \text{ and } g \text{ in } G.$$

This raises a few questions.

1. What about right cosets?

2. Is normality necessary?

3. What's normality all about?

1. Right cosets?

Let's start with 1.

Had we worked with right cosets instead of left ones, Lemma 3.1.10 would have said $(Ha)(Hb) = Hab$ if $aha^{-1} \in H$ for all h in H, because

$$h_1ah_2b = h_1ah_2a^{-1}ab = \underbrace{(h_1)(ah_2a^{-1})}_{\in H}ab.$$

And in order for the multiplication to have worked for *all* cosets, we would have required H to satisfy

$$aha^{-1} \in H \text{ for all } h \text{ in } H, \text{ for all } a \text{ in } G$$

or, more succinctly,

$$aHa^{-1} \subseteq H \text{ for all } a \text{ in } G.$$

This is *equivalent* to normality as previously defined, because $(a^{-1})^{-1} = a$.

So, using right cosets instead of left ones doesn't change the required "normality" condition. But, does it change the group?

Proposition 3.1.22 (Equality of Left and Right Cosets)

If $H \trianglelefteq G$, then $aH = Ha$ for all a in G.

Proof. Suppose H is normal. To show $aH = Ha$ we must show

$$\text{for all } h_1 \text{ in } H \text{ there exists } h_2 \text{ in } H \text{ such that } ah_1 = h_2a$$

and vice versa. This is accomplished using the identities

$$ah_1 = \underbrace{ah_1a^{-1}}_{\in H}a \quad \text{and} \quad h_2a = a\underbrace{a^{-1}h_2a}_{\in H}$$

where both underbraced elements are in H because H is normal. $\qquad\square$

> **Exercise 102.** Show that the converse holds, namely, that if $Ha = aH$ for all a in G, then H is normal.

So, using right cosets instead of left ones doesn't change the group elements. And it doesn't change the group operation, either, as the following Corollary shows.

Corollary 3.1.23

If $H \trianglelefteq G$, then $(aH)(bH) = (Ha)(Hb)$ for all a, b in G.

Proof. $(aH)(bH) = abH = Hab = (Ha)(Hb)$. $\qquad\square$

In short, if H is normal, then $H\backslash G = G/H$. ¯_(ツ)_/¯

2. Normality—needed?

Next, 2. Is normality necessary? Well, if we want the product of any two cosets to be a coset, then H has to be normal.

> **Lemma 3.1.24**
>
> Let $H \leq G$. If $(aH)(bH) \in G/H$ for all a, b in G, then $H \trianglelefteq G$.

Proof. We know from last lecture that if $(aH)(bH)$ is a coset, then it must be the coset abH. In particular, for all a in G,

$$(aH)(a^{-1}H) = aa^{-1}H = eH = H.$$

Thus if $h \in H$ and $a \in G$, then $aha^{-1} = (ah)(a^{-1}e) \in H$. $\qquad\square$

3. Normality—what?

Finally, 3. What's normality all about?

The key idea is *conjugacy*.

In general, any expression involving g on one side and g^{-1} on the other is an instance of conjugation. For example, x and gxg^{-1} (as well as $g^{-1}xg$) are *conjugate elements*. Similarly, H and gHg^{-1} are *conjugate subgroups*.

Informally, conjugacy can be seen as a "change in perspective", and, loosely speaking, normal subgroups are the ones which look the same from all "points of view".

> **Example 3.1.25** — Let $\sigma = (1\ 2\ 3)(4\ 5) \in S_5$ and let
>
> $$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$
>
> Which permutation is $\gamma\sigma\gamma^{-1}$?
>
> Well, $\gamma^{-1}(1) = 5$, $\sigma(5) = 4$, and $\gamma(4) = 2$, so $\gamma\sigma\gamma^{-1}(1) = 2$. Similarly,
>
> $$2 \xmapsto{\gamma^{-1}} 4 \xmapsto{\sigma} 5 \xmapsto{\gamma} 1$$
>
> so $\gamma\sigma\gamma^{-1}(2) = 1$. Continuing in this manner, we get
>
> $$\gamma\sigma\gamma^{-1} = (1\ 2)(3\ 5\ 4).$$

So what? Well, with a little rewriting...

$$\gamma\sigma\gamma^{-1} = (1\ 2)(3\ 5\ 4) = (5\ 4\ 3)(2\ 1)$$

which looks exactly like $\sigma = (1\ 2\ 3)(4\ 5)$ but with the letters replaced by their images under γ.

Proposition 3.1.26

For all k-cycles and all γ's,

$$\gamma(a_1\ \ldots\ a_k)\gamma^{-1} = (\gamma(a_1)\ \ldots\ \gamma(a_k))$$

Proof. Exercise. $\square$

Combined with the fact that conjugation is an automorphism [PS2Q2], we know that conjugation maps products of cycles to products of relabelled cycles, so conjugacy in S_n amounts to *relabelling*.

In fact, the converse of this statement is true:

Proposition 3.1.27

If σ and τ have the same cycle type, they are conjugate in S_n!

Proof. This is PS4XQ6c). [*Hint*: Try to find a "relabeller" δ that relabels cycles in σ to cycles in τ.] $\square$

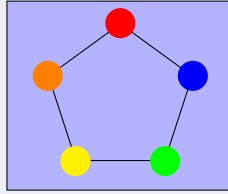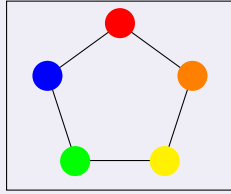Together, we know that two elements in S_n are conjugate iff they have the same cycle type.

> **Exercise 103.** Show that the above is not necessarily true in subgroups of S_n.

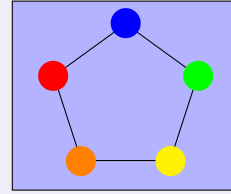> **Exercise 104.** Is the above result true in S_∞? What about in $S_\mathbb{R}$?

Example 3.1.28 — In D_n,
$$frf^{-1} = frf = r^{-1}.$$

In other words, observing a clockwise rotation from behind makes it look like a counterclockwise rotation.
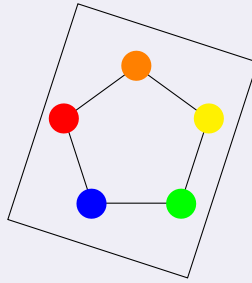
from behind   after a rotation(still behind)

Similarly,
$$rfr^{-1} = fr^{-2},$$
which means that observing a flip with your head tilted makes it look like a flip over a tilted axis.
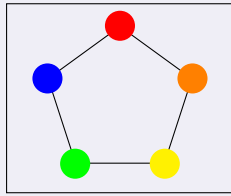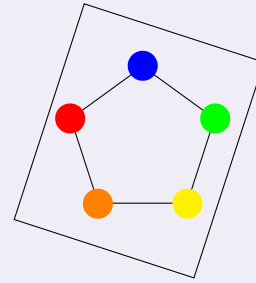
tilting your head   watching someone flip

Example 3.1.29 (Change of Basis) — Let V be a vector space with two bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$. Every vector x in V can be uniquely written as a linear combination of basis vectors:
$$x = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$
where $a_1, \ldots, a_n$ are scalars. In other words, x corresponds to the vector $(a_1 \ \ldots \ a_n)^\top$ with respect to the basis $v_1, \ldots, v_n$. To express x in terms of the basis $w_1, \ldots, w_n$, we first express each v_i:
$$v_i = \sum_{j=1}^{n} b_{ij} w_j$$

Then
$$x = \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} a_i \sum_{j=1}^{n} b_{ij} w_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_i b_{ij} \right) w_j =: \sum_{j=1}^{n} a_j' w_j$$

so that x corresponds to the vector $(a_1' \ \ldots \ a_n')^\top$ with respect to the basis $w_1, \ldots, w_n$.

Thus, "change of coordinates" is given by the formula

$$\begin{pmatrix} a_1' \\ \vdots \\ a_n' \end{pmatrix} = \begin{bmatrix} b_{11} & \dots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{1n} & \dots & b_{nn} \end{bmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

or, briefly, $(a_i') = B(a_i)$ where B is the *change of basis* matrix.
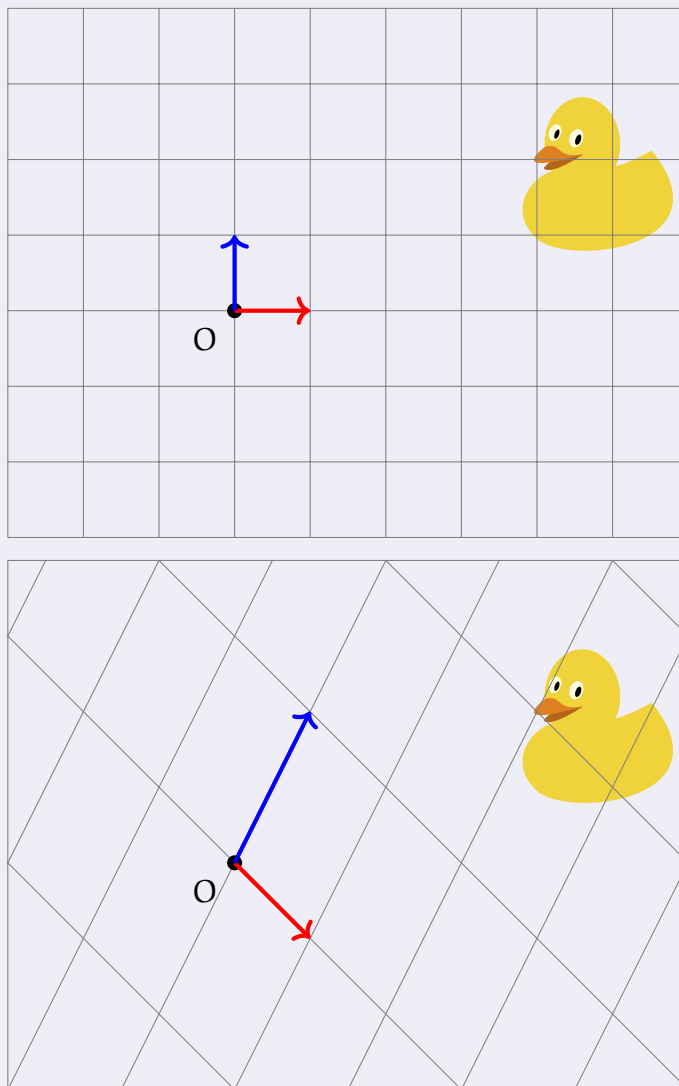
For example, if we wish to go from the "default" basis $v_1 = (1, 0)$, $v_2 = (0, 1)$ to the "custom" basis $w_1 = (1, -1)$, $w_2 = (1, 2)$, we can use the change of basis matrix:

$$B = \frac{1}{3} \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}.$$

The duck's beak lies at the tip of the vector $4v_1 + 2v_2$, which is $(4\ 2)^\mathsf{T}$ w.r.t. "default" coordinates. Where's the duck's beak w.r.t. "custom" coordinates?

$$\frac{1}{3}\begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}\begin{pmatrix} 4 \\ 2 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 8-2 \\ 4+2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

Indeed, one can check directly that $4v_1 + 2v_2 = 2w_1 + 2w_2$. So far, so good.

Now imagine we have a linear operator* T on V, given by some matrix T_{old} w.r.t. the first basis $v_1, \ldots, v_n$. To represent T completely in terms of the second basis $w_1, \ldots, w_n$, we need a matrix T_{new} which

(1) accepts input in new coordinates,

(2) changes it back to old coordinates,

(3) performs the operation of T_{old}, and

(4) returns an answer in new coordinates.

In other words,

$$T_{new} = BT_{old}B^{-1}$$

is the *conjugate* of T_{old} by B.

For example, let T be a 90-degree counterclockwise rotation. In the "default" basis, the matrix of T is

$$T_{old} = \begin{bmatrix} \cos\frac{\pi}{2} & -\sin\frac{\pi}{2} \\ \sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

We can express T entirely in the "custom" basis by conjugating T_{old} by B:

$$T_{new} = BT_{old}B^{-1} = \frac{1}{3}\begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & -5 \\ 2 & -1 \end{bmatrix}.$$

Thus, revolving the duck about the origin moves the tip of its beak to

$$\frac{1}{3}\begin{bmatrix} 1 & -5 \\ 2 & -1 \end{bmatrix}\begin{pmatrix} 2 \\ 2 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 2-10 \\ 4-2 \end{pmatrix} = \begin{pmatrix} -8/3 \\ 2/3 \end{pmatrix}.$$

The duck leaves.

*"Linear operator" is to "endomorphism" as "linear transformation" is to "homomorphism".
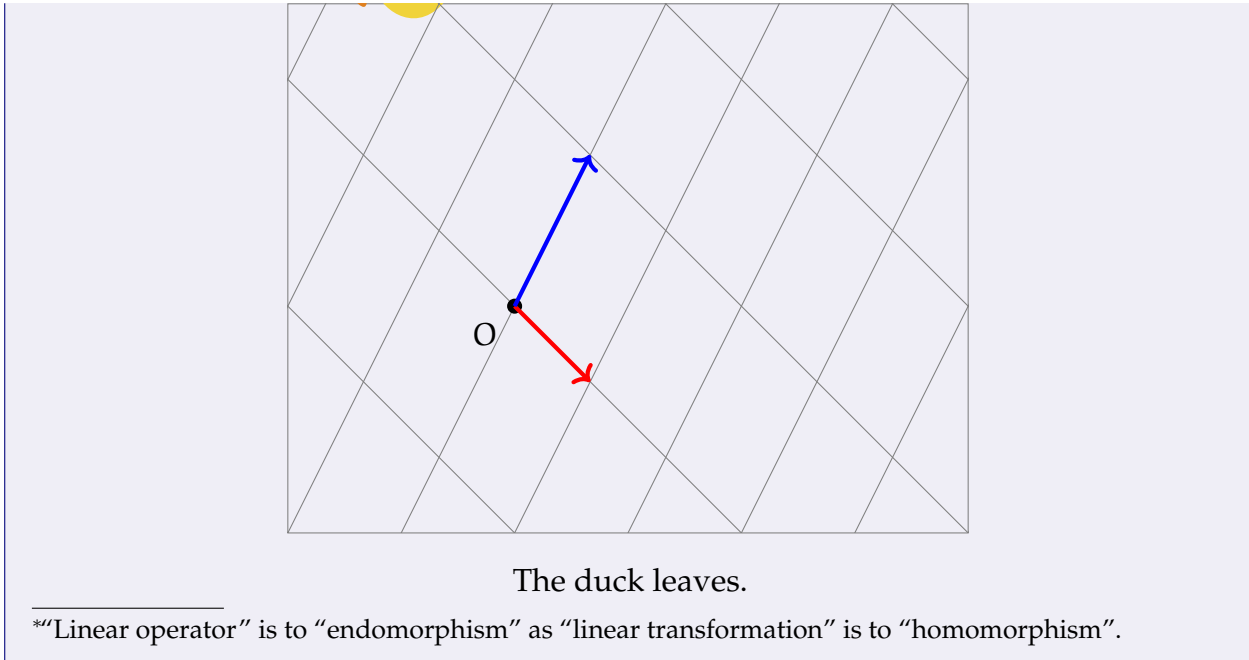
Conjugacy as automorphism

For each g in G, the function $c_g(x) = gxg^{-1}$ is an automorphism of G. [This is PS2Q2.] If G is abelian, then $c_g(x) = gxg^{-1} = gg^{-1}x = ex = x$ for all x in G, so each c_g is the identity map—conjugation doesn't *do* anything. So, conjugation is only interesting in the nonabelian setting.

Like any automorphism, conjugation moves subgroups to other subgroups. [Why?] Since every subgroup contains e, the distinct conjugates of a given subgroup always overlap.*

For example, here are the conjugates of $\langle f \rangle$ in D_3 and of $\langle r^3, f \rangle$ in D_6:
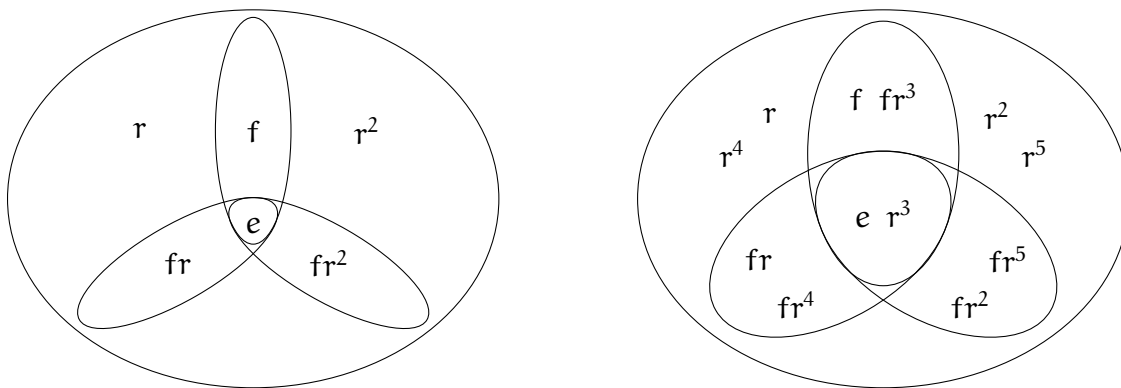
Meanwhile, $\langle r^2, f \rangle \trianglelefteq D_4$, so all its conjugates are itself:

*Do not confuse conjugates and cosets. The distinct cosets of a given subgroup *never* overlap.
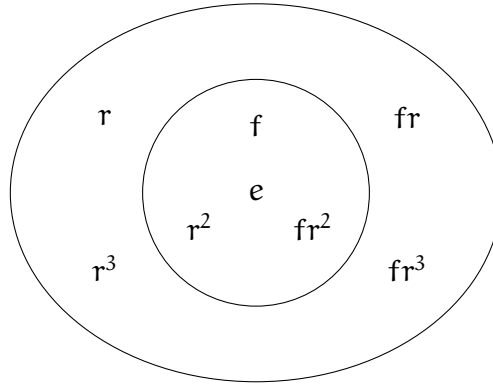
The next Proposition proves that the final picture is accurate—normal subgroups are *self-conjugate*.

> **Proposition 3.1.30**
> Let $H \trianglelefteq G$. Then $gHg^{-1} = H$ for all g in G.

Proof. Exercise. [Show that $H \subseteq gHg^{-1}$ for all g in G.] $\qquad\square$

Exercise 105. Let $H \leq G$ and let $f \in \mathrm{Aut}(G)$ such that $f(H) \leq H$. Is it necessarily true that $f(H) = H$?

[Hard] Let $H \leq G$ and let $g \in G$ such that $gHg^{-1} \leq H$. Is it necessarily true that $gHg^{-1} = H$?

3.1.6   Summary of normality

We summarize our findings in this handy theorem:

> **Theorem 3.1.31**
> Let G be a group and let $H \leq G$. The following are equivalent.
>
>   1. $H \trianglelefteq G$. That is, $gHg^{-1} \subseteq H$ for all g in G.
>
>   2. $gH = Hg$ for all g in G.
>
>   3. G/H is a group under coset multiplication.
>
>   4. H is self-conjugate: $gHg^{-1} = H$ for all g in G.

3.2 Morphisms

3.2.1 Motivation

> **Question —** We've been using the idea of *isomorphisms*, which are bijective maps between groups that preserve the group structure.
>
> Instead of adding conditions to form new concepts, let's remove a condition for once—what if we don't require the map to be bijective?

> **Example 3.2.1 —** For any group G with a normal subgroup $H \trianglelefteq G$, we may consider the coset map
>
> $$f : G \to G/H, g \mapsto gH.$$
>
> This map, as we showed, preserves group structure—$f(ab) = abH = aHbH = f(a)f(b)$. However, it is not bijective when H is nontrivial.

Let's start by introducing the fundamental concept underpinning the rest of the course:

> **Definition 3.2.2 —** Let G and H be groups with composition laws $\cdot_G$ and $\cdot_H$ respectively. A function $f : G \to H$ is called a *homomorphism* if
>
> $$f(a \cdot_G b) = f(a) \cdot_H f(b)$$
>
> for all a, b in G.

Remark 3.2.3. As with isomorphisms, in the future we will simply write

$$f(ab) = f(a)f(b)$$

if no further information is given.

Remark 3.2.4. If G and H are written *additively*, we instead write

$$f(a + b) = f(a) + f(b).$$

If G is written multiplicatively, and H additively:

$$f(ab) = f(a) + f(b).$$

And if G is written additively, and H multiplicatively:

$$f(a + b) = f(a)f(b).$$

Remark 3.2.5. Being a homomorphism is like the commutativity of the operations "compose" and "send":

- first compose, then send: $(a, b) \to ab \to f(ab)$
- first send, then compose: $(a, b) \to (f(a), f(b)) \to f(a)f(b)$

3.2.2 Concrete examples

Example 3.2.6 — The magnitude of a complex number defines a homomorphism

$$|\cdot| : \mathbb{C}^\times \to \mathbb{C}^\times$$

because

$$|zw| = |z||w|$$

for all z, w in $\mathbb{C}$. [Write $z = a + ib$, $w = c + id$ and use $|u + iv| = \sqrt{u^2 + v^2}$.]

Example 3.2.7 — For any positive real base β, the function

$$x \mapsto \beta^x$$

is a homomorphism $\mathbb{R} \to \mathbb{R}^\times$:

$$\beta^{x+y} = \beta^x \beta^y$$

for all x, y in $\mathbb{R}$.

Example 3.2.8 — The interval $\mathbb{R}_{>0} := (0, \infty)$ is a subgroup of $\mathbb{R}^\times$. [What is its index?]
For any real exponent α, the function

$$x \mapsto x^\alpha$$

is a homomorphism $\mathbb{R}_{>0} \to \mathbb{R}_{>0}$:

$$(xy)^\alpha = x^\alpha y^\alpha \text{ for all } x, y > 0.$$

Example 3.2.9 — The logarithm (to any positive real base $\beta \neq 1$) is a homomorphism
$\mathbb{R}_{>0} \to \mathbb{R}$ because
$$\log_\beta(xy) = \log_\beta x + \log_\beta y$$
for all $x, y > 0$. [Can you find an extension $\mathbb{R}^\times \to \mathbb{R}$?]

Example 3.2.10 — The trace and determinant satisfy

$$\text{tr}(A + B) = \text{tr}\, A + \text{tr}\, B \quad \text{and} \quad \det(AB) = \det A \det B$$

making them homomorphisms $M_n(\mathbb{R}) \to \mathbb{R}$ and $GL_n(\mathbb{R}) \to \mathbb{R}^\times$.

Example 3.2.11 — Let C^∞ be the group of smooth* functions on $\mathbb{R}$ under addition. Then the derivative

$$f \mapsto \frac{df}{dx}$$

and the antiderivative

$$f \mapsto F(x) = \int_a^x f(t)\, dt$$

(for any fixed a) are homomorphisms $C^\infty \to C^\infty$.

------

*i.e., infinitely differentiable

Example 3.2.12 — The group $\mathbb{Z}/n\mathbb{Z}$ of congruence classes modulo n admits a natural homomorphism from $\mathbb{Z}$, namely the "class of" function!

$$[\cdot]_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

That's because

$$[a + b] = [a] + [b]$$

for all a, b in $\mathbb{Z}$.

Example 3.2.13 — Let n, m be positive integers such that $m \mid n$. Then the function

$$\mu_n \to \mu_m$$
$$\zeta \mapsto \zeta^{n/m}$$

is a homomorphism. [Why is it well-defined? Show that primitive roots get mapped to primitive roots.]

Example 3.2.14 — Let G be a dihedral group. Then the function $i_r : G \to \mu_2$ which is $+1$ on rotations and -1 on flips is a homomorphism, because

- two rotations make a rotation: $(+1)(+1) = +1$

- two flips make a rotation: $(-1)(-1) = +1$

- a flip and a rotation make a flip: $(-1)(+1) = -1$.

Exercise 106. Is the map i_f that is $+1$ on flips and -1 on rotations a homomorphism?

Alright, alright—homomorphisms are everywhere. What about them?

3.2.3 Terminology

Definition 3.2.15 — The familiar properties of general functions (injectivity, surjectivity, etc.) take on new names and (sometimes) notations in the context of homomorphisms:

function	homomorphism	
injection	monomorphism	$\hookrightarrow$
injective	monic	
surjection	epimorphism	$\twoheadrightarrow$
surjective	epic	
bijection	isomorphism	$\xrightarrow{\sim}$
bijective	-	
self-map	endomorphism	
permutation	automorphism	
constant	trivial	

Remark 3.2.16. The words "monic" and "epic" are problematic: "monic" already means something else*, and "epic" is silly. For these reasons, we'll stick to the long forms.
Remark 3.2.17. You'd think that the term corresponding to "bijective" would be "isomorphic", but it's not. It's the *domain* and *codomain* which are "isomorphic" (to each other) if the map between them is an isomorphism.

The two most important words concerning homomorphisms are "image" and "kernel".

Definition 3.2.18 — Let $f : G \to H$ be a homomorphism. The *image* of f is the set

$$\operatorname{im} f = \{f(a) : a \in G\}$$

---

*A polynomial is said to be *monic* if its leading coefficient is 1.

and the *kernel* of f is the set

$$\ker f = \{a \in G : f(a) = e\}.$$

Like any function, a homomorphism is surjective iff if its image equals its codomain. But *unlike* arbitrary functions, the injectivity of homomorphisms is extremely easy to assess:

> **Proposition 3.2.19**
>
> A homomorphism is injective iff its kernel is trivial.

We'll prove this later. Let's see some examples first!

Exercise 107. Complete the following table.

morphism	domain $\to$ codomain	mono-	epi-	iso-	endo-	auto-
$\lvert \cdot \rvert$	$\mathbb{C}^\times \to \mathbb{C}^\times$					
x^α	$\mathbb{R}_{>0} \to \mathbb{R}_{>0}$					
β^x	$\mathbb{R} \to \mathbb{R}^\times$					
$\log_\beta$	$\mathbb{R}_{>0} \to \mathbb{R}$					
tr	$M_n(\mathbb{R}) \to \mathbb{R}$					
det	$GL_n(\mathbb{R}) \to \mathbb{R}^\times$					
d/dx	$C^\infty \to C^\infty$					
$\int_a dt$	$C^\infty \to C^\infty$					
$[\cdot]_n$	$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$					
$\zeta^{n/m}$	$\mu_n \to \mu_m$					
i_r	$D_n \to \mu_2$					

[*Hint*: Some of these may depend on the values of the constants involved.]

3.2.4 Properties of morphisms

> **Proposition 3.2.20**
>
> i) The composition of two injective (resp. surjective, bijective) homomorphisms is again an injective (resp. surjective, bijective) homomorphism.
>
> ii) The inverse of an *invertible* homomorphism is a homomorphism.

Proof.

i) That the functional properties are preserved was proved in Exercise 9. As for the homomorphic properties, well, suppose f and g are homomorphisms and let a and b

be in G. Then
$$f\big(g(ab)\big) = f\big(g(a)g(b)\big) = f\big(g(a)\big)f\big(g(b)\big)$$
which shows that fg is a homomorphism.

ii) This is done in Exercise 40. [Why?] □

Exercise 108. Is "G is related to H if there is a homomorphism $G \to H$" an equivalence relation?

The multiplicative property of homomorphisms,
$$f(ab) = f(a)f(b),$$
which can be viewed as "commutativity" with composition, implies a similar "commutativity" with identity and inversion.

Exercise 109. Let G and H be groups with identity elements e_G and e_H respectively, and let $f : G \to H$ be a homomorphism. Then

i) $f(e_G) = e_H$

ii) $f(x^{-1}) = f(x)^{-1}$ for all x in G.

Example 3.2.21 (Trivial map) — There is only one possible constant homomorphism, called the *trivial map*: $f(x) = e$ for all x in G. This *is* actually a homomorphism, because $f(xy) = e$ while $f(x)f(y) = e^2 = e$.

Corollary 3.2.22

Let $f : G \to H$ be a homomorphism of groups. Then the image

$$\text{im } f = f(G) = \{f(x) : x \in G\}$$

is a subgroup of H, and the kernel

$$\ker f = f^{-1}(e) = \{x \in G : f(x) = e\}$$

is a subgroup of G. In short, im $f \le H$ and ker $f \le G$.

Proof. Fill in the blanks:

im f is not empty because ...
and if $f(a), f(b) \in$ im f then ...

ker f is not empty because ...
and if $a, b \in$ ker f then ... □

Example 3.2.23 — The image and kernel of $|\cdot| : \mathbb{C}^\times \to \mathbb{C}^\times$ are

$$\mathbb{R}_{>0} = (0, \infty) \text{ and } S^1 = \{z \in \mathbb{C} : |z| = 1\}$$

respectively.

Example 3.2.24 — The image and kernel of $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ are

$$\mathbb{R}^\times \text{ and } \mathrm{SL}_n(\mathbb{R})$$

respectively.

Example 3.2.25 — The derivative map on C^∞ is surjective with nontrivial kernel (constant functions), while the antiderivative map

$$f \mapsto F(x) = \int_a^x f(t)\, dt$$

is injective with proper image (functions that evaluate to zero at a).

Corollary 3.2.26

A homomorphism is injective iff its kernel is trivial.

Proof. Let f be a homomorphism.

Suppose f is injective. If $x \in \ker f$ then $f(x) = e = f(e)$, so $x = e$. Thus $\ker f = \{e\}$.

Now suppose $\ker f = \{e\}$. If $f(x) = f(y)$ then $f(xy^{-1}) = f(x)f(y)^{-1} = e$, so $xy^{-1} \in \ker f$. But the only thing in there is e, so $xy^{-1} = e$, whence $x = y$. Thus f is injective. $\qquad\square$

Exercise 110. Let $f : G \twoheadrightarrow H$ be an epimorphism with finite kernel and let $y \in H$. Show that the number of solutions x in G to the equation

$$f(x) = y$$

is independent of y. What is that number?

Now that we know $\mathrm{im}\, f$ is a group, we can record a few important observations.

Every homomorphism is an epimorphism onto its image:

$$f_1 : G \twoheadrightarrow f(G)$$

In particular, every monomorphism

$$f_2 : G \hookrightarrow H$$

yields an isomorphism onto its image:

$$f_3 : G \xrightarrow{\sim} f_2(G)$$

For this reason, monomorphisms are also called *embeddings*.

The notion of embedding is a generalization of the notion of subgroup: if $H \leq G$, then the inclusion map $f : H \to G$, $f(x) = x$, is an embedding.

> **Example 3.2.27 —** We may restate Cayley's Theorem in Theorem 2.4.9 as:
>
> Let G be a group. For each g in G, let $f_g(x) = gx$. Then the function $F(g) = f_g$ is an embedding
> $$G \hookrightarrow \mathrm{Sym}(G).$$

Exercise 111. Which of the following inclusions hold?

a) $S_8 \hookrightarrow S_9$

b) $D_4 \hookrightarrow S_8$

c) $D_4 \hookrightarrow S_9$

d) $\mu_{99} \hookrightarrow \mu_{199}$

e) $S_2 \hookrightarrow C_3$

f) $\mathbb{Z} \hookrightarrow \mathbb{Z}/14\mathbb{Z}$

g) $\mathbb{Z}/14\mathbb{Z} \hookrightarrow \mathbb{Z}$

h) $\mathbb{Z} \hookrightarrow S_\infty$

3.3   Quotients v. Morphisms

The single most important source of normal subgroups is: kernels of homomorphisms.

> **Proposition 3.3.1**
> Kernels of homomorphisms are normal.

Proof. Let $f : G \to H$ be a homomorphism. For each k in $\ker f$ and each g in G, we have $gkg^{-1} \in \ker f$ because

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)f(g)^{-1} = e. \qquad \square$$

> **Example 3.3.2 —**
>
> $$\ker \det = \mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$$
> $$\ker i_r = \langle r \rangle \trianglelefteq D_n$$

Exercise 112. Are *images* of homomorphisms normal?

Since $\ker f$ is normal, we can take the quotient $G/\ker f$. What could it be?

The connection between homomorphisms and quotient groups is given by the so-called *First Isomorphism Theorem*.

> **Theorem 3.3.3**
> If $f : G \to H$ is a homomorphism then $G/\ker f \cong \operatorname{im} f$.

Proof. Let $K = \ker f$. Define a map $\widetilde{f} : G/K \to H$ by $\widetilde{f}(aK) = f(a)$. This is going to be our isomorphism.

$\widetilde{f}$ is well-defined: If $aK = bK$, then $ab^{-1} \in K$ and so $f(a)f(b)^{-1} = f(ab^{-1}) = e$, so $f(a) = f(b)$. Thus the definition of $\widetilde{f}$ is unambiguous.

$\widetilde{f}$ is a homomorphism:

$$\widetilde{f}\big((aK)(bK)\big) = \widetilde{f}\big(abK\big) = f(ab) = f(a)f(b) = \widetilde{f}(aK)\widetilde{f}(bK).$$

$\widetilde{f}$ is injective: If $\widetilde{f}(aK) = e$ then $f(a) = e$, so $a \in \ker f = K$, and so $aK = K$ is the identity element of G/K. Thus $\ker \widetilde{f} = \{K\}$ is trivial.

$\operatorname{im} \widetilde{f} = \operatorname{im} f$: By construction, $\widetilde{f}(aK) = f(a)$ for all a in G, so every value of $\widetilde{f}$ is a value of f, and vice versa.

Finally, since every monomorphism is an isomorphism onto its image (just as every injection is a bijection onto its image), we have that

$$\widetilde{f} : G/\ker f \overset{\sim}{\longrightarrow} \operatorname{im} \widetilde{f} = \operatorname{im} f.$$

In other words,
$$G/\ker f \cong \operatorname{im} f. \qquad \square$$

The following diagram summarizes the situation in the proof of the First Isomorphism Theorem. [Remember this from Tutorial 1?]

$$G / \ker f$$

The first isomorphism theorem gives you lots of cool isomorphisms for free!

Example 3.3.4 — Concluding our previous example,

$$GL_n(\mathbb{R}) / SL_n(\mathbb{R}) \cong \operatorname{im} \det = \mathbb{R}^\times,$$
$$D_n / \langle r \rangle \cong \operatorname{im} i_r = \mu_2$$

Beyond these examples, we also can get extra isomorphisms even if we already knew the subgroup is normal:

$$\mathbb{C}^\times / S^1 \cong \mathbb{R}_{>0},$$
$$C^\infty / \mathbb{R}^\times \cong C^\infty / \{f(x) = c : c \in \mathbb{R}^\times\} \cong C^\infty,$$
$$C^\infty / \{f(x) = 0\} \cong \{f(x) \in C^\infty : f(a) = 0\}.$$

Exercise 113. Let $f : G \to H$ be a homomorphism and suppose G is finite. Show that

$$o(G) = o(\operatorname{im} f) o(\ker f).$$

Remark 3.3.5. Strange stuff can happen when G is infinite, like $G/H \cong G$ for nontrivial H!

Of course, we can also go the other way around: If we have an isomorphism $\widetilde{f} : G/K \cong H$, we can construct the homomorphism

$$f : G \to H, g \mapsto \widetilde{f}(gK).$$

Like we did in the beginning example of this section.

Exercise 114. What are the *endomorphisms* of $\mathbb{Z}$? of $\mathbb{Z}/n\mathbb{Z}$?

Example 3.3.6 — Vector spaces are abelian groups under addition, and the first isomorphism theorem from group theory can be used to give a neat proof of the rank-nullity theorem from linear algebra.

Let V and W be vector spaces and let $T : V \to W$ be a linear map. The image of T is a subspace of W, while the kernel of T is a subspace of V. Their respective dimensions are referred to as the *rank* and *nullity* of T. The rank–nullity theorem says that these

numbers always add up to the dimension of the domain, i.e.

$$\dim \operatorname{im} \mathsf{T} + \dim \ker \mathsf{T} = \dim \mathsf{V}$$

According to the first isomorphism theorem,

$$\mathsf{V}/\ker \mathsf{T} \cong \operatorname{im} \mathsf{T}$$

as *abelian groups*. It's not hard to show that $\mathsf{V}/\ker \mathsf{T}$ is actually a vector space, and that $\widetilde{\mathsf{T}}$ is actually a linear map. Thus

$$\mathsf{V}/\ker \mathsf{T} \cong \operatorname{im} \mathsf{T}$$

as *vector spaces*. In particular,

$$\dim \left(\mathsf{V}/\ker \mathsf{T} \right) = \dim \operatorname{im} \mathsf{T}. \tag{*}$$

But $\dim(\mathsf{V}/\mathsf{U}) = \dim \mathsf{V} - \dim \mathsf{U}$ for any subspace U of V, so by rearranging (*) the rank–nullity theorem follows.

3.4   The Alternating Group

Recall that a *permutation group* is any subgroup of a symmetric group.

The most important permutation groups are the *alternating* groups A_n. It takes a bit of work to construct it, so let's get to it.

3.4.1   The parity of a permutation

As we've seen, the cycle type is a useful *invariant* of a permutation—although knowing the cycle type doesn't determine the permutation, it can at least be used to tell two permutations apart.

A much cruder invariant of a permutation is its *sign*, or *parity*. We'll define it in just a minute, but basically we can split up permutations according to whether they're "even" or "odd" (their parity). The sign of a permutation is 1 if it's even, and -1 if it's odd.[*] Recall that a transposition is a permutation that moves only two letters. Transpositions are precisely the 2-cycles $(a\ b)$ where $a \neq b$.[†]

We've shown that we can write any permutation as a product of (nondisjoint) transpositions. In fact, there are infinitely many ways to write a given permutation as a product of transpositions. So, what good is this?

---

[*]The parity is "crude" in comparison to the cycle type because there are only two possible parities compared to several possible cycle types.

[†]This assumption of distinctness is *always* implicit when we talk about cycles having a certain form.

> **Lemma 3.4.1**
>
> Let $\sigma \in S_n$. If
> $$\sigma = \tau_1 \dots \tau_k = \rho_1 \dots \rho_l$$
> are two decompositions of σ into transpositions, then k and l have the same parity [as integers].

Proof. Given σ, consider the following map

$$f_\sigma : A \mapsto A_\sigma$$

where the ith row of A is moved the $\sigma(i)$th row of A_σ. This is a bijective map because $f_{\sigma^{-1}}$ is its two-sided inverse.

Since σ can be written as *a* product of transpositions, we can regard f_σ as a series of row swaps $\tau_1 \dots \tau_k$ on A. Now swapping two rows flips the signs of $\det A$, so $\det A_\sigma = (-1)^k \det A$. But we get the same A_σ through the row swaps $\rho_1 \dots \rho_l$! So we can conclude that $(-1)^k = (-1)^l$ and so k and l are either both even or both odd. $\square$

This lemma allows us to make the following definition.

> **Definition 3.4.2** — The *parity* of a permutation σ is the parity of the number of factors in any decomposition of σ into transpositions. Explicitly, if
> $$\sigma = \sigma_1 \dots \sigma_m$$
> then
> $$\text{sgn}(\sigma) = (-1)^m = \begin{cases} 1 & \text{if } m \text{ is even} \\ -1 & \text{if } m \text{ is odd} \end{cases}$$

Remark 3.4.3. We may define sgn using the map in the Lemma as

$$\text{sgn}(\sigma) = (\det \circ f_\sigma)(I_n).$$

> **Example 3.4.4** — Transpositions are odd—there is only one factor, and 1 is odd.

> **Exercise 115.** Are transpositions weird?[*]
>
> ---
> [*]This is a joke.

Example 3.4.5 — The identity permutation is even. Either you can view it as the empty product (no factors; 0 is even), or you can write it as $\epsilon = (1\ 2)(1\ 2)$.

Example 3.4.6 — The 4-cycle $(a\ b\ c\ d)$ can be written as

$$(a\ b\ c\ d) = (a\ b)(b\ c)(c\ d)$$

which has three factors, so it's odd.

Example 3.4.7 — The 7-cycle $(1\ 2\ 3\ 4\ 5\ 6\ 7)$ can be written as

$$(1\ 2\ 3\ 4\ 5\ 6\ 7) = (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$$

which has six factors, so it's even.

Example 3.4.8 — In general, the parity of a k-cycle is **opposite** the parity of k. In other words, cycles of even length are odd, and cycles of odd length are even.

Example 3.4.9 — The permutation $(1\ 2\ 3)(4\ 5\ 6)$ can be written as

$$(1\ 2\ 3)(4\ 5\ 6) = (1\ 2)(2\ 3)(4\ 5)(5\ 6)$$

which has four factors, so it's even.

Proposition 3.4.10

$\text{sgn} : S_n \to \mu_2 = \{1, -1\}$ is a homomorphism.

Proof. We can decompose σ and τ into k and l transpositions respectively,

$$\sigma = \alpha_1 \ldots \alpha_k \quad \text{and} \quad \tau = \beta_1 \ldots \beta_l.$$

Then

$$\sigma\tau = \alpha_1 \ldots \alpha_k \beta_1 \ldots \beta_l$$

which is a product of $k + l$ transpositions. By the formula for sgn,

$$\text{sgn}(\sigma\tau) = (-1)^{k+l} = (-1)^k (-1)^l = \text{sgn}(\sigma)\,\text{sgn}(\tau). \qquad \square$$

Combining the Cycle Decomposition Theorem with the fact that sgn is multiplicative, we can compute of the parity of any permutation by taking the product of the signs of its constituent cycles.

Exercise 116. Show that permutations of the same cycle type have the same parity, and derive a formula for $sgn(\sigma)$ given its cycle type $(c_1, \ldots, c_n)$. [Your answer should take the form

$$\prod_{l \text{ even}} a_l$$

where $a_l \in \mathbb{R}$. The notation means $a_2 a_4 a_6 \ldots$]

Exercise 117. Permutations of odd order are even.

3.4.2 A_n

Definition 3.4.11 — The set of even permutations in S_n,

$$A_n = \{\sigma \in S_n : sgn(\sigma) = 1\},$$

is called the *alternating group*.

Proposition 3.4.12

$A_n \trianglelefteq S_n$.

Proof. $A_n = \ker sgn$. □

Proposition 3.4.13

$[S_n : A_n] = 2$ for $n > 1$.

Proof. For $n > 1$, the image of sgn is all of μ_2 because transpositions are odd. So we have $S_n/A_n \cong \mu_2$. Then $o(S_n) = o(A_n)o(\mu_2) = 2o(A_n)$. □

Corollary 3.4.14

$A_n \trianglelefteq S_n$.

Proof. This follows from PS4XQ5. □

Example 3.4.15 — A_1 and A_2 are trivial.

Example 3.4.16 — A_3 has order 3 because S_3 has order 6. The signs of all the elements of S_3 are:

σ	ϵ	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\text{sgn}(\sigma)$	1	-1	-1	-1	1	1

Thus $A_3 = \{\epsilon, (1\ 2\ 3), (1\ 3\ 2)\}$. Note that A_3 is cyclic.

Example 3.4.17 — A_4 has order 12. Since it's unwieldy to write down all 24 elements of S_4, we'll use cycle types. [See PS4XQ4 for the enumeration of elements in S_n of each cycle type.]

cycle type	order	number	sign
$(4, 0, 0, 0)$	1	1	1
$(2, 1, 0, 0)$	2	6	-1
$(1, 0, 1, 0)$	3	8	1
$(0, 2, 0, 0)$	2	3	1
$(0, 0, 0, 1)$	4	6	-1

Example 3.4.18 — A_5 has order 60. The cycle types of its elements are highlighted below.

cycle type	order	number	sign
$(5, 0, 0, 0, 0)$	1	1	1
$(3, 1, 0, 0, 0)$	2	10	-1
$(2, 0, 1, 0, 0)$	3	20	1
$(1, 2, 0, 0, 0)$	2	15	1
$(0, 1, 1, 0, 0)$	6	20	-1
$(1, 0, 0, 1, 0)$	4	30	-1
$(0, 0, 0, 0, 1)$	5	24	1

3.4.3 Why do we care?

Okay, so A_n is an interesting group. But why do we care about it?

One reason is that the family of alternating groups have a lot of interesting properties, and generally is a great source of examples (and counterexamples).

Let G be a finite group. By Lagrange's theorem, if H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.

A natural question, then, is:

> **Question 3.4.19 —** If d is a divisor of $o(G)$, does G have a subgroup of order d?

We know this is *sometimes* true: for example, if $G = \langle g \rangle$ is cyclic of order n, and if $d \mid n$, then $H = \langle g^{n/d} \rangle$ is a subgroup of G with order d. And it's not hard to see that the converse of Lagrange's theorem is also true for dihedral groups using Theorem 2.3.7.

However...

> **Proposition 3.4.20** (Ruffini, 1799)
> A_4 has no subgroup of order 6.

Proof. Recall that A_4 comprises the even permutations on 4 letters: 8 3-cycles $(a\ b\ c)$, 3 double-transpositions $(a\ b)(c\ d)$, and 1 identity.

Let H be a subgroup of A_4 of order 6. Now Tutorial 6 showed us that $H \cong C_6$ or $H \cong D_3$. But A_4 contains no element of order 6, so H is generated by two involutions. But *all three* nontrivial involutions together only generate a subgroup of order 4! [It's V.] $\square$

Remark 3.4.21. Gallian proved this with cosets: Let a be any 3-cycle in A_4. Since $[A_4 : H] = 2$, the "three" cosets H, aH, a^2H are actually only *two* in number. Equality of any two of them implies $a \in H$. Since a was arbitrary, H contains all 8 3-cycles, which is a contradiction.

So, the converse of Lagrange's theorem does not hold in general. However, we can still say *something* about subgroups of general finite groups—we will talk about it when we discuss Cauchy's Theorem.

Another, deeper, reason why we care about the alternating group is because A_5 is the smallest example of a nonabelian *simple* group: A group with no nontrivial normal subgroups. Moreover, for $n \geq 5$, A_n is the *only* nontrivial normal subgroup of S_n.

We will not prove either of these facts in this course [except the A_5 case, which we will defer to later], but these facts mean the alternating groups are intimately connected with the solvability of polynomial equations of degree n. It's because of A_n that S_n fails to be what's known as a "solvable group" for $n \geq 5$. For more on this topic, see Abel–Ruffini theorem. This content will be covered in MAT401.

Finally, the alternating groups also arise naturally as the groups of rigid motions of some Platonic solids, like the tetrahedron, octahedron, dodecahedron, and the icosahedron. We will talk about it in the next chapter, when we revisit group actions.

Chapter 4

Group Actions

4.1 Orbit–Stabilizer Theorem

4.1.1 Recall...

Recall that we introduced group actions in Section 1.5.

> **Definition 4.1.1** — 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.
>
> For $x \in X$, the *orbit* of x is the set of elements that G sends x to. That is,
>
> $$\mathrm{Orb}_G(x) = Gx = \{g . x : g \in G\}.$$
>
> The set of all orbits in X is denoted X/G.
>
> A subset Y of X is called G-*invariant* if $g . y \in Y$ 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.

In this course, unless otherwise specified, we always talk about and notate in left actions, but the results in this chapter can be proved about right actions with some changes in notation. So you may assume these results apply to right actions as well.

4.1.2   An equivalent definition of action

Given an action of G on X, we get a homomorphism $\Phi : G \to \operatorname{Sym}(X)$ by setting $\Phi(g)$ to be the map $x \mapsto g \cdot x$. Informally,

$$\Phi(g) = g \cdot -$$

for all g in G.

Proof. Certainly, each $\Phi(g)$ is a self-map of X. The *identity* axiom tells us that $\Phi(e)$ is the identity map:

$$\Phi(e)(x) = e \cdot x = x$$

for all x in X. Meanwhile, the *compatibility* axiom tells us that if $g, h \in G$ then

$$\Phi(gh)(x) = gh \cdot x = g \cdot h \cdot x = \Phi(g)\big(\Phi(h)(x)\big)$$

for all x in X, so $\Phi(gh) = \Phi(g)\Phi(h)$.

It follows that each $\Phi(g)$ is a permutation of X, because $\Phi(g)^{-1} = \Phi(g^{-1})$, and thus $\Phi : G \to \operatorname{Sym}(X)$ is a homomorphism. $\qquad\square$

Remark 4.1.2. If G is any group, then a homomorphism from G to a symmetric group is termed a *permutation representation*.

> **Exercise 118.** Show that the converse is true: every permutation representation $\Phi : G \to \operatorname{Sym}(X)$ gives rise to a left action $G \curvearrowright X$.

The significance of this equivalence is that, whenever $G \curvearrowright X$, we should think of the elements of g pretending to be permutations of G.

> **Example 4.1.3 —** The permutation representation of the trivial action in Example 1.5.7 is the trivial map $f : G \to \operatorname{Sym}(X), f(g) = e$.
>
> The action of D_n on the n vertices of the regular n-gon in Example 1.5.10 gives rise to a map $D_n \to S_n$.
>
> The action of S_X on X in Example 1.5.13 gives rise to the identity map $\operatorname{id} : S_X \hookrightarrow S_X$.
>
> The action of G on G by left multiplication gives rise to an embedding $G \to S_G$. [This is Cayley's Theorem again.]
>
> The action of G on G by conjugation gives rise to the map
>
> $$G \to S_G : g \mapsto c_g$$
>
> where $c_g(x) = gxg^{-1}$ as in PS2Q2.

Exercise 119. Are these maps injective? Surjective?

4.1.3 More actions

Let G be an action on X. We can introduce even more actions derived from this action!

Example 4.1.4 (Pullback action) — Let $f : H \to G$ be a homomorphism. Then H acts on X by

$$h.x = f(h).x$$

for all x in X and h in H. It satisfies *identity* because

$$e_H.x = f(e_H).x = e_G.x = x$$

for all x in X, and *compatibility* because

$$h_1h_2.x = f(h_1h_2).x = f(h_1)f(h_2).x = f(h_1).f(h_2).x = h_1.h_2.x$$

for all x in X and all h_1, h_2 in H.

Exercise 120. Let $H \leq G$ and let $f : H \hookrightarrow G$ be the inclusion map $f(h) = h$. What is the pullback action in this case?

Example 4.1.5 (Powerset action) — Let $\mathcal{P}(X)$ denote the *powerset* of X, i.e. the collection of all subsets of X. Then G acts on $\mathcal{P}(X)$ by $g.A = \{g.x : x \in A\}$.

Example 4.1.6 — Let G be a group. Then both left multiplication and conjugation induce actions on $\mathcal{P}(G)$, hence on G-invariant subsets thereof. In particular,

- G acts on the set G/H of left cosets of any subgroup H by left multiplication: $g.(xH) = gx.H$. [This is Tutorial 3 Q3]

- G acts on the set $\mathcal{S}(G)$ of its own subgroups by conjugation: $g.H = gHg^{-1}$.

4.1.4 Stabilizers

Dual to the notion of the orbit of a point—the subset all places it can go—is the notion of the *stabilizer* of a point.

**Definition 4.1.7** — Suppose $G \curvearrowright X$ and let $x \in X$. The *stabilizer* (in G) of x is the set of

elements in G that fix x:

$$\text{Stab}_G(x) = G_x = \{g \in G : g \cdot x = x\}.$$

Exercise 121. The stabilizer is always a subgroup of the ambient group G.

The stabilizer of x can be regarded as the *symmetry group* of the object under consideration, with respect to the given action.

Example 4.1.8 — The stabilizers (in $C_4 = \langle r \rangle$) of each 'type' of puzzle piece are indicated below:

| $\langle r \rangle$ | $\langle e \rangle$ | $\langle e \rangle$ | $\langle r^2 \rangle$ | $\langle e \rangle$ | $\langle r \rangle$ |
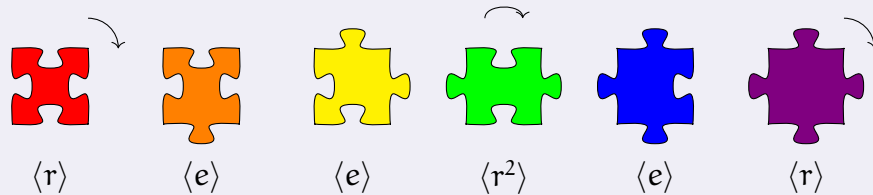
Notice that the pieces with the largest stabilizer groups are the ones with the smallest orbits, and vice versa.

	|orbit|	o(stabilizer)
	1	4
	2	2
	4	1

Notice that the product of orbit size and stabilizer order is always 4 (the order of C_4).

Exercise 122. Repeat the above example with C_4 replaced by D_4. That is, find the puzzle-piece stabilizers in D_4, and in each case, determine the product of the size of the orbit with the order of the stabilizer.

Example 4.1.9 — Consider the trivial action of G on X. Then every orbit is trivial, and every stabilizer is G. So, we have $|orbit| \times o(\text{stabilizer}) = o(G)$.

Example 4.1.10 — Consider the inversion action of $G = \mu_2$ on any group X. We have:

x	orbit	stabilizer
$o(x) \leq 2$	$\{x\}$	$\langle -1 \rangle$
$o(x) > 2$	$\{x, x^{-1}\}$	$\langle 1 \rangle$

Example 4.1.11 — Consider the (right) action of D_n on the n-gon. All n vertices lie in one orbit. What is the stabilizer of a vertex v? $\text{Stab}_{D_n}(v)$ cannot contain any rotations, nor any flips that move v. However, the flip over the axis through v certainly fixes v, and so $\text{Stab}_{D_n}(v) \cong C_2$.

Notice *again* that $|\text{orbit}| \times o(\text{stabilizer}) = n \times 2 = o(D_n)$.

Example 4.1.12 — The stabilizer in $\text{Aff}(\mathbb{R})$ of a real number x_0 is the set of all affine maps $x \mapsto ax + b$ that fix x_0. But

$$ax_0 + b = x_0 \iff b = x_0 - ax_0 = (1 - a)x_0$$

which means
$$\text{Aff}(\mathbb{R})_{x_0} = \{x \mapsto ax + (1 - a)x_0 : a \in \mathbb{R}^\times\}.$$

Here, we had only one (infinite) orbit, but the stabilizer isn't trivial—it's infinite too!

Example 4.1.13 — When G acts on itself by left multiplication, all stabilizers are trivial, because $g . x = x$ iff $gx = x$ iff $g = e$.

Example 4.1.14 — Consider the action of G on itself by conjugation. The stabilizer of a group element x is

$$\begin{aligned} G_x &= \{g \in G : g . x = x\} \\ &= \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\}. \end{aligned}$$

In other words, $\text{Stab}_G(x)$ is the set of all elements that commute with x. It's called the *centralizer* of x in G, denoted $C_G(x)$. [This is Tutorial 7 Q1.]

Exercise 123. Show that $Z(G) = \bigcap_{x \in G} C_G(x)$.

Remark 4.1.15. The notion of stabilizer makes sense for arbitrary subsets S of X, not just points. The *pointwise stabilizer* of S is

$$\{g \in G : g . x = x \text{ for all } x \text{ in } S\} = \bigcap_{x \in S} G_x$$

while the *setwise stabilizer* of S is

$$\{g \in G : g \cdot S = S\} = G_S$$

in the powerset action.

4.1.5 The Orbit–Stabilizer Theorem

By now you've hopefully caught on to the relationship between orbits and stabilizers: for any given element x, the product of the size of $Gx = \mathrm{Orb}_G(x)$ with the order of $G_x = \mathrm{Stab}_G(x)$ seems to always equal the order of the group.

This makes intuitive sense, because if x has a large orbit, then most of the elements of G are busy moving x around, while if x has a small orbit, then most of the elements of G leave x alone.

The elements of G that leave x alone—they're precisely the ones in G_x, the stabilizer of x. And if two different elements move x to the same place, then their "difference" must leave x alone, hence lie in the stabilizer. That is, if $g_1 \cdot x = g_2 \cdot x$ then $g_2^{-1} g_1 \cdot x = x$, so $g_2^{-1} g_1 \in G_x$.

Thus the set of places x can go is in 1-to-1 correspondence with the *cosets* of G_x in G. In other words:

> **Lemma 4.1.16**
>
> Let $G \curvearrowright X$ and let $x \in X$. Then the function
>
> $$\Phi : G/G_x \to Gx$$
> $$gG_x \mapsto g \cdot x$$
>
> is a bijection.

Remark 4.1.17. Here, G/G_x is just the set of left cosets of G_x in G. (We're not viewing G/G_x as a quotient group; there's no reason to believe that G_x is normal.)

Proof. As always, we must check that the definition of Φ does not depend on the choice of representative. If $g_1 G_x = g_2 G_x$ are two representations of the same coset, then $g_2^{-1} g_1 \in G_x$, which means $g_2^{-1} g_1 \cdot x = x$. Applying g_2 to both sides yields $g_1 \cdot x = g_2 \cdot x$ (because $g_2 \cdot g_2^{-1} g_1 \cdot x = g_2 g_2^{-1} g_1 \cdot x$ by *compatibility*). Thus $\Phi(g_1 G_x) = \Phi(g_2 G_x)$ is well-defined.

Running the argument backwards shows that Φ is injective: if $\Phi(g_1 G_x) = \Phi(g_2 G_x)$ then $g_1 \cdot x = g_2 \cdot x$, so $g_2^{-1} g_1 \cdot x = x$, whence $g_2^{-1} g_1 \in G_x$, and thus $g_1 G_x = g_2 G_x$.

It remains to show that Φ is surjective. But if $y \in Gx$ then $y = g \cdot x$ for some g in G, in which case $\Phi(gG_x) = y$. $\qquad \square$

The Lemma shows that the orbit of x is in bijective correspondence with the cosets of the stabilizer of x. Using this, we are ready to prove the all-important *Orbit–Stabilizer Theorem*.

> **Theorem 4.1.18** (Orbit–Stabilizer Theorem)
>
> Let $G \curvearrowright X$ and let $x \in X$. Then
>
> $$[G : G_x] = |Gx|.$$
>
> In particular, G is finite iff both Gx and G_x are finite, in which case
>
> $$o(G) = |Gx| \cdot o(G_x).$$

Proof. By the Lemma, each coset of G_x in G corresponds to precisely one element in the orbit of x,

$$(gG_x) \longleftrightarrow g.x,$$

and so the index—the number of cosets—is equal to the size of the orbit. In other words, $[G : G_x] = |Gx|$. Putting this together with Lagrange's Theorem, we conclude that

$$o(G) = [G : G_x] \cdot o(G_x) = |Gx| \cdot o(G_x). \qquad \square$$

Remark 4.1.19. Remember how we proved Lagrange's Theorem with orbits—and now we've come (almost)* full circle to prove Orbit–Stabilizer with Lagrange! In fact, these results are so closely related that you can prove one and immediately prove the other.

> **Exercise 124.** Without appealing to Lagrange's Theorem, prove Orbit–Stabilizer Theorem.

> **Exercise 125.** Prove Lagrange's Theorem using Orbit–Stabilizer Theorem.

4.2   Counting

4.2.1   Freeness and Transitivity[†]

> **Definition 4.2.1 —** An action $G \curvearrowright X$ is called
>
> - *faithful* if no nontrivial element acts trivially, that is, if $g.x = x$ for all x, then $g = e$;
>
> - *(fixed-point-)free* if every stabilizer is trivial, that is, for any x, if $g.x = x$, then $g = e$;
>
> - *transitive* if there's just one orbit, that is, if for any x, y, there is always some g such that $g.x = y$.

---

*"Almost" because this isn't a circular argument.
[†]Not to be confused with "Freedom of Transit".

We say G acts on X *faithfully / freely / transitively* in these cases respective*ly.*

Remark 4.2.2. Every free action is faithful.

Exercise 126. What's it called when every orbit is trivial?

Exercise 127. Which of the following actions are faithful? Free? Transitive?

- C_4 on puzzle pieces

- $\mathbb{Z}$ on $\mathbb{Z}$ by $n.x = x - n$

- the trivial action on an infinite set

- the inversion action on a nontrivial group

- D_n on vertices of an n-gon

- S_X on X

- $\text{Aff}(\mathbb{R})$ on $\mathbb{R}$

- $\langle 2 \rangle$ on $\{440 \cdot 2^{k/12} : k \in \mathbb{Z}\}$

- D_2 on mattress states

- G on itself by left multiplication

- G on itself by conjugation (depends on G)

By the Orbit–Stabilizer theorem,

$$o(G) = o(G_x) \cdot |Gx|,$$

if $G \curvearrowright X$ freely, then $o(G_x) = 1$ for all x in X, so $o(G) = |Gx|$, which means every orbit has the same size; since their union is X, we get that $o(G)$ divides $|X|$. Meanwhile, if $G \curvearrowright X$ transitively, then $Gx = X$ for all x in X, so $o(G) = o(G_x)|X|$, and we get that $|X|$ divides $o(G)$.

So, "freeness" and "transitivity" can be seen as opposing forces. An action which is *both* free and transitive is called *regular*.

What about faithfulness? Well...

Proposition 4.2.3

Let $G \curvearrowright X$ with the associated permutation representation $\Phi : G \to S_X$. Then Φ is injective iff the action is faithful.

Proof. Exercise. □

131

4.2.2   Platonic solids

A Platonic solid is a convex polyhedron all of whose faces are congruent regular polygons meeting in the same number at each vertex.

The five Platonic solids are:

	faces	vertices	edges
tetrahedron	4	4	6
cube	6	8	12
octahedron	8	6	12
dodecahedron	12	20	30
icosahedron	20	12	30

The symmetry group of a solid $\Sigma \subset \mathbb{R}^3$ is the group of rotations* about its center that leave it looking the same:
$$G_\Sigma = \{R \in SO(3) : R . \Sigma = \Sigma\}.$$

Fact 4.2.4

The symmetry groups of *Platonic* solids are very nice: each of them acts transitively on the solid's faces, on its vertices, and on its edges.

Visually, this fact makes sense—we can always rotate the Platonic solid in a way that moves one face to another, one vertex to another, or one edge to another.

This "threefold transitivity" does not hold for general polyhedra. For example, the square-based pyramid has two different types of face (4 triangles, 1 square), so the orbit of a face cannot contain the entire set of faces.

Let's use the Orbit–Stabilizer theorem to compute the order of the symmetry group of the cube.

Example 4.2.5 — Let $G = G_{[-1,1]^3}$ be the symmetry group of the cube. We are going to show that $o(G) = 24$ in three different ways.

- Face-wise:

  The orbit of any face is the set of all 6 faces. The stabilizer of each face is C_4 (since you can rotate the cube about the axis through the center of the face). Thus $o(G) = 6 \cdot 4 = 24$.

- Vertex-wise:

---

*We do not count reflections because we cannot reflect objects in real life in a tangible manner.

The orbit of any vertex is the set of all 8 vertices. The stabilizer of each vertex is C_3 (since you can rotate the cube about the axis through the vertex). Thus $o(G) = 8 \cdot 3 = 24$.

- Edge-wise:

    The orbit of any edge is the set of all 12 edges. The stabilizer of each edge is C_2 (since you can rotate the cube about the axis through the midpoint of the edge). Thus $o(G) = 12 \cdot 2 = 24$.

Exercise 128. Find the orders of the symmetry groups of the remaining four Platonic solids.

Proposition 4.2.6

The symmetries of the cube are as follows:

1. The 1 identity element e.

2. The 9 rotations by $90°$, $180°$, and $270°$ about the axes through the centers of opposing faces.
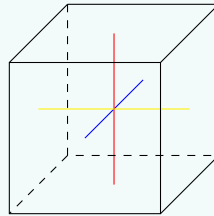
3. The 6 rotations by $180°$ about the axes through the midpoints of opposing edges.

4. The 8 rotations by $120°$ and $240°$ about the axes through opposing vertices.

> **Exercise 129.** Find a faithful action of G (the symmetry group of the cube) on a set of 4 objects. Deduce that $G \cong S_4$. [*Hint*: Grand diagonals.]

4.2.3 Mathematical jewellery

Suppose you have an unlimited supply of beads in an endless variety of colours, and you want to make some jewellery.

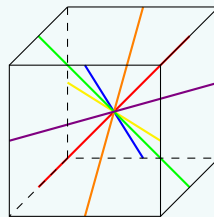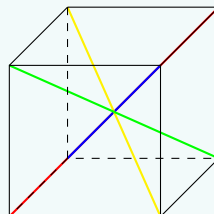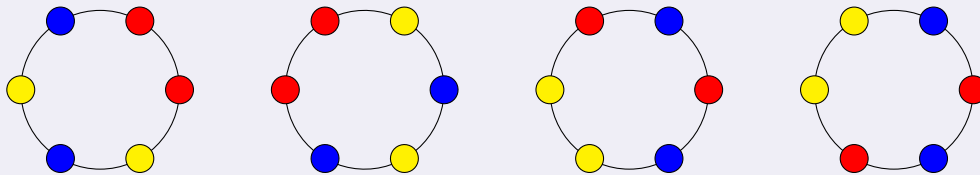Necklaces and bracelets can be idealized as perfect circles with n equally-spaced coloured beads. Two necklaces (or two bracelets) are considered the same if they are rotation-equivalent; bracelets, furthermore, are also considered the same if they are flip-equivalent. Thus a mathematical *necklace* is a C_n-orbit of necklaces, while a mathematical *bracelet* is a D_n-orbit of bracelets (n being the number of beads).

> **Exercise 130.** Which kind of mathematical jewellery are puzzle pieces? How many beads and how many colours?

Without considering equivalence, there are k^n possible necklaces/bracelets with n beads of up to k colours (because for each of the n beads, there are k choices for the colour). But what if we want to count the *orbits* of necklaces/bracelets?

> **Example 4.2.7 —** Here are some possible necklaces/bracelets (idealized).
>
>
>
> The first two are rotation-equivalent so they are the same necklace/bracelet.
>
> The last two are flip-equivalent so they are the same bracelet. [Are they the same necklace?]

> **Exercise 131.** How many "necklaces" are there on *one* bead with k possible colours?

> **Exercise 132.** How many necklaces are there on n beads with *one* possible colour?

> **Example 4.2.8 —** Let's look at 2 beads and k colours. The number of necklaces equals the number of bracelets, because rotation alone can do anything a flip can. The two beads are either the same colour (monochromatic) or different colours (dichromatic). The number of monochromatic necklaces is clearly k, while the number of dichromatic

ones is $\binom{k}{2}$, so the total is

$$k + \binom{k}{2} = k + \frac{k(k-1)}{2} = \tfrac{1}{2}(k^2 + k) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ 1 & 3 & 6 & 10 & \dots \end{pmatrix}$$

Example 4.2.9 — Consider jewellery on 3 beads with 3 colours. The necklaces are
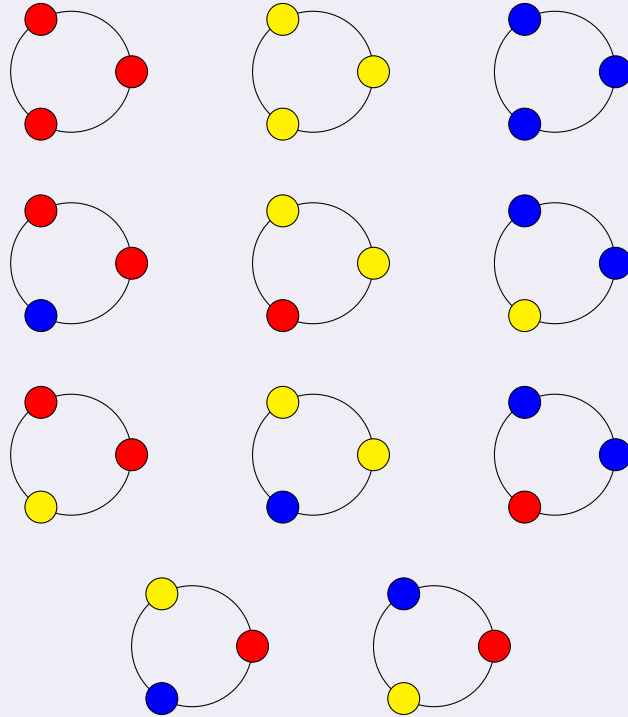
Three are monochromatic, six are dichromatic, and two are trichromatic. Thus there are $3 + 6 + 2 = 11$ necklaces in total.

What about bracelets? Nothing really changes if we add flip-equivalence, except for the last row: the two trichromatic necklaces are the same if we turn one over the horizontal axis. Thus there are 10 bracelets in total.

As you can probably tell, the general counting problem is quite challenging. We'll revisit it once we learn Burnside's Lemma.

4.2.4 Burnside's Lemma

"A method is a device which you used twice."

—George Pólya

Burnside's Lemma is a formula that counts the number of orbits of a finite set under the action of a finite group. Informally, it says that

number of orbits = average number of fixed points

where "fixed point" means an x in X such that $g.x = x$ for some g in G.

> **Definition 4.2.10** — Let $G \curvearrowright X$ and let $g \in G$. The *fix-set* of g is denoted
>
> $$X^g = \{x \in X : g.x = x\}$$

Don't confuse fix-sets and stabilizers; $X^g \subseteq X$ while $G_x \leq G$.

> **Lemma 4.2.11** (Burnside's Lemma)
>
> If a finite group G acts on a finite set X, then
>
> $$|X/G| = \frac{1}{o(G)} \sum_{g \in G} |X^g|.$$

Proof. Consider the set

$$S = \{(g, x) \in G \times X : g.x = x\}.$$

Note that S is a subset of the Cartesian product $G \times X$, so S is finite. We're going to count the number of elements of S in two ways.

1) First, by summing over the first component:

$$|S| = \sum_{g \in G} |\{x \in X : g.x = x\}| = \sum_{g \in G} |X^g|.$$

2) Second, by summing over the second component:

$$|S| = \sum_{x \in X} |\{g \in G : g.x = x\}| = \sum_{x \in X} o(G_x).$$

Eliminating the middleman, we obtain

$$\sum_{g \in G} |X^g| = \sum_{x \in X} o(G_x).$$

Next, let's focus on simplifying the right-hand side. By the Orbit–Stabilizer theorem,

$$\sum_{x \in X} o(G_x) = \sum_{x \in X} \frac{o(G)}{|Gx|} = o(G) \sum_{x \in X} \frac{1}{|Gx|}.$$

Because the sum is over *all* x in X, each term $1/|Gx|$ appears exactly $|Gx|$ times—once per element in the orbit! So

$$\sum_{x \in X} \frac{1}{|Gx|} = |X/G|.$$

Putting it all together,

$$\sum_{g \in G} |X^g| = o(G)|X/G|$$

and Burnside's Lemma follows upon dividing both sides by $o(G)$. □

So why do we use Burnside's Lemma? Think of it this way.

Counting orbits the naïve way is hard because you have to go through every element of X. Using Burnside's formula, you instead go through every element of G. Generally, G is much smaller than X, which already saves us some work!

Example 4.2.12 (Mathematical jewellery) — We can use Burnside's lemma to count the distinct colourings of necklaces and bracelets.

Let X be the set of all $3^3 = 27$ different ways of making jewellery with 3 beads and 3 colours. [Including when we don't actually use all 3 colors.] The groups that act on X are $D_3 = \langle r, f \rangle$ (for bracelets) and its subgroup $C_3 = \langle r \rangle$ (for necklaces).

To count the number of orbits, we'll take the average of $|X^g|$ over all g in G.

- $|X^e| = 27$ i.e. the identity element fixes all 27 arrangements.

- $|X^r| = |X^{r^2}| = 3$ because both nontrivial rotations (by 120° or 240°) fix just the 3 monochromatic necklaces.

At this point, we immediately deduce that the number of necklaces is

$$\frac{1}{3}(27 + 3 + 3) = \frac{33}{3} = 11.$$

- $|X^f| = |X^{fr}| = |X^{fr^2}| = 3^2 = 9$ because a piece of jewellery is fixed by a reflection iff the two beads on either side of the axis have the same colour.

Therefore, the number of bracelets is

$$\frac{1}{6}(27 + 3 + 3 + 9 + 9 + 9) = \frac{60}{6} = 10.$$

Exercise 133. What if we want to count the jewellery that actually use all 3 colours of beads? [*Hint*: How many pieces of jewellery use fewer than 3 colours?]

> **Example 4.2.13** (Colouring a cube) — Suppose we want to colour the faces of a cube with 3 colours. There are $3^6 = 729$ different colourings, but how many are actually distinct up to rotation?
>
> Check out this demonstration to see how different colourings are affected by rotation.
>
> We can compute the fix-sets of each element in the symmetry group of the cube:
>
> 1. $|X^e| = 3^6$ i.e. the identity element fixes all 3^6 colourings.
>
> 2. The 6 90-degree face-rotations fix the colourings that have the same colour for the other faces There are $3^3 = 27$ such colourings.
>
> 3. The 3 180-degree face-rotations fix the colourings that have the same colour for the opposite faces on the other faces. There are $3^4 = 81$ such colourings.
>
> 4. The 6 180-degree edge-rotations fix the colourings with the same colour on the two faces adjacent to each edge and the same colour on the two remaining faces. There are $3^3 = 27$ such colourings.
>
> 5. The 8 120-degree vertex-rotations fix the colourings with the same colour on the three faces meeting at the vertex and its opposite. There are $3^2 = 9$ such colourings.
>
> Putting it all together, the average number of fixed points is
>
> $$\frac{1}{24}\left(3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 6 \cdot 3^3 + 8 \cdot 3^2\right) = \frac{1368}{24} = 57$$
>
> meaning there are 57 distinct 3-colourings of a cube up to rotation.

4.3 Groups acting on groups

4.3.1 Groups acting on groups

Many useful results about groups can be obtained from the fruitful study of their actions on other groups.

> **Example 4.3.1** (Recall) — Every group G acts on itself by multiplication: $g.x = gx$.
>
> This action is transitive (meaning there is only one orbit) because for any two group elements x, y we can take $g = yx^{-1}$ and get $g.x = y$.
>
> This action is also free (meaning all stabilizers are trivial) because $g.x = x$ iff $gx = x$ iff $g = e$. Hence this action is *faithful*.
>
> The associated permutation representation $G \to \text{Sym}(G)$ is precisely the map $\Phi(g) =$

ρ_g from our proof of Cayley's theorem.

The previous example admits a generalization to coset spaces, *even when they are not groups*:

> **Example 4.3.2** — Let $H \leq G$. Then $G \curvearrowright G/H$ by $g . aH = gaH$. That this is actually an action is straightforward to verify.
>
> If it's faithful, then the associated permutation representation Φ embeds G into $\text{Sym}(G/H)$, which constitutes an "improvement" to Cayley's theorem if $[G : H] < o(G)$. In particular, if H has finite index k, then $G \hookrightarrow S_k$.

> **Exercise 134.** Is the action of G on the cosets of H transitive? Free? Faithful? [Hint. For the last one, let $\Phi : G \to \text{Sym}(G/H)$ be the associated permutation representation. Show that $\ker \Phi = \bigcap_{a \in G} aHa^{-1}$, the so-called "normal core" of H.]

> **Exercise 135.** Show that the action of D_n on $D_n/\langle f \rangle$ is faithful and use it to find an embedding $D_n \hookrightarrow S_n$.

> **Exercise 136.** Let $f : G \to H$ be a group homomorphism. Show that G acts on H by $g . h = f(g)h$. When is this action transitive? Free? Faithful?

4.3.2 Conjugation: Orbits

While both those examples are nice, our main focus for today will be on the action of a group on itself *by conjugation*.

Every group G acts on itself by conjugation: $g . x = gxg^{-1}$. The corresponding permutation representation $G \to \text{Sym}(G)$ is precisely the map $g \mapsto c_g$.

> **Definition 4.3.3** — The orbit of a point x is called the *conjugacy class* of x, denoted $\text{cl}(x)$, and the number of conjugacy classes of G is called the *class number* of G, denoted $k(G)$.

> **Question 4.3.4** — When is this action transitive? Free? Faithful?

> **Example 4.3.5** — If G is abelian, then $\text{cl}(x) = \{x\}$ for all x in G, and so $k(G) = o(G)$. [And conversely if G is finite.]
>
> So this action is neither transitive, nor free, nor faithful.

Exercise 137. Find a nonabelian infinite group with $k(G) = o(G)$.

Conjugacy classes give yet another useful characterization of normality:

> **Proposition 4.3.6**
>
> Let G be a group and let $H \leq G$. Then $H \trianglelefteq G$ iff $cl(x) \subseteq H$ for all x in H.

Proof. This follows immediately from our definition of normality. □

Another way to view the Proposition is that a subgroup H is normal iff it's the union of the conjugacy classes of all its elements.

Exercise 138. Explain why the phrasing "H is normal iff H is the union of all its conjugacy classes" is inaccurate.

Exercise 139 (Long). Classify the conjugacy classes of D_n, then classify its normal subgroups.

Exercise 140. Use PS4XQ4 to find the class number of S_n. Classify the conjugacy classes of S_6.

> **Example 4.3.7 —** We can now prove that the only nontrivial normal subgroup of S_5 is A_5.
>
> Recall from PS4XQ4 the cycle types in S_5 are as below:
>
> | conjugacy class | size |
> |---|---|
> | ϵ | 1 |
> | $(a\ b)$ | 10 |
> | $(a\ b)(c\ d)$ | 15 |
> | $(a\ b\ c)$ | 20 |
> | $(a\ b\ c)(d\ e)$ | 20 |
> | $(a\ b\ c\ d)$ | 30 |
> | $(a\ b\ c\ d\ e)$ | 24 |
>
> Since any proper nontrivial normal subgroup H must contain the identity and at least one other conjugacy class, we must have $o(H) \geq 11$. By Lagrange's theorem, $o(H) \in \{12, 15, 20, 24, 30, 40, 60\}$.
>
> Of these numbers, only $40 = 1 + 15 + 24$ and $60 = 1 + 15 + 20 + 24$ can be written as

sums of sizes of conjugacy classes including 1. In both cases, all 5-cycles (of which there are 24) and all double-transpositions (of which there are 15) lie in H. It follows that H also contains all 3-cycles, because, e.g.,

$$(1\,2\,3\,4\,5)(1\,2)(3\,4) = (1\,3\,5).$$

So, $o(H) = 60$ and $H \supseteq A_5$. Since $o(A_5) = 60$ as well, we have equality: $H = A_5$.

Remark 4.3.8. Conjugacy classes in A_n are *finer* than they are in S_n because the "conjugator" is required to be even. For example, the 3-cycles $(1\,2\,3)$ and $(1\,3\,2)$ are conjugate in S_3 but not in the abelian group A_3.

Aside. If you're interested, here is the *splitting criterion*: a conjugacy class in S_n with cycle type (c_i) splits into two A_n-conjugacy classes iff $(c_1, c_2, c_3, c_4, \dots) \geq (1, 0, 1, 0, \dots)$ pointwise.

4.3.3 Conjugation: Stabilizers

Consider the action of G on itself by conjugation. The stabilizer of a group element x is:

$$\begin{aligned} G_x &= \{g \in G : g \cdot x = x\} \\ &= \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\} \end{aligned}$$

In other words, $\mathrm{Stab}_G(x)$ is the set of all elements that commute with x. It's called the *centralizer* of x in G, denoted $C_G(x)$.

Exercise 141. Show that $Z(G) = \bigcap_{x \in G} C_G(x)$.

Proposition 4.3.9

For any group G and x in G,

$$|\mathrm{cl}(x)| = [G : C_G(x)].$$

Proof. This is just a restatement of the Orbit–Stabilizer theorem in the context of the conjugation action. The orbit of x is its conjugacy class $\mathrm{cl}(x)$, and the stabilizer of x its its centralizer $C_G(x)$. $\square$

141

Theorem 4.3.10 (Class equation)

Let G be a finite group. Then

$$o(G) = o(Z(G)) + \sum_{\substack{\text{one x per} \\ \text{nontrivial class}}} [G : C_G(x)].$$

Proof. The smallest conjugacy classes are those of the central elements: $cl(x) = \{x\}$ iff $x \in Z(G)$. Let $x_1, \ldots, x_k \in G$ be representatives of the nontrivial conjugacy classes. Then

$$G = Z(G) \cup \bigsqcup_{i=1}^{k} cl(x_i)$$

because G is partitioned by its conjugacy classes. Taking cardinalities of both sides gives

$$o(G) = o(Z(G)) + \sum_{i=1}^{k} |cl(x_i)|$$

and the result follows from Proposition 4.3.9. □

The class equation comes up over and over again in finite group theory.

Definition 4.3.11 — If $o(G) = p^n$ for some prime number p and some integer $n \geq 1$, then G is called a p-*group*.

Corollary 4.3.12

p-groups have nontrivial centers. Here, nontrivial means $Z(G) \neq \{e\}$.

Proof. Let G be a p-group with $Z(G) \neq G$. We'll use the class equation to prove $Z(G) \neq \{e\}$. The goal is to reduce the equation

$$o(G) = o(Z(G)) + \sum_{\substack{\text{one x per} \\ \text{nontrivial class}}} [G : C_G(x)]$$

modulo p. If we can show $[G : C_G(x)] \equiv 0 \pmod{p}$ for each x with nontrivial conjugacy class, then we'll get $o(Z(G)) \equiv 0 \pmod{p}$ (since G is a p-group). That will mean $o(Z(G)) \geq p$ (since $e \in Z(G)$ always).

So. Since G is a p-group, $[G : C_G(x)]$ is a prime power, possibly p^0 (by Lagrange's theorem). But for each x with *nontrivial* conjugacy class, the centralizer of x is *proper* (by the Orbit–Stabilizer theorem). Thus $[G : C_G(x)] > 1 = p^0$, and so $[G : C_G(x)] = p^k$ for some $k \geq 1$. In particular, $[G : C_G(x)] \equiv 0 \pmod{p}$. □

142

Exercise 142. Show that $k(G) = 1$ iff G is trivial.

Exercise 143. Show that $k(G) = 2$ iff $G = C_2$.

Exercise 144. Show that $k(G) = 3$ iff $G = C_3$ or S_3.

Remark 4.3.13. More generally, Landau's Theorem tell us there are only finitely many finite groups of each class number. We will not present a proof here.

What does Burnside's lemma say about $k(G)$?

Recall Burnside's lemma says that if a finite group G acts on a finite set X, then

$$|X/G| = \frac{1}{o(G)} \sum_{g \in G} |X^g|.$$

In the case of G acting on itself by conjugation, Burnside's lemma furnishes a formula for $k(G)$, the number of conjugacy classes of G.

Before we write it out, we need to determine what the "fix-sets" of the conjugation action are. Strangely enough, the fix-set of an element g is none other than its centralizer:

$$\{x \in G : g \cdot x = x\} = \{x \in G : gx = xg\} = C_G(x).$$

Therefore,

$$k(G) = \frac{1}{o(G)} \sum_{g \in G} o(C_G(g)).$$

That is, $k(G)$ is the average size of centralizers of elements in G.

4.4   Theorems of Cauchy and Sylow

Consider the following question inspired by Lagrange's Theorem:

Question 4.4.1 — If d is a divisor of $o(G)$, does G have a subgroup of order d?

Recall that we showed in Proposition 3.4.20 that the answer to this is negative in general. Not to despair—there's still much to be said.

- Cauchy's theorem (1825) implies that for each *prime* divisor p of $o(G)$, G has a subgroup of order p.

- Sylow's theorems (1872) imply that for each *maximal prime-power* divisor p^k of $o(G)$, G has a subgroup of order p^k.

- Hall's theorem (1928) implies that for every *unitary** divisor d of $o(G)$, G has a subgroup of order d—assuming G is solvable!

We will use group actions to give proofs of the theorems of Cauchy and Sylow.

Remark 4.4.2. The history of Lagrange's theorem is complicated. The idea has its origins in a 1771 memoir by Lagrange on "polynomial substitutions" where he showed, in modern terms, that the size of the orbit of an n-variate polynomial under the action of S_n is a divisor of $n!$ (cf. Orbit–Stabilizer). It wasn't until 1844 that Cauchy proved Lagrange's theorem for subgroups of S_n, and finally in 1861 came Jordan's proof for all permutation groups (hence *all* groups by Cayley's theorem).

> **Exercise 145.** Do infinite groups have infinite proper subgroups?* [Hint. μ_{2^∞}.]
>
> *Does "infinite subgroups" mean "subgroups which are infinite" or "infinitely many subgroups"?

4.4.1 Cauchy's theorem

Cauchy's theorem guarantees the existence of elements of prime order for primes dividing the order of the group. The explicit connection to Lagrange's theorem is made by the formula $o(\langle g \rangle) = o(g)$: if the element g has order p, then the cyclic subgroup it generates does too.

> **Theorem 4.4.3** (Cauchy, 1845)
>
> Let G be a finite group and let p be a prime number. If p divides $o(G)$ then G has an element of order p.

Proof (McKay, 1959). Let $C_p = \langle r \rangle$ act on the set

$$X = \{(g_1, g_2, g_3, \ldots, g_p) \in G^p : g_1 g_2 g_3 \ldots g_p = e\}$$

by "rotation":

$$r . (g_1, g_2, \ldots, g_{p-1}, g_p) = (g_2, g_3, \ldots, g_p, g_1).$$

This is well-defined (i.e., r actually *is* a map $X \to X$) because if $g_1 g_2 g_3 \ldots g_p = e$ then

$$g_2 g_3 \ldots g_p g_1 = g_1^{-1} \underbrace{g_1 g_2 g_3 \ldots g_p}_{e} g_1 = g_1^{-1} g_1 = e.$$

The fixed points of this action are precisely the p-tuples of the form $(g, \ldots, g)$ where $g \ldots g = e$, i.e., $g^p = e$. Obviously, $(e, \ldots, e)$ one such fixed point; if we can prove there's *at least one more* fixed point, then we'll have Cauchy's theorem.

---

*A divisor d of an integer n is called *unitary* if $\gcd(d, n/d) = 1$. For example, $4 = 2^2$ is a unitary divisor of 12, whereas 2 and 6 are not.

In order to prove something about the number of fixed points (orbits of size 1), it's worth considering *all* orbits, of *all* possible sizes. The size of any orbit divides $o(C_p) = p$ (by the Orbit–Stabilizer theorem). Since p is *prime*, that means every orbit has size 1 or p.

So, let

$$n_1 = \text{number of orbits of size 1 (fixed points)}$$
$$n_p = \text{number of orbits of size } p$$

To show $n_1 > 1$ we'll show $p \mid n_1$.

Since X is the union of its orbits,
$$|X| = n_1 + pn_p.$$

Reducing modulo p gives
$$n_1 \equiv |X| \pmod{p},$$

so we just need to show $p \mid |X|$.

To that end, let's count the number of elements in X. Every p-tuple in X can be specified by $p - 1$ arbitrary initial coordinates $g_1, \ldots, g_{p-1}$, which then determine the last coordinate: $g_p = (g_1 \ldots g_{p-1})^{-1}$. Thus $|X| = o(G)^{p-1}$. Since p divides $o(G)$ and $p - 1 \neq 0$, we conclude that p divides $|X|$. $\qquad\square$

Remark 4.4.4. On PS4XQ3, you proved Cauchy's theorem for the prime $p = 2$ by studying the cycle type of the involution $x \mapsto x^{-1}$ on G. In terms of the inversion action, G is the disjoint union of its orbits. There is one trivial orbit: the orbit of e. Were there no others, then $o(G)$ would be odd.

> **Exercise 146.** To check your understanding of McKay's proof, describe the set X as explicitly as possible when $p = 2$. What are n_1 and n_2 in terms of φ_G?

Example 4.4.5 (The Rubik's Cube) — One can show that there are

$$43252003274489856000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$$

different permutations of the cube—just over 43 quintillion (10^{18}). By Cauchy's theorem, there must exist an element of order 11—a sequence of moves that messes up the cube, but, when performed a total of 11 times, restores the cube to its original configuration.

Elements of order 11 are hard to find—there are "only" $44590694400 \approx 44$ billion of them (0.0000001%), making them the rarest in terms of order.* It can be seen that the 14-step sequence of moves

$$\text{L B}' \text{ F}^2 \text{ L}^2 \text{ U R U L R B}^2 \text{ D R}^2 \text{ B D}'$$

145

has order 11.

4.4.2 Sylow Theorems

One down, one to go. Remember, we're investigating *converses to Lagrange's theorem*. The Sylow theorems are actually *three* theorems concerning the existence, properties, and number of subgroups of size p^k.

> **Definition 4.4.6** — Let G be a finite group and p be a prime. A *Sylow p-subgroup* of G is a subgroup of order p^k, where $p^{k+1} \nmid o(G)$. The set of all Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$.

Remark 4.4.7. The word "Sylow" is the surname of the Norwegian mathematician Peter Ludwig Sylow who proved the theorems now bearing his name. For all intents and purposes, "Sylow" functions just like the adjective "maximal".

Remark 4.4.8. Nobody says "sub-p-groups".

> **Theorem 4.4.9** (Sylow, 1872)
>
> Let G be a finite group and let p be a prime. Then
>
> a) $\mathrm{Syl}_p(G) \neq \varnothing$
>
> b) $\mathrm{Syl}_p(G)$ is a single conjugacy class of subgroups of G. Moreover, every p-subgroup of G is contained in a Sylow p-subgroup.
>
> c) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$ and, if $o(G) = p^k r$ with $p \nmid r$, then $|\mathrm{Syl}_p(G)| \mid r$.

This is a big theorem. It's important for you to understand what it's actually saying, so we'll do a few examples before going over the proof.

> **Example 4.4.10** — Sylow's theorem is trivial for finite cyclic groups. We already know that if $G = \langle g \rangle$ is cyclic of order n, then G has exactly one subgroup of each possible order d dividing n, namely, $\langle g^{n/d} \rangle$. If p is a prime and $n = p^k r$ with $p \nmid r$, then $\langle g^r \rangle$ is the unique Sylow p-subgroup of G.

> **Example 4.4.11** — Let $G = D_6$. Since $o(D_6) = 12 = 2^2 \cdot 3$, the primes of interest are $p = 2$ and $q = 3$. So, let's determine the Sylow 2- and 3-subgroups of D_6, starting with the latter.

No subgroup of D_6 of order 3 can contain any flips ($2 \nmid 3$), so $\langle r^2 \rangle$ is the unique Sylow 3-subgroup of D_6. It's also *normal*—precisely because it's all alone in its conjugacy class.

What about the Sylow 2-subgroups? Well, they ought to have order 4, and, by Sylow's theorem, a) they exist, b) they're all conjugate, and c) there's either 1 or 3 of them.

We know that every subgroup of D_6 is cyclic (a subgroup of $\langle r \rangle$) or dihedral. Since $4 \nmid 6$, our Sylow 2-subgroups must all be dihedral. Each dihedral subgroup of D_6 of index k has the form $\langle r^k, fr^i \rangle$ with $0 \leq i < k$. Order 4 means index 3, so our subgroups of order 4—our Sylow 2-subgroups—are

$$\langle r^3, f \rangle, \quad \langle r^3, fr \rangle, \quad \langle r^3, fr^2 \rangle.$$

As we saw back in Lecture 16, these really are all conjugate:
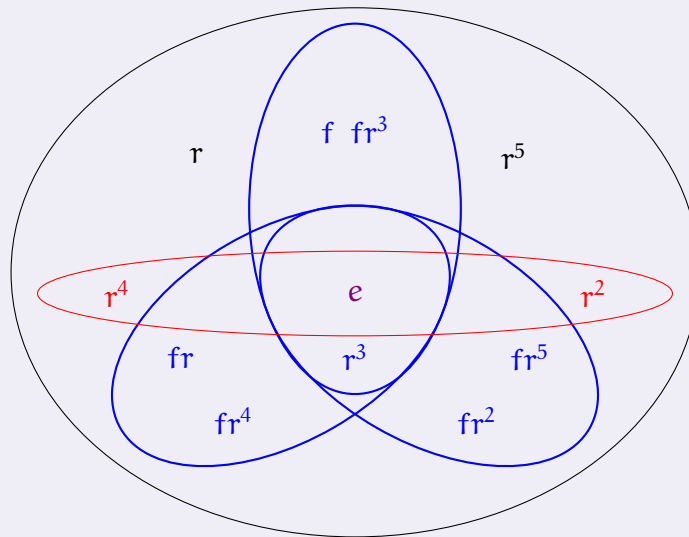
Example 4.4.12 — Let G be a group of order pq where $p < q$ and $q \not\equiv 1 \pmod{p}$ (e.g. $15 = 3 \cdot 5$). Let $n_p = |\mathrm{Syl}_p(G)|$, ditto n_q. By Sylow's theorem,

$$n_p \mid q \implies n_p = 1 \text{ or } q$$
$$n_p \equiv 1 \pmod{p} \implies n_p = 1 \text{ because } q \not\equiv 1 \pmod{p}$$

and

$$n_q \mid p \implies n_q = 1 \text{ or } p$$
$$n_q \equiv 1 \pmod{q} \implies n_q = 1 \text{ because } 1 < p < q.$$

Thus G has just one Sylow p-subgroup just one Sylow q-subgroup. Thus G has exactly

one subgroup of every possible order, so, by our "subgroup characterization" theorem, G is cyclic.

What happens if $q \equiv 1 \pmod{p}$? The general answer needs *semidirect products*, which we haven't seen (yet). However, in the simplest case $p = 2$, we *can* say something:

Example 4.4.13 — Let G be a group of order 2q where q is an odd prime. By Sylow's theorem,

$$n_2 \mid q \implies n_2 = 1 \text{ or } q$$
$$n_2 \equiv 1 \pmod{2} \text{ gives no further information because q is odd,}$$

and

$$n_q \mid 2 \implies n_q = 1 \text{ or } 2$$
$$n_q \equiv 1 \pmod{q} \implies n_q = 1 \text{ because } 1 < 2 < q.$$

If G has just one Sylow 2-subgroup, then, as before, G is cyclic.

If G has q Sylow 2-subgroups, then each one is generated by an involution. These q involutions, along with the q elements of the unique Sylow q-subgroup, already constitute all $q + q = 2q$ elements of G.

So if we let r be an element of order q, and f an element of order 2, then $f \notin \langle r \rangle$, so

$$G = \langle r \rangle \cup f \langle r \rangle = \{e, r, \ldots, r^{q-1}, f, fr, \ldots, fr^{q-1}\}$$

which means G is generated by r and f: $G = \langle r, f \rangle$. Since also $fr \notin \langle r \rangle$, that means fr must have order 2 as well, which implies $frf = r^{-1}$. Thus G is dihedral.

Example 4.4.14 — Let's determine $\mathrm{Syl}_5(S_5)$.

By Sylow's theorem, $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 24$, so $n_5 = 1$ or 6. Which is it?

Since $o(S_5) = 5! = 5 \cdot 4!$ and $5 \nmid 4!$, each Sylow 5-subgroup of S_5 has order 5. Thus, each one must be cyclic, generated by a 5-cycle. Conversely, each 5-cycle generates a Sylow 5-subgroup already. We know S_5 has 24 5-cycles, so, with only 4 in each 5-subgroup, it must be that $n_5 = 6$.

$$\langle (1\,2\,3\,4\,5) \rangle, \langle (1\,2\,3\,5\,4) \rangle, \langle (1\,2\,4\,5\,3) \rangle,$$

$$\langle (1\,2\,4\,3\,5) \rangle, \langle (1\,2\,5\,4\,3) \rangle, \quad \text{and} \quad \langle (1\,2\,5\,3\,4) \rangle.$$

Example 4.4.15 — Let $G = S_4$. Since $o(S_4) = 4! = 24 = 2^3 \cdot 3$, we look to determine the Sylow 2- and 3-subgroups of S_4.

Before we begin, it's useful to keep in mind the types of permutations in S_4:

cycle type	number
ϵ	1
$(a\ b)$	6
$(a\ b\ c)$	8
$(a\ b\ c\ d)$	6
$(a\ b)(c\ d)$	3

Let $n_p = |\mathrm{Syl}_p(S_4)|$ for $p = 2, 3$. By Sylow's theorem,

$$n_2 \mid 3 \implies n_2 = 1 \text{ or } 3$$
$$n_2 \equiv 1 \ (\mathrm{mod}\ 2) \text{ gives no further information}$$

and

$$n_3 \mid 8 \implies n_3 = 1, 2, 4, 8$$
$$n_3 \equiv 1 \ (\mathrm{mod}\ 3) \implies n_3 = 1 \text{ or } 4.$$

The Sylow 3-subgroups are easy: if σ is any 3-cycle, then $\langle \sigma \rangle \in \mathrm{Syl}_3(S_4)$. Since S_4 has 8 3-cycles in total, and $\langle \sigma \rangle$ only contains 2 of them (σ and σ^{-1}), we must have $n_3 > 1$. Thus $n_3 = 4$. Indeed,

$$\mathrm{Syl}_3(S_4) = \{\langle (1\ 2\ 3) \rangle, \langle (1\ 2\ 4) \rangle, \langle (1\ 3\ 4) \rangle, \langle (2\ 3\ 4) \rangle\}$$

The Sylow 2-subgroups are less easy. Let $P \in \mathrm{Syl}_2(S_4)$ and note that $o(P) = 8$. If P were unique, then, by Sylow's theorem, P would contain *all* the elements of S_4 of orders 1, 2, and 4. But there are 16 such elements—way too many—so P cannot be not unique. Thus $n_2 = 3$.

Let P_1, P_2, P_3 be the three distinct Sylow 2-subgroups of S_4. Recall that S_4 contains a copy of the Klein 4-group as a normal subgroup:

$$V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \trianglelefteq S_4.$$

Because V has order $4 = 2^2$, it's contained in a Sylow 2-subgroup; and because it's normal, it's contained in all of them.

That means P_1, P_2, P_3 already have 4 elements in common. By Lagrange's theorem, $P_1 \cap P_2 \cap P_3$ cannot be *any* larger lest the P_i's all coincide.

To determine the remaining 4 elements of each P_i we observe that every 4-cycle and its inverse must live in some P_i. Since there are only 6 4-cycles to go around, and since each of the 3 P_i's has at least 2 of them, it follows that each P_i contains exactly 2 4-cycles.

Without loss of generality, suppose $(1\,2\,3\,4) \in P_1$. Then P_1 contains
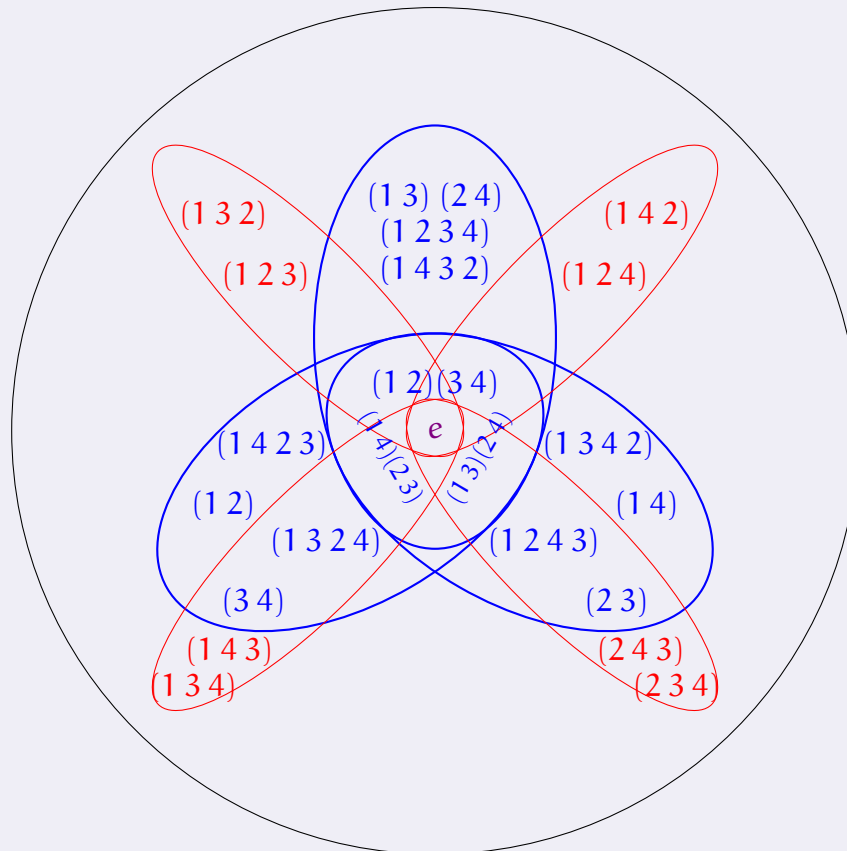
$$(1\,2)(3\,4)(1\,2\,3\,4) = (2\,4)$$

as well as

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

and so we deduce that

$$P_1 = \{\epsilon, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1\,4\,3\,2), (1\,3), (2\,4)\}.$$

The descriptions of P_2 and P_3 are analogous.

Exercise 147. Prove that every Sylow 2-subgroup of S_4 is isomorphic to D_4.

Exercise 148. Here's an intriguing interpretation of the Sylow 2-subgroups of S_4. Observe that there are 3 ways to split $\{1, 2, 3, 4\}$ in half:

$$\{\{1, 2\}, \{3, 4\}\} \quad \text{and} \quad \{\{1, 3\}, \{2, 4\}\} \quad \text{and} \quad \{\{1, 4\}, \{2, 3\}\}.$$

Such partitions are called *block systems*. Permutations act on block systems by moving them around in the obvious way; for example,

$$(1\ 2\ 3) . \{\{1, 2\}, \{3, 4\}\} = \{\{2, 3\}, \{1, 4\}\}$$

is moved, while

$$(1\ 2)(3\ 4) . \{\{1, 2\}, \{3, 4\}\} = \{\{2, 1\}, \{4, 3\}\}$$

is fixed. Show that the Sylow 2-subgroups of S_4 are precisely the stabilizers of the above three block systems.

Now that it is clearer how we use Sylow's Theorems, let's get to proving them.

Proof (Wielandt, 1959). We consider three actions of G (or subgroups of G) on different sets.

a) Let X_a be the set of all size-p^k sub*sets* of G and let G act on X_a by left-multiplication*.

   We first need to work out how big X_a is.

   $$|X_a| = \binom{p^k r}{p^k} = \frac{p^k r}{p^k} \cdot \frac{p^k r - 1}{p^k - 1} \cdot \frac{p^k r - 2}{p^k - 2} \cdot \ldots \cdot \frac{p^k r - p^k + 1}{1}.$$

   We claim that p does *not* divide $|X_a|$. To prove it, we have to show that p does not divide *any* of the terms $\dfrac{p^k r - j}{p^k - j}$ for $j < p^k$.

   It's true for $j = 0$ because $\dfrac{p^k r}{p^k} = r$ and $p \nmid r$. And it's true for $j > 0$, because if write $j = p^l s$ where $p \nmid s$, then $l < k$ (because $j < p^k$) and

   $$\frac{p^k r - j}{p^k - j} = \frac{p^k r - p^l s}{p^k - p^l s} = \frac{p^{k-l} r - s}{p^{k-l} - s},$$

   which is not divisible by p.

   So, the size of the set X_a is not divisible by p. That means that in every partition of X_a, some part is not divisible by p.

   This means the action of G on X_a must have an orbit whose size is *not* divisible by p. Call it the orbit of some subset S.

---

*$g . S = \{gx : x \in S\}$.

Now, although S has the right size, p^k, it's not necessarily a Sylow p-subgroup of G—it might not even be a subgroup! But it's close.

Let $H = \text{Stab}_G(S) \leq G$. By the Orbit–Stabilizer theorem,

$$|\text{Orb}_G(S)| \cdot o(H) = o(G) = p^k r.$$

Since p is prime and $p \nmid |\text{Orb}_G(S)|$, we know $o(H)$ is a multiple of p^k.

But since H is the stabilizer of S, $hS = S$ for all h in H. It follows that $H \subseteq Ss^{-1}$ for any fixed s in S. Comparing cardinalities, we conclude $o(H) = p^{k*}$. Thus $\text{Syl}_p(G) \neq \varnothing$.

b) Let K be a p-subgroup of G and let $H \in \text{Syl}_p(G)$. Consider the action of the group K by left-multiplication on the set $X_b = G/H$ of left cosets of H in G. If we can prove there exists a singleton orbit, then we'll be done, as $kgH = gH$ for all k in K implies $K \subseteq gHg^{-1}$.

But there *must* exist a singleton orbit: by the Orbit–Stabilizer theorem and the fact that $o(K)$ is a power of p, every orbit has size a power of p (including $p^0 = 1$ possibly); were there no orbits of size 1, then $|X_b| = [G : H] = o(G)/o(H) = p^k r/p^k = r$ would be divisible by p.

Taking K to be a *Sylow* p-subgroup of G, the above argument shows that for any H in $\text{Syl}_p(G)$ there exists g in G such that $K = gHg^{-1}$. Thus the Sylow p-subgroups of G are pairwise conjugate.

c) Let G act by conjugation on the set $X_c = \text{Syl}_p(G)$ of Sylow p-subgroups of G. By parts a) and b) the action is transitive, so if $H \in X_c$, then, by the Orbit–Stabilizer theorem,

$$|X_c| = [G : N_G(H)].$$

(NB. The stabilizer of H in G w.r.t. the conjugation action is called the *normalizer of H in G* and denoted $N_G(H)$. See Tutorial 7 Question 1.) But $N_G(H) \geq H$ since $hHh^{-1} = H$ for all h in H, so by the Tower Law for Indices,

$$|X_c| = \frac{[G : H]}{[N_G(H) : H]} = \frac{r}{[N_G(H) : H]}$$

is a divisor of r.

It remains to prove $|X_c| \equiv 1 \pmod{p}$. To that end, we zoom in a little, by looking at the conjugation action on X_c by a Sylow p-subgroup of G, say H. As before, every orbit must have size a power of p, which means $|X_c|$ is congruent, modulo p, to the number of orbits of size 1. So it suffices to show that this number is 1.

Now, a typical K in X_c will have trivial H-orbit if and only if $h.K = K$ for all h in H, which is to say $hKh^{-1} = K$ for all h in H. More concisely, K has trivial H-orbit iff $H \leq N_G(K)$.

---

*Indeed, this means $H = s^{-1}S$, which justifies why we say S is close—it is a coset of H!

Observe that, by Lagrange's theorem,

$$o(H) = o(K) = p^k \mid o(N_G(K)) \mid o(G) = p^k r$$

which means H and K are Sylow p-subgroups *of* $N_G(K)$! By part b) of Sylow's theorem, H and K must be conjugate *in* $N_G(K)$—there must exist g in $N_G(K)$ such that $K = gHg^{-1}$. But then $H = g^{-1}Kg = K$, because g stabilizes K.

What all this shows is that if $|\text{Orb}_H(K)| = 1$ for some Sylow p-subgroup K of G, then $K = H$. In other words, the only possible orbit of size 1 is the orbit of H itself (which, incidentally, *is* trivial). □

To summarize, here are the group actions used in each part of the proof: Here, H is a Sylow p-subgroup of G.

Theorem	Group	Set	Action
Sylow I	G	size-p^k subsets of G	left multiplication
Sylow II	p-subgroup K	G/H	left multiplication
Sylow III	G	$\text{Syl}_p(G)$	conjugation

Exercise 149. Prove Sylow's theorems directly in the case $p \nmid o(G)$.

Exercise 150. Let p be a prime and let G be a p-group. Describe $\text{Syl}_q(G)$ for all primes q.

Exercise 151. Let G be a finite group. Prove that Sylow p-subgroups of G are *maximal* in the sense that there are no p-subgroups strictly between them and G. Conversely, prove that every maximal p-subgroup of G is a Sylow p-subgroup.

Chapter 5

Groups & Symmetries

5.1 More Direct Products

We've learned a lot about the structure of groups, so it's time to revisit the classification of groups and see what more we know now.

5.1.1 External direct products

Given two groups H and K, in Tutorial 4, we defined a composition law on $H \times K$ by

$$(h, k)(h', k') = (hh', kk')$$

i.e. coordinatewise multiplication.

This gives rise to a group structure on $H \times K$. We call this group the *direct product* of H and K.

> **Proposition 5.1.1**
> If h and k have finite order, then $o((h, k)) = \text{lcm}\{o(h), o(k)\}$.

Proof. See Tutorial 4. □

> **Corollary 5.1.2**
> $C_n \times C_m$ is cyclic iff $\gcd(n, m) = 1$.

Proof. See Tutorial 4. □

With the language of morphisms and normal subgroups, we can revisit the idea of direct products and obtain some more properties about the direct product.

> **Proposition 5.1.3**
>
> Let H and K be groups.
>
>   (i) The projection maps $\pi_1 : H \times K \to H$ and $\pi_2 : H \times K \to K$ are epimorphisms.
>
> (ii) $H \times \{e\}$ and $\{e\} \times K$ are normal subgroups of $H \times K$ with trivial intersection.
>
> (iii) $(H \times K)/(H \times \{e\}) \cong K$ and $(H \times K)/(\{e\} \times K) \cong H$.

Proof.

  (i) For all (h, k) and (h', k') in $H \times K$ we have

$$(h, k)(h', k') = (hh', kk')$$

so

$$\pi_1\big((h, k)(h', k')\big) = hh' = \pi_1\big((h, k)\big)\pi_1\big((h', k')\big)$$

which shows that π_1 is a homomorphism; same for π_2. For any h in H and k in K we have $\pi_1\big((h, k)\big) = h$ and $\pi_2\big((h, k)\big) = k$, so π_1 and π_2 are epic.

 (ii) $H \times \{e\} = \ker \pi_2$ and $\{e\} \times K = \ker \pi_1$ are automatically normal. If

$$(h, k) \in \big(H \times \{e\}\big) \cap \big(\{e\} \times K\big)$$

then $k = e$ and $h = e$ so $(h, k) = (e, e)$ is the identity element.

(iii) This is just a consequence of the First Isomorphism Theorem. □

So, direct products are really nice. How do we spot them "in the wild"? How do we know when a group G is a direct product?

5.1.2   Internal direct products

Let G be a group, H and K subgroups of G. When is $G \cong H \times K$?

Observe that $H \times K$ acts on G by $(h, k) \cdot x = hxk^{-1}$ (the reason for the $^{-1}$ will be clear in a moment). Indeed, for all x in G,

$$(e, e) \cdot x = exe^{-1} = x$$

so we have *identity*, and

$$(h_1, k_1) \cdot (h_2, k_2) \cdot x = (h_1, k_1) \cdot h_2 x k_2^{-1}$$

155

$$= h_1(h_2 x k_2^{-1})k_1^{-1}$$
$$= (h_1 h_2)x(k_1 k_2)^{-1}$$
$$= (h_1 h_2, k_1 k_2).x$$

for all (h_1, k_1) and (h_2, k_2) in $H \times K$, so we have *compatibility*.

The orbit of e is the set

$$\mathrm{Orb}_{H \times K}(e) = \{(h, k).e : (h, k) \in H \times K\}$$
$$= \{hk^{-1} : h \in H, k \in K\}$$
$$= HK^{-1}.$$

But since K is a subgroup, $K^{-1} = K$, and so $\mathrm{Orb}_{H \times K}(e) = HK$.

The stabilizer of e is the subgroup

$$\mathrm{Stab}_{H \times K}(e) = \{(h, k) \in H \times K : (h, k).e = e\}$$
$$= \{(h, k) \in H \times K : h = k\}.$$

The only possible such elements are (x, x) with $x \in H \cap K$. It's easy to see that the map $H \cap K \to \mathrm{Stab}_{H \times K}(e)$ sending x to (x, x) is an isomorphism, and so $\mathrm{Stab}_{H \times K}(e) \cong H \cap K$.

Appealing to the Orbit–Stabilizer theorem, we derive a fundamental "product formula" relating the orders of H, K, HK, and $H \cap K$:

Theorem 5.1.4

Let H and K be subgroups of a group G. Then

$$|HK| \cdot o(H \cap K) = o(H)o(K).$$

Example 5.1.5 — Consider the subgroups $H = \langle f \rangle$ and $K = \langle fr \rangle$ of D_3. By the product formula,
$$|HK| = \frac{o(H)o(K)}{o(H \cap K)} = \frac{2 \cdot 2}{1} = 4.$$

Indeed,
$$HK = \{e, f\}\{e, fr\} = \{e, f, fr, r\}.$$

What does this formula say toward our goal of expressing G as the direct product of H and K? Observe that

$$H \cap K \subseteq H, K \subseteq HK \subseteq G$$

so that $H \cap K$ is "small" and HK is "big", relatively speaking. It's not a bad guess to think that if G is to be the direct product of H and K, then $H \cap K$ should trivial (as small as possible) and HK should be G (as big as possible). Unfortunately, that's not enough.

Example 5.1.6 — Let $G = D_n$ and let $H = \langle f \rangle$ and $K = \langle r \rangle$. Since no flip is a rotation, $H \cap K$ is trivial, and by the product formula,

$$|HK| = \frac{o(H)o(K)}{o(H \cap K)} = \frac{2 \cdot n}{1} = 2n = o(G).$$

Yet $G \not\cong H \times K$ because the latter is abelian.

The problem is that although the *sizes* match up (i.e. there is certainly a bijection $H \times K \to G$), the *operations* don't agree (i.e. no bijection $H \times K \to G$ is a homomorphism). In $H \times K$ the operation is

$$(h, k)(h', k') = (hh', kk')$$

while in HK the operation is

$$(hk)(h'k') = hkh'k'.$$

Notice that $hkh'k' = hh'kk'$ iff $kh' = h'k$ for all h' in H and all k in K, so the missing ingredient is this: all elements of H must commute with all elements of K.

Theorem 5.1.7

Let G be a group with subgroups H and K. If

  (i) $HK = G$

  (ii) $H \cap K$ is trivial

  (iii) every element of H commutes with every element of K

then the multiplication map $m : H \times K \to G$ is an isomorphism.

Proof. Hypothesis (i) is equivalent to the statement that m is surjective, because $m(H \times K) = HK$.

Hypothesis (ii) is equivalent to the statement that m is injective, because $m(h_1, k_1) = m(h_2, k_2)$ iff $h_1 k_1 = h_2 k_2$ iff $h_2^{-1} h_1 = k_2 k_1^{-1}$. This element lives in both H and K, so if $H \cap K = \{e\}$ then $h_1 = h_2$ and $k_1 = k_2$, while if $H \cap K > \{e\}$ then $m^{-1}(e)$ contains nontrivial pairs.

Finally, hypothesis (iii) is, as we've seen, equivalent to the statement that m is a homomorphism:

$$m(h_1, k_1)m(h_2, k_2) = h_1 k_1 h_2 k_2$$

while

$$m(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2.$$

Therefore if all three hypotheses are met, then m is a bijective homomorphism, i.e., an isomorphism. $\square$

> **Exercise 152.** Show that the hypotheses are independent. That is, construct situations where one hypothesis fails but the other two hold.

In the presence of the first two hypotheses, the third hypothesis can be replaced (as it often is) by the seemingly weaker statement that H and K are both normal in G.[*]

Lemma 5.1.8

Let G be a group with subgroups H and K. If

  (i) $HK = G$

  (ii) $H \cap K$ is trivial

then every element of H commutes with every element of K if and only if H and K are both normal in G.

Proof. If every element of H commutes with every element of K, and $h_0 \in H$ and $g \in G$, then by (i) we have $g = hk$ for some h in H and some k in K, so

$$gh_0 g^{-1} = (hk)h_0(hk)^{-1} = hkh_0 k^{-1}h^{-1} = hh_0 h^{-1} \in H$$

which shows $H \trianglelefteq G$ (and an analogous argument works for K).

On the other hand, if H and K are both normal in G and $h \in H$, $k \in K$, then h and k commute iff $[h, k] = e$. But

$$[h, k] = hkh^{-1}k^{-1} = h\underbrace{kh^{-1}k^{-1}}_{\in H} \in H$$

and

$$[h, k] = hkh^{-1}k^{-1} = \underbrace{hkh^{-1}}_{\in K}k^{-1} \in K$$

so $[h, k] \in H \cap K$, which is trivial by (ii). Thus $[h, k] = e$. $\qquad\square$

Remark 5.1.9. Hypotheses (i) and (ii) state that every element of G can be expressed uniquely in the form hk with h in H and k in K. Whenever this happens in general, H and K are called *complementary subgroups*, and we say H is a *complement* of K and vice versa.

Remark 5.1.10. A group G is called *decomposable* if it's the internal direct product of two proper subgroups, otherwise *indecomposable*.

Example 5.1.11 — Let $G = D_n$ with n twice an odd number. Consider the subgroups $H = \langle r^2, f \rangle$ and $K = Z(D_n) = \langle r^{n/2} \rangle$. Note that $H \cap K$ is trivial because $r^{n/2}$ cannot be

---

[*]It's weaker because while (iii) says $hk = kh$, normality only says $khk^{-1} \in H$—not $khk^{-1} = h$.

an integer power of r^2 (as $n/2$ is odd). By the product formula, we have

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = \frac{n \cdot 2}{1} = 2n = o(D_n)$$

so $HK = D_n$. Thus H and K are complementary. Is D_n their direct product? Yes: H is normal because its index is 2, and K is normal because it's the center. Thus $D_n \cong H \times K$ is decomposable.

Exercise 153. Continuing the example with n twice an odd number, show that $D_n \cong D_{n/2} \times C_2$.

Exercise 154. What goes wrong when n is odd? When n is twice an even number?

Example 5.1.12 — Let n be odd. Then $GL_n(\mathbb{R})$ is the direct product of its center $\mathbb{R}^\times I$ and its normal subgroup $SL_n(\mathbb{R})$.

Indeed, if λI is a scalar matrix with unit determinant, then $\lambda^n = 1$, so $\lambda = 1$ since n is odd. Thus $(\mathbb{R}^\times I) \cap SL_n(\mathbb{R}) = \{I\}$.

And if A is an arbitrary matrix with nonzero determinant δ, then $\delta^{-1/n} A \in SL_n(\mathbb{R})$. Thus $GL_n(\mathbb{R}) = (\mathbb{R}^\times I) SL_n(\mathbb{R})$.

Exercise 155. Let n be even. What are $(\mathbb{R}^\times I) \cap SL_n(\mathbb{R})$ and $(\mathbb{R}^\times I) SL_n(\mathbb{R})$?

Subgroups of abelian groups are always normal. As such, direct products are especially well suited to the study of abelian groups.

Example 5.1.13 — C_4 has only one proper nontrivial subgroup, which is isomorphic to C_2. As we saw earlier, $C_2 \times C_2 \cong D_2$ is not cyclic, so C_4 is indecomposable.

Exercise 156. Fill in the blank: C_n is indecomposable iff ...

Exercise 157. Show that every finite indecomposable abelian group is cyclic.

5.2 Fundamental Theorem of Finite Abelian Groups

We can use direct products to fully classify finite abelian groups.

The fundamental theorem of finite abelian groups says that every finite abelian group can be written uniquely as a direct product of cyclic groups of prime-power order.

159

> **Theorem 5.2.1** (Fundamental Theorem of Finite Abelian Groups)
>
> Let G be a finite abelian group. Then there exists an integer $s \geq 0$, prime numbers $p_1, \ldots, p_s$ (not necessarily distinct), and positive integer exponents $k_1, \ldots, k_s$ such that
>
> $$G \cong C_{p_1^{k_1}} \times \ldots \times C_{p_s^{k_s}}.$$

> **Example 5.2.2** — $C_{60} \cong C_4 \times C_3 \times C_5$.

Compare this to the fundamental theorem of arithmetic:

> **Theorem**
>
> Let n be a positive integer. Then there exists an integer $s \geq 0$ and prime numbers $p_1, \ldots, p_s$ (not necessarily distinct) such that
>
> $$n = p_1 \ldots p_s.$$

> **Example 5.2.3** — $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

It's also similar to our cycle decomposition theorem (rewritten for finite X):

> **Theorem**
>
> Let σ be a permutation on a finite set. Then there exists an integer $s \geq 0$ and cycles $\sigma_1, \ldots, \sigma_s$ (pairwise disjoint) such that
>
> $$\sigma = \sigma_1 \ldots \sigma_s.$$

> **Example 5.2.4** — $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\ 5)(3\ 7)(2\ 4\ 6).$

In all cases, the decomposition theorems are accompanied with "uniqueness" statements asserting that any two decompositions are the same *up to* reordering of factors.

"Reordering of factors" makes sense for positive integers because multiplication is commutative; it also makes sense for permutations because disjoint cycles commute (as we showed).

Does "reordering of factors" make sense for direct products? Yes. The direct product, as an operation on groups, enjoys a variety of nice properties.

> **Proposition 5.2.5**
>
> Let G, H, K be groups and let 1 denote the trivial group.
>
> $$\text{``identity'': } G \times 1 \;\cong\; 1 \times G \;\cong\; G$$
>
> $$\text{``associativity'': } G \times (H \times K) \;\cong\; (G \times H) \times K \;\cong\; G \times H \times K$$
>
> $$\text{``commutativity'': } H \times K \;\cong\; K \times H$$

Re: "associativity"—to be clear,

- elements of $G \times (H \times K)$ look like $\big(g, (h, k)\big)$
- elements of $(G \times H) \times K$ look like $\big((g, h), k\big)$
- elements of $G \times H \times K$ look like (g, h, k).

The proof of the Proposition is straightforward and left as an exercise.

5.2.1 Plan of action

So, now that we know what the fundamental theorem of abelian groups *means*, how do we *prove* it?

There are two main steps.

Step 1. Decompose our group into a product of p-groups.

Step 2. Decompose each p-group into a product of cyclic groups.

5.2.2 Step 1. Sylow meets Abel

Let G be an abelian group of order n. For each prime p, let k_p and r_p be positive integers such that $n = p^{k_p} r_p$ and $p \nmid r_p$. Then every Sylow p-subgroup of G has order p^{k_p}. Since G is abelian, every Sylow p-subgroup—indeed, every subgroup—of G is normal, and so we have $\mathrm{Syl}_p(G) = \{H_p\}$, say, for all p.

> **Lemma 5.2.6**
>
> Let $x \in G$. Then $x^{r_p} \in H_p$ for all primes p.

Proof. For ease of notation, let's drop the subscripts. We have

$$(x^r)^{p^k} = x^{r p^k} = x^n = e$$

so, by the Division Lemma, $o(x^r) \mid p^k$. Since p is prime, $o(x^r) = p^l$ for some $l \le k$. By Sylow's theorem, the p-subgroup generated by x^r is contained in some *Sylow* p-subgroup of G. Since H_p is the *only* Sylow p-subgroup of G, it follows that $x^r \in H_p$. $\qquad \square$

> **Theorem 5.2.7**
>
> Let G be a finite abelian group of order n and let r_p, H_p be as above. Then the map
>
> $$f : G \to \prod_{p|n} H_p$$
>
> whose p-coordinate is x^{r_p} is an isomorphism.

Proof. f is a homomorphism because G is abelian; in each coordinate, we have $(xy)^r = x^r y^r$.

To show f is injective, we show its kernel is trivial. If $f(x) = e$ then $x^{r_p} = e$ for all p, so $o(x) \mid r_p$ for all p. But no prime can divide *every* r_p, because $2 \nmid r_2$, $3 \nmid r_3$, etc. So: $o(x) = 1$, $x = e$, and ker f is trivial.

It follows that our embedding is an isomorphism because the orders match:

$$o(G) = n = \prod_{p|n} p^{k_p} = \prod_{p|n} o(H_p) = o\left(\prod_{p|n} H_p\right). \qquad \square$$

> **Example 5.2.8 —** Let $G = U(61)$. Then G is an abelian group of order $\varphi(61) = 60 = 2^2 \cdot 3 \cdot 5$. We have $r_2 = 15$, $r_3 = 20$, $r_5 = 12$. Our map f takes the form
>
> $$f(x) = (x^{15}, x^{20}, x^{12}).$$
>
> For example, $f(\overline{2}) = (\overline{11}, \overline{47}, \overline{9})$ and $f(\overline{-1}) = (\overline{-1}, \overline{1}, \overline{1})$.* One can verify that
>
> $$\begin{aligned} \text{im } f &= \{\overline{1}, \overline{11}, \overline{60}, \overline{50}\} \times \{\overline{1}, \overline{13}, \overline{47}\} \times \{\overline{1}, \overline{9}, \overline{20}, \overline{58}, \overline{34}\} \\ &= \langle \overline{11} \rangle \times \langle \overline{13} \rangle \times \langle \overline{9} \rangle \\ &= C_4 \times C_3 \times C_5. \end{aligned}$$
>
> ---
> *We write $\overline{a}$ instead of $[a]$ for clarity.

> **Corollary 5.2.9**
>
> Suppose $n = p_1^{k_1} \ldots p_s^{k_s}$ where $p_i \neq p_j$ for $i \neq j$. Then
>
> $$C_n \cong \prod_{i=1}^{s} C_{p_i^{k_i}}.$$

Exercise 158. What are the Sylow p-subgroups of $\mathbb{Z}/n\mathbb{Z}$? Find a formula for the map f. [Hint. Just determine $f(\overline{1})$.]

Exercise 159. Let G be a finite abelian group. Define the p-part of G to be the set

$$G_p = \{x \in G : x^{p^k} = e \text{ for some } k \geq 0\}.$$

Show that $G_p = H_p$.

5.2.3   Step 2. Primary decomposition

Definition 5.2.10 — A *primary group* is an abelian p-group for some prime p.

We've just shown that every finite abelian group can be written as a direct product of primary groups. Next, we'll show that every primary group can be written as a direct product of cyclic groups.

At the very least, we'd like to able to discern whether a given primary group is already cyclic. The "subgroup characterization" theorem says that, in general, if a given finite group G contains at most one subgroup of each possible order, then G is cyclic.

It turns out that for finite *primary* groups (i.e., finite *abelian* groups *of prime-power order*), a much better "subgroup characterization" theorem is available:

Lemma 5.2.11

Let G be a primary group with $o(G) = p^k$. If G has just one subgroup of order p, then G is cyclic.

Proof. By induction on k. The base case $k = 1$ is trivial because every group of order p is cyclic. Suppose the Lemma is true for all primary groups of order p^k, and let G be a primary group of order p^{k+1} with just one subgroup of order p. Call it H.

Consider the pth-power map $\pi(x) = x^p$. Since G is abelian, $\pi \in \text{End}(G)$. Since $o(H) = p$, $H \leq \ker \pi$ [because $x^p = e$ for all x in H]. Since H is unique, $\ker \pi \leq H$ [because if $x^p = e$ and $x \neq e$ then $\langle x \rangle$ is a subgroup of G of order p, so $\langle x \rangle = H$ meaning $x \in H$.] Thus $H = \ker \pi$.

Write G^p for $\text{im } \pi$. By the First Isomorphism Theorem, $G/H \cong G^p$, so, in particular, $o(G^p) = o(G)/o(H) = p^{k+1}/p = p^k$. Since $G^p \leq G$, every order-p subgroup of G^p is an order-p subgroup of G, so G^p can have at most *one* subgroup of order p. (And by Cauchy's theorem, G^p *does* have one.) By the inductive hypothesis, $G^p \cong G/H$ is cyclic.

163

Let $\bar{g}$ be a generator for G/H. We claim that g is a generator for G. Since the natural map $G \twoheadrightarrow G/H$ is a homomorphism, $o(\bar{g}) \mid o(g)$. Thus $o(g) = p^k$ or p^{k+1}. Either way, $\langle g \rangle$ contains a subgroup of order p, which must be H. Now if $x \in G$ is arbitrary, then $\bar{x} = \bar{g}^i$ for some i, so $x = g^i h$ for some h in H. But $H \leq \langle g \rangle$ means $h = g^j$ for some j, whence $x = g^{i+j}$. $\qquad\qquad\square$

Turning the Lemma on its head tells us that if G is a primary group with $o(G) = p^k$ which *isn't* cyclic, then G has *at least two* subgroups of order p. Before we take advantage of this crucial fact, we just need to introduce one more concept.

> **Definition 5.2.12 —** Let G be a finite group. A *maximal cyclic subgroup* of G is a cyclic subgroup C such that $o(C) \geq o(g)$ for all g in G.

Maximal cyclic subgroups all have the form $C = \langle c \rangle$ where $o(c) = \max\limits_{g \in G} o(g)$. Clearly, maximal cyclic subgroups exist: just pick an element with the biggest order.

Remark 5.2.13. While it's true that "maximal cyclic" subgroups are maximal among cyclic subgroups,* the converse is false [Exercise] so beware!

Now we're ready.

> **Theorem 5.2.14**
>
> Let G be a primary group with $o(G) = p^k$. Then every maximal cyclic subgroup of G has a complement.

Proof. If G is cyclic, then the only maximal cyclic subgroup of G is G itself, and we may (indeed, must) take the trivial subgroup as its complement.

If G is not cyclic, then let C be a maximal cyclic subgroup of G. Since C is cyclic (and nontrivial), C has exactly *one* subgroup of order p. Since G is *not* cyclic, G has *another* subgroup of order p, say K. Because K has prime order, $C \cap K$ must be trivial.[†]

If $k = 2$ then we're done: K is the desired complement to C (by the product formula).

Otherwise, consider the subgroup CK/K of G/K. By the *Diamond Theorem* [See Tutorial 9] we have that $CK/K \cong C/(C \cap K) \cong C$ is cyclic. Moreover, for all $\bar{g}$ in G/K, $o(\bar{g}) \mid o(g) \leq o(C) = o(CK/K)$ because C is maximal cyclic. Therefore CK/K is maximal cyclic!

---

*If C is maximal cyclic and $\langle g \rangle$ is a cyclic subgroup of G containing C, then $o(C) \leq o(g)$ because $C \leq \langle g \rangle$. But $o(C) \geq o(g)$ by definition of maximal cyclic. Thus $o(C) = o(g)$, so $C = \langle g \rangle$.

[†]$C \cap K \leq K$ so $o(C \cap K) \mid o(K) = p$ by Lagrange's theorem. Therefore $o(C \cap K) = 1$ or p—but the latter would imply $K \leq C$.

By induction, CK/K has a complement in G/K, say H/K for some subgroup H of G containing K.* We claim that H is the desired complement to C.

To show that CH = G, let $g \in G$. Since G/K = (CK/K)(H/K), there exist c in C and h in H such that $\overline{g} = \overline{ch}$, so g = chk for some k in K. But $K \leq H$ so $g \in CH$.

To show that $C \cap H$ is trivial, use the product formula *twice*:

$$o\,(G/K) = o(CK/K)o(H/K) \qquad \text{because G/K is the direct product}$$
$$= \frac{o(CK)o(H)}{o(K)^2} \qquad \text{by Lagrange's theorem}$$
$$= \frac{o(C)o(K)o(H)}{o(K)^2} \qquad \text{because } C \cap K \text{ is trivial}$$
$$= \frac{o(C)o(H)}{o(K)} \qquad \text{cancelling an } o(K)$$

Clearing denominators, we obtain o(G) = o(C)o(H). In light of the fact that G = CH (so o(G) = o(CH)) we conclude $o(C \cap H) = 1$, at last. □

> **Corollary 5.2.15**
> Every finite primary group is a direct product of cyclic groups.

Proof. Let G be a finite primary group.

Let G_1 be a maximal cyclic subgroup of G. If $G_1 = G$, we're done. Otherwise, by the Theorem, $G \cong G_1 \times H_1$ for some subgroup H_1 of G. Since G_1 is nontrivial, H_1 is proper, so $o(H_1) < o(G)$. By Lagrange's theorem, H_1 is again a finite primary group.

Let G_2 be a maximal cyclic subgroup of H_1. If $G_2 = H_1$, we're done. Otherwise, by the Theorem, $H_1 \cong G_2 \times H_2$ for some subgroup H_2 of H_1. Since G_2 is nontrivial, H_2 is proper, so $o(H_2) < o(H_1)$. By Lagrange's theorem, H_2 is again a finite primary group.

Continuing in this manner, we must eventually arrive at $G_s = H_{s-1}$ (lest $o(H_i)$ be a strictly decreasing sequence of integers). Putting it all together,

$$G \cong G_1 \times H_1$$
$$\cong G_1 \times G_2 \times H_2$$
$$\vdots$$
$$\cong G_1 \times G_2 \times \ldots \times G_{s-1} \times H_{s-1}$$
$$= G_1 \times G_2 \times \ldots \times G_{s-1} \times G_s$$

and the G_i are all cyclic. □

---

*That every subgroup of G/K has this form follows from the *Lattice Theorem*, a.k.a. the third isomorphism theorem [See PS6XQ5].

Here's an example to illustrate the proof.

> **Example 5.2.16 —** Let $G = U(60)$. We have
>
> $$o(G) = \varphi(60) = \varphi(4)\varphi(3)\varphi(5) = 2 \cdot 2 \cdot 4 = 16.$$
>
> It turns out that $\max\limits_{x \in U(60)} o(x) = 4 = o(\overline{7})$, so let
>
> $$G_1 = \langle \overline{7} \rangle = \{\overline{1}, \overline{7}, \overline{49}, \overline{43}\}.$$
>
> Then G_1 is a maximal cyclic subgroup of G. A complement of G_1 is
>
> $$H_1 = \langle \overline{11}, \overline{31} \rangle = \{\overline{1}, \overline{11}, \overline{31}, \overline{41}\}.$$
>
> Since $x^2 = \overline{1}$ for all x in H_1, every nontrivial cyclic subgroup of H_1 is maximal cyclic. Let
>
> $$G_2 = \langle \overline{11} \rangle = \{\overline{1}, \overline{11}\}.$$
>
> A complement of G_2 is
>
> $$H_2 = \langle \overline{31} \rangle = \{\overline{1}, \overline{31}\}.$$
>
> Since H_2 is cyclic, we're done: $G_3 = H_2$ and
>
> $$G \cong G_1 \times G_2 \times G_3,$$
>
> i.e.,
>
> $$U(60) \cong \langle \overline{7} \rangle \times \langle \overline{11} \rangle \times \langle \overline{31} \rangle$$
> $$\cong C_4 \times C_2 \times C_2.$$

> **Proposition 5.2.17**
>
> Suppose $n = p_1^{k_1} \dots p_s^{k_s}$ where $p_i \neq p_j$ for $i \neq j$. Then, up to isomorphism, the number of abelian groups of order n is
>
> $$\prod_{i=1}^{s} p(k_i)$$
>
> where p is the partition-counting function [See PS4XQ4c].

Proof. By Step 1, every abelian group of order n decomposes into s primary groups of orders $p_1^{k_1}, \dots, p_s^{k_s}$. By Step 2, every primary group of order p^k decomposes into cyclic groups of orders $p^{a_1}, \dots, p^{a_m}$. It follows that $k = a_1 + \dots + a_m$ so the numbers $a_1, \dots, a_m$ constitute a partition of the integer k. $\qquad \square$

Recall

n	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	2	3	5	7	11	15	22	30	42

Corollary 5.2.18

Here is the table of abelian groups of small orders.

order	number	groups
1	1	C_1
2	1	C_2
3	1	C_3
$4 = 2^2$	$p(2) = 2$	C_4, C_2^2
5	1	C_5
$6 = 2 \cdot 3$	$p(1)p(1) = 1$	$C_2 \times C_3 = C_6$
7	1	C_7
$8 = 2^3$	$p(3) = 3$	$C_2^3, C_2 \times C_4, C_8$
$9 = 3^2$	$p(2) = 2$	C_3^2, C_9
$10 = 2 \cdot 5$	$p(1)p(1) = 1$	$C_2 \times C_5 = C_{10}$
11	1	C_{11}
$12 = 2^2 \cdot 3$	$p(2)p(1) = 2$	$C_2^2 \times C_3, C_4 \times C_3 = C_{12}$

Example 5.2.19 — Given any n, we can classify the abelian groups of order n using its prime factorization. Let's do it for groups of order $n = 40 = 2^3 \times 5$.

Step 1 tells us any group of this form must be isomorphic to $H_2 \times H_5$, where $o(H_2) = 8$ and $o(H_5) = 5$. Then $H_5 \cong C_5$. As for H_2, its maximal cyclic group can be C_8, C_4, or C_2. In the first case, we are done. In the next two cases, the complements are C_2 and $C_2 \times C_2$ (since the complement cannot be cyclic and bigger than C_2) respectively.

Putting it together, the abelian groups of order 40 are

$$C_8 \times C_5, C_2 \times C_4 \times C_5, \text{ and } C_2 \times C_2 \times C_2 \times C_5.$$

Exercise 160. Classify the number of abelian groups of order 120.

5.2.4   About $U(n)$

The most important finite abelian groups are the multiplicative groups of integers $U(n)$. The greedy algorithm described above is *not* the most practical way to decompose these

particular groups into products of cyclic p-groups.

We do know, however:

> **Theorem 5.2.20** (PS3Q3b))
>
> Suppose $n = p_1^{e_1} \dots p_k^{e_k}$ where $p_i \neq p_j$ for $i \neq j$. Then
>
> $$U(n) \cong \prod_{i=1}^{k} U(p_i^{e_i}).$$

Thus the problem of decomposing $U(n)$ is reduced to the problem of decomposing $U(p^k)$. As we saw in Theorem 2.2.16, if p is odd, then $U(p^k)$ and $U(2p^k)$ are cyclic, while if p is 2, then $U(2)$ is trivial, $U(4) = \langle \overline{3} \rangle$ is cyclic, and $U(2^k)$ is *not* cyclic for $k \geq 3$.

> **Proposition 5.2.21**
>
> $U(2^k) = \langle \overline{-1} \rangle \langle \overline{5} \rangle \cong C_2 \times C_{2^{k-2}}$ for $k \geq 3$.

Proof. Exercise. [Show that $o([5]) = 2^{k-2}$. Then show that $\langle [-1] \rangle$ is a complement of $\langle [5] \rangle$.] $\qquad \square$

With that, we may decompose any $U(n)$.

> **Example 5.2.22 —**
>
> $$U(60) \cong U(4) \times U(3) \times U(5)$$
> $$\cong C_2 \times C_2 \times C_4.$$
>
> Painless!

> **Example 5.2.23 —**
>
> $$U(301) \cong U(7) \times U(43)$$
> $$\cong C_6 \times C_{42}$$
> $$\cong (C_2 \times C_3) \times (C_2 \times C_3 \times C_7)$$
> $$\cong C_2 \times C_2 \times C_3 \times C_3 \times C_7.$$

> **Example 5.2.24 —**
>
> $$U(2024) \cong U(8) \times U(11) \times U(23)$$

$$\cong C_2 \times C_2 \times C_{10} \times C_{22}$$
$$\cong C_2 \times C_2 \times C_2 \times C_2 \times C_5 \times C_{11}.$$

5.3 Isometries

This lecture is mostly pictures.

5.3.1 Symmetries, mathematically

When we talk about symmetries of real-life objects, we're really talking about symmetries of their abstract, idealized forms. Losing contact with reality is unavoidable when passing into the mathematical realm. For example, nothing in real life *actually* has true translational symmetry—everything real is finite. Even finite symmetry—invariance under rotation or reflection—is practically impossible to verify. To be absolutely certain, you'd have to be able to compare the positions of ~~molecules~~ no, ~~atoms~~ no, electrons and quarks, before and after your transformation.

So when we speak of symmetries of real-life objects, we do so only in an approximate sense. But what are we approximating? What are symmetries, mathematically?

5.3.2 Isometries of the Euclidean space

Definition 5.3.1 — An *isometry* is a bijective function $f : \mathbb{R}^n \to \mathbb{R}^n$ satisfying

$$d(f(u), f(v)) = d(u, v)$$

for all u and v in $\mathbb{R}^n$. The set of all isometries of $\mathbb{R}^n$ is denoted $\mathrm{Isom}(\mathbb{R}^n)$.

Proposition 5.3.2

$\mathrm{Isom}(\mathbb{R}^n) \le \mathrm{Sym}(\mathbb{R}^n)$.

Proof. Exercise. □

The two most important kind of isometries are:

- Translations. For every vector v, the function $t(x) = x + v$ is called *translation-by-v*. The set of all translations of $\mathbb{R}^n$ is denoted T.

- Isometries that fix the origin. The set of all origin-fixing isometries of $\mathbb{R}^n$ is denoted O.

> **Proposition 5.3.3**
>
> $T \cong \mathbb{R}^n$ and $T \le \mathrm{Isom}(\mathbb{R}^n)$.

Proof. See the non-examinable handout. □

> **Proposition 5.3.4**
>
> O is the group of orthogonal matrices $O_n(\mathbb{R})$.

Proof. See the non-examinable handout. □

> **Theorem 5.3.5**
>
> $\mathrm{Isom}(\mathbb{R}^n) = TO$.

> **Corollary 5.3.6** (Fundamental theorem of Euclidean isometries)
>
> Every isometry of $\mathbb{R}^n$ is affine (i.e. has the form $x \mapsto Ax + b$ for some orthogonal matrix A and some vector b).

We may now use the language of isometries to describe symmetries of objects.

Definition 5.3.7 — Let $S \subseteq \mathbb{R}^n$. The *relative isometry group* of S is the setwise stabilizer of S in $\mathrm{Isom}(\mathbb{R}^n)$:

$$\mathrm{Isom}_{\mathbb{R}^n}(S) = \mathrm{Stab}_{\mathrm{Isom}(\mathbb{R}^n)}(S) = \{f \in \mathrm{Isom}(\mathbb{R}^n) : f(S) = S\}$$

We call this "the isometry group of S in $\mathbb{R}^n$", or "the symmetry group of S".

Example 5.3.8 — The isometry group of the unit circle in $\mathbb{R}^2$ is $O(2)$.

Example 5.3.9 — The isometry group of a regular n-gon in $\mathbb{R}^2$ with its center at the origin is the subgroup generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}.$$

Exercise 161. Show that this group is isomorphic to D_n.

Exercise 162 (Tedious)**.** Express the isometry groups of the Platonic solids as matrices in $\mathbb{R}^3$.

> **Example 5.3.10 —** The isometry group of a solid line in $\mathbb{R}^2$ is the group generated by the translations along that line, the reflections across it, and the rotations about its points.

> **Example 5.3.11 —** The isometry group of a rectangle R in $\mathbb{R}^2$ comprises the reflections h and v over the horizontal and vertical, and the 180-degree rotation r. We have $hv = vh = r$ so $\text{Isom}_{\mathbb{R}^2}(R) = \{e, h, v, r\} \cong D_2$.

> **Example 5.3.12 —** The isometry group of $\mathbb{Z}$ in $\mathbb{R}$ is the set of all isometries of $\mathbb{R}$ that send integers to integers. If $\mathbb{Z}$ is fixed by $x \mapsto x + b$ then $b \in \mathbb{Z}$, and this is the only restriction: every translation-by-an-integer fixes $\mathbb{Z}$ setwise. Similarly, if $x \mapsto b - x$ fixes $\mathbb{Z}$ then $b \in \mathbb{Z}$, and every reflection across a half-integer fixes $\mathbb{Z}$ setwise. Thus $\text{Isom}_{\mathbb{R}}(\mathbb{Z}) = \{x + n, -x + n : n \in \mathbb{Z}\}$.
>
> In fact, we can show in Exercise 79 that $\text{Isom}_{\mathbb{R}}(\mathbb{Z})$ is infinite dihedral.

Exercise 163. Embed $\mathbb{Z}$ in $\mathbb{R}^2$ by sending it to the integer points on the x-axis. What is $\text{Isom}_{\mathbb{R}^2}(\mathbb{Z})$?

Remark 5.3.13. Careful—the negation map $x \mapsto -x$ is a *reflection* in odd dimension and a *rotation* in even dimension!

For the purposes of this lecture, let's say that an *isometry group* is the relative isometry group of any subset of $\mathbb{R}^n$. Given an isometry group G, we can discuss the translations and origin-fixing isometries in G separately.

> **Definition 5.3.14 —** Let G be an isometry group. The *translation part* of G is the subgroup of translations in G, namely $G_{tr} = G \cap T$.

Since T is normal in $\text{Isom}(\mathbb{R}^n)$, it follows that G_{tr} is normal in G. The quotient has a special name:

> **Definition 5.3.15 —** Let G be an isometry group. The *point part* of G is the quotient of G by its translations, namely $G_{pt} = G/G_{tr}$.

The world of isometry groups is vast and wild; they're extremely hard to classify. Even if we restrict our attention to isometry groups with finite point-part and finitely-generated translation-part, the situation is quite complex. As an illustration, suppose that the translation part cannot be generated by fewer than n independent translations, where n is the dimension of the ambient space. Such groups are called *space groups**. While it is known that there are only finitely many different "types" of space groups in each dimension, their exact number is only known in dimensions 1–4:

n	number	name
1	2	-
2	17	wallpaper group
3	230	crystallographic group
4	4783	-

We are nowhere near being able to classify space groups beyond dimension 1, but we *can* say a little about isometry groups in dimension 2.

5.3.3 Isometry groups in $\mathbb{R}^2$

Let G be the isometry group of some set S in $\mathbb{R}^2$ with finite point-part and finitely-generated translation-part. Then we have three families of groups depending on the size of G_{tr}:

If G_{tr} is trivial, S has no translational symmetry, and G is called a *rosette group*. We've already seen every rosette group:

> **Proposition 5.3.16**
>
> Let G be an isometry group in $\mathbb{R}^2$ such that G_{tr} is trivial and G_{pt} is finite. Then $G \cong C_n$ or $G \cong D_n$ for some $n \geq 1$.

Proof. See the non-examinable handout. □

If G_{tr} is cyclic, S has translational symmetry along one direction, and G is called a *frieze group*. There are 7 such groups, and we will leave the classification of Frieze groups for a non-examinable handout.

If G_{tr} is not cyclic, it is generated by two translations, and so S fills the entire space. G is called a *wallpaper group* and there are 17 of these groups. The classification of G is way

---

*Because S extends to infinity along n independent directions and so must fill the entire space.

beyond the scope of this course, but the link on the previous page provides some visuals of what the symmetries look like.