Abstract Algebra and Number Theory
Course notes and exercises

Duncan Clark, PhD

Last updated: January 22, 2025

Sections

0 Preface

0.1 How to use these notes

These course notes and exercises are intended to serve as an aid to the class. Notes for sections contain big picture ideas, definitions, statements and proofs of theorems and main propositions, and worked out examples (when appropriate). They are not meant as a substitution for attending class, but rather as a reference.

I *highly encourage* you to work through the exercises as we cover the topics in class. My intention is to have problems at various difficulty levels (problems prefaced with the symbol * are challenge problems). Keep in mind, the struggle you experience when trying and failing at a problem *is* learning—keep at it and ask me questions as you have them.

Terms in **bold** are typically (parts of) definitions. Definitions are the basis of mathematics, and this course is one in your mathematical journey where they become very important. In this course we also learn a handful of nontrivial theorems. In addition to solving problems, a good place to start with studying is to know the definitions and theorems for the content

covered: i.e., know why the definition does what we want it to, and what each of the theorems are, how to use them, and why the conditions are needed.

0.2 Computational resources

We will learn a variety of algorithms that become somewhat tedious to execute by hand. WolframAlpha is perhaps the easiest to use due to its natural language processing of input queries (though is somewhat limited in its modularity). Knowledge of programming is not strictly required for this course, but some familiarity with computational packages (i.e., Numpy via Python, MATLAB is also suitable) can go a long way.

0.3 Licensing

This note and exercise packet is licensed under the Creative Commons CS BY-NC-SA 4.0 License.

1 Set theory

(Most) modern mathematics uses the language of *set theory* to make precise statements. Even if you've never used set theory explicitly, I'm sure you already have *some* familiarity with the formality involved. Abstractly, a **set** is just a collection of **things**[1], where by *collection* we mean an unordered list without repeat entries.

Sets can have finite or infinitely many things in them. For finite sets there's nothing wrong with just listing the elements of the set, i.e.,

$$A = \{a, b, c\}$$

Sets are the same (i.e., "equal") when they contain the same things. That is, if a, b, c are distinct things then the following sets are all equal

$$\{a, b, c\} = \{b, c, a\} = \{a, a, b, c\}$$

The set $\{\}$ which has no elements is called the **empty set**. Typically we use $\emptyset$ to denote this set.

1.1 Set builder notation

Often it is not feasible to define a set by simply listing all of its elements. **Set builder notation** is a useful formality for describing the elements of a set based on some rule. For instance, writing the statement

$$A = \{x : x \text{ is an even integer}\}$$

defines the set $A = \{\dots, -2, 0, 2, 4, 6, \dots\}$. Note here that the "..." on either end denote that *the evident pattern should continue*. An upshot to set-builder notation is that is gets around the somewhat imprecise "evident pattern" by giving a description of the properties shared by generic elements in your set.

Similarly,

$$B = \{x : \ x \text{ is a real number and } 2 < x \leq 3\}$$

defines the half-open interval $(2, 3]$.

In general, you can think of set builder notation as telling you the following meta-information

$$\{ \text{ "stuff" : properties that this stuff has to have}\}$$

1.2 Example. Some common symbols for useful sets are listed below

- The set of integers $\mathbf{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$
- The set of strictly positive integers $\mathbf{N} = \{1, 2, 3, 4, \cdots\}$, i.e., "natural numbers" (There's always a nitpicking issue of do we want 0 to be a natural number or not[2], but this is the symbol we'll use)

[1] Things which, themselves, must be sets. Is this paradoxical?

[2] You may have strong opinions on this if you're a computer scientist (or if you're in France)

- The set of nonnegative integers $\mathbf{Z}_{\geq 0} = \{0, 1, 2, 3, \cdots\}$
- The set of rational numbers $\mathbf{Q} = \{p/q : p \in \mathbf{Z} \text{ and } q \in \mathbf{N}\}$, i.e., "fractions"
- The set of real numbers $\mathbf{R}$ (*Question: how do you define this?*)
- The set of complex numbers $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$
- The empty set $\emptyset$, i.e., "the set with no elements"

It may seem silly now to have a set with no elements, but it's perhaps one of the most useful sets of all.

1.3 Set operations

Sets do not live in isolation, we need operations with which to compare them. Let A be a set. We need a symbol to talk about things that are in this set. We call such things **elements** and write $x \in A$ to mean "x is an element of A".

Similarly, if B is also a set then writing $A \subset B$ means "A is a subset of B". That is, any element $x \in A$ is also an element $x \in B$.

1.4 Definition. *Let A, B be sets. We say that A and B are **equal** if both $A \subset B$ and $B \subset A$. If A and B are equal we write $A = B$.*

If $A \subset B$ we will also write A^c to mean the **complement** of A (in B). That is, $A^c = B \setminus A$.

1.5 Definition. *Let A and B be sets. The following are also sets*

$A \cup B = \{x : x \in A \text{ or } x \in B\}$	"A ***union*** B"
$A \cap B = \{x : x \in A \text{ and } x \in B\}$	"A ***intersect*** B"
$A \setminus B = \{x : x \in A \text{ and } x \notin B\}$	"A ***minus*** B"
$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$	"A ***times*** B" or the ***product*** of A and B

Note when taking the product of a set A with itself we usually write $A^2 = A \times A$, $A^3 = A \times A \times A$, etc.[3]. Two sets A and B are said to be **disjoint** if $A \cap B = \emptyset$.

1.6 Power sets

If A is a set, we write $\mathcal{P}(A)$ to denote the **power set** of A. In words $\mathcal{P}(A)$ is the collection of all subsets of A (note that $\emptyset$ is trivially a subset). We give a precise mathematical definition as

$$\mathcal{P}(A) = \{X : X \subset A\} \tag{1.6.1}$$

[3]Hence the notation you may recall from calculus: $\mathbf{R}^2$ the real plane, $\mathbf{R}^3$ the real space, etc.

1.7 Functions

A **function** is a rule that assigns elements from one set to elements in another set. We write $f\colon A \to B$ to say that f is a function from set A to set B. A is called the **domain**. If $x \in A$ we write $f(x)$ for the image of x under f in B[4].

The set $f(A)$ defined by

$$f(A) = \{f(x) : x \in A\} \subset B$$

is called the **image** or **range** of f (in B). Similarly, if $Y \subset B$ is a subset then $f^{-1}(Y) = \{a \in A : f(a) \in Y\}$ is called the **pre-image** of f (in A).

1.8 Example. Note that in the world of set theory, everything has to be a set. That means functions are sets; that is, a function $f\colon A \to B$ is just the collection

$$G_f = \{(a, f(a)) : a \in A\} \subset A \times B \tag{1.8.1}$$

The letter G here is suggestive of graph, which is what this set is (given that we have "pictures" for A and B). Conversely, any set $G \subset A \times B$ such that for each $a \in A$ there is a unique $b \in B$ ($b = f(a)$) with $(a, b) \in G$ is the graph of a function f. When is a function is indeed a function we say that it is **well-defined**.

1.9 Injective and surjective functions

Let A, B be sets and f a function $f\colon A \to B$.

- We say that f is **injective** (or **one-to-one**) if for any elements $x \in A$ and $y \in A$ such that $f(x) = f(y)$, then $x = y$.
- We say that f is **surjective** (or **onto**) if for any element $x \in B$ there is an element $a \in A$ such that $f(a) = x$
- A function f is called **bijective** if f is both injective and surjective.

1.10 Inverse functions

For any set A, the **identity function** on A, denoted $\mathbf{1}_A$ is the function $A \to A$ such that $\mathbf{1}_A(x) = x$ for all $x \in A$. Let A, B be sets and $f\colon A \to B$, $g\colon B \to A$ be functions. We say that f and g are **inverse** if both

$$g \circ f = \mathbf{1}_A \quad \text{and} \quad f \circ g = \mathbf{1}_B$$

If f and g are inverse we write $g = f^{-1}$ (and similarly, $f = g^{-1}$). It's a nice exercise then to show the following: If a function $f\colon A \to B$ is bijective, it must have an inverse.

[4]Note: $f(x)$ is an element of the set B, f is the function. If you want to talk about a function while mentioning a generic input, you can use the notation $f\colon x \mapsto f(x)$.

1.11 Equivalence relations

An **equivalence relation** $\sim$ on a set X is a way of creating a new set by equating elements from X if they share some common feature. Think of $\sim$ as an abstraction of usual equality "=" of numbers—it must satisfy certain axioms.

Given a set X an equivalence relation $\sim$ must satisfy the following properties

- $x \sim x$ for all $x \in X$
- If $x, y \in X$ such that $x \sim y$, then $y \sim x$
- If $x, y, z \in X$ such that $x \sim y$ and $y \sim z$, then $x \sim z$

For instance, you can define the relation $\sim$ on $\mathbf{Z}$ by $n \sim m$ if $n - m$ is an even integer.

In the same way that functions are *sets*, equivalence relations are also sets. You can check that $\sim$ being an equivalence relation on X is same as being a subset of $S \subset X \times X$ such that $x \sim y$ if and only if $(x, y) \in S$.

1.12 Partitions of a set

Any equivalence relation on X defines a **partition** of X into disjoint pieces X_i, for i in some indexing set I, by $x, y \in X_i$ if and only if $x \sim y$. These sets X_i must satisfy the following properties

- $X = \bigcup_{i \in I} X_i$
- $X_i \cap X_j = \emptyset$ if $i \neq j$.

It's a good exercise to check that this goes the other way as well: that is, that partitions of X are in one-to-one correspondence with equivalence relations on X. Given an equivalence relation $\sim$ on a set X we write $X/\sim$ for the associated partition by set of equivalence classes.

1.13 Exercises

1. Let $A = \{a, b, c\}, B = \{1, 2, 3\}$ and $C = \{x\}$. List the elements in each of the following sets
   a. $A \cup B$
   b. $A \cap (B \cup C)$
   c. $B \times C$
   d. $A \times B \times C \times \emptyset$
2. Let A and B be subsets of some set X and write A^c, B^c for their complements (in X). Prove the following[5]
   a. $(A \cup B)^c = A^c \cap B^c$

[5] These are often called De Morgan's Laws

b. $(A \cap B)^c = A^c \cup B^c$

3. Let $S = \{1, 2, 3, 4, 5\}$ and defined $\pi \colon S \to S$ by the following

$$\pi(1) = 2, \quad \pi(2) = 3, \quad \pi(3) = 1, \quad \pi(4) = 5, \quad \pi(5) = 4$$

   a. Prove that π is a bijection

   b. Describe π^{-1}

   c. Is there any k such that $\pi^k = \underbrace{\pi \circ \pi \circ \cdots \circ \pi}_{k \text{ times}} = \mathbf{1}_S$?

4. Let $f \colon X \to Y$ and $g \colon Y \to Z$ both be bijective functions. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

5. For each of the following functions determine (i) if the function is well-defined, (ii) if the function is injective, (iii) if the function is surjective

   a. $f \colon \mathbf{R} \to \mathbf{R}$, $f(x) = e^x$

   b. $g \colon \mathbf{Z} \to \mathbf{Z}$, $g(n) = \dfrac{n(n+1)}{2}$

   c. $h \colon \mathbf{N} \to \mathbf{Q}$, $h(n) = \dfrac{1}{n}$

   d. $s \colon \mathbf{Z} \to \mathbf{R}$, $s(x) = \sin(\pi x/2)$

   e. $q \colon \mathbf{R} \to \mathbf{Z}$, $q(x) = \lfloor x \rfloor$ (note that $\lfloor x \rfloor$ is defined as the largest integer $n \leq x$).

6. Define a function $f \colon \mathbf{N} \to \mathbf{N}$ that is injective but not surjective. Define a function $\mathbf{Q} \to \mathbf{Z}$ that is surjective but not injective.

7. Your friend Jimbo tries to define a function $f \colon \mathbf{Q} \to \mathbf{Z}$ given by $f(p/q) = p$. Explain why this is not well-defined.

8. Let $f \colon X \to Y$ be a function and $A, B \subset X$. Show that $f(A \cap B) \subset f(A) \cap f(B)$. Give an example where the two sets are not equal.

9. Define an equivalence relation $\sim$ on $\mathbf{Z} \times \mathbf{N}$ so that the associated set of partitions is equal to $\mathbf{Q}$.

10. Show that the following produces an equivalence relation on $\mathbf{R}^2 \backslash \{(0,0)\}$: $(a, b) \sim (x, y)$ if there is a real number $c \neq 0$ such that $a = cx$ and $b = cy$.[6]

11. For a finite set X, let $|X|$ denote the number of elements of X. Let X be a finite set. Does the following define an equivalence relation on $\mathcal{P}(X)$? For $A, B \subset X$, $A \sim B$ if and only $|A| = |B|$.

[6] The associated set of equivalence classes is called the *real projective plane* and is equal to the set of lines through the origin in $\mathbf{R}^2$. This set can be topologized in a standard way, and is one of the classic examples of a non-orientable surface (See also the Klein bottle and Möbius strip).

12. Write $\mathrm{GL}(2, \mathbf{R})$ for the set of 2×2 invertible matrices with real entries. Define a relation $\sim$ on $\mathrm{GL}(2, \mathbf{R})$ as follows. Matrices A, B have $A \sim B$ if and only if there is an invertible matrix $P \in \mathrm{GL}(2, \mathbf{R})$ such that $A = PBP^{-1}$. Show that this is an equivalence relation. What is the associated set of equivalence classes?

13. Let's call a set X **countable** if there is a surjection $\mathbf{N} \to X$ (or equivalently, an injection $X \to \mathbf{N}$). Show that the following sets are countable.

    a. The set of even integers

    b. The set of prime numbers

    c. The power set $\mathcal{P}(S)$ for $S = \{1, 2, 3\}$

    d. *Challenge.* The set $\mathbf{Q}$ of rational numbers

14. *Challenge.* A set which is not countable is called **uncountable**. Which of the following sets do you think are uncountable.

    a. $\mathbf{Z}$

    b. $\mathbf{N} \cup \{\text{☺}\}$

    c. $\mathbf{R}$

    Hint: Complete the argument shown in class: Suppose that there is an onto function f from $\mathbf{N}$ to the interval $(0, 1) \subset \mathbf{R}$. For $n \in \mathbf{N}$, write $f(n) = 0.a_{n,1}a_{n,2}a_{n,3}a_{n,4}\cdots$ as the infinite decimal corresponding to $f(n)$. Define $b \in (0, 1)$ by its decimal expansion $b = 0.b_1b_2b_3b_4\cdots$ where b_i is given by

    $$b_i = \begin{cases} 7 & \text{if } a_{i,i} = 6 \\ 6 & \text{otherwise} \end{cases}$$

    The claim is not b is not in the range of f. See also Cantor's diagonal argument.

    d. The set of all (straight) lines in the plane $\mathbf{R}^2$.

15. *Challenge.* Let $X \neq \emptyset$ be a set. How many functions are there $f\colon X \to \emptyset$? How many functions are there $\emptyset \to \emptyset$?

2 Divisors and prime numbers

We now begin our section on number theory. One of the oldest fields of mathematics, number theory classically deals with understanding the properties of the integers. As you probably know, integers can be *added* and *multiplied*—the additive structure of $\mathbf{Z}$ is fairly straightforward—it's the multiplicative structure that is very rich.

2.1 Divisors

Let n, m be integers. We say that m **divides** n if there is another integer q such that $n = mq$. In notation this is written $m \mid n$. Given that n, n' are integers with $n' \mid n$ we call n' a **divisor** of n. Note that trivially, 1 divides all integers.

2.2 The division algorithm

It's one thing to know *if* an integer divides another, but it leaves the question of *how* still open. An answer comes from one of the oldest algorithms: the *division algorithm*. This is in essence "long division" as you know it, but let's be very careful in explaining *why* this is permitted.

2.3 Theorem (The division algorithm)**.** *Given integers n, m with $m > 0$, there are unique integers q, r with $0 \leq r < m$ such that*

$$n = mq + r$$

Proof. Let n, m be given with $m > 0$. What we need to do here is construct the numbers q, r claimed to exist by this theorem. Let's define the set S by

$$S = \{n - km : k \in \mathbf{Z} \text{ and } n - km \geq 0\}$$

Think of S as a collection of "possible remainders" for the division. Note right away that if $0 \in S$ we're done, since then $r = 0$ and q is given by the k such that $n - km = 0$. Also, if $n = 0$ this problem is solved trivially.

So let's suppose that $0 \neq S$. The first claim is that $S \neq \emptyset$. If $n > 0$ note $n - 0 \cdot m = n \in S$, if $n < 0$ then since $m > 0$, we must have $n - (2n)m = n(1 - 2m) \in S$. Either way $S \neq \emptyset$.

Now $S \subset \mathbf{N}$ by construction, so from theorem A.5 we know S has a least element. Let's call it r. We then have $r = n - mq$ for some $q \in \mathbf{Z}$. We claim that these r, q are the integers we want. Note that $r \geq 0$ by design. Let's show that $r < m$. Suppose otherwise, that is $r \geq m$. Set $r' = n - m(q + 1)$. Note that

$$r' = n - mq - m = r - m \geq 0$$

but also $r' < r$. This is a contradiction, since r was assumed to be the smallest element of S. Therefore we have integers q, r with $0 \leq r < m$ such that

$$n = mq + r$$

as claimed.

Now we show that this decomposition is unique. Suppose there were another pair q', r' such that $n = mq' + r'$ and $0 \leq r' < m$. Without loss of generality, assume $r' > r$. Then we must have

$$mq + r = mq' + r'$$

so that $m(q' - q) = r' - r$. But that is to say that m divides $r' - r$. However, $0 \leq r' - r < m$, and therefore $r' - r = 0$. Thus $r = r'$ and $q = q'$. □

The term q is called the **quotient** and r the **remainder**. Note that $m \mid n$ if and only if the corresponding remainder $r = 0$.

2.4 Common divisors

Given integers n, m we say that $d \in \mathbf{Z}$ is a **common divisor** of n and m if both $d \mid n$ and $d \mid m$. Note that the collection of common divisors of n, m is a finite subset of $\mathbf{Z}$ so must have a largest element.

We say that $d \in \mathbf{Z}$ is the **greatest common divisor** of n and m if the following are satisfied

- $d > 0$
- d is a common divisor of n and m
- for any other common divisor d' of n and m, we have $d' \mid d$

Notation-wise we write $\gcd(n, m)$ for the greatest common divisor of n, m. A pair of integers n, m is called **relatively prime** if $\gcd(n, m) = 1$.

As it turns out, computing the gcd of a pair of integers is an extremely useful tool (we'll see this is our section on cryptography later on). One famous and useful algorithm for doing so is the Euclidean algorithm[7].

2.5 Example (The Euclidean algorithm[8]). Let $n, m \in \mathbf{Z}$. We will describe an algorithm for how to determine $\gcd(n, m)$ by repeatedly using theorem 2.3. Without loss of generality, let's assume that $n, m \geq 0$ and that $n > m$. First note that $\gcd(n, 0) = n$, since any integer divides 0 trivially. So, let's use theorem 2.3 to write

$$n = mq + r, \quad 0 \leq r < m \tag{2.5.1}$$

Now, we claim that $\gcd(n, m) = \gcd(m, r)$. This follows from noting that from (2.5.1) if $d \mid m$ then $d \mid n$ if and only if $d \mid r$.

Note what has happened: we've reduced the "size" of the numbers appearing and have kept the came greatest common divisor. Here's where the algorithm comes in. Define $(q_i, r_i)_{i \geq 1}$ of pairs of integers as follows. For $i \geq 1$, use the division algorithm theorem 2.3 to define q_i, r_i as follows:

$$\begin{aligned} n &= mq_1 + r_1 \\ m &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ r_2 &= r_3 q_4 + r_4 \\ &\vdots \end{aligned} \tag{2.5.2}$$

where $r_{i-1} = r_i q_{i+1} + r_{i+1}$ for $i \geq 1$. The claim is that $r_k = 0$ for some k. Note that from theorem 2.3, we must have $r_i \geq 0$ for all $i \geq 1$, and $m > r_1 > r_2 > r_3 > \cdots$[9]. So, since

[7] Named after Euclid, the famous ancient Greek mathematician, and who you might recall from Euclidean geometry

[8] Euclid, *Elements* Book 7, proposition 2

[9] In fact more is ture, see Sec. 2.14 Ex. 8.

there are only finitely many positive integers strictly less than m, it must be the case that $r_k = 0$ for some k.

Suppose that k is the smallest k with $r_k = 0$. The claim is that $r_{k-1} = \gcd(n, m)$. This follows from the above discussion, since each step in (2.5.2) preserves the greatest common divisor and so

$$\gcd(n, m) = \gcd(m, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(d, 0) = d$$

Moreover, the steps from (2.5.2) can be reversed to produce integers r, s such that $d = nr + ms$, resulting in a constructive proof of the following theorem. This is something of a pain to do by hand, but a computer is more than happy to calculate it for you.

2.6 Theorem. *For any pair of integers n, m there are integers r, s such that $\gcd(n, m) = nr + ms$.*

2.7 Corollary (Bézout's identity)**.** *Let $n, m \in \mathbf{Z}$ such that n, m are coprime. Then there are integers $r, s \in \mathbf{Z}$ such that $1 = nr + ms$.*

Corollary 2.7 can be thought of geometrically as follows: If n, m are coprime integers, then the *line*

$$1 = nx + my$$

in the xy-plane $\mathbf{R}^2$ must pass through some integer lattice point (i.e., point of the form $(r, s) \in \mathbf{Z}^2 \subset \mathbf{R}^2$). In fact more is true, as knowing just one solution (r, s) to the greatest common divisor problem produces *all* possible integer solutions as follows.

2.8 Theorem. *Let $n, m \in \mathbf{Z}$ and write $d = \gcd(n, m)$. Suppose that (r, s) is solution to the equation $d = nr + ms$. Then the set of all solutions (x, y) to $d = nx + my$ is given by*

$$\{(r + km/d, s - kn/d) : k \in \mathbf{Z}\}$$

2.9 Prime numbers

Of important use in number theory are the prime numbers. If you are familiar with the idea of a *basis* from linear algebra, you can think of the set of primes as "multiplicative basis" for the integers with respect to the multiplication. Let's start with a definition.

2.10 Definition. *An positive integer $p \geq 2$ is **prime** if the only (positive) divisors of p are 1 and p.*

It's somewhat of a moot point, but 1 is not prime. You can think of an equivalent description of a prime number as one whose set of (positive) divisors has exactly two elements.

Let's define $\mathbf{P}$ to be the collection of all prime integers. Clearly $\mathbf{P} \subset \mathbf{N}$, and if we were to enumerate the prime numbers we'd have a list that begins

$$\mathbf{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \cdots\}.$$

We'll see later on that prime numbers play a very important role in the number of elements that can appear in (finite) groups. For now, let's build up some intuition about prime numbers and learn some tools that we can use in working with them.

2.11 Theorem. *There are infinitely many prime numbers.*

Proof. This is a recent proof, dating back to Euclid circa 300BC[10]. Suppose that $\mathbf{P}$ were finite. Then there is $k \geq 1$ such that

$$\mathbf{P} = \{p_1, p_2, p_3, \cdots, p_k\}$$

We'll show that this list cannot be complete. Define an integer n as follows:

$$n = p_1 p_2 \cdots p_k + 1$$

The claim is now that n has a prime factor q not contained in $\mathbf{P}$.

Since $n \in \mathbf{N}$ it is either a prime or not. If n is a prime, then since $n > p$ for each $p \in \mathbf{P}$ (by construction) it can't be in $\mathbf{P}$. Oops, looks like our list was not complete.

If n isn't prime, then it must have a divisor p which is prime. Let $p \in \mathbf{P}$ be such a divisor. Then $p \mid n$. But then also $p \mid p_1 p_2 \cdots p_k = (n-1)$. So, $p \mid (n - (n-1)) = 1$. But no prime divides 1, so p could not have come from the collection $\mathbf{P}$.

Either way, $\mathbf{P}$ was not a complete list of all primes. Since k was arbitrary, $|\mathbf{P}| > k$ for all $k \geq 1$, so $\mathbf{P}$ must be infinite. □

The next theorem tells us a precise manner in which the primes form a "multiplicative basis" for the integers.

2.12 Theorem (Unique decomposition into prime components)**.** *For any $n \geq 2$, there is a unique list of prime numbers $p_1, p_2, \cdots, p_k \in \mathbf{P}$ together with exponents $m_1, m_2, \cdots, m_k \geq 1$ such that*

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

Proof. First let's show that such a decomposition into primes exists. Let $S \subset \mathbf{N}$ be the collection of integers (≥ 2) that don't have such a decomposition. If $S \neq \emptyset$, then S has a smallest element, call it n. By assumption n cannot be prime, so $n = ab$ for some integers $a, b > 1$. But then both $a < n$ and $b < n$, so $a, b \notin S$. Therefore a, b have decompositions into prime numbers, and so n must as well. Thus $S = \emptyset$.

Now we show uniqueness. This is a good application of induction[11]. Clearly 2 has a unique decomposition into prime numbers. So let's assume that we have an $n \in \mathbf{N}$ such that all integers n' with $2 \leq n' < n$ have unique decompositions into primes. Suppose that n has two decompositions

$$n = p_1^{m_1} p_2^{m} m_2 \cdots p_k^{m_k} = q_1^{r_1} q_2^{r_2} \cdots q_\ell^{r_\ell}$$

into primes, and let's arrange them such that p_1 and q_1 are the smallest such prime factors appearing in the list. Note that if $k = \ell = 1$ we're done, so there's really only something interesting going on here when these are at least 2.

[10] Euclid, *Elements* Book 9, Proposition 20

[11] Technically this uses what is often called *complete induction* but the two are equivalent

By assumption both p_1 and q_1 divide n, so $p_1 \mid q_i$ for some i, and $q_1 \mid p_j$ for some j[12]. Thus $p_1 = q_i$ and $q_1 = p_j$. But also by assumption $p_1 \leq p_j = q_1 \leq q_i = p_1$, so $p_1 = q_1$. So n/p_1 is also an integer, and $n' = n/p_1 < n$, so n' has a unique decomposition into primes. Thus n does as well. □

2.13 Remark. In fitting with the fashionable trend of the mid 1800s of naming things the "Fundamental theorem of X"[13], Theorem 2.12 is sometimes called the *Fundamental theorem of arithmetic*.

2.14 Exercises

1. (Euclid's Lemma) Let $n, m \in \mathbf{Z}$ and p be a prime. Use corollary 2.7 to show that if $p \mid nm$ then either $p \mid n$ or $p \mid m$. Is this still true if p is not a prime number?

   Proof provided in class: Suppose p, n, m given and that p does not divide n. We'll show $p \mid m$. Since p is prime, if p does not divide n then $\gcd(p, n) = 1$. So, there must be integers r, s such that $1 = pr + ns$ by theorem 2.7. Multiplying by m we have $m = prm + nsm$. Now $p \mid prm$ and $p \mid nsm = snm$ by assumption, so p divides the right hand side. Thus $p \mid m$.

2. Let n, m be integers with $m > 0$. Write $n = mq + r$ as guaranteed by Theorem 2.3, and define $n \pmod m$ as the remainder r from this theorem. Note that $n \pmod m \in \{0, 1, 2, 3, \cdots, m-1\}$ by construction.

   Prove that the following relation $\sim$ on $\mathbf{Z}$ is an equivalence relation

   $$n \sim n' \text{ if and only if } n = n' \pmod m$$

3. Modify the proof of theorem 2.11 to show that there are infinitely many primes of the form $4k + 1$ for some $k \in \mathbf{Z}$.

4. Prove corollary 2.8, then use it to describe all solutions (x, y) with $x, y \in \mathbf{Z}$ such that $105x + 121y = 1$.

5. Either by hand or via a program which you write, compute $\gcd(19789, 23548)$ and $\gcd(22241739, 19848039)$.

6. Use theorem 2.3 to show that every perfect square (i.e., integer of the form n^2 for some $n \in \mathbf{N}$) is of the form $4k$ or $4k + 1$ for some $k \in \mathbf{N}$

7. Prove that if $p \in \mathbf{N}, p \geq 2$ such that $2^p - 1$ is prime, then p is prime.

   Hint: If $p = ab$, then factor $2^{ab} - 1 = (2^a)^b - 1$

8. Show that for $(r_i)_{i \geq 1}$ the sequence of remainders created in example 2.5 that $r_{i+2} < r_i/2$ for $i \geq 1$. Use this to produce an upper bound on the number of iterates required by

[12] Why is this? This requires what is sometimes called *Euclid's lemma*, see Ex. 1. in section 2.14

[13] See Fundamental theorem of calculus, Fundamental theorem of algebra, Fundamental theorem of Galois theory, etc.

the Euclidean algorithm in terms of the number of digits in the base 2 expansions of n and m.

9. Let $u, v, w \in \mathbf{Z}$. Conjecture what must be true about u, v, w for there to exist $x, y, z \in \mathbf{Z}$ such that $ux + vy + wz = 1$. Can you prove your conjecture?

10. *Challenge.* Let $\mathbf{Z}[i]$ denote the set of *Gaussian integers*

$$\mathbf{Z}[i] = \{a + bi : i^2 = -1 \text{ and } a, b \in \mathbf{Z}\}$$

$\mathbf{Z}[i]$ has a similar structure to $\mathbf{Z}$, in that Gaussian integers can be added, subtracted, and multiplied; and it's possible to talk about divisors: that is $a+bi \mid c+di$ if there is $u + vi \in \mathbf{Z}[i]$ such that $(a + bi)(u + vi) = c + di$. Given $a + bi \in \mathbf{Z}[i]$ define its **norm** by $|a + bi| = a^2 + b^2$. We say a Gaussian integer $p + qi$ is **prime** if it has no divisors $a + bi$ with norm $a^2 + b^2 \neq 1, p^2 + q^2$.

    a. Enumerate the sets of Gaussian integers with norms equal to 1, 3, and 5

    b. Compute a list of all prime Gaussian integers $p + qi$ of norm $p^2 + q^2 \leq 25$.

    c. Prove that if a Gaussian integer $p + 0i$ is prime then $p = 4k + 3$ for some $k \in \mathbf{Z}$.

11. *Challenge.* Show that $\sqrt{2}$ is not a rational number by showing that there are no integers $n, m \in \mathbf{Z}$ such that $n^2 = 2m^2$.

12. *Challenge.* This problem is a nice alternative proof of theorem 2.11 originally attributed to Euler. Some notation: given a sequence $(a_i)_{i\geq 1}$ of real numbers, let's write

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdots a_n, \ (n \geq 1) \qquad \text{and} \qquad \prod_{i=1}^{\infty} a_i = \lim_{n\to\infty} \prod_{i=1}^{n} a_i$$

    a. Enumerate $\mathbf{P} = \{p_1, p_2, p_3, \cdots\}$ such that $p_1 \leq p_2 \leq p_3 \leq \cdots$. Use the Geometric sum formula $\sum_{k=0}^{\infty} a^k = 1/(1 - a)$ for $|a| < 1$ and theorem 2.12 to show that

$$\prod_{i=1}^{\infty} \frac{1}{1 - (1/p_i)} = \sum_{n=1}^{\infty} \frac{1}{n}$$

    b. Use that $\sum_{n=1}^{\infty} 1/n = \infty$ to argue why part a. tells us that the set $\mathbf{P}$ must be infinite.

3 The algebra of modular arithmetic

Let $n \in \mathbf{Z}$, $n > 1$ be given and define the set $n\mathbf{Z} \subset \mathbf{Z}$ by

$$n\mathbf{Z} = \{nk : k \in \mathbf{Z}\}. \tag{3.0.1}$$

Define an equivalence relation $\sim$ on $\mathbf{Z}$ such that $a \sim b$ if and only if $a - b \in n\mathbf{Z}$. The set corresponding set of equivalence classes $\mathbf{Z}/\sim$ is denoted $\mathbf{Z}_n$[14] and is called the **set of integers modulo** n. Other notation for this set includes $\mathbf{Z}/n\mathbf{Z}$ or $\mathbf{Z}/(n)$—we'll understand where this notation comes from soon enough.

[14] This won't be a problem for us but this notation is somewhat discouraged in general, since $\mathbf{Z}_p$ sometimes is used to denote the p-adic integers.

3.1 The ring of integers mod n

Let $n > 1$ be given. As a set, $\mathbf{Z}_n$ consists of the equivalence classes of $\sim$: that is if we write $[k]$ for the set $\{k + mn : m \in \mathbf{Z}\}$ then

$$\mathbf{Z}_n = \{[0], [1], [2], [3], \cdots, [n-1]\}$$

Here's where it gets interesting: the set $\mathbf{Z}_n$ isn't *just* a set though. Since we began with a set $\mathbf{Z}$ *together* with its operations $+$ and $\cdot$, we can ask if these operations still carry over to well defined notions of "addition" and "multiplication" on the set of equivalence classes $\mathbf{Z}_n$.

Let's define operations $+$ and $\cdot$ on $\mathbf{Z}_n$ as follows: For $[a], [b] \in \mathbf{Z}_n$,

$$[a] + [b] := [a + b] \qquad [a] \cdot [b] := [ab] \tag{3.1.1}$$

It's useful to drop the brackets and just write a for the equivalence class $[a] \in \mathbf{Z}_n$. When we want to then distinguish $a \in \mathbf{Z}_n$ from a as an integer, we can append our equations with $(\text{mod } n)$[15] to specify that everything should be taken modulo n. We'll explore this more in depth later, but what's happening is that we've dividded out by a "nice" equivalence relation, so $\mathbf{Z}_n$ inherits algebraic structure from the set $\mathbf{Z}$. The following theorem tells us that these operations behave as one "expects" for addition and multiplication. In more precise terms, it tells us that $\mathbf{Z}_n$ is a (commutative) ring.

3.2 Theorem. *Let $n > 1$ be given, and $a, b, c \in \mathbf{Z}_n$. With operations $+$ and $\cdot$ defined on $\mathbf{Z}_n$ as in (3.1.1), the following identities hold*

a. $a + b = b + a \pmod{n}$

b. $a \cdot b = b \cdot a \pmod{n}$

c. $(a + b) + c = a + (b + c) \pmod{n}$

d. $(a \cdot b) \cdot c = a \cdot (b \cdot c) \pmod{n}$

e. $a + 0 = a \pmod{n}$

f. $a \cdot 1 = a \pmod{n}$

g. $a \cdot (b + c) = a \cdot b + a \cdot c \pmod{n}$

h. There is a unique number $-a \in \mathbf{Z}_n$ such that $a + (-a) = 0 \pmod{n}$

i. If $\gcd(a, n) = 1$ there is a unique $a^{-1} \in \mathbf{Z}_n$ such that $a \cdot a^{-1} = 1 \pmod{n}$

Arithmetic, as performed with the rules of addition and multiplication above in theorem 3.2 is referred to as **modular arithmetic**.

3.3 Example (Cayley Table for $\mathbf{Z}_5$). One helpful way to visualize the additive and multiplicative structure of $\mathbf{Z}_n$ is via *Cayley tables*. The Cayley table for addition and multiplication in $\mathbf{Z}_5$ is given below

[15] As in Exercise 2. in section 2.14, for any $a \in \mathbf{Z}$, $a \pmod{n}$ is defined to be the remainder upon dividing a by n.

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

·	0	1	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

(3.3.1)

While $\mathbf{Z}_n$ may still have operations that resemble $+$ and $\cdot$ from $\mathbf{Z}$, we run into "oddities' when solving equations in $\mathbf{Z}_n$ that aren't always present in $\mathbf{Z}$ (or $\mathbf{Q}$ or $\mathbf{R}$). For instance, in $\mathbf{Z}_6$ we have

$$2 \cdot 3 = 6 = 0 \pmod 6$$

which goes against our very intuition about what happens when a product equals zero[16]. Therefore, we're going to need some guidance on what type of solutions to expect when "doing algebra" with modular arithmetic.

3.4 Linear equations in $\mathbf{Z}_n$

The simplest type of equations are linear equations: i.e., things of the form $ax = c$. In $\mathbf{Q}$ and $\mathbf{R}$ solutions to these equations are straightforward: there is always a unique solution, granted $a \neq 0$, specifically, $x = c/a$. In $\mathbf{Z}$, we have that $ax = c$ has a unique solution if and only if $a \mid c$. In $\mathbf{Z}_n$ arithmetic, the story is similar, but depends in a crucial way on how a, c and n relate. What's interesting is that in $\mathbf{Z}_n$ equations such as $ax = c \pmod n$ can have *multiple* solutions.

Some terminology first: any equation $ax = c \pmod n$ is a **linear equation** in $\mathbf{Z}_n$. These are also sometimes called **linear congruences**[17].

3.5 Theorem. *Let $n > 1$ be given and $a, c \in \mathbf{Z}$. Set $d = \gcd(a, n)$. Then:*

- *If d does not divide c, $ax = c \pmod n$ has no solutions*
- *If $d \mid c$, then $ax = c \pmod n$ has exactly d distinct solutions in $\mathbf{Z}_n$. Furthermore, any such solution is of the form*

$$x = (cx_0 + kn)/d \pmod n, \qquad k = 0, 1, 2, 3, \cdots, d-1 \tag{3.5.1}$$

where x_0 comes from any solution (x_0, y_0) to the equation $ax + ny = d$.

3.6 Corollary. *With the setup of theorem 3.5 above, if $\gcd(a, n) = 1$ then there is a unique solution in $\mathbf{Z}_n$ to $ax = c \pmod n$ for any $c \in \mathbf{Z}_n$ obtained as $cx_0 \pmod n$ where x_0 is any solution to $ax + ny = 1$.*

It's one thing to know that a solution *should* exist, but we'd like to actually produce such a solution in an efficient manner. Rather than give a formal prove of the above, we'll provide

[16] In this case, elements $2, 3 \in \mathbf{Z}_6$ are called **zero divisors**. Note that if the modulus n is not prime, $\mathbf{Z}_n$ has nonzero zero divisors (*can you show this?*)

[17] More generally, equations in $\mathbf{Z}_n$ are sometimes referred to as *congruences* or *congruence equations*

the following "proof by example" for each of the the cases one might find themselves in when needing to apply theorem 3.5.

3.7 Example ("Proof by example" – solving congruences modulo n). Suppose we have the equation

$$3x = 7 \pmod{11} \tag{3.7.1}$$

and want to solve for x. Appealing to theorem 3.5 we have $\gcd(3, 11) = 1$, so we expect a unique solution to (3.7.1) in $\mathbf{Z}_{11}$[18]. Note that a solution to (3.7.1) comes from finding a solution $3x = 7 + 11k$ for some $k \in \mathbf{Z}$. Written differently, $3x + 11(-k) = 7$. Note that we can always find a solution $(x_0, y_0)$to the equation $3x + 11y = 1$ (since $\gcd(3, 11) = 1$) using theorem 2.6 or the Euclidean algorithm. At that point, since $1 \mid 7$, we can multiply this by 7 to get:

$$3(7x_0) + 11(7y_0) = 7.$$

All that we need then is to take the remainder modulo 11 of $7x_0$ to get the desired solution. In this case it's $x = 6$, since $3 \cdot 6 = 18 = 7 + 11 = 7 \pmod{11}$.

Similarly, we can consider a nonexample as following. Suppose we want to apply the same idea from above to find a solution to

$$9x = 7 \pmod{15} \tag{3.7.2}$$

Rewriting, we'd want a solution to $9x - 15k = 7$. Since $\gcd(9, 15) = 3$, by theorem 2.6, we'd be guaranteed to find a solution (x_0, y_0) to $9x + 15y = 3$. However, 3 does not divide 7, so there's no integer to multiply by to get this into the desired form of $9x + 15y = 7$.

Last, let's see what happens when we run into multiple solutions. Consider

$$12x = 9 \pmod{15} \tag{3.7.3}$$

First we check: $\gcd(12, 15) = 3$ and $3 \mid 9$, so we're expecting 3 distinct solutions in $\mathbf{Z}_{15}$ to (3.7.3). First we can find a solution (x_0, y_0) to $12x + 15y = 3$, for instance $(4, -3)$. This gives a solution $12(4 \cdot 3) + 15(3 \cdot (-3)) = 3 \cdot 3 = 9$. We can then check that the solutions to (3.7.3) in $\mathbf{Z}_{15}$ are $2, 7$ and 12 by using formula (3.5.1) as follows

- $k = 0$: $\dfrac{9 \cdot 4 + 0 \cdot 15}{3} = 12$
- $k = 1$: $\dfrac{9 \cdot 4 + 1 \cdot 15}{3} = 12 + 5 = 17 = 2 \pmod{15}$
- $k = 2$: $\dfrac{9 \cdot 4 + 2 \cdot 15}{3} = 12 + 10 = 22 = 7 \pmod{15}$

It's also worth pointing out that you always *could* solve equations like (3.7.1), (3.7.2), or (3.7.3) by brute force (i.e., checking all possibilities). This might seem reasonable if the modulus is small, but when working with large moduli (for instance, when dealing with

[18] Actually, $\mathbf{Z}_{11}$ (or more generally $\mathbf{Z}_p$ for p some prime) is a *field*, so there are always multiplicative inverses to any nonzero element

encryption algorithms) it's good to have a systematic approach. Also, when finding multiple solutions to a linear congruence, the solutions will always be spaced out by the same factor of n/d[19]

3.8 Polynomial equations in $\mathbf{Z}_n$

In general it is very difficult to solve higher order polynomial equations in $\mathbf{Z}_n$ by any single systematic process. This is not particularly unexpected, it's also similarly difficult to *algebraically* solve polynomial equations in $\mathbf{R}$ once the degree gets too large[20]. We'll develop some further techniques in the next section. For now, we can rest assured that at least the following comforting fact is still true, at least when the modulus is a prime.

3.9 Theorem. *Let p be a prime number and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ be a degree d polynomial such that for $i = 0, \ldots, d$ $a_i \in \mathbf{Z}_p$ and $a_d \neq 0$. Then the equation $f(x) = 0 \pmod p$ has at most d solutions in $\mathbf{Z}_p$.*

3.10 Remark. This theorem is useful in showing, say, that the only self-inverse elements in $\mathbf{Z}_p$ are 1 and $p-1$. Note that $1^2 = 1$ and $(p-1)^2 = p^2 - 2p + 1 = 1 \pmod p$. If p is a prime then $x^2 = 1 \pmod p$ has at most two solutions, there they are: two distinct solutions, at least when $p > 2$.

3.11 Equations with a prime modulus

3.12 Theorem (Fermat's little theorem)**.** *Let p be a prime and $a \neq 0 \in \mathbf{Z}_p$, then $a^{p-1} = 1 \pmod p$.*

When we start with group theory, we'll find short and slicker proof of theorem 3.12. The following is more direct. First, we'll need a lemma

3.13 Lemma. *Let p be a prime and $a \neq 0 \in \mathbf{Z}_p$. Then, the sets $\{a, 2a, 3a, \cdots, (p-1)a\}$ and $\{1, 2, 3, \cdots, p-1\}$ are equal in $\mathbf{Z}_p$.*

Proof. Since p is prime p does not divide a or $1, \ldots, p-1.$, so it's enough to show that the two sets have the same cardinality. Suppose that there were some numbers k, ℓ such that $ka = \ell a \pmod p$. Then $a(k-\ell) = 0 \pmod p$ so $p \mid a(k-\ell)$. Now, p does not divide a, so $p \mid k - \ell$. Without loss of generality, $k \geq \ell$ (in $\mathbf{Z}$), but also $k - \ell < p$ since $k, \ell < p$ to begin with. So, $k - \ell = 0$. That is to say, all the entires from $\{a, 2a, 3a, \cdots, (p-1)a\}$ are distinct. □

Proof of theorem 3.12. From the lemma, $\{a, 2a, 3a, \cdots, (p-1)a\}$ and $\{1, 2, 3, \cdots, p-1\}$ are equal sets in $\mathbf{Z}_p$. So, the products of all their elements must be the same. That is,

$$a(2a)(3a)\cdots((p-1)a) = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

[19] Why is this? It follows from theorem 2.8, this is a good exercise to show why.

[20] You probably know the quadratic formula. There are similar "formulas" for 3rd and 4th degree polynomials, but no general solution for the roots of 5th and higher degree involving only "simple" functions like the square root

But, the numbers $1, 2, 3, \ldots, p-1$ are all coprime to p, so can be canceled out in the equality above[21]. This gives that $a^{p-1} = 1 \pmod{p}$ as required. □

3.14 Equations with a composite modulus

A main difference we'll see is that inverses are more difficult to discuss when working with a composite modulus. For instance, in $\mathbf{Z}_6$, there's only solutions to $ax = 1 \pmod 6$ for $a \in \{1, 5\}$, specifically only if a is coprime with 6. This motivates the following definition.

3.15 Definition (Euler's totient function)**.** *Let $n \geq 1$, define $\varphi(n)$ to be the number of integers m with $1 \leq m \leq n$ such that m is coprime to n.*

The function $\varphi \colon \mathbf{N} \to \mathbf{N}$ given by definition 3.15 is called *Euler's totient*[22] *function* (also *Euler's phi function*). It counts the number of elements $a \in \mathbf{Z}_n$ that have solutions to $ax = 1 \pmod n$, and as well see, fits nicely into discussing the multiplicative structure of $\mathbf{Z}_n$ as a group.

It's not hard to check that if p is a prime, then $\varphi(p) = p - 1$. In fact, φ has a lot of additional structure. We'll show one such fact about φ in proposition 3.17, but will first need the following lemma.

3.16 Theorem (Chinese remainder theorem)**.** *Let $m, n > 1$ such that $\gcd(m, n) = 1$ and pick elements $b \in \mathbf{Z}_m, c \in \mathbf{Z}_n$. Then, the system $x = b \pmod m, x = c \pmod n$ has a unique solution $x \in \mathbf{Z}_{mn}$.*

Proof. First, note that any solution to $x = b \pmod m$ is of the form $x = my + b$ where y is some integer. Substituting this into the second equation we get $my + b = c \pmod n$ and so $my = c - b \pmod n$. Since $\gcd(m, n) = 1$, we must have a unique solution y_0 to this equation in $\mathbf{Z}_n$. Then $x_0 = my_0 + b$ is the desired solution to the system. □

Theorem 3.16 takes its takes it name from a problem posed in the book *Sunzi Suanjing*

> "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"

A more general statement of the Chinese remainder theorem is left as an exercise (see ex. 11. in Section 3.20).

3.17 Proposition. *Let $m, n > 0$ be given such that $\gcd(m, n) = 1$. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Let $S = \{a : 0 < a < mn \text{ and } \gcd(a, mn) = 1\}$ and

$$S' = \{(b, c) : 0 < b < m, 0 < c < n \text{ and } \gcd(b, m) = \gcd(c, n) = 1\}$$

[21] Said differently, there is a multiplicative inverse, i.e., solution to $ax = 1 \pmod p$ for each of these elements in $\mathbf{Z}_p$—see theorem 3.5

[22] As far as I can tell, there is no non-circular definition of the word "totient" as anything other than the number of primes less than a given number

Define a function $f\colon S \to S'$ by $f(a) = (a \pmod m, a \pmod n)$. It's enough to show that f is a bijection. To show f is injective, suppose that $a, a' \in S$ such that $a = a' \pmod m$ and $a = a' \pmod n$. Then both m, n divide $a - a'$, so since m, n coprime their product must divide $a - a'$ as well. But then $a = a' \pmod{mn}$. That f is surjective comes follows from theorem 3.16. □

For now, we have the following theorem (compare with theorem 3.12). The proof of this theorem is more or less a direct modification to the proof of that theorem, and is left as an exercise (ex. 16. in section 3.20).

3.18 Theorem (Euler's theorem)**.** *Let $n > 1$ and $a \in \mathbf{Z}_n$ such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} = 1 \pmod n$*

3.19 Remark. Note if n is composite it is generally **not** true that $a^{n-1} = 1 \pmod n$. For instance, in $\mathbf{Z}_6$, we have $a^5 = a \neq 1$ for $a = 2, 3, 4, 5$ (check this). There are *some* moduli for which an analogous statement to theorem 3.12 holds without the modulus being prime[23]. Such numbers are called *Carmichael numbers*, the smallest such is 561 (see ex. 19. in section 3.20)

3.20 Exercises

1. Prove theorem 3.2.
2. Prove that theorem 3.18 implies theorem 3.12
3. Find *all* solutions to the following equations
   a. $7x = 3 \pmod{15}$
   b. $6x = 5 \pmod{15}$
   c. $9x = 3 \pmod 5$
   d. $3x = 1 \pmod 6$
   e. $x^2 = 1 \pmod 8$
   f. $x^2 = 2 \pmod 7$
   g. $6025x = 11113 \pmod{511111}$
4. True or False: For any $a, b \in \mathbf{Z}_n$, $(a + b)^n = a^n + b^n \pmod n$. What if n is a prime number?
5. Let's call $a \in \mathbf{Z}_n$, $a \neq 0$, a **zero divisor** if there is $b \in \mathbf{Z}_n$, $b \neq 0$, such that $ab = 0 \pmod n$. Prove that $\mathbf{Z}_n$ has zero divisors if and only if n is a composite number (i.e., not prime).
6. Let $n > 1$. Prove that the elements 1 and 0 in $\mathbf{Z}_n$ guaranteed to exist from theorem 3.2 are not equal

[23] That is, $a^{n-1} = 1 \pmod n$ for all a coprime to n

7. Find all roots of $f(x) = x^2 + x$ in $\mathbf{Z}_5$ and $\mathbf{Z}_6$. Does this violate theorem 3.9?

8. Use Fermat's little theorem (theorem 3.12) or Euler's theorem (theorem 3.18) together with the method of successive squares to evaluate the following

   a. $3^{77} \pmod{31}$

   b. $10^{101} \pmod{79}$

   c. $(-6)^{1266} \pmod{151}$

9. Use Fermat's little theorem to prove that $x^2 = -1 \pmod{p}$ has no solutions when p is a prime of the form $p = 4k+3$ (see also ex. 15. in this section). Conversely prove that $x^2 = -1 \pmod{p}$ always has a solution when p is of the form $4k+1$ for some $k \in \mathbf{Z}$.

10. Prove that $(p-1)! = (p-1)(p-2)\cdots 2\cdot = -1 \pmod{p}$ for p a prime. Use this to show that if $p = 4k+1$, then $((p-1)/2)!$ is a solution to $x^2 = -1 \pmod{p}$. Why does this argument not work for p of the form $4k+3$?

11. Prove the following *Generalized Chinese remainder theorem* (see theorem 3.16)

    Let $k > 1$ be given along with numbers $n_1, \ldots, n_k$ such that $\gcd(n_i, n_j) = 1$ for $1 \leq i \neq j \leq k$ (i.e., the numbers n_i are pairwise coprime). For $i = 1, \ldots, k$ let $a_i \in \mathbf{Z}_{n_i}$ be given. Show that the system of equations

    $$x = a_1 \pmod{n_1}, \quad x = a_2 \pmod{n_2}, \quad \cdots, \quad x = a_k \pmod{n_k}$$

    has a unique solution $x \in \mathbf{Z}_n$, where $n = n_1 n_2 \cdots n_k$.

12. Show that if $n = pq$ for p, q distinct primes, then $\varphi(n) = (p-1)(q-1)$.

13. Let $n > 1$ be given. Prove that the total number of elements $a \in \mathbf{Z}_n$ such that there is a solution to $ax = 1 \pmod{n}$ is equal to $\varphi(n)$[24].

14. Let $n \geq 1$, and write $D(n)$ for the set of integers $d > 0$ such that $d \mid n$. Prove that

    $$\sum_{d \in D(n)} \varphi(d) = n$$

15. Let p be a prime and set $R_p \subset \mathbf{Z}_p$ to be the set

    $$R_p = \{n^2 : n \in \mathbf{Z}_p, n \neq 0\}$$

    Calculate R_p for primes $p \leq 20$, then make a conjecture about the cardinality (number of elements) of R_p. Can you prove this conjecture?[25]

    Hint/proof: As done in class: $|R_p| = (p-1)/2$ for p an odd prime. This follows from two claims: (i) For $x = 1, 2, \ldots, (p-1)/2$, $x^2 = (p-x)^2$, and (ii) the set $S = \{1, 2, \ldots, (p-1)/2\}$ "creates" all quadratic residues, in that $R_p = \{x^2 : x \in S\}$.

[24] The subset $U_n \subset \mathbf{Z}_n$ of such elements is called the *group of units* mod n. We'll see this again later.

[25] The set R_p is called the set of *quadratic residues* mod p. If we have time we'll take more about these, including discussing Legendre symbols and quadratic reciprocity.

16. Modify the argument given in the proof of theorem 3.12 to prove theorem 3.18.

17. *Challenge.* From theorem 3.12 it follows that $x^p = x \pmod{p}$ for any prime p and $x \in \mathbf{Z}_p$.

    a. Determine the number of *distinct*[26] polynomial functions $\mathbf{Z}_p \to \mathbf{Z}_p$

    b. *True or False.* Every function $\mathbf{Z}_p \to \mathbf{Z}_p$ can be represented by a polynomial

18. *Challenge.* Let $n \geq 1$ and write $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ for its prime decomposition. Compute Euler's totient function $\varphi(n)$. (*Hint: start with proving that* $\varphi(p^k) = p^{k-1}(p-1)$ *for* p *a prime*).

19. *Challenge.* Use that $561 = 3 \cdot 11 \cdot 17$ to show that $a^{560} = 1 \pmod{561}$ for all a such that $\gcd(a, 561) = 1$.

4 Cryptography and RSA encryption

Cryptography is a fairly modern branch of mathematics that really has blossomed since the advent of modern computers. Historically, the first example of a cyptosystem is usually the Caesar cipher, attributed to Roman emperor Julius Caesar. Evidently, the idea was to encode messages of military important by shifting the letters down the alphabet as follows:

- Enumerate the alphabet (we'll use the modern English alphabet) `A`=0, `B`=1, `C`=2, $\cdots$, `Z`=25
- Write your message as a string of elements from $\mathbf{Z}_{26}$,

$$\texttt{ILIKECATS} = 8\,11\,8\,14\,4\,2\,0\,19\,18$$

- Apply the cipher: i.e., take the string of elements in $\mathbf{Z}_{26}$ and apply the encryption function E_n described below to each element of the string (note this is just "shift by $n \pmod{26}$")

$$E_n(x) = x + n \pmod{26}$$

- For instance, our message above, encoded with a shift of 6 would look like

$$14\,17\,14\,16\,10\,8\,5\,25\,24 = \texttt{OROQKIFZY}$$

- This encoded message is what you share. You can decode by applying the following to each entry from the string

$$D_6(x) = x - 6 \pmod{26}$$

As far as encryption algorithms go this one is *pretty bad*. The problem being that letters in the English alphabet are not evenly distributed in their frequency of appearance in words, so

[26] i.e., consider two polynomials the same if their values are the same for all $x \in \mathbf{Z}_p$ (even if they have different expressions)

it's often quite simply to break these codes by brute force[27]. More superficial issues include that the "space" character has not been encoded, so longer phrases could be hard to parse (this is easily fixed and not a problem with the particular encryption method, however).

4.1 Public key cryptography

The Caesar cipher also has the more nuanced issue that in order to both encode and decode a message the *shift* must be set ahead of time. That is, both parties much meet or somehow otherwise agree on the shift. In modern language, this is a *private key* encryption algorithm. There's reasons to want to use private key algorithms, but for modern use it's often desirable to for someone to be able to send you an encrypted message, using publicly available information, in a way such that only you are able to decode the message. Specifically, you shouldn't have to meet the sender ahead of time or agree on any kind of encoding style upfront.

With this in mind, the idea behind *public key* cryptography is to have two "keys" available;

- A **public key** that is freely available. This is what people use to encode a message to send *to you*
- A **private key** that you keep secret. This is what you use to *decrypt* messages that were sent to you

A good encryption algorithm then should be "relatively easy" to encrypt messages using the public key, and also relatively easy to decrypt messages using your private key; but should be very difficult to decrypt an encoded message without knowledge of the private key.

4.2 The RSA algorithm

There are many modern encryption algorithms of varying usefulness and usability. Our focus will be on the RSA[28] encryption algorithm as initially developed in the late 1970s. The basis of the RSA encryption algorithm is that factoring a number into prime components is a *technically difficult* problem. Recall from theorem 2.12 that any number $n > 1$ has a unique decomposition into its prime factors. From an existence standpoint this theorem is trivial, but from a construction standpoint, actually producing these factors is very difficult. This shouldn't necessarily be a surprise though: we know that any polynomial $f\colon \mathbf{C} \to \mathbf{C}$ factors uniquely as a product of linear terms; this can be used conceptually just fine, but actually finding the roots of a given (high degree) polynomial is often very difficult.

Let p, q be prime numbers and set $n = pq$. The idea here is that p, q should be "large" so that factoring n (even knowing that it is a product of only two primes) is a difficult problem.

[27] I believe newspapers used to include a code-breaking game of this type as part of the weekly games such as Crosswords, Sudoko, etc.

[28] Named for the first (public) inventors: Rivest, Shamir, and Adleman; a group of computer scientists working at MIT. Interestingly, an equivalent system was described by a British intelligence agency earlier that decade, but kept secret, only to be declassified in the 1990s.

For instance, if you're given the number 346171992671, it's not immediately obvious that

$$346171992671 = 444449 \cdot 778879 \text{[29]} \tag{4.2.1}$$

How then to use this information to encode a message? We can use the following theorem

4.3 Theorem. *Let $n > 1$ and integers b, e be given. If $\gcd(b, n) = 1$ and $\gcd(e, \varphi(n)) = 1$, the equation $x^e = b \pmod{n}$ has a solution.*

Proof. This proof is not particularly difficult, and even constructs for us a method for computing the desires solution x. Since $\gcd(e, \varphi(n)) = 1$, there is an integer d with $ed = 1 \pmod{\varphi(n)}$ (theorem 3.5). Then by Euler's theorem (theorem 3.18), $b = b^{ed} = (b^d)^e \pmod{n}$. So, $x = b^d$. □

The idea behind RSA is then to use a modulus n which is the product of two "large" primes, and bundle the security of the encryption algorithm into the computational difficulty of producing the factorization of n[30]. The process is described below:

4.4 Algorithm (RSA encryption). To encode or decode a message via RSA encryption

- Pick $n = pq$ for (large) primes p, q (from theorem 3.17, we know $\varphi(n) = (p-1)(q-1)$)
- Pick a number e with $\gcd(e, \varphi(n))$.
- Compute the inverse to $e \pmod{\varphi(n)}$; i.e. find a solution d to $ed = 1 \pmod{\varphi(n)}$ (this can be done using the Euclidean algorithm).
- Your **public key** is the pair (n, e). A message can be encoded by the encryption function
$$E(x) = x^e \pmod{n} \tag{4.4.1}$$
- Your **private key** is the pair (n, d). An encoded message is decoded by
$$D(x) = x^d \pmod{n} \tag{4.4.2}$$

Theorem 4.3 then tells us that $D(E(x)) = x$, since

$$D(E(x)) = (x^e)^d = x^{ed} = x^{1+\ell\varphi(n)} = x \pmod{n}$$

(The number ℓ here is some number expressing that $km = 1 \pmod{\varphi(n)}$.

4.5 Remark. Note that if you start with the primes p, q each step from algorithm 4.4 is computable using algorithms we've learned; in particular finding d is doable since

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

[29] or even that the two numbers 444449 and 778879 are primes (they are)

[30] In fact, the RSA laboratories put out a list of factorization challenges with cash prizes in the 1990s. Though the challenge has now been ended, many of the numbers presented remain unfactored.

Once you've created the public and private keys, it's then possible to discard the original primes p, q keeping only the number n. Another observation is that using RSA does require encoded your message as a *number* first of all, but this is fairly routine from a modern-computer standpoint, using ASCII or some other agreed upon standard.

Here is a useful tool for creating public and private key pairs for RSA encryption.

4.6 Example. Let's return to my message of feeling admiration from before. We'll encode it via ASCII this time, including spacing between the words to aid in readability. My message then becomes:

$$\texttt{I LIKE CATS} = 073\,032\,076\,073\,075\,069\,032\,067\,065\,084\,083$$

where each three digit chunk is the corresponding number for that character in ASCII. I'll pick relatively small numbers, $p = 113, q = 379$, so that $n = 42827$. I'll use $e = 59$ and $d = 17939$, from which

$$ed = 1058401 = 1 \pmod{\varphi(42827)}$$

Applying the encryption function $E(x) = x^e \pmod{42827}$ to each of the three-digit chunks from my message, we get the encoded message

$$23546\,9264\,7826\,23546\,15435\,34031\,9264\,1738\,35221\,3371\,41478$$

So if, say, you wanted to express to me that you also like cats, this is what you would create and send to me using the public key $(42827, 59)$. I'm then free to decode the message by applying the decryption function D below to each entry

$$D(x) = x^{17939} \pmod{42827}$$

4.7 Additional thoughts on RSA

There is a slight problem with applying algorithm 4.4 in general. Suppose $n = pq$ is given along with integers e, d as needed for RSA, and let M be the message we wish to send. To send M via RSA we need to encode M first as a number in $\mathbf{Z}_n$. There is a slight problem in applying theorem 4.3 to *any* message M since we need to ensure that M is coprime to n. In practice this is usually not so much of an issue; for instance if p, q are at least 129 and we encode our message one ASCII character at a time (which is a number in $\mathbf{Z}_{128}$, then we'll never run into this problem (*why is this?*). When actually applying RSA, typically the primes are *huge* (100+ digits), in which case the probability of picking a non-invertible element of $\mathbf{Z}_{pq}$ is fairly small (see Exercise 4. in section 4.8).

Moreover, like any cryptosystem, RSA is susceptible to attacks on its integrity. There is currently a somewhat pressing desire to move away from RSA given that quantum computers are likely to essentially trivialize the exact type of factorization problem it relies on for security[31]. Regardless, it's a good real-world use for our introduction to modular arithmetic, and many more powerful encryption algorithms still rely on some of the basic ideas from RSA.

[31] The mathematics of this are beyond the scope of our course, but there's some good YouTube videos that partially explain the ideas

4.8 Exercises

1. The following text is encoded using a Caesar cipher. Determine the message

```
Hvscfsa:  Ozz bohifoz biapsfg ofs wbhsfsghwbu.
Dfcct:  Qcbgwrsf hvs gsh G ct ibwbhsfsghwbu bohifoz biapsfg.  Pm
hvs kszz cfrsfwbu dfwbqwdzs, hvwg gsh vog o gaozzsgh asapsf.  Pih
hvs gaozzsgh ibwbhsfsghwbu biapsf wg o jsfm wbhsfsghwbu biapsf!
Qcbhforwqhwcb.  Hvig G wg sadhm, obr ozz bohifoz biapsfg ofs wbhsfsghwbu.
```

2. Use prime numbers $p = 7829$ and $q = 7177$ to produce a public and private key pair for RSA encryption.

3. Using the decryption key (42827,17939) provided in example 4.6, decrypt the following message[32] (written in ASCII)

   19372 22685 17036 1418 9264 33614 8144 9264 23190 16449 29181 9264 22685
   29181 42777 9264 33614 29181 17036 39922 23618 39922 8144 17036 33614
   29181 12639 9264 17036 33101 9264 42387 39922 22685 23618 29181

4. Given primes p, q what what is the probability of picking a message M in $\mathbf{Z}_{pq}$ that is not encryptable via RSA? Is this problem made better or worse by changing the modulus to $n = p^2q$?

5 Group theory: Definitions and terminology

Our first foray in modular arithmetic gives us a good foundation for working with algebraic structures distinct from that of the integers or real numbers. One way to capture the arithmetic of $\mathbf{Z}_n$ abstractly is to use the language of *groups*. Historically group theory arose from attempting to understanding the (geometric) symmetries of an object: this idea is still very much use today in fields such as algebraic topology and geometry.

5.1 Binary operations

In order to understand groups, we start with the idea of a **binary operation** on a set.

5.2 Definition (Binary operation)**.** *Let X be a set. A **binary operation** is a function $X \times X \to X$.*

This is an extremely general definition, but we know many examples already.

5.3 Example. $\mathbf{Z}$ has a binary operation "+" (that we commonly call addition) defined by

$$+ : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} \qquad (a, b) \mapsto a + b \tag{5.3.1}$$

The integers also have an operation " $\cdot$ " (which we call multiplication) defined

$$\cdot : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} \qquad (a, b) \mapsto a \cdot b \tag{5.3.2}$$

[32] This tool might be useful

These operations feel familiar to us but are already fairly distinct from each other. For instance, with respect to $+$, each element $a \in \mathbf{Z}$ has an inverse; specifically $-a \in \mathbf{Z}$. This is not true of multiplication[33].

5.4 Groups and a bunch of examples

There are a lot of binary operations, but most of them may not be explicitly useful. A **group** is a set with a particular brand of "useful" binary operation. Ultimately, what we call a "group" is a matter of definitions; the one that historically has stuck is the following[34]

5.5 Definition (Group)**.** *Let G be a set with binary operation $\cdot : G \times G \to G$. We call the pair $(G, \cdot)$ a **group** if $\cdot$ satisfies the following:*

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in G$
- *There is an element $e \in G$ called the **identity** such that $e \cdot a = a \cdot e = a$ for all $a \in G$*
- *Given any $a \in G$ there is an element a^{-1} called the **inverse** of a such that $a \cdot a^{-1} = a^{-1} \cdot a = e$*

The binary operation " $\cdot$ " is called the **group operation** and frequently write ab for $a \cdot b$ when there is no risk of confusion. We also write $a^n = \underbrace{a \cdot a \cdots a}_{n}$ and $a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n}$ for $n \geq 2$. When the group operation is clear from context, we write G for the pair $(G, \cdot)$.

5.6 Warning. The axioms for a group make no mention that the group operation be commutative; that is to say, in general $a \cdot b \neq b \cdot a$ for a, b in some arbitrary group. Groups that have this property get a special name (abelian), but there are many reasons to want to study both abelian and non-abelian groups (or things somewhere in between).

5.7 Definition (Abelian)**.** *A group $(G, \cdot)$ is called **abelian**[35] if the group operation is commutative. That is, for all $a, b \in G$; $a \cdot b = b \cdot a$.*

5.8 Example (Examples of groups). Though we may not be explicitly familiar with the terminology right now, we've lived most of our lives experiencing groups (both in mathematics and "in the real world"). Here are some examples of things you may have worked with before that satisfy the axioms required of being a group.

a. Let $n > 1$. The integers modulo n $(\mathbf{Z}_n, +)$ form a group with respect to addition. Any such group is called a **cyclic group**.

b. If p is prime, then the set $\mathbf{Z}_p^*$ defined by

$$\mathbf{Z}_p^* = \{a \in \mathbf{Z}_p : a \neq 0\}$$

[33] Even if you move to rational numbers this is still not true; 0 has no multiplicative inverse.

[34] There's also plenty of reason to study related "not quite group" sets with binary relations, we may see some of these later

[35] Named after the 19th century Norwegian mathematician Niels Abel. There's a saying in math that you know you've "made it" when your name gets used as an adjective. This is fairly common, but typically the name is capitalized. Less common is when your name is used as an *uncapitalized* adjective. As far as I know Abel is one of the few people (if not the only person) to have this honor.

is a group with respect to multiplication (this follows from lemma 3.13). In general, even if n is not a prime, we set

$$\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n : \gcd(a, n) = 1\} \tag{5.8.1}$$

and call $\mathbf{Z}_n^*$ the **group of units** modulo n.

c. Let $V = \{e, a, b, ab\}$ where $a^2 = b^2 = (ab)^2 = e$. Then V is a group, often the **Klein four group** (or *Klein Vierergruppe*) – see also example 5.18.

d. Let $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$. Then $\mathbf{R}^*$ is a group with respect to multiplication. Same goes for $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$. Both $\mathbf{R}$ and $\mathbf{C}$ are groups with respect to addition.

e. Recall the notation $\mathrm{GL}_n(\mathbf{R})$ for the set of invertible $n \times n$ matrixes of real numbers. Then $(\mathrm{GL}_n(\mathbf{R}), +)$ where $+$ denotes matrix addition. Similarly, let $\circ$ denote matrix composition, $(\mathrm{GL}_n(\mathbf{R}), \circ)$ is also a group. The latter is typically called the **general linear group**[36] and is a good example of a group for which in general $A \circ B \neq B \circ A$.

f. Similar to the previous example, let $n > 1$ and write $\mathrm{SL}_n(\mathbf{R})$ for the set

$$\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : \det A = 1\} \tag{5.8.2}$$

Then $\mathrm{SL}_n(\mathbf{R})$ is a group with respect to matrix multiplication. $\mathrm{SL}_n(\mathbf{R})$ is called the **special linear group**.

g. Let X_n be a regular n-gon[37] in the xy-plane and let D_n denote the set of symmetries of this n-gon. D_n is called the **dihedral group** of order n.

h. Let X be a set and write $\mathcal{F}(X)$ for the set of bijections $f\colon X \to X$. Then $(\mathcal{F}(X), \circ)$ is a group, where $\circ$ denotes function composition. Such a group is called a **permutation** or **symmetric** group. We'll see more of these later.

i. Let C_4 and Q_8 denote the following sets of matrices (i here denotes the complex unit $i^2 = -1$)

$$C_4 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} \tag{5.8.3}$$

and

$$Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\} \tag{5.8.4}$$

Both C_4 and Q_8 are groups with respect to matrix multiplication. Q_8 is called the **quaternion group** (whether or not you know this by name, we've all worked with this group before—it captures the symmetry of rotating objects in 3D-space).

j. The *Rubik's cube* is a well-known 3D-puzzle game popularized in the US in the 1980s. The Rubik's cube is a good example of (an action of) a group; basic group elements

[36] "GL" means **g**eneral **l**inear. These letters are almost always capitalized, if you see them in lower-case or a funny looking Gothic font like $\mathfrak{gl}_n(\mathbf{R})$ this is almost certainly referring to something more complicated (like a Lie algebra).

[37] That is, a polygon with n sides all of the same length, whose inner angles are all congruent

consist of rotations of any of the six faces by an angle of $\pi/2$ (we can call these F, B, U, D, L, R for front, back, up, down, left, and right assuming some fixed perspective of the group). There are relations to applying different rotations of faces, for instance applying any of the rotations F, B, U, D, L, R four times results in the identity e–the permutation of the blocks on the cube which "does nothing".

5.9 Homomorphisms

Groups do not (and should not) exist in isolation. In fact many mathematicians would argue that one of the main reasons to study groups is to study how they *act* on things (we'll do this later), in which the abstract structure of the group in question becomes more meaningful than some particular presentation of that group. To compare groups, we need a good notion of a function between groups. A function just of the underlying sets is not enough, since it's really the *structure* of the groups that we wish to compare.

5.10 Definition. *Let $(G, \cdot)$ and $(H, \star)$ be groups. A function $\varphi\colon G \to H$ is called a* ***homomorphism***[38] *if the following holds: for all $g, g' \in G$*

$$\varphi(g \cdot g') = \varphi(g) \star \varphi(g') \tag{5.10.1}$$

5.11 Remark. Here we use the notation $\star$ for the group operation in H for preciseness. In words, we can think of a homomorphism as a function which "respects the group structures" of G and H. If a homomorphism $\varphi\colon G \to H$ is also a bijection we say that φ is an **isomorphism**[39]

Abstractly, we say that groups G and H are **isomorphic** if there is an isomorphism $\varphi\colon G \to H$ and write

$$G \cong H \tag{5.11.1}$$

to denote that G and H are isomorphic. Isomorphic groups should be thought of as "different ways of expressing the same thing". We'll frequently be able to classify objects "up to isomorphism", meaning up to a natural way of "only superficially" changing the group structure.

5.12 Subgroups

A subgroup is a group which naturally lives inside of another group. As it turns out, we can understand a lot about a group G by understanding what subgroups live inside G. Compare the following definition with that of a *subspace* of $\mathbf{R}^n$ from linear algebra[40].

[38] The root *homo-* here is from the Greek meaning "same". *Morphism* is (basically) another commonly used word for function, used particularly frequently in advanced fields of mathematics like category theory. We'll see variants on the x-morphism naming convention (for instance, if you know some complex analysis you may be familiar with the terms *holomorphism* and *meromorphism*).

[39] *Iso-* coming from the Greek root meaning "equal to". You'll also see the word isomorphism being used more generally as any type of structure preserving bijection between algebraic objects. When the type of structure is unclear, you can always preface it by the type of object you're considering: i.e., *group-isomorphism*. A *set-isomorphism* then is just a bijection, emphasizing further that plain old sets have "the least structure you can put on them"

[40] Recall $V \subset \mathbf{R}^n$ is a subspace of $\mathbf{R}^n$ if given $v, v' \in V$ and constant c that $v + v' \in V$ and $cv \in V$.

5.13 Definition (Subgroup)**.** *Let G be a group. A **subgroup** H of G is a set $H \subset G$ such that the following are satisfied*

- *The group identity $e \in H$*
- *For any $h, h' \in H$, $hh' \in H$*
- *For any $h \in H$, $h^{-1} \in H$*

Notation-wise we write

$$H \leq G \tag{5.13.1}$$

(yes this is the less than or equal to sign[41]) to denote that H is a subgroup of G. Informally, to be a subgroup of G, H needs to consist of a collection of elements of G that themselves form a "closed system" with respect to the group operations from G. A somewhat easier to check characterization of H being a subgroup of G is the following:

5.14 Proposition. *Let G be a group. A set nonempty subset $H \subset G$ is a subgroup of G if for any $g, h \in H$, $gh^{-1} \in H$.*

Proof. This characterization of subgroups has a nice short proof. We must show that the conditions from definition 5.13 are met. Suppose that H is a nonempty subset of G such that for any $g, h \in H$, $gh^{-1} \in H$. Note that then the group identity $e = gg^{-1} \in H$. Then, if $h \in H$, we must have $h^{-1} = eh^{-1} \in H$. So, if $g, h \in H$ then $gh = g(h^{-1})^{-1} \in H$. □

We'll discuss the subgroup structure of groups much more in depth later, but here is a nice short proposition to start off with

5.15 Proposition. *If $n, m > 1$ and $m \mid n$, then there is a subgroup $H \leq \mathbf{Z}_n$ such that $H \cong \mathbf{Z}_m$*

Proof. Let $n, m > 1$ and suppose $m \mid n$, write $n = km$ for some integer k and let

$$H = \{0, k, 2k, 3k, \cdots, (m-1)k\}.$$

The claim is that $H \leq G$. The group structure on H is defined by $ak + bk = ck$ where $c = a + b \pmod{m}$. To show that this defines a subgroup of G, first note that $0 \in H$. Second, let $ak, bk \in H$ and write $c = a + b \pmod{m}$, then $ck \in H$. Last, if $ak \in H$ then $(m - a)k = -(ak)$ in H.

There is then an isomorphism $\mathbf{Z}_m \cong H$ given by $\varphi(a) = ak$ for $a \in \mathbf{Z}_m$. □

5.16 Direct sums

Last of our vocabulary introduction to group world is the notion of a direct sum. The idea being, if we have groups G and H we want to build a group out of the two of them, the same way we would consider the Cartesian product $X \times Y$ of sets X and Y.

[41] And you can interpret "is (isomorphic to) a subgroup of" as being a partial ordering on a collection of groups

5.17 Definition. *Let G, H be groups. Write $G \oplus H$[42] for the set*

$$G \oplus H = \{(g, h) : g \in G, h \in H\} \tag{5.17.1}$$

*$G \oplus H$ is called the **direct sum** of G and H, and is a group with respect to the operation*

$$(g, h) \cdot (g', h') = (gg', hh') \qquad g \in G, h \in H$$

5.18 Example. Recall the Klein four group $V = \{e, a, b, ab\}$ with $a^2 = b^2 = (ab)^2 = e$. Consider the function $\varphi\colon V \to \mathbf{Z}_2 \times \mathbf{Z}_2$ by

$$\varphi(e) = (0, 0), \quad \varphi(a) = (1, 0), \quad \varphi(b) = (0, 1), \quad \varphi(ab) = (1, 1)$$

Then φ is an isomorphism (you should check this). In fact, this tells us more: $H_a = \{e, a\}, H_b = \{e, b\}$ and $H_{ab} = \{e, ab\}$ are all subgroups of V; and each $H_a, H_b, H_{ab} \cong \mathbf{Z}_2$.

There is also a more general condition to check when a group is naturally isomorphic to a direct sum of its subgroups (see theorem 8.27). Somewhat confusingly, direct sums are also called *direct products*[43] or just *products* (at least when only finitely many groups are considered). Equivalent notation is to write $G \times H$ for $G \oplus H$.

5.19 Exercises

1. Determine if the following set and binary operation pair is a group or not. Prove or disprove your answer
   a. $(\mathcal{P}(X), \cup)$, where X is some set and $\cup$ denotes set union. (Recall that $\mathcal{P}(X)$ is the collection of subsets of X.)
   b. $(\mathcal{P}(X), \otimes)$ where X is some set and for $A, B \subset X$, $A \otimes B = (A \setminus B) \cup (B \setminus A)$
   c. $(\mathbf{Z}, \odot)$ where for $a, b \in \mathbf{Z}$, $a \odot b = a^2 - b^2$
   d. $(\mathbf{R}, \odot)$ where $a \odot b = a + b - 1$
   e. $(\mathbf{R}^3 \setminus \{0\}, \times)$, consisting of nonzero vectors $v \in \mathbf{R}^3$ where $\times$ denotes the cross product of vectors
   f. $(S^1, \cdot)$ where $S^1 = \{z \in \mathbf{C} : |z| = 1\}$ is the set of complex numbers of norm[44] 1 and $\cdot$ denotes complex multiplication.
   g. $(\mathrm{GL}_n(\mathbf{R}), [\,,\,])$ where for $A, B \in \mathrm{GL}_n(\mathbf{R})$, $[A, B] = AB - BA$

[42] You may have seen this symbol $\oplus$ before (perhaps in the context of Boolean algebra), this is a different use of the symbol though. In the context of groups, the symbol $\oplus$ is usually referred to as "sum" or "direct sum". This is not to be confused with $\otimes$ which refers to the tensor product (we may get to this later, maybe not).

[43] These two things have "natural descriptions" of what they should be: for instance a "sum" of *sets* X and Y is the (disjoint) union of those two sets, the "product" of sets is the Cartesian product $X \times Y$. It's actually a neat feature of groups that these two notions are the same, when the number of groups being combined together is finite

[44] Recall the *norm* of a complex number $a + bi$ is $|a + bi| = a^2 + b^2$

h. *Challenge.* $(\pi(X), \circ)$ where for some (open) region $X \subset \mathbf{R}^2$, $\pi(X)$ consists of all paths in X (note: a path is represented by a continuous function $f\colon [a,b] \to X$ for some interval $[a,b] \subset \mathbf{R}$), and $\circ$ denotes concatenation of paths

2. Determine which of the examples from example 5.8 is (i) a finite group, (ii) an abelian group

3. Let G be a group with identity element e. Prove the following statements:

   a. e is unique

   b. For any $g \in G$, its inverse g^{-1} is unique

   c. For any $g \in G$, $(g^{-1})^{-1} = g$

   d. For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$

   e. If $g, x, y \in G$ with $gx = gy$ then $x = y$. Similarly, if $xg = yg$ then $x = y$.

4. Let $\varphi\colon G \to H$ be a homomorphism and write $e \in G$ and $e' \in H$ for the identities of G, H respectively. Prove the following

   a. $\varphi(e) = e'$

      Proof from class: $e'\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, and so therefore $e' = e'\varphi(e)\varphi(e)^{-1} = \varphi(e)\varphi(e)\varphi(e)^{-1} = \varphi(e)$.

   b. $\varphi(g)^{-1} = \varphi(g^{-1})$ for any $g \in G$

5. Determine if the following groups are isomorphic or not. Prove your answers

   a. $(\mathbf{Z}_{10}^*, \cdot)$ (see ex. 5.8 item b.) and $(\mathbf{Z}_4, +)$

   b. $(\mathbf{Z}_8^*, \cdot)$ (see ex. 5.8 item b.) and $(\mathbf{Z}_4, +)$

   c. Q_8 (see ex. 5.8 item i.) and $(\mathbf{Z}_8, +)$

   d. C_4 (see ex. 5.8 item i.)and $(\mathbf{Z}_4, +)$

   e. $\mathbf{Z}_6$ and $\mathbf{Z}_3 \oplus \mathbf{Z}_2$

   f. $\mathbf{Z}_4$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$

6. Determine whether H is a subgroup of the given group G

   a. $G = (\mathbf{Z}_{10}, +)$, $H = \{1, 3, 5, 7, 9\}$

   b. $G = (\mathbf{Z}_{12}^*, \cdot)$, $H = \{1, 5\}$

   c. $G = (\mathbf{Z}_{12}^*, \cdot)$, $H = \{1, 3, 7\}$

   d. *Challenge.* $G = \mathrm{GL}_2(\mathbf{R})$, $H = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbf{R} \right\}$

7. Let G be a group with finitely many elements, and let $g \in G$. Show that there is $n \geq 1$ such that $g^n = e$.

8. Let G be a group and H, K subgroups of G. Show that $H \cap K$ is always a subgroup of G. What about $H \cup K$?

9. Let G be an abelian group. Show that $H = \{g \in G : g^n = e \text{ for some odd integer } n\}$ is a subgroup of G

10. *True or False.* Determine if the following statements are true or false. Prove your answers.

    a. Let G be a group. There can be distinct elements $g, h \in G$ such that both $g^2 = h^2$ and $g^3 = h^3$

    b. There is a group G with exactly two elements g, h such that $g^2 = h^2 = e$ with $g \neq e \neq h$.

    c. If G has exactly 10 elements, it cannot have any elements $g \neq e$ such that $g^3 = e$.

    d. If G is not an abelian group and $H \leq G$ then H is not abelian.

    e. If p is a prime and G is a finite group with p total elements, then $G \cong \mathbf{Z}_p$

11. Let X be a set with six elements. Describe all possible group operations that can be defined on X. Are any of these abelian groups?

12. Let $n > 2$ and G be a group with n elements. Show that there is no subgroup $H \leq G$ with $n - 1$ elements.

13. Let G denote the group of symmetries of an equilateral triangle. Is G cyclic (i.e., $G \cong \mathbf{Z}_n$ for some n)? Is G abelian?

14. Let G be a group and define

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\} \tag{5.19.1}$$

    Show that $Z(G) \leq G$. (Note $Z(G)$ is called the *center* of G, coming from the German word *Zentrum*)

15. In keeping with the notation from 5.8, we write $\mathrm{SL}_2(\mathbf{Z})$ for the set of matrices

$$\mathrm{SL}_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}$$

    a. Prove that $\mathrm{SL}_2(\mathbf{Z})$ is a group.

    b. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ and define a function $f_A \colon \mathbf{C} \to \mathbf{C}$ by $f_A(z) = \dfrac{az + b}{cz + d}$. Show that this assignment $A \mapsto f_A$ defines a homomorphism $\mathrm{SL}_2(\mathbf{Z}) \to \mathcal{F}(\mathbf{C})$ (here $\mathcal{F}(\mathbf{C})$ is the group of functions $\mathbf{C} \to \mathbf{C}$ with function composition as the operation).

    Note: $\mathrm{SL}_2(\mathbf{Z})$ is also called the **modular group**

6 Finite groups

A finite group is just a group G whose underlying set consists of finitely many elements. We write $|G|$ for the number of elements in the set G (i.e., $|G|$ is the cardinality of G). We also call $|G|$ the **order** of the group G.

6.1 Theorem (Lagrange's theorem)**.** *Let G be a finite group and $H \leq G$ be a subgroup of G. Let $n = |G|$ and $k = |H|$. Then k divides n.*

Proof. Let G and $H \leq G$ be given. We'll define an equivalence relation $\sim$ on G as follows: $g \sim h$ if and only if $gh^{-1} \in H$. Let's show this is an equivalence relation: That $g \sim g$ is trivial. Suppose that g, h given with $g \sim h$. Then $gh^{-1} \in H$ and so $(gh^{-1})^{-1} = hg^{-1} \in H$, which is to say $h \sim g$. Last suppose that $g \sim h$ and $h \sim k$. Then $gk^{-1} = gh^{-1}hk^{-1} = (gh^{-1})(hk^{-1}) \in H$ since H is a subgroup (i.e., closed under the operation from G). So, $\sim$ is an equivalence relation.

For $g \in G$ let's write $gH = \{gh : h \in H\}$. This is called a (left) coset of H in G, we'll do more with this later. The claim to focus on now is the following: for $g \in G$, the sets H and gH have the same number of elements. This follows from the claim that the function $f_g \colon H \to gH$ given by $f_g(h) = gh$ is a bijection. Clearly f is a surjection, note that f is an injection as well as if $gh = gh'$ for $h, h' \in H$, then $h = g^{-1}gh = g^{-1}gh' = h'$. Thus the equivalence classes formed by $\sim$ are a partition of G. Suppose that $k = |H|$ and m is the number of equivalence classes formed by $\sim$. Then $|G| = km$ and so $|H| = k$ divides the order of G. □

6.2 Cyclic subgroups

6.3 Proposition. *If G is a finite group and $g \in G$ then there is $n \in \mathbf{N}$ such that $g^n = e$.*

Proof. This is a fun proof. Let G be a finite group and $g \in G$. First we claim that there must be a pair of integers n, m with $g^n = g^m$ and $n \neq m$. Otherwise, the set $S = \{e, g, g^2, g^3, g^4, \cdots, g^n, \cdots\}$ would be all distinct. But then S would have infinitely many elements. Since $S \subset G$ by construction this would be a contradiction, since there can't be an infinite subset of a finite set G.

So let n, m be integers with $n > m$ and $g^n = g^m$. Then $g^{n-m} = g^n g^{-m} = g^n(g^n)^{-1} = e$. □

Let G be a finite group and $g \in G$. From prop 6.3 there is $n \in \mathbf{N}$ such that $g^n = e$. Note then that $g^{2n} = e$ as well since $g^{2n} = (g^n)^2 = e^2 = e$ (and so in fact will all multiples kn for $k \geq 2$). Let $S \subset \mathbf{N}$ be the collection of all integers such that $g^n = e$. Then S has a smallest element[45] call it n_g. This number n_g is called the **order** of the element $g \in G$.

6.4 Proposition. *If G is a group and $g \in G$ of order n_g then $\langle g \rangle = \{e, g, g^2, g^3, \ldots, g^{n_g - 1}\}$ is a subgroup of G.*

In words we call $\langle g \rangle$ the **cyclic subgroup** generated by g (in G).

[45] Because $\mathbf{N}$ is well-ordered, theorem A.5

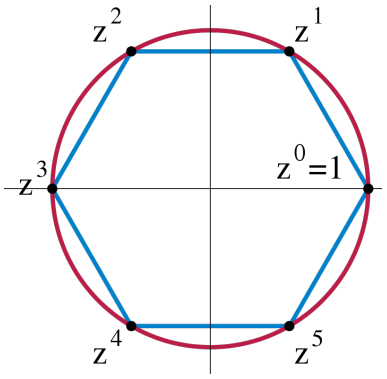
6.5 Corollary (Order of an element divides order of the group)**.** *Let G be a finite group and $g \in G$. Then then order of g divides the order of G.*

Proof. From prop 6.4, $\langle g \rangle \leq G$. Let n_g be the order of g. Then $n_g = |\langle g \rangle| \mid |G|$ by Lagrange's theorem (theorem 6.1). □

6.6 Definition (Cyclic group)**.** *A group G is a cyclic group if G has a single generator.*

In other words, a group G is cyclic if G either (i) G is isomorphic to $\langle a \mid a^n = e \rangle$ for some $n \geq 1$, or $G \cong \langle a \rangle$. Note that $\langle a \rangle \cong \mathbf{Z}$ and $\langle a \mid a^1 = e \rangle$ is just the trivial group $\{e\}$. Any of the groups $(\mathbf{Z}_n, +)$ with $n \geq 1$ are cyclic: they are generated (via addition) by the element 1 together with the relation that $n \cdot 1 = 0$.

6.7 Example (Symmetries encoded by cyclic groups). Let $n \geq 1$, and let X_n be a regular n-gon. Then X_n has "$\mathbf{Z}_n$-symmtery" given by rotation by angle $2\pi/n$ about its center. For instance, $\mathbf{Z}_6 = \langle z | z^6 = 1 \rangle$ is the symmetry group of the regular hexagon as below.



It's natural to ask, what "object" naturally has $\mathbf{Z}$ as its symmetry group? One answer is that $\mathbf{Z}$ "counts" full 2π rotations of the unit circle about the origin[46].

6.8 Some corollaries to Lagrange's theorem for cyclic groups

6.9 Proposition. *If G is a cyclic group and $H \leq G$ then H is also a cyclic group.*

Proof. Suppose that G is a cyclic group and write $G = \langle g \rangle$. Let n be the order of g so that $g^n = e$. Let $H \leq G$ be a subgroup. The claim is that $H = \langle h \rangle$ for some $h \in H$. If H is the trivial group this is uninteresting. Note that since $H \subset G$, any $h \in H$ is of the form $h = g^k$ for some k. Let K be the set $\{k \in \mathbf{N} : h = g^k, h \in H\}$ and let k_0 be the smallest element of K, and $h_0 = g^{k_0}$. Set $\ell = |\langle h_0 \rangle|$. Then $\ell \mid n$ from Lagrange's theorem. But that is to say $n = k_0 \ell$. So H must be given by the set $\{e, h_0, h_0^2, \cdots, h_0^\ell\}$; i.e. H is generated by h_0 and so is cyclic. □

6.10 Remark. In fact, in the above proof $H = \langle h \rangle$ for any $h \in H$, $h \neq e$.

[46] In fact, this can be phrased as a classic result in algebraic topology, that the fundamental group of the circle is (isomorphic to) $\mathbf{Z}$

6.11 Proposition. *G is a group with $|G| = p$ a prime, then $G \cong \mathbf{Z}_p$*

Proof. Let G be a group and suppose that $|G| = p$ for some prime p. Let $g \in G$, $g \neq e$. Then $\langle g \rangle \leq G$, and so $|\langle g \rangle|$ divides p. So, either $|\langle g \rangle| = 1$ or $|\langle g \rangle| = p$. The only element of order 1 in a group is the identity e, so we must have $|\langle g \rangle| = p$. But then $G = \langle g \rangle \cong \mathbf{Z}_p$ as claimed. □

6.12 Proposition. *If $n, m \in \mathbf{N}$ are coprime then $\mathbf{Z}_n \oplus \mathbf{Z}_m$ is cyclic.*

Proof. This is really just a more sophisticated statement of the Chinese remainder theorem (theorem 3.16), i.e., that the map $f : \mathbf{Z}_{mn} \to \mathbf{Z}_n \oplus \mathbf{Z}_m$ given by $f(k) = (k \pmod n, k \pmod m)$ is an isomorphism. I leave this to you as an exercise. □

In general, Groups are not solely comprised of cyclic subgroups, as we'll learn in the next section. If G is an abelian group, however, we have the following statement (provided below without proof—we may get to it later).

6.13 Theorem (Fundamental theorem of finite abelian groups)**.** *If G is a finite abelian group then there is a collection of positive integers $n_1, \cdots, n_k$ such that $G \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_k}$*

6.14 Free Groups and group presentations

Cyclic groups are a good starting point as they have a single generator. However, not all groups have this property. For instance, the Klein four group $V = \{e, a, b, ab\}$ is not generated by any of the elements a or b alone (e.g., $\langle a \rangle, \langle b \rangle$ are *strict* subgroups of V). One useful language for talking about more complicated groups is by *generators* and *relations*, this is also called a **group presentation**.

Looking at V again, we can think of it as the collection of all "words" in the alphabet a, b together with the relations that $a^2 = b^2 = (ab)^2 = e$. For instance, in V the word $abbabbaa$ reduces to the identity via

$$abbabbaa = a(e)a(e)(e) = aa = e$$

The relations $a^2 = e$ and $b^2 = e$ furthermore tell us that $a^{-1} = a$ and $b^{-1} = b$ (since $aa = e$ and $bb = e$ and inverses are unique). The following might look complicated, but we'll investigate it much further.

6.15 Definition (Free group)**.** *Let X be a set. The **Free group** on the set X, denoted $F(X)$, is the collection of words*

$$F(X) = \{x_1^{k_1} x_2^{k_2} x_3^{k_3} \cdots x_n^{k_n} : n \geq 0, x_i \in X, k_i \in \mathbf{Z} \text{ for } i = 1, 2, \ldots, n\} \tag{6.15.1}$$

*The group operation on $F(X)$ is **concatenation** of words*

Here, concatenation of the words means for instance that elements xy and yz concatenate to $xy \cdot yz = xy^2z$. This operation is not abelian.

We call any element $x \in X$ a **generator** for the free group $F(X)$. Note that $F(X)$ is always (countably) infinite. Moreover, if $X = \{x\}$ then there is an isomorphism $f\colon \mathbf{Z} \to F(X)$ given by $f(n) = x^n$ (with the convention that $x^0 = e$).

6.16 Example. For instance, say $X = \{x, y, z\}$ then $F(X)$ is the collection of "words" in the alphabet x, y, z and their inverses. For instance,

$$x, xy^{-1}, xzxzyx, x^2y^4z^{-11}, \cdots$$

are all elements of $F(X)$. The identity in $F(X)$ is the "empty word" (which we can denote as e). In notation we write

$$F(X) = \langle x, y, z \rangle$$

to denote that x, y, z are the generators of $F(X)$. The group operation is concatenation of words, for instance, suppose we have xy and yz in $F(X)$, then $xy \cdot yz = xyyz = xy^2z$. This operation is nonabelian as say $yz \cdot xy = yzxy \neq xy^2z = xy \cdot yz$. It's perhaps not immediately clear that $F(X)$ has inverses, but it does: you simple the read the word backwards replacing all powers by their negatives: i.e.,

$$(xy^{-1}z^2y^3)^{-1} = y^{-3}z^{-2}yx^{-1}$$

6.17 Definition (Group presentation)**.** *Let X be a set (generators) and E a set of equations (relations) in $F(X)$. A **group presentation** is the collection of words $F(X)$ with the stipulation that any word can be "rewritten" using the relations from E.*

In meta notation we write

$$\langle \text{generators} \mid \text{relations} \rangle \tag{6.17.1}$$

for the group presentation given by set of generators X and equations E. Difficult to parse? Perhaps, but hopefully it starts to come together in the next sections when we look at examples of groups. One complicating factor with group presentations it that while it gives us a it's often very difficult (if not impossible) to determine *if* two different presentations actually present the same group.

6.18 Example (Presentations of groups)*.* Here are some examples of group presentations for groups we've already seen.

- **Klein four group**. V has the presentation

$$V = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle \tag{6.18.1}$$

  Note that it's not immediately clear that V has only four elements. First note that $a^2 = b^2 = e$ so that $a^{-1} = a, b^{-1} = b$. Then, since $e = (ab)^2$, we then have

$$ab = aeb = a(ab)^2b = aababb = ebae = ba$$

  so that $ab = ba$. Further any word with more than one consecutive a or b can be reduced via $a^2 = b^2 = e$. So the only possible words are e, a, b and ab.

- **Permutation group of three elements**. Let $X = \{x, y, z\}$ and set S_3 to be the set of bijections of X with the group operation of function composition. Then X has generators $\alpha\colon X \to X$ and $\beta\colon X \to X$, permutations given by

$$\alpha(x) = y,\ \alpha(y) = y,\ \alpha(z) = z \qquad \beta(x) = x,\ \beta(y) = z,\ \beta(z) = y$$

The composition $\alpha\beta$ (her this is read as β first and then α, as with function composition) is then defined by

$$\alpha\beta(x) = y,\ \alpha\beta(y) = z,\ \alpha\beta(z) = x$$

and is identified withe cyclic permutation $x \to y \to z \to x$ which has order 3. The permutation $x \to z \to x$ which fixes y is the composite $\alpha\beta\alpha$. A presentation of S_3 is then

$$S_3 \cong \langle \alpha, \beta \mid \alpha^2 = \beta^2 = (\beta\alpha)^3 = e \rangle \tag{6.18.2}$$

We'll deal more with permutations groups soon enough (including some more reasonable notation for understanding their structure).

- **Quaternion group**. Q_8 the group with presentation

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk,\ i^4 = j^4 = k^4 = e \rangle \tag{6.18.3}$$

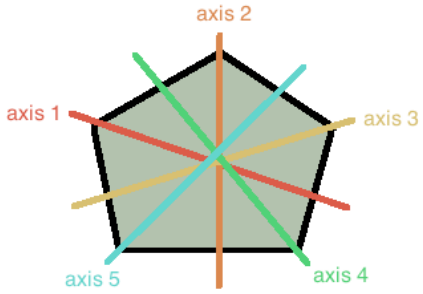
This might look complicated (and it is) but you've actually dealt this with group structure before: this Quaternion group axiomatizes rotations in $\mathbf{R}^3$. Each element i, j, k is a quarter turn in one of the three coordinate planes. Moreover, this group structure underlies the *cross product* of vectors in $\mathbf{R}^3$. In fact this is the same as the group Q_8 of 2×2 matrices given in example 5.8 i.; via the mapping

$$i \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad k \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

6.19 Dihedral groups

Dihedral groups arise as the groups of symmetry of regular n-gons. For instance, D_5 is the group of symmetries of the regular pentagon. We describe this now.

6.20 Example. Let X be a regular pentagon, it can be helpful to think of X as a slightly thickened pentagon with "sides" that are different. Certainly any rotation through the center of X by an angle of $2\pi/5$ is a symmetry of X. Call this r, then $r^5 = e$, and r is a generator for D_5. Also, reflection across any of the following axes (in the picture below) also is a symmetry of X. Let s denote a reflection about the axis labeled axis 1.



Note first that s is not a rotation, so $s \notin \langle r \rangle \leq D_5$. That is s is *another* generator for D_5. It remains to determine how s and r interact with *each other*. A quick encounter with reality tells us that $sr = r^{-1}s$, that is, s and r don't quite commute, but there is a rule for swapping their orders. This gives a presentation

$$D_5 = \langle s, r \mid s^2 = r^5 = e, sr = r^{-1}s \rangle \tag{6.20.1}$$

6.21 Definition. *The **dihedral group** of order n is the group D_n given by the following presentation*

$$D_n = \langle s, r \mid s^2 = r^n = e, sr = r^{-1}s \rangle \tag{6.21.1}$$

In general, D_n describes the symmetries of a regular n-gon (viewed as a sided shape living in the plane): r is a rotation by $2\pi/n$ and s is a reflection through the origin and a chosen vertex of the n-gon.

6.22 Example (Examples of dihedral groups). For small n, we already know the dihedral groups of order n (up to isomorphism, at least). For instance,

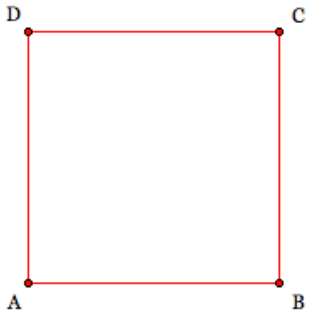
- $D_1 \cong \{e\}$ the trivial group
- $D_2 \cong \mathbf{Z}_2$
- $D_3 \cong S_3$, the permutation group on three symbols and the only nonabelian group of order 6
- To describe the groups D_n for $n \geq 4$ requires semi-direct products, which we probably wont get to until later

Let $n \geq 1$. The group D_n has order $2n$, since any word can be rearranged to be of form either r^k or sr^k for $k \in \{0, 1, \ldots, n-1\}$. The cyclic subgroup of D_n generated by r has $\langle r \rangle \cong \mathbf{Z}_n$, similarly $\langle s \rangle \cong \mathbf{Z}_2$.

6.23 Exercises

1. Complete the proof of proposition 6.12
2. Let $G = \langle a, b \mid ab = ba \rangle$ is G a finite group? What about $H = \langle a, b \mid ab^2 = b^3a \rangle$
3. How many subgroups of D_{20} have order 5?
4. Write out the subgroup lattices for $\mathbf{Z}_{20}$, D_{10}, and Q_8
5. List all finite abelian groups of order ≤ 40. (Hint: use theorem 6.13)
6. True or False: There is a nontrivial subgroup $H \leq \mathbf{Z}$ such that H is finite.
7. Does there exist a subgroup $H \leq D_{20}$ of order 4?
8. Prove that the group Q_8 from (6.18.3) has exactly eight elements
9. Let $n \geq 3$, prove that D_n is not a cyclic group

10. Let S be a square with vertices A, B, C and D below. Is it true that *any* permutation of the letters A, B, C, D is a symmetry of this square?



11. Let n, m be numbers such that $\gcd(n, m) \neq 1$. Prove that $Z_m \oplus Z_n$ is not cyclic.

12. Let $n \geq 1$ and write D_n for the n-th dihedral group. Show that $D_n \cong \langle s, r \mid r^n = s^2 = (sr)^2 = e \rangle$.

    Challenge Show that $D_n \cong \langle s, t \mid s^2 = t^2 = (st)^n = e \rangle$

13. *Challenge* Let G be group generated by the 26 letters of the English alphabet with the relation that words are equivalent if they have the same pronunciation (in English). Show that G is trivial.

7 Symmetric groups

Among the most important finite groups are the symmetric groups (also called permutation groups). In fact, the theory of groups was initially told entirely in terms of symmetric groups and their subgroups.

7.1 Definition. *Let X be a finite set. Define* $\mathrm{Sym}(X)$ *to be the group who elements are bijections $\varphi \colon X \to X$ with the group operation of function composition.*

Let X be a set. In $\mathrm{Sym}(X)$ we denote by Id the identity function $\mathrm{Id}(x) = x$ for all $x \in X$. Any bijection $\varphi \colon X \to X$ is called a *permutation* of the set X. Note that composition of permutations is read *right to left* (consistent with function composition). That is, if φ and φ' are permutations of X, then $(\varphi\varphi')(x) = \varphi(\varphi'(x))$

It's trivial to show that if X and Y have the same number of elements, then $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$, therefore the isomorphism type of $\mathrm{Sym}(X)$ really only depends on the number of elements in X. For $n \geq 0$ let's set $\underline{0} = \emptyset$ and

$$\underline{n} = \{1, 2, 3, \cdots, n\} \qquad n \geq 1 \tag{7.1.1}$$

7.2 Definition (n-th symmetric group)**.** *Let $n \geq 0$, the n-th symmetric group is defined to be $S_n = \mathrm{Sym}(\underline{n})$.*

7.3 Proposition. *Let $n \geq 0$. Then $|S_n| = n!$*

Proof. This is standard proof by induction. For $n = 0, 1$ this is trivial. Suppose n given such that we know that $|S_{n-1}| = (n-1)!$. We want to show that $|S_n| = n!$. Let a bijection $\alpha \colon \underline{n} \to \underline{n}$ be given. Suppose that $\alpha(n) = k$. Then α is a bijection of the set $\{1, 2, \cdots, n-1\}$ and $\underline{n} \setminus \{k\}$. There are $(n-1)!$ such bijections (by the inductive hypothesis), and n such choices of k. So, the total number of bijections $\alpha = n(n-1)! = n!$. □

7.4 Remark. Since $|S_0| = |S_1| = 1$ we must have $S_0 \cong S_1 \cong \{e\}$ the trivial group. Similarly, $S_2 \cong \mathbf{Z}_2$ the only group of order 2.

For $n \geq 3$, S_n is not abelian. S_3 has $3! = 6$ elements, so since there are only two groups of order 6, we must have $S_3 \cong D_3$. In fact, this isomorphism can be seen by first labelling the vertices of an equilateral triangle as 1,2,3; then identifying a permutation of $\underline{3}$ with the symmetry from D_3 which permutes the vertices in that order. (Note that this does not work for the square (or n-gons with $n \geq 4$) since, e.g. no symmetry of the square will swap the vertices 1 and 2 keeping 3, 4 fixed.)

The natural "object" on which the group S_n is the symmetries of is a regular $(n-1)$-simplex. For instance, S_4 encodes the symmetries of a regular tetrahedron (include those which reverse the orientation of the tetrahedron), which is just a regular 3-simplex. This is maybe somewhat unsatisfying for $n \geq 5$ since then the geometric objects become 4+ dimensional which is obviously hard to visualize.

7.5 Cycle decomposition of permutations

Standard notation for working with permutation groups is to use what is called *cycle notation*. Suppose a permutation from $\alpha \in S_5$ is given by:

$$\alpha(1) = 2, \quad \alpha(2) = 4, \quad \alpha(3) = 5, \quad \alpha(4) = 3, \quad \alpha(5) = 1$$

This is rather clunky, and generally there's not going to be a "nice" algebraic formula for a given permutation. We can instead write the information of α as follows (12435). That is, the function is read "cyclically" in that

$$1 \to 2 \to 4 \to 3 \to 5 \to 1$$

Since α is a bijection this notation makes sense. In particular, α can just as well be interpreted as a permutation in S_6 where the element 6 is not moved.

7.6 Definition (Cycle in S_n)**.** *Let $n \geq 0$ and suppose that $\alpha \in S_n$ such that the following holds: There is a number k with $1 \leq k \leq n$ and collection of elements $A = \{a_1, \cdots, a_k\} \subset \underline{n}$ such that*

$$\alpha(a_1) = a_2, \quad \alpha(a_2) = a_3, \quad \cdots \quad \alpha(a_{k-1}) = a_k, \quad \alpha(a_k) = a_1$$

*and $\alpha(a) = a$ for all $a \notin A$. Then α is called a **cycle of length** k (in S_n). In this setup, we write*

$$\alpha = (a_1\, a_2\, a_3\, \cdots\, a_{k-1}\, a_k) \tag{7.6.1}$$

for the cycle $\alpha \in S_n$.

The word *cycle* here is consistent with the notion of a cyclic group: if α is a cycle of length k then $\langle\alpha\rangle \cong \mathbf{Z}_k \leq S_n$. Let's say that given a cycle $\alpha \in S_n$, and the collection A as outlaid in the above definition, that any $a \in A$ is an *element moved by* α (and that if $a \notin A$ then a is *not moved* by α). If α is a cycle of length 2 we call α a **transposition**.

Let $n \geq 1$ and let α, β be cycles in S_n. Then, α and β are said to be **disjoint** if they do not move any common elements. Note that while S_n is generally not abelian, the following statement is true.

7.7 Proposition. *Let $n \geq 0$. If $\alpha, \beta \in S_n$ are disjoint cycles then $\alpha\beta = \beta\alpha$.*

Proof. Left as an exercise. □

7.8 Theorem. *Let $n \geq 0$. Every permutation in S_n is a product of disjoint cycles. Moreover, this decomposition is unique up to rearrangement of factors.*

Proof. This is a nice example of a theorem which is "evident" but a bit annoying to write a proof of. Here's the idea. We'll use (complete) induction on n. For $n = 0, 1$ and 2 this is obvious.

So let n be given so that for all $k < n$ the claim holds. Let $\alpha \in S_n$. Then α is a bijection of the set $\underline{n} = \{1, 2, \ldots, n\}$. Consider the set $X = \{1, \alpha(1), \alpha(\alpha(1)), \alpha^3(1), \cdots\}$. Then $X \subset \underline{n}$. If $X = \underline{n}$ we're done, as then α is a cycle of length n. If not then we can consider the set $\underline{n} \setminus X$ which must be have a bijection with some set $\underline{k}$ for $1 \leq k < n$. So, by induction α restricted to the set $\underline{n} \setminus X$ has a decomposition into disjoint cycles. By construction, these cycles are disjoint from the cycle $(1\, \alpha(1)\, \alpha^2(1) \cdots)$. So the claim holds.

Uniqueness I leave to you as an exercise. □

The decomposition of a permutation α into disjoint cycles is called its **cycle decomposition**.

7.9 Corollary. *Let $n \geq 2$. Every permutation in S_n can be written as a product of transpositions.*

Proof. From theorem 7.8 it's enough to show that any cycle can be written as a product of transpositions. Let $2 \leq k \leq n$ and $\alpha \in S_n$ be given of the form $\alpha = (a_1\, a_2\, a_3\, \cdots\, a_{k-1}\, a_k)$

for some elements $a_1, \ldots, a_k \subset \underline{n}$. Then, by Ex. 13. we can write each α a product of transpositions; e.g. as

$$\alpha = (a_1\, a_2)(a_2\, a_3)\cdots(a_{k-2}\, a_{k-1})(a_{k-1}\, a_k)$$

This completes the proof. □

7.10 Conjugacy classes and cycle decomposition

If G is a group and $g, h \in G$ we call the term ghg^{-1} the conjugate of h by g. The first observation is the following:

7.11 Proposition. *Let G be a group. Define an relation $\sim$ on G by $h \sim h'$ if there is $g \in G$ with $ghg^{-1} = h'$. Then $\sim$ is an equivalence relation.*

Any set of the associated partition $G/\sim$ is called a **conjugacy class** of G. If $h, h' \in G$ such that there is a $g \in G$ such that $ghg^{-1} = h'$ we say that h and h' are **conjugate** (by g).

7.12 Example. We've seen an example of this before[47]. In the group $\mathrm{GL}_2(\mathbf{R})$ (with matrix multiplication), matrices A and B are conjugate if and only if there is $P \in \mathrm{GL}_2(\mathbf{R})$ with $PAP^{-1} = B$. In this case, A and B must have the same eigenvalues. In fact, matrices $A, B \in \mathrm{GL}_2(\mathbf{R})$ are conjugate if and only if they have the same eigenvalues.

7.13 Proposition. *Let $n \geq 0$ and $\alpha, \beta \in S_n$. Suppose that α is a cycle of length k given by $\alpha = (a_1\, a_2 \cdots a_k)$. Then*

$$\beta\alpha\beta^{-1} = (\beta(a_1)\, \beta(a_2) \cdots \beta(a_k))$$

In particular, any conjugate of a cycle of length k in S_n is another cycle of length k.

7.14 Definition. *Let $n \geq 0$ and $\alpha \in S_n$. Let $k \geq 1$ and $n_1, n_2, \ldots, n_k \geq 1$ such that $n_1 + n_2 + \cdots + n_k = n$. We say that α is a **cycle of type** $(n_1, n_2, \cdots, n_k)$ if α has a decomposition into disjoint cycles $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ such that α_i is a cycle of length i for $i = 1, 2, \ldots, k$.*

Note by theorem 7.8 that any decomposition of a permutation $\alpha \in S_n$ into cycles must have the same cycle type.

7.15 Theorem. *Let $n \geq 0$. The conjugacy classes of S_n are in one-to-one correspondence with the cycle types of S_n.*

7.16 Example. In S_2 there are two conjugacy classes: $\{\mathrm{Id}\}$ and $\{(12)\}$. These correspond to the two decompositions $2 = 2$ and $2 = 1 + 1$.

In S_3 we have conjugacy classes corresponding to the decompositions of 3 as $3 = 3, 3 = 2+1$ and $3 = 1 + 1 + 1$. These correspond to the conjugacy classes

$$\{(123), (231)\}, \quad \{(12), (23), (13)\}, \quad \{\mathrm{Id}\}$$

[47] I believe I showed this in class way back in the first or second week

7.17 Sign of a permutation

From corollary 7.9 we know that transpositions generate S_n.

7.18 Theorem. *Let $n \geq 0$. If $k \geq 1$ and $\alpha_i \in S_n$ is a transposition for $i = 1, \cdots, k$ such that $\mathrm{Id} = \alpha_1\alpha_2\alpha_3\cdots\alpha_k$; then k is an even number.*

Proof. A warning, this is somewhat of a tricky proof. We use proof by induction. The identity cannot be a transposition, so $k \neq 1$. If $k = 2$ then this follows since any transposition is its own inverse.

So, let $k > 2$ such that the claim holds for all integers ℓ with $2 \leq \ell < k$. Let $\alpha_k = (a\,b)$, there are then four cases to consider for the form of the terms $\alpha_{k-1}\alpha_k$:

$$\text{(i) } (a\,b)(a\,b), \quad \text{(ii) } (a\,c)(a\,b), \quad \text{(iii) } (b\,c)(a\,b), \quad \text{(iv) } (c\,d)(a\,b)$$

(here, $c, d \in \underline{n}$)

Let's go case by case. In case (i), we have that $(a\,b)(a\,b) = \mathrm{Id}$, so that α can be reduced to a string of $k-2$ transpositions. By induction, $k-2$ must be even, $k = (k-2)+2$ is even as well.

In cases (ii)–(iv) we can use the following equations (you should verify these)

$$(a\,c)(a\,b) = (a\,b)(b\,c) \quad (b\,c)(a\,b) = (a\,c)(c\,b), \quad (c\,d)(a\,b) = (a\,b)(c\,d) \tag{7.18.1}$$

to replace $\alpha_{k-1}\alpha_k$ by an equivalent pair of transpositions with a not appearing in α_k. If $\alpha_{k-1} = \alpha_{k-2}$ then we're done by induction: cancel these terms and learn by induction that $k-2$ must be even. If not, we can run the same operation again replacing $\alpha_{k-2}\alpha_{k-1}$ by an equivalent string with a not appearing in the term α_{k-1}.

Now let's look at the product $\alpha_1\alpha_2\cdots\alpha_{k-2}$. If this is the identity then we're done, since by the inductive hypothesis we must have $k-2$ even, and therefore k even as well. If not, then we can continue this game: replace $\alpha_{k-3}\alpha_{k-2}$ by a pair of equivalent transpositions with a moved by α_{k-3} only, then $\alpha_{k-4}\alpha_{k-3}$, etc. The claim is that at some point, this pairwise exchange of transpositions must produce the same transposition next to itself. This then cancels out, leaving Id written as a product of $k-2$ transpositions, and the theorem follows.

Suppose that this never happens. Then we can exchange transpositions all the way back to $\alpha_1\alpha_2$ such that α_1 moves a and no α_k for $k \geq 2$ does. This is a problem, because by assumption we must still have $\mathrm{Id} = \alpha_1\alpha_2\cdots\alpha_k$; but if only α_1 moves then $\mathrm{Id}(a) \neq a$ as would be required. This completes the proof. □

7.19 Corollary. *Let $n \geq 0$ and $\alpha \in S_n$ some permutation. If α is represented as an even number of transpositions, then any other representation of α by transpositions must also contain an even number of factors. Similarly, if α is represented as an odd number of transpositions, then any other representation of α by transpositions must contain an odd number of factors.*

Proof. Suppose that we had two representations of α by transpositions, i.e., that

$$\alpha = \tau_1\tau_2\tau_3\cdots\tau_n = \sigma_1\sigma_2\sigma_3\cdots\sigma_m$$

where τ_i and σ_j are transpositions for $i = 1,\dots,n$ and $j = 1,\dots,m$. The first claim is that

$$\alpha^{-1} = \tau_n\tau_{n-1}\cdots\tau_3\tau_2\tau_1$$

Indeed, any transposition is its own inverse, so that

$$\tau_1\tau_2\cdots\tau_{n-1}\tau_n\tau_n\tau_{n-1}\cdots\tau_2\tau_1 = \tau_1\tau_2\cdots\tau_{n-1}\tau_{n-1}\cdots\tau_2\tau_1 = \cdots = \tau_2\tau_1\tau_1\tau_2 = \tau_1\tau_1 = \mathrm{Id}\,.$$

Then we cxan write

$$\mathrm{Id} = \alpha\alpha^{-1} = \sigma_1\sigma_2\sigma_3\cdots\sigma_m\tau_n\tau_{n-1}\cdots\tau_3\tau_2\tau_1$$

But, by theorem 7.18 we must have $n+m$ be an even number. This means that either n and m are both even or n and m are both odd. Thus the claim is proved. □

7.20 Definition (Sign of permutation)**.** *Let $n \geq 0$ and $\alpha \in S_n$. Let k be the number of transpositions in some representation of α by transpositions. If k is even, α is called an **even** permutation; if k is odd, α is called an **odd** permutation.*

It's worth pointing out that corollary 7.19 tells us that this definition is indeed well-defined. The number of individual transpositions in some representation of a permutation $\alpha \in S_n$ is not necessarily unique, but the *parity* (i.e., even or oddness) of that number is. You can think of this a function

$$\mathrm{sgn}\colon S_n \to \mathbf{Z}_2 \tag{7.20.1}$$

such that sgn(even permutations) = 0 and sgn(odd permutations) = 1. In fact, sgn is a homomorphism $S_n \to \mathbf{Z}_2$ (see Ex. 15.). We'll dig deeper into general homomorphisms (i.e., not just isomorphisms) in the next section.

7.21 The alternating group

Let $n \geq 0$ and define $A_n \subset S_n$ to be

$$A_n = \{\alpha \in S_n : \alpha \text{ has a representation as an even number of transpositions}\} \tag{7.21.1}$$

The following proposition tells us that A_n is indeed a subgroup of S_n. We call A_n the **alternating group** (on n symbols).

7.22 Proposition. *A_n is a subgroup of S_n*

Proof. $\mathrm{Id} = \tau^2$ for any transposition τ, so $\mathrm{Id} \in A_n$. If $\alpha, \beta \in A_n$, then α and β both have presentations as an even number of transpositions. Since the sum of even numbers is even, $\alpha\beta \in A_n$ then. Similarly, if $\alpha = \tau_1\tau_2\cdots\tau_k$ is decomposed into transpositions τ_i, then $\alpha^{-1} = \tau_k\tau_{k-1}\cdots\tau_1$, which has the same number of transpositions. So if $\alpha \in A_n$ then $\alpha^{-1} \in A_n$ as well. □

7.23 Proposition. *Let $n \geq 2$, then $|A_n| = n!/2$.*

Either a permutation is even or odd, so it's half the total permutations (that's a joke, but only sort of). Let $A_n \subset S_n$ be the even permutations and $O_n \subset S_n$ be the odd permutations. Note that A_n and O_n are disjoint, so if we show that there is a bijection $A_n \to O_n$ we're done. Fix any transposition $\tau \in S_n$ and define $\varphi\colon A_n \to O_n$ by $\varphi(\alpha) = \tau\alpha$. Note that if $\alpha \in A_n$ then $\tau\alpha$ has one more transposition, so is odd, and therefore this function is well defined.

Let's show that φ is a bijection. φ is injective as, if $\tau\alpha = \tau\beta$ for some permutations $\alpha, \beta \in A_n$, then $\alpha = \tau\tau\alpha = \tau\tau\beta = \beta$. Similarly if $\beta \in O_n$ then $\tau\beta \in A_n$ and $\varphi(\tau\beta) = \tau\tau\beta = \beta$, so φ is surjective as well. Thus $|A_n| = |O_n|$ and therefore since $|A_n| + |O_n| = |S_n| = n!$ we must have $|A_n| = n!/2$.

7.24 The alternating group in action

7.25 Example. It's straightforward to check that $A_1 = A_2 = \{\mathrm{Id}\}$. A calculation reveals that $A_3 = \{\mathrm{Id}, (123), (132)\} \cong \mathbf{Z}_3$. A_3 can be interpreted as the orientation-preserving symmetries of the regular 2-simplex; that is, the subgroup $\langle r\rangle \leq D_3$.

For $n \geq 4$, A_4 is not abelian. It's possible to enumerate the elements of A_4:

$$A_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$$

This is a non-abelian group corresponding to the orientation-preserving[48] symmetries of a regular tetrahedron. It's one of the five non-isomorphic groups of order 12; we know three of the others: $\mathbf{Z}_{12}, \mathbf{Z}_6 \oplus \mathbf{Z}_2$ and D_6. The last has the presentation $\langle a, b, c \mid a^3 = b^2 = c^2 = abc = e\rangle$[49]. It's not supposed to be obvious that these are all the groups of order 12.

7.26 Example (A_n and roots of polynomials). You may know of the following theorem:

> *Let p be a polynomial with real coefficients of degree n. There is an explicit formula for the roots (i.e., x such that $p(x) = 0$) of p using radicals if and only if $n = 1, 2, 3, 4$.*

For instance, if $n = 2$ there is the good old quadratic formula. For $n = 3, 4$ there are corresponding cubic and quartic formulas which become increasingly complicated. There is, however, no general formula for 5-th and larger degree polynomials using only roots. This has to do with the structure of the groups A_n, in particular that A_n is not *solvable*[50] for $n \geq 5$. It's a lot more involved group theory and Galois theory to show this, but an interesting and nontrivial connection to what we're learning.

[48] That is, if you have an honest tetrahedron (a four-sided die, say) in the 3d space in which we live, the symmetries of that tetrahedron. Some people/books/authority figures will say this A_4 is indeed the group of symmetries of the tetrahedron but this inconsistent with D_3 being the group of symmetries of the equilateral triangle. "Symmetries" in this context is not exactly clear enough: only those from the alternating group preserve the orientation of the space these shapes are immersed into.

[49] Groupprops tells me this is called the *Dicyclic group*, so I suppose I must believe them

[50] Being solvable is weaker than being abelian, but still somewhat similar. We probably won't get to talk about solvability of groups

7.27 Example (Symmetry groups of the Platonic solids). A neat application of symmetric and alternating groups comes from the groups of symmetries of the five Platonic solids. Recall that a platonic solid is a polyhedron in $\mathbf{R}^3$ all of whose faces are the same. There are only five such polyhedra: The cube, the tetrahedron, the octahedron, the icosahedron, and the dodecahedron.

A **rotational symmetry** means *orientation-preserving symmetry*[51], which is again to say, some symmetry you could realize as an honest symmetry of the shape X in $\mathbf{R}^3$. We have the following

Solid	Shape of faces	Number of faces	Rotational symmetry group
Tetrahedron	Triangle	4	A_4
Cube	Square	6	S_4
Octahedron	Triangle	8	S_4
Dodecahedron	Pentagon	12	A_5
Icosahedron	Triangle	20	A_5

What's more is that, together with the cyclic and dihedral groups, the groups appearing in the above table are the *only* finite groups that can be realized as the rotational symmetry of some polyhedron in $\mathbf{R}^3$.

7.28 Subgroups of S_n

In general, any finite group can be embedded[52] into a symmetric group. As mentioned before, "groups" as a concept were initially thought of inasmuchas their embeddings into S_n for some n. Cayley's theorem, as follows, solidifies this interpretation. We'll talk more about some of the subtletites of this argument when we discuss group actions in depth.

7.29 Theorem (Cayley's theorem)**.** *Let $n \geq 1$ and G be any finite group of order n. Then $G \leq S_n$.*

Proof. Let $n \geq 1$ and suppose that G is any finite group of order n. Let's define X_G to be the set with the same elements as G, and define $\widetilde{G}$ to be the set of functions $\varphi_g \colon X_G \to X_G$ given by $\varphi_g(x) = gx$ for $g \in G$. Any such function φ_g is a bijection (you should prove this), and so $\widetilde{G} \subset \mathrm{Sym}(X_G)$. The first claim is that $\widetilde{G}$ is indeed a subgroup of $\mathrm{Sym}(X_G)$, the second is that $G \cong \widetilde{G}$. Let $n = |G|$, then since X_G is a set with n elements, $\mathrm{Sym}(X_G) \cong S_n$, which proves the theorem. □

[51] For instance, the reflection $s \in D_n$ are not rotational symmetries of the n-gon. Recall that a rotation of the plane is given by the matrix

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

for some $\theta \in \mathbf{R}$. If we view the n-gon as living inside $\mathbf{R}^2$, no such rotation matrix will take the n-gon to its reflection (such a matrix would have to have a negative determinant). It's maybe a bit subtle to really define what a rotation is: one way is to say that a rotation in $\mathbf{R}^n$ is an element of the special orthogonal group $\mathrm{SO}(\mathbf{n})$ of orthogonal $n \times n$ matrices with determinant 1. This a good example of what's called a Lie group, I'd like to talk about these more later in the term.

[52] This has a precise definition, i.e., that a group H embeds into G if there is an injective homomorphism $H \to G$.

7.30 Exercises

1. Let $\alpha = (12), \beta = (23)$ and $\gamma = (34)$. Construct a presentation of the symmetric group S_4 with generators α, β and γ.
2. Let $\alpha = (a_1\, a_2\, \cdots\, a_k) \in S_n$. Prove that $\alpha = (a_2\, a_3\, \cdots\, a_k\, a_1)$ and $\alpha^{-1} = (a_k\, a_{k-1}\, \cdots\, a_1)$
3. Construct a generating set for A_4 and write a presentation based on your set of generators.
4. Let $H = \{\alpha \in S_5 : \alpha(1) = 4\}$. Is $H \leq S_5$?
5. Prove proposition 7.7.
6. Let $\alpha, \beta \in S_n$ such that α is a cycle of length k of the form $\alpha = (a_1\, a_2\, \cdots\, a_k)$. Prove that
$$\beta\alpha\beta^{-1} = (\beta(a_1)\, \beta(a_2)\, \cdots\, \beta(a_k))$$
7. Recall that $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$. Prove that $Z(S_n) = \{\mathrm{Id}\}$ for all $n \geq 3$.
8. Determine (i) the cycle decomposition of, (ii) the order of each of the following permutations
   a. $(12)(357)$
   b. $(12)(237)$
   c. $(345)(245)$
   d. $(1235)(24567)$
9. Let α be a 6-cycle and β be a 5-cycle. Determine if $\alpha^4\beta^4\alpha^{-1}\beta^2$ is even or odd.
10. Describe all conjugacy classes (i.e., cycle types) in S_7 and A_7.
11. Show that A_{10} contains an element of order 5.
12. Prove that A_3 is the group of orientation-preserving symmetries of a regular 3-gon[53] Harder: prove that A_4 is the group of orientation preserving symmetries of a regular tetrahedron.
13. Let $n \geq 0$ and write $\alpha = (a_1\, a_2\, a_3\, \cdots, a_k)$ for some cycle in S_n. Prove that α can be decomposed into transpositions in the two following ways
$$\alpha = (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_3)(a_1\, a_2) = (a_1\, a_2)(a_2\, a_3) \cdots (a_{k-2}\, a_{k-1})(a_{k-1}\, a_k)$$
14. Let D_n be the n-th dihedral group. Prove that $D_n \leq S_n$ for all $n \geq 1$.
15. Prove that $\mathrm{sgn}\colon S_n \to \mathbf{Z}_2$ is a homomorphism.
16. Let $\alpha, \beta \in S_n$. Prove that their *commutator* $\alpha\beta\alpha^{-1}\beta^{-1}$ is always an element of A_n.

[53] You may know this shape by the name *equilateral triangle* (but it will also be the regular 3-gon to me).

17. True or False: For any $n \geq 3$, there is a presentation of S_n with exactly two generators.
18. True or False: If $\alpha \in S_n$ is a cycle, then α^k is a cycle for all $k \geq 1$.
19. *Challenge.* Prove that the group of rotational symmetries of a regular cube in $\mathbf{R}^3$ is isomorphic to S_4. Use that the octahedron and cube are *dual* (as polyhedra) to show that the group of rotational symmetries of a regular octahedron is also S_4.

    Challeng-ier. Use the same type of duality argument to prove that the regular icosahedron and dodecahedron both have rotational symmetry group isomorphic to A_5.
20. *Challenge.* Let $n \geq 1$. Describe the set K_n of all integers k for which S_n has a subgroup of order k.
21. (A_n is generated by 3-cycles). Let $n \geq 3$. Prove that $(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d)$ and $(a\,b)(a\,c) = (a\,c\,b)$ for any $a, b, c, d \in \underline{n}$. Use this to prove that the collection of cycles of length 3 generate A_n.

8 Normal subgroups and group quotients

So far we've seen many examples of group, and some examples of how to construct new groups from old. One crucial operation is missing: Quotients. The first observation is that not all subgroups "permit" quotienting. In order to create a quotient of a group by a subgroup, we need to first describe the language of cosets.

8.1 Cosets

Let G be a group and $H \leq G$ some subgroup of G. Let $g \in G$. We write gH and Hg for the sets

$$gH = \{gh : h \in H\} \qquad Hg = \{hg : h \in H\} \tag{8.1.1}$$

In words, a set of the form gH is called a **left coset**[54] of H by g (in G), and Hg is called a **right coset** of H by g (in G). Note that in general these sets are not equal, since groups are not assumed to be commutative. Note that cosets gH and $g'H$ may have $gH = g'H$ without group elements g and g' being equal.

8.2 Proposition. *Let G be a group and $H \leq G$. Then $g \sim h$ if and only if $gH = hH$ is an equivalence relation on G. Similarly, $g \sim h$ iff $Hg = Hh$ is also an equivalence relation on G.*

I believe we proved the above proposition (or something equivalent to it) in lecture. Regardless, I leave it to you as an exercise. The key here is that cosets (either left or right) form a partition of the original group G.

8.3 Example. Recall that any subgroup $H \leq \mathbf{Z}$ is of the form $H = n\mathbf{Z} = \{nk : k \in \mathbf{Z}\}$ for some $n \in \mathbf{Z}$. Such a subgroup has cosets given by the equivalence classes $[0], [1], \cdots, [n-1]$ where again

$$[k] = \{k + n\ell : \ell \in \mathbf{Z}\} = k + n\mathbf{Z}$$

[54] Note that g acts on the *left* here

In this case, cosets $k + n\mathbf{Z}$ and $n\mathbf{Z} + k$ are equal, since addition of integers is commutative.

8.4 Remark. In general, if $H \leq G$ and $g \in G$ such that $gH \neq eH$, then gH **will not** be a subgroup of G. An upshot is that a lot of the intuition from linear algebra carries over. A subgroup $H \leq G$ is analogous to a *subspace* $U \subset V$ of some vector space V (i.e., $V = \mathbf{R}^n$). Recall that all subspaces must contain the origin, in the same way that all subgroups must contain the identity. Cosets of U in V are the translations of U by some nonzero vector: i.e., $v + U$ for some $v \in V$. They aren't quite subspaces[55], but *shifts* of subspaces.

8.5 Normal subgroups

For certain types of subsets of G, it is possible to define a group structure on the set of cosets. These subsets are called normal subgroups as we discuss below.

8.6 Definition (Normal subgroup)**.** *Let G be a group and $N \leq G$ a subgroup of G. We say that N is a **normal** subgroup of G if for any $g \in G$ we have*

$$gNg^{-1} = \{ghg^{-1} : h \in N\} = N. \tag{8.6.1}$$

Notation-wise, we write

$$N \trianglelefteq G \tag{8.6.2}$$

to denote that $N \leq G$ is a normal subgroup of G. This operation of multiplying by g on the left and g^{-1} on the right is called **conjugation**—we will see this appear more in the term. An equivalent statement to N being normal is that all *conjugates* of N are the same.

8.7 Proposition. *Let G be a group. The follow statements are equivalent*

(i) N is a normal subgroup of G

(ii) $gN = Ng$ for all $g \in G$ (i.e., left and right cosets of N are the same)

(iii) $gNg^{-1} \subset N$ for all $g \in G$

Proof. Note first that, for any $g \in G$, $gNg^{-1} = N$ if and only if $gN = gNg^{-1}g = Ng$. This shows (i) is equivalent to (ii). Clearly (i) implies (iii), so it's enough to show that (iii) implies (i). Suppose that $gNg^{-1} \subset N$ for all $g \in G$. Then

$$N = g^{-1}gNg^{-1}(g^{-1})^{-1} \subset g^{-1}Ng$$

for all $g \in G$. In particular, rewriting $h = g^{-1}$, $N \subset hNh^{-1}$ for all $h \in G$. □

The following proposition is basically trivial, but still very useful to have for reference. I leave it to you to show why this is trivial.

8.8 Proposition. *If G is abelian, and $N \leq G$ then $N \trianglelefteq G$.*

[55] Sometimes you'll see the adjective *affine* used here

8.9 Quotient groups

Given any subgroup $H \leq G$ we write G/H for the set of (left) cosets of H in G (that is, the associated set of equivalence classes given by the partition by left cosets). Note that this is generally different from the partition of G by *right* cosets, you may see people write $H\backslash G$ for this. The distinction is important, but let's no worry about it for now.

8.10 Theorem (Quotient group)**.** *Let G be a group and $N \trianglelefteq G$ a normal subgroup. Then G/N inherits a group structure from G.*

Proof. Let $gN, gH \in G/H$. The evident group operation is given by

$$(gN)(hN) = (gh)N$$

Note that this is well-defined since N is normal in G; i.e., $(gN)(hN) = g(Nh)N = g(hN)N = ghN$. Moreover, this product does not depend on choice of representative for each coset. Meaning, if $gN = g'N, hN = h'N$ then $g' = gn$ and $h' = hm$ for some elements $n, m \in N$. Then

$$(g'N)(h'N) = (g'h')N = (gnhm)N = ghn'mN = ghN$$

(note here that $nh = hn'$ for some $n' \in N$ since the right coset and left coset by h agree.) The identity in G/N is given by the subgroup $N = eN$. If $gN \in G/N$ then $(gN)^{-1} = g^{-1}N$. □

The resulting group G/N is called the **quotient of G by N**. Some examples below:

8.11 Example (Quotients of cyclic groups). Let $n \geq 1$, then $n\mathbf{Z} = \{nk : k \in \mathbf{Z}\}$ is a normal subgroup of $\mathbf{Z}$. The quotient $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$. As another example, let $n \geq 1$ and $k \mid n$. Then $\langle n/k \rangle \trianglelefteq \mathbf{Z}_n$. In particular, $\mathbf{Z}/\langle n/k \rangle \cong \mathbf{Z}_k$.

8.12 Example (Normal subgroups of D_n). Let $n \geq 1$. The dihedral group $D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{-1}s \rangle$ has the subgroup $N = \langle r \rangle \cong \mathbf{Z}_n$. The claim is that subgroup is normal in G. We'll show that $gNg^{-1} \subset N$ for all $g \in G$. It suffices to show this for the generators s, r of D_n. That $rNr^{-1} \subset N$ is trivial. To show that $sNs^{-1} \subset N$ we observe that an element in sNs^{-1} is one of the from $sr^k s$, which by the group relations can be rewritten $sr^k s = r^{-k}ss = r^{-k} \in N$.

The associated quotient group $D_n/\langle r \rangle = \{eN, sN\} \cong \mathbf{Z}_2$. Note that this quotient group is "crushes" the rotational aspect of D_n, leaving only the reflections. In terms of the presentation, we're simply adding in an additional relations which say any $g \in N$ is equal to e.

8.13 Definition (Index of H in G)**.** *Let G be a group and $H \leq G$ any subgroup. The **index of H in G** is the positive integer n such that the partition of G by cosets of H has exactly n elements.*

We write $[G : H]$ for the index of H in G. If G/H has infinitely many elements we write $[G : H] = \infty$[56]. Note that if G, H are finite groups then $[G : H]$ is always finite. If G is an infinite group there could still be (infinite) subgroups H such that $[G : H]$ is finite.

[56] Technically, you should worry about the cardinality of infinity here, but we'll let this slide

In example 8.12 we found that $\langle r \rangle \leq D_n$ is a subgroup of index 2. Similarly, $A_n \leq S_n$ is a subgroup of index 2. In general, any subgroup of index 2 is normal (see problem 2.).

8.14 Kernel and image of a homomorphism

8.15 Definition. *Let G, H be groups and $\varphi\colon G \to H$ a homomorphism. Define the* ***kernel****,* $\ker\varphi$*, and* ***image****,* $\operatorname{im}\varphi$*, of φ by*

$$\ker\varphi = \{g \in G : \varphi(g) = e_H\} \qquad \operatorname{im}\varphi = \{\varphi(g) : g \in G\} \tag{8.15.1}$$

8.16 Proposition. *Let G, H be groups and $\varphi\colon G \to H$ a homomorphism. Then $\ker\varphi \leq G$ and $\operatorname{im}\varphi \leq H$. Moreover, $\ker\varphi$ is a normal subgroup of G.*

Proof. Let $\varphi\colon G \to H$ be given and write $K = \ker\varphi$. Note that $\varphi(e_G) = e_H$ so that $e_G \in K$. Similarly, if $g, h \in \ker\varphi$ then $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = e_H e_H^{-1} = e_H$. So that $K \leq G$. To show that K is normal, let $g \in G$. Note that $gK = \{gh : \varphi(h) = e_H\}$. So for any $h \in K$ we claim that $gh = h'g$ for some other $h' \in K$. Indeed, set $h' = ghg^{-1}$, then

$$\varphi(h') = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g)^{-1} = e_H$$

so that $h' \in K$. Thus $gK = Kg$, and so K is normal. That $\operatorname{im}\varphi \leq H$ we leave as an exercise. □

Generally whenever you have a function $f\colon A \to B$ between sets with algebraic structure, the "stuff" in A that gets sent to the identity in B will always be a "nice" subset of A.

For instance, you may recall the nullspace of a matrix: Any matrix represents a linear transformation $T\colon V \to U$ for some vector spaces V, U (for instance, $\mathbf{R}^n$). Vector spaces generally have more structure than just a group[57], but do always have an underlying (abelian) group whose operation is sum of vectors. The nullspace of T is a linear subspace of V of vectors which get sent to the zero vector in U. This is simply the kernel of the linear transformation T.

8.17 Proposition. *Let $\varphi\colon G \to H$ be a group homomorphism. Then φ is injective if and only if $\ker\varphi = \{e\}$.*

The idea of this proof is that since groups have inverses, any property can be "shifted" to the identity. Essentially, one-to-one-ness at the identity is enough to show one-to-one-ness overall.

Proof. Suppose that φ is injective and write $e \in G$ and $e' \in H$ for th respective group identities. Since $\varphi(e) = e'$ must be true of a homomorphism, then $\ker\varphi = \{e\}$ since φ is injective. Similarly, suppose that $\ker\varphi = \{e\}$ and that $g, h \in G$ such that $\varphi(g) = \varphi(h)$. Then $\varphi(gh^{-1}) = e'$ so that $gh^{-1} \in \ker\varphi$. But then $gh^{-1} = e$ so that $g = h$. Thus φ is injective. □

[57] A vector space is what is called a *module* over a *field*. Fields are algebraic structures where you can add, subtract, multiply and divide, like $\mathbf{R}$ or $\mathbf{C}$. *Module* means that in addition to the (abelian) group structure (addition of vectors) you can also multiply by scalars from the field.

8.18 The isomorphism theorems

The following are some general statements about the structure of groups, mostly regarding quotients, which on the whole are called "The isomorphism theorems". However, the isomorphism theorems do not form an ordered set, or even a set with a well-defined cardinality. As far as labeling which theorem is which, it's the wild west out there. It seems to be a long standing tradition in the world of Algebra textbook authors to use whatever bespoke enumeration is at their particular whim. I'm presenting them here with the enumeration roughly by which I learned them, which comes from the book *Abstract Algebra* by Dummit and Foote. But just be warned, saying "the n-th isomorphism theorem" is about a precise as saying "Euler's theorem".

8.19 Theorem (First isomorphism theorem)**.** *Let G, H be groups and $\varphi\colon G \to H$ a homomorphism. Then $G/\ker\varphi \cong \operatorname{im}\varphi$*

Proof. Write $K = \ker\varphi$ and $I = \operatorname{im}\varphi$. From proposition 8.16 we know that $K \trianglelefteq G$, so the quotient G/K is well-defined. Let's $f\colon G/K \to I$ by $f(gK) = \varphi(g)$. The claim is that f is an isomorphism.

First, let's show that f is well-defined, this means that if $gK = hK$ represent the same coset in G/K then $f(gK) = f(hK)$. Note that if $gK = hK$ then $h = gk$ (note $\varphi(k) = e$) for some $k \in K$. Therefore,

$$f(gK) = \varphi(g) = \varphi(g)e = \varphi(g)\varphi(k) = \varphi(gk) = \varphi(h) = f(hK)$$

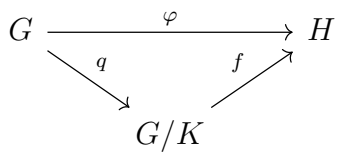
Second, we'll show that f is actually a homomorphism. This follows from the observation that

$$f(gKhK) = f(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = f(gK)f(hK).$$

That f is onto is essentially trivial. If $h \in I$ then $h = \varphi(g)$ for $g \in G$ so $f(gK) = h$. That f is injective follows from the observation that if $f(gK) = f(hK)$ then $\varphi(g) = \varphi(h)$ so that $\varphi(g^1h) = e$ and therefore $g^{-1}h \in K$. But $g^{-1}h \in K$ if and only if $gK = hK$. This completes the proof. □

8.20 Remark. This is a great opportunity to introduce what is called a **commutative diagram**. That is, a direct graph, where arrows between nodes are functions (homomorphisms) such that any (directed) path between nodes results in the same value.

Let G, H be groups, $\varphi\colon G \to H$ a homomorphism, and $K = \ker\varphi$. There is always a map $q\colon G \to G/K$ given by $q(g) = gK$ for all $g \in G$. One way of phrasing the first isomorphism theorem is that there is always a canonical map $f\colon G/K \to H$ such that $\varphi(g) = f(q(g))$ for all $g \in G$—i.e., that the following diagram commutes.



Moreover, (i) q is a surjection, (ii) f is an injection, (iii) f is a bijection onto the image of φ in H. If you find a commutative diagram enjoyer[58] in the wild they will describe this as follows "*A homomorphism always factors through the quotient by the kernel*".

8.21 Example (Order of A_n). Let $n \geq 1$. Recall that $\operatorname{sgn}\colon S_n \to \mathbf{Z}_2$ is a homomorphism, and that by definition $A_n = \ker \operatorname{sgn}$. Since sgn is a surjection we have $\mathbf{Z}_2 \cong S_n/A_n$. Therefore, A_n has index two in S_n. Which is to say that $|A_n| = n!/2$. (More generally, this tells us that any time you can quantify "stuff" as even or odd via a homomorphism to $\mathbf{Z}_2$, then the amount of even stuff has to be the same as the amount of odd stuff).

8.22 Example. You may recall that famous *Rank-nullity theorem*, which states that for a matrix A its rank plus its nullity is equal to the number of columns of that matrix. If A represents a linear transformation of vector spaces $T\colon V \to U$, the rank of the matrix is equal to the dimension of its image, the nullity is the dimension of its kernel, and the number of columns is the dimension of its domain. Thus,

$$\dim V = \dim(\ker T) + \dim(\operatorname{im} T).$$

One way to show this is using the first isomorphism theorem: $V/\ker T \cong \operatorname{im} T$ as vector spaces, and vector spaces are characterized (up to isomorphism) by their dimension. (Note $\dim(V/\ker T) = \dim V - \dim(\ker T)$)

8.23 Remark. To be completely honest, I've never used any of the remaining "isomorphism theorems" in my life as a practicing mathematician. The first isomorphism theorem is a very useful statement, and exists in a much more general context. The remainder of these theorems might be useful were you to do a deep dive on the structure of a particular group. We'll skip them for now. I've written the statements of the 2nd and 3rd isomorphism theorems below, should you desire to learn more please feel free to inquire.

8.24 Theorem (Second isomorphism theorem)**.** *Let G be a group, $N \trianglelefteq G$ and $H \leq G$. Then $HN = \{hn : h \in H, n \in H\} \leq G$, $N \cap H \trianglelefteq H$ and*

$$H/(H \cap N) \cong (HN)/N \tag{8.24.1}$$

8.25 Theorem (Third isomorphism theorem)**.** *Let G be a group and H, N normal subgroups of G such that $N \trianglelefteq H$. Then $H/N \trianglelefteq G/N$ and*

$$G/H \cong (G/N)/(H/N) \tag{8.25.1}$$

Proof. Let's define a function $\psi\colon G/N \to G/H$ by $\psi(gN) = gH$. Note that ψ is well defined, since if $gN = hN$ then $g = hn$ for some $n \in N$, so that $\psi(gN) = hnH = hH = \psi(hN)$ (note that $n \in N \subset H$). We claim that ψ is a homomorphism. Indeed,

$$\psi(gNhN) = gHhH = ghHH = ghH$$

[58] These tools are particularly useful in homological algebra and are essentially *the* language in which category theory is written.

since $H \trianglelefteq G$. The kernel of ψ is given by $\ker\psi = \{gN : gH = H\}$ which is to say that $\ker\psi = H/N$ (and so $H/N \trianglelefteq G/N$). Last, ψ is surjective since any coset gH is obtained from ψ by $\psi(gN)$. So, by the first isomorphism theorem

$$(G/N)/(H/N) \cong G/H$$

as desired. □

8.26 Identifying groups as direct products of subgroups

8.27 Theorem (Condition for G to be a direct product of subgroups)**.** *Let G be a group and $H, K \leq G$ be subgroups such that*

- $H \cap K = \{e\}$
- $H, K \trianglelefteq G$
- *For any $g \in G$ there is $h \in H$ and $k \in K$ such that $g = hk$*

Then $G \cong H \oplus K$

8.28 Exercises

1. Let $K \leq H \leq G$. Prove that $[G : K] = [G : H][H : K]$
2. Prove that if $H \leq G$ is any subgroup of index 2, then $H \trianglelefteq G$. (*Hint: if $gH \neq H$ then $gH = G \setminus H$. Can you use this to show that $Hg = gH$?*)
3. Give an example of an infinite group G and subgroup H such that $[G : H] = \infty$
4. Find *all* three subgroups of index 2 in $\mathbf{Z} \oplus \mathbf{Z}$.
5. Let $H = \{\mathrm{Id}, (12), (34), (12)(34)\}, N = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \subset S_4$. Show that both H and N are isomorphic to the Klein four group $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, but that N is normal in S_4 while H is not.
6. Determine if the following subgroups are normal. If so, describe the quotient group.
   a. $\langle (13), (1234) \rangle \leq S_4$
   b. $\{\pm e, \pm i\} \leq Q_8$ (Recall Q_8 form 5.8 i.)
   c. The group of matrices of the form $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbf{R} \right\}$ as a subgroup of $\mathrm{GL}_2(\mathbf{R})$
   d. The group of matrices of the form $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbf{R} \right\}$ as a subgroup of the group of upper triangular matrices $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}$
7. Prove that if $N, N' \trianglelefteq G$ then $N \cap N' \trianglelefteq G$.
8. Let G be a group and define $Z(G) = \{g \in G : zg = gz \text{ for all } z \in G\}$.

a. Prove that $Z(G)$ is a normal subgroup of G.

b. Prove that if $G/Z(G)$ is cyclic, then G is abelian

9. Prove that if G has exactly one subgroup H of order k then $H \trianglelefteq G$.

10. *True or False.* Determine if the following statements are true or false. Prove your answer.

a. If H and G/H are cyclic, then G is cyclic.

b. If H and G/H are abelian, then G is abelian.

c. If $\varphi\colon G \to H$ is a homomorphism and G is cyclic then $\operatorname{im}\varphi$ is cyclic.

d. If $\varphi\colon G \to H$ is a homomorphism and G is abelian then $\operatorname{im}\varphi$ is abelian.

e. $\mathbf{Q}/\mathbf{Z} \cong \mathbf{Z}$

11. Prove that the determinant $\det\colon \mathrm{GL}_n(\mathbf{R}) \to (\mathbf{R}^*, \cdot)$ is a homomorphism.

12. Give a description of the set of matrices $A \in \mathrm{GL}_2(\mathbf{R})$ such that $A \in \ker(\det)$

13. If $N, N' \trianglelefteq G$ such that $N \cap N' = \{e\}$ prove that G is isomorphic to a subgroup of $G/N \oplus G/N'$

14. Let $g \in G$. Prove that $\varphi_g\colon G \to G$ defined by $x \mapsto gxg^{-1}$ is a homomorphism. Describe the elements in $\ker\varphi_g$.

15. Let G, H be abelian groups and define $\mathrm{Hom}(G, H)$ be the set of all homomorphisms $\varphi\colon G \to H$. For $\varphi, \psi \in \mathrm{Hom}(G, H)$ define $\varphi \cdot \psi$ by $(\varphi \cdot \psi)(g) = \varphi(g)\psi(g)$. Show that $(\varphi, \psi) \mapsto \varphi \cdot \psi$ defines a group structure on $\mathrm{Hom}(G, H)$. Then, prove that $\mathrm{Hom}(\mathbf{Z}, \mathbf{Z}) \cong \mathbf{Z}$

16. For G a group define $\mathrm{Aut}(G)$ to be the subset of $\mathrm{Hom}(G, G)$ consisting of group isomorphisms (*Note*: such a bijection $G \to G$ is called an **automorphism**). Prove the following:

a. $\mathrm{Aut}(\mathbf{Z}_n) \cong \mathbf{Z}_n^*$

b. $\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$

c. $\mathrm{Aut}(S_3) \cong S_3$

9 Group actions

Most reasonable mathematicians will say something along the lines of "we care about groups because of what they act on". That is to say, groups allow us to express the symmetries of some type of objet: be it geometric, algebraic, topological, etc. This is not to disparage those who do deep structural results about groups, but rather to express the typical mathematical interpretation about the usefulness of group theory. Groups are *the way* in which symmetries of an object are expressed. These symmetries are expressed by group actions.

9.1 Definition. *Let G be a group. A* ***(left) G-set*** *or* ***set with a (left) G action*** *is a set X together with map $G \times X \to X$ given by $(g, x) \mapsto g.x$ which satisfies*

i. $e.x = x$ *for all* $x \in X$

ii. $g.(h.x) = (gh).x$ *for all* $g, h \in G$, $x \in X$

The notation $g.x$ is also written as gx when there is minimal risk of confusion. One thing to note is that an equivalent definition to 9.1 is to say that a (left) G action on X consists of a collection of functions

$$\varphi_g \colon X \to X \quad g \in G$$

such that $\varphi_e = \mathrm{Id}_X$ and $\varphi_g \circ \varphi_{g'} = \varphi_{gg'}$ for all $g, g' \in G$. That is to say, a G-action is just a collection of self-mappings $X \to X$ that compose according to the group laws from G.

Note that any group G and set X has a **trivial group action** given by $g.x = x$ for all $g \in G, x \in X$. The goal is to understand useful and interesting G-sets.

9.2 Remark (Left vs. right actions). A **right G-set** is defined in exactly the way you might expect: i.e., there is must be a map $X \times G \to X$ given by $(x, g) \mapsto x.g$ which satisfies $x.e = x$ and $(x.g).h = x.(gh)$. The difference is (mostly) immaterial[59]: let us unambiguously say "G-set" and "action by G" to mean left actions, and only bring the adjectives left and right in when absolutely necessary.

9.3 Example. Let $n \geq 1$, then $\mathrm{GL}_n(\mathbf{R})$ acts on $\mathbf{R}^n$ by matrix multiplication. That is, an element $A \in \mathrm{GL}_n(\mathbf{R})$ is an $n \times n$ matrix, and a vector $v \in \mathbf{R}^n$ is a column vector ($1 \times n$ matrix). So, we have a mapping

$$(A, v) \mapsto Av$$

such that Av is then another column vector (and therefore in $\mathbf{R}^n$. That this is a (left) group actions comes from the fact that matrix multiplication is associative: i.e., for $A, B \in \mathrm{GL}_n(\mathbf{R})$, $A(Bv) = (AB)v$.

9.4 Example. Let $G = D_n$ and X be a regular n-gon. Then G acts on X by expressing the symmetries of the n-gon. For instance, D_4 acts on the square as follows: label the vertices of the square cyclically as $X = \{0, 1, 2, 3\}$. Then the D_4 action on X is generated by the operations $r.n = n + 1 \pmod 4$ and $s.n = 3 - n \pmod 4$ for $n \in X$.

9.5 Example. Let G be a group and $H \leq G$. Then H acts on G by **conjugation**: i.e.,

$$(h, g) \mapsto h.g = hgh^{-1} \tag{9.5.1}$$

Note that if $h, k \in H$ then

$$k.(h.g) = k.(hgh^{-1}) = khgh^{-1}k^{-1} = (kh)g(kh)^{-1} = (kh).g$$

[59] Though, with the interpretation of a G action as a collection of functions $\varphi_g \colon X \to X$, the difference is that a right G-action composes "in reverse", i.e., $\varphi_g \circ \varphi_{g'} = \varphi_{g'g}$ for $g, g' \in G$. Use this information how you see fit.

We've seen examples of this group action before, for instance, in determine cycle types of the symmetric group S_n. More specifically, when $H = G$, the orbits (definition 9.10) of this action are called **conjugacy classes** of G.

9.6 Example. If $H \leq G$ then G acts on the collection of (left) cosets of H in G, by

$$(g, xH) \mapsto g.(xH) = gxH.$$

This defines a (transitive, see definition 9.11) G action on the set G/H.

The following is left as an exercise, but is fairly straightforward to show. In words, if G acts on a set X and $H \leq G$, then the given action of G *restricts* to an action of H on X.

9.7 Proposition. *If X is a set with a G action and $H \leq G$ then X inherits an H action.*

9.8 Orbits and fixed points

For the remainder of this section let us generically refer to X as a set with an action by some group G.

9.9 Proposition. *Define a relation $\sim_G$ on X by $x \sim_G y$ if there is $g \in G$ such that $g.x = y$. Then $\sim_G$ is an equivalence relation.*

Proof. We've essentially proved this before, so I'll leave it as an exercise □

The corresponding set of equivalence classes $X/\sim_G$, or X/G, is called the collection of *orbits* of the G action on X.

9.10 Definition (Orbits)**.** *Given $x \in X$ write $\mathcal{O}_x$ for the **orbit of** x **under** G, defined by*

$$\mathcal{O}_x = \{y \in X : y = g.x \text{ for some } g \in G\} \tag{9.10.1}$$

Note that $\mathcal{O}_x \subset X$. You can think of the orbit of some $x \in X$ as the collection of all objects in X that "obtainable" by applying some operation from G. For instance with example 9.3, given any vector $v \in \mathbf{R}^n$ the orbit $\mathcal{O}_v$ is all of $\mathbf{R}^n$. Reason being is that given any other vector $v' \in \mathbf{R}^n$ there is some matrix $A \in \mathrm{GL}_n(\mathbf{R})$ such that $Av = v'$. In general, if a group action has this property we call G transitive, as below

9.11 Definition (Transitive group action)**.** *An action of G on X is called **transitive** if for any $x, y \in X$ there is $g \in G$ such that $g.x = y$.*

Note that any transitive group action has exactly one orbit. Complementary to the notion of orbit is that of a G-fixed point.

9.12 Definition (Fixed points)**.** *Let $g \in G$ and define the **g-fixed point set** of X to be the set*

$$X^g = \{x \in X : g.x = x\} \tag{9.12.1}$$

*Similarly, we define $X^G = \{x \in X : g.x = x \text{ for all } g \in G\}$ to be the set of **G-fixed points of** X.*

We have $X^g, X^G \subset X$ and certainly $X^G \subset X^g$ for any $g \in G$. Fixed point is a fairly self explanatory term, the idea being that action of G acts trivially on the fixed points X^G.

9.13 Example. For instance, with the example from 9.3, we have that $(\mathbf{R}^n)^{\mathrm{GL}_n(\mathbf{R})} = \{0\}$ since the only vector which is fixed by all matrices is the zero vector. Similarly, given $A \in \mathrm{GL}_n(\mathbf{R})$ the set of A-fixed points of $\mathbf{R}^n$ is trivial, unless A has an eigenvalue 1, in which case $(\mathbf{R}^n)^A$ is the eigenspace corresponding to 1.

As an even more concrete example, the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R})$ has fixed points in $\mathbf{R}^2$ given by the span of the vector $v = (1, 1)$. Visually, A is a reflection of $\mathbf{R}^2$ over the line $y = x$, any vector in this subspace will be fixed by A.

9.14 Stabilizer subgroups

Orbits and fixed-points are reflected in the how the "things" in the set X get moved (or not) by the group action. Similarly, we can ask about the structure of group elements that have some property with regards to the group action.

9.15 Definition (Stabilizer subgroup)**.** *Let $x \in X$ and set $\mathrm{Stab}_G(x) = \{g \in G : g.x = x\}$. Then $\mathrm{Stab}_G(x) \subset G$ is called the **stabilizer subgroup of** $x \in X$.*

The word *stabilizer* is meant to convey that group elements $g \in G$ which act trivially on this element $x \in X$. The first observation is that the collection of these group elements forms a subgroup of G. Other notation is to write G_x for $\mathrm{Stab}_G(x)$.

9.16 Proposition. *For any $x \in X$, $\mathrm{Stab}_G(x) \leq G$.*

Proof. Let $x \in X$, and suppose that $g, h \in \mathrm{Stab}_G(x)$. Certainly $e \in \mathrm{Stab}_G(x)$ since $e.x = x$ is one the axioms of a group action. If $g, h \in \mathrm{Stab}_G(x)$ then $(gh).x = g.(h.x) = g.x = x$ so $gh \in \mathrm{Stab}_G(x)$. Similarly, $g.x = x$ implies that $x = g^{-1}.(gx) = g^{-1}.x$, so that $g^{-1} \in \mathrm{Stab}_G(x)$. □

For instance, following our theme of unraveling the mysteries of example 9.3, let's suppose there is $A \in \mathrm{GL}_n(\mathbf{R})$ and vector $v \in \mathbf{R}^n$ such that $Av = v$. That is to say that v is an eigenvector for A with corresponding eigenvalue 1. $\mathrm{Stab}_{GL_n(\mathbf{R})}(v)$ is then the collection of all matrices with an eigenspace given by the linear span of v with corresponding eigenvalue 1. This is a subgroup of $\mathrm{GL}_n(\mathbf{R})$ (I leave it to you to prove why).

9.17 Definition (Free group action)**.** *If G acts on X such that the stabilizer subgroups $\mathrm{Stab}_G(x) \leq G$ are trivial for all $x \in X$, then we say that the action of G on X is **free**.*

In other words, a group action is *free* if for all $x \in X$, $g.x = x$ only if $g = e$. For example, $\mathbf{Z}_n$ acting on a regular n-gon by rotation is a free action. Here X is the set of vertices of the n-gon, cyclically labelled as $\{0, 1, 2, \cdots, n-1\}$, and $(k, x) \mapsto x + k \pmod n$ for $k \in \mathbf{Z}_n, x \in X$ is the group action (note: $x + k = x \pmod n$ if and only if $k = 0 \pmod n$).

9.18 Counting with group actions

What's left is to incorporate two worlds of (i) orbits and fixed points (in X) and (ii) stabilizer subgroups (in G) together, and then use this to understand some structural statements about group actions. The main results here are theorems 9.19 and 9.22, which allows us to count the symmetries of some group action without necessarily having the fully enumerate each orbit.

9.19 Theorem (Orbit-stabilizer theorem)**.** *Suppose that X is a finite set with an action of a finite group G. Let $x \in X$ and $g \in G$. Then $[G : \mathrm{Stab}_G(x)] = |\mathcal{O}_x|$.*

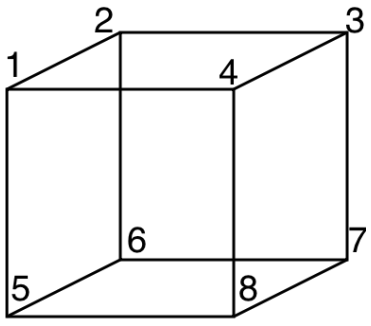
Proof. Let $x \in X$ and set $H = \mathrm{Stab}_G(x)$. Recall that $[G : H]$ is the number of cosets of H in G. We will define a map of sets $\mathcal{O}_x \to G/H$ and then prove that this map is a bijection. Note for any $y \in \mathcal{O}_x$ there must be $g = g \in G$ with $g.x = y$. Thus, there is a function $\varphi\colon \mathcal{O}_x \to G/H$ given by $\varphi(y) = gH$ where $g \in G$ is such that $g.x = y$.

To show that φ is injective suppose that $\varphi(y) = \varphi(y')$ for some $y, y' \in \mathcal{O}_x$. Therefore, there are group elements g, g' with $gH = g'H$ and $g.x = y, g'.x = y'$. But if $gH = g'H$ then there is $h \in H$ with $g' = gh$. By assumption $h.x = x$ (since h is in the stabilizer of x), so therefore

$$y' = g'.x = (gh).x = g.(h.x) = g.x = y$$

Similarly, given $gH \in G/H$ let $y = g.x \in \mathcal{O}_x$. Then $\varphi(y) = gH$, so that φ is onto. Thus φ is a bijection and the claim is proved. □

9.20 Example (Counting the symmetries of the cube). The orbit stabilizer theorem (theorem 9.19) can be used to enumerate the order of symmetry groups that are otherwise difficult to calculate. For instance, let's consider the symmetries (not necessarily orientation preserving) of the cube. First let's label the vertices of the cube as $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ as in the following picture.



Let G be the group of (not necessarily orientation preserving) symmetries of the square. Then G acts on X by permutation of vertices. It's straightforward to see that this G action is transitive, since, e.g. vertex 1 can be sent to any of the 7 other vertices. Therefore, $|\mathcal{O}_1| = 8$ and so $[G : \mathrm{Stab}_G(1)] = 8$. That is to say

$$|G| = 8 \cdot |\mathrm{Stab}_G(1)|$$

The key is that now we can apply the orbit stabilizer theorem to the restricted $\text{Stab}_G(1)$ action on X[60]. Let's write $G_1 = \text{Stab}_G(1)$. So, $[G_1 : \text{Stab}_{G_1}(2)] = \mathcal{O}_2^{G_1}$ (we write $\mathcal{O}_1^{G_1}$ here to denote the orbit of 2 under the action by G_1 rather than G). When 1 is fixed, the element 2 can only be sent to an adjacent vertex to 1. There are three such vertices $2, 4$ and 5, so $|\mathcal{O}_2^{G_1}| = 3$. Therefore,

$$|G_1| = 3 \cdot |\,\text{Stab}_{G_1}(2)|$$

Continuing in this process, let's write G_2 for $\text{Stab}_{G_1}(2)$, we can then look at the orbit $\mathcal{O}_3^{G_2}$ of vertex 3 under the action by G_2. Since G_2 fixes both vertices 1 and 2, 3 must be sent to either itself or 3, that is to say $|\mathcal{O}_3^{G_2}| = 2$. Therefore, $[G_2 : \text{Stab}_{G_2}(3)| = 2$, and so

$$|G_2| = 2 \cdot |\,\text{Stab}_{G_2}(3)|$$

At this point, if we let $G_3 = \text{Stab}_{G_2}(3)$ note that any stabilizers of the G_3 action are trivial as a rotation of the cube which fixes vertices $1, 2$ and 3 must be the identity. Therefore,

$$|G| = 8 \cdot |G_1| \cdot |G_2| = 8 \cdot 3 \cdot 2 = 48$$

9.21 Remark. You may recall from example 7.27 that the group of 3D-rotational symmetries of the cube is S_4. Note that $|S_4| = 24$, not 48 as the previous example shows. What's going on here is that these 3D-rotations must preserve the orientation on 3D space. In example 9.20, we calculated the total group of symmetries. Half of these preserve the orientation of the cube, and half don't.

In fact, we can see exactly what goes wrong. In the last step, we found that $\mathcal{O}_3^{G_2}$ has two elements: 3 and 6. But, if we fix vertices 1 and 2, and swap 3 and 6, the orientation of the cube has been flipped (meaning, this permutation of vertices is not a rotation but a reflection). The previous calculations all preserve orientation, so, if we were tasked with computing the order of the rotational symmetry group of the cube, it would be $8 \cdot 3 = 24$ as expected.

In fact, the group of all symmetries of the cube is isomorphic to $S_4 \oplus \mathbf{Z}_2$[61].

9.22 Theorem (Burnside's counting lemma)**.** *Let G be a finite group and X a finite set with a G action. Let $k = |X/G|$ be the number of orbits of the given G action. Then*

$$k = \frac{1}{|G|} \sum_{g \in G} |X^g| \tag{9.22.1}$$

In plain English, the term on the right is just the average number of fixed points from the group action. Theorem 9.22 can be useful for counting the number of orbits of an action, it's generally easier to intuit fixed points than orbits.

[60] See prop. 9.7

[61] The order checks out, but this shouldn't be "obvious". For instance, when talking about dihedral groups D_n is not isomorphic to $\mathbf{Z}_n \oplus \mathbf{Z}_2$, which would be the analog of "rotational symmetries summed with orientation flip"

Proof of theorem 9.22. This proof employs one of the best combinatorial methods: counting the same thing both ways. Note that

$$\sum_{g\in G}|X^g| = |\{(g,x)\in G\times X : g.x = x\}| = \sum_{x\in X}|\operatorname{Stab}_G(x)|$$

(Think of laying the points in $G\times X$ out in a grid and counting along the X-axes and the G-axes respectively in the middle set.)

From theorem 9.19 we know that $[G : \operatorname{Stab}_G(x)] = |\mathcal{O}_x|$ and so $|\operatorname{Stab}_G(x)| = |G|/|\mathcal{O}_x|$. Therefore,

$$\sum_{g\in G}|X^g| = \sum_{x\in X}|\operatorname{Stab}_G(x)| = \sum_{x\in X}\frac{|G|}{|\mathcal{O}_x|} = \sum_{Y\in X/G}\left(\sum_{y\in Y}\frac{|G|}{|Y|}\right) = \sum_{Y\in X/G}|G| = |G|\cdot|X/G|$$

(The third equation follows from the observation that orbits partition X, so a sum over X can be broken into two sums: an outer sum over all orbits and inner over each element of the orbit). And thus we have that

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

□

9.23 Example (Counting the colors of a square). (This is the same example from Judson's book, but his formatting of the answer is difficult to read in my opinion.) Suppose we want to answer the following question:

> *The vertices of a square are colored either red or green. Up to rotations and reflections, how many such colorings are there?*

Note that the answer is not $2^4 = 16$, since for instance this number counts each of the labellings of "all red" and "all green" four times each. We can answer this question using theorem 9.22. Let's first put into language that group actions can handle.

Let $X = \{1,2,3,4\}$ be the vertices of a square (labeled cyclically). A *coloring* of the square is just a function $c\colon X\to\{\text{red},\text{green}\}$. Let's let C denote the set of all such colorings, i.e.

$$C = \{f\colon X\to\{\text{red},\text{green}\}\}$$

Note that D_4 acts on C as follows: first identify D_4 with subgroup[62]

$$D_4' = \{\text{Id}, (1234), (13)(24), (1432), (14)(23), (12)(34), (13), (24)\} \leq S_4$$

Then, there is a group action $D_4'\times C\to C$ given by $(\alpha, f)\mapsto f\alpha$, that is, D_4' acts on C by *precomposition* with a permutation

$$X\xrightarrow{\alpha} X\xrightarrow{f}\{\text{red},\text{green}\}$$

[62]Here, $r = (1234), s = (12)(34)$

Then, a coloring *up to rotation and reflection* is just an *orbit* of this action. Burnside's lemma allows us to calculate the number of orbits by calculating the number of fixed points for each $\alpha \in D_4'$. We have:

- $|C^{\mathrm{Id}}| = 16$ — Any coloring of the square is fixed by the identity permutation.
- $|C^{(1234)}| = |C^{(1432)}| = 2$ — Only the colorings of "all red" or "all green" are fixed by a rotation
- $|C^{(12)(34)}| = |C^{(13)(24)}| = |C^{(14)(23)}| = 4$ — Put the vertices into groups of two and color each group the same, there are 4 total such colorings
- $|C^{(13)}| = |C^{(24)}| = 8$ — Diagonally opposite vertices get the same color, the other two are colored independently.

Therefore, the total number of orbits, k, is given by

$$k = \frac{1}{8}(16 + 2 \cdot 2 + 3 \cdot 4 + 2 \cdot 8) = 6$$

and thus there are six such distinct colorings of the square.

9.24 Exercises

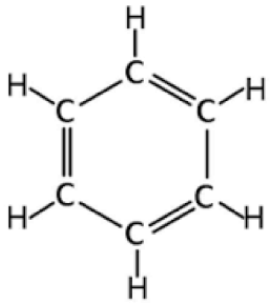
1. Let $X = \{1, 2, 3, 4, 5, 6\}$ and $G = \{\mathrm{Id}, (12), (345), (354), (12)(345), (12)(354)\} \leq S_6$. For each $g \in G$ compute the fixed points X^g. For each $x \in X$ compute the stabilizer subgroup $\mathrm{Stab}_G(x)$.
2. Determine the conjugacy classes for $D_5, \mathbf{Z}_9$ and Q_8[63]
3. Let A_4 act on S_4 by conjugation, i.e., $\beta.\alpha = \beta\alpha\beta^{-1}$ for $\alpha \in S_4, \beta \in A_4$. Describe the orbits of this action.
4. Let $X = \{1, 2, 3, \ldots, n\}$ and let S_n act on X by permutation. Is this action transitive? Is the action by the alternating group A_n on X transitive?
5. Let $X = \{(u, v) : u, v \in \mathbf{R}^2 \text{ are linearly independent vectors}\}$ and $\mathrm{GL}_2(\mathbf{R})$ act on X by $A.(u, v) = (Au, Av)$. Is this action transitive?
6. Let $\mathrm{SL}_2(\mathbf{R})$ act on $\mathbf{R}^2$ by $A.v = Av$. Is this action transitive?
7. Let X be a set with an action of a group G. Prove the following:
   a. $\bigcap_{g \in G} X^g = X^G$
8. Use the proof technique from example 9.20 to compute the order of the symmetry groups for the tetrahedron, octahedron, icosahedron, and dodecahedron (see also, example 7.27)
9. Up to 3D rotations how many distinct enumerations of a six-sided die are there? What about a four-sided die?

[63] Recall that Q_8 is the **quaternion group** given by $\langle i, j, k | i^2 = j^2 = k^2 = ijk, i^4 = j^4 = k^4 = e \rangle$

10. Up to rotations and reflections, how many ways can the vertices of a hexagon be colored red or green?

11. A cube consists of 12 edges. Suppose these edges are colored yellow and green. Up to 3D rotations, how many such colorings of the cube are there?

12. Benzene is an organic compound made of a ring of six carbon atoms C attached to hydrogen atoms H as below:



Suppose one or more hydrogen atoms is replaced with chlorine. How much different compounds can be made? What if three of the six H atoms were replaced by a single CH_3.

13. Suppose that G acts on a set X. This action is called **faithful** if given $g \in G$ such that $g.x = g.y$ then $x = y$ (i.e., the functions $\varphi_g \colon X \to X$ are injective) Similarly the action is called **full** if given $y \in X$ there is $x \in X$ with $g.x = y$ (i.e., φ_g are surjective). Determine if the following actions are faithful and/or full:

    a. S_3 acting on $\{1, 2, 3\}$

    b. $V = \{\mathrm{Id}, (13), (24), (13)(24)\}$ on $\{1, 2, 3, 4\}$

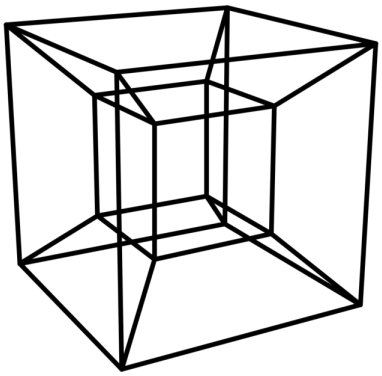
    c. $\mathrm{GL}_2(\mathbf{R})$ acting on $\mathbf{R}^2$ by $A.v = Av$

    d. $\mathbf{Z}_5$ acting on a regular pentagon by rotation on the vertices.

    e. $\mathbf{Z}_4$ acting on the cube by rotation through one central axis of the cube

14. Let G be the symmetry group of the *hypercube* (i.e., 4-dimensional cube, see picture below). Let $X = \{1, 2, 3, 4, \cdots, 15, 16\}$ be the set of vertices of the hypercube, and let G act on X by permutation of vertices. Use a similar argument to example 9.20 to

determine the order of G.



10 Matrix groups

Historically, all groups were subgroups of symmetric groups. A (slightly) more modern approach is to think of groups in how they can be "put" inside groups of matrices[64]. Our focus will be on matrices will real coefficients, but there is an equally deep story for the following content when $\mathbf{R}$ is replaced by $\mathbf{C}$, the complex numbers, or more generally some arbitrary field (for instance, matrices with coefficients in $\mathbf{Z}_p$ are another big topic to explore).

Recall that definitions we've been working with so far

$$\mathrm{GL}_n(\mathbf{R}) = \{A : A \text{ is an } n \times n \text{ invertible matrix with real entires}\} \tag{10.0.1}$$

and

$$\mathrm{SL}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : \det A = 1\} \tag{10.0.2}$$

In words, we call these the **general linear** group and **special linear** group of $n \times n$ matrices (with real coefficients), respectively. We've already seen that $\mathrm{SL}_n(\mathbf{R}) \trianglelefteq \mathrm{GL}_n(\mathbf{R})$, since $\mathrm{SL}_n(\mathbf{R})$ is the kernel of the determinant $\det\colon \mathrm{GL}_n(\mathbf{R}) \to \mathrm{SL}_n(\mathbf{R})$.

Let's denote by $I \in \mathrm{GL}_n(\mathbf{R})$ the identity matrix (i.e., I has 1s along the diagonal and 0s everywhere else). Matrices can be given by double indexed sets, i.e., $A = \{a_{i,j}\}_{1 \le i,j \le n}$ where the entries $a_{i,j}$ for $i = 1, \dots n$ are the entries over the j-th column, and $a_{i,j}$ for $j = 1, \dots, n$ are the entries from the i-th row of A

10.1 Definition (Matrix transpose)**.** *Let $A = \{a_{i,j}\} \in \mathrm{GL}_n(\mathbf{R})$. Then the **transpose of** A is the matrix A^T given by $A^T = \{a_{j,i}\}$*

Visually, the transpose of a matrix is just the reflection of the entries of A over the main diagonal. I leave you to check the following proposition. More generally, matrix transposition is an instance of $\mathbf{Z}_2$ acting on $\mathrm{GL}_2(\mathbf{R})$, which I also leave you to check.

10.2 Proposition. *For matrices $A, B \in \mathrm{GL}_n(\mathbf{R})$, we have $(AB)^T = B^T A^T$ and $(A^{-1})^T = (A^T)^{-1}$.*

10.3 Definition (Symmetric matrix)**.** *Let A be an $n \times n$ matrix. Then A is **symmetric** if $A = A^T$.*

[64] This is essentially the field of representation theory

10.4 Orthogonal matrices

10.5 Definition (Orthogonal matrix)**.** *An $n \times n$ matrix with real entries is called* ***orthogonal*** *if $A^T A = I$.*

10.6 Example. Let's unpack what this definition is telling us: Suppose we are given a matrix $A \in \mathrm{GL}_3(\mathbf{R})$ of the form

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Then:

$$A^T = \begin{pmatrix} a_{1,1} & a_{2,1} & a_{3,1} \\ a_{1,2} & a_{2,2} & a_{3,2} \\ a_{1,3} & a_{2,3} & a_{3,3} \end{pmatrix}$$

Let's write out the product $A^T A$ (it's going to be long)

$$A^T A = \begin{pmatrix} (a_{1,1})^2 + (a_{2,1})^2 + (a_{3,1})^2 & a_{1,1}a_{1,2} + a_{2,1}a_{2,2} + a_{3,1}a_{3,2} & a_{1,1}a_{1,3} + a_{2,1}a_{2,3} + a_{3,1}a_{3,3} \\ a_{1,2}a_{1,1} + a_{2,2}a_{2,1} + a_{3,2}a_{3,1} & (a_{1,2})^2 + (a_{2,2})^2 + (a_{2,3})^2 & a_{1,2}a_{2,3} + a_{2,2}a_{2,3} + a_{3,2}a_{3,3} \\ a_{1,3}a_{1,1} + a_{2,3}a_{2,1} + a_{3,3}a_{3,1} & a_{1,3}a_{1,2} + a_{2,3}a_{2,2} + a_{3,3}a_{3,2} & (a_{1,3})^2 + (a_{2,3})^2 + (a_{3,3})^2 \end{pmatrix}$$

This looks like a nightmare but something nice is happening. Let's suppose that A is orthogonal. Recall then that this means that $A^T A$ from the equation above is then equal to the identity matrix

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Let's let $v_1 = (a_{1,1}, a_{2,1}, a_{3,1})$, $v_2 = (a_{2,1}, a_{2,2}, a_{2,3})$ and $v_3 = (a_{1,3}, a_{2,3}, a_{3,3})$ be vectors in $\mathbf{R}^3$. And note that the dot products $v_i \cdot v_j$ are precisely the entries of $A^T A$:

$$A^T A = \begin{pmatrix} v_1 \cdot v_1 & v_1 \cdot v_2 & v_1 \cdot v_3 \\ v_2 \cdot v_1 & v_2 \cdot v_2 & v_3 \cdot v_2 \\ v_3 \cdot v_1 & v_3 \cdot v_2 & v_3 \cdot v_3 \end{pmatrix}$$

That is to say, if A is orthogonal, then the column vectors (in this case v_1, v_2, v_3) from A satisfy the following:

$$v_1 \cdot v_1 = 1,\ v_2 \cdot v_2 = 1,\ v_3 \cdot v_3 = 1; \quad v_i \cdot v_j = 0 \text{ (for } i \neq j)$$

In other words still, the columns of A form an **orthonormal basis**[65] of $\mathbf{R}^3$.

10.7 Definition. *Let $n \geq 1$. Define $\mathrm{O}(n)$ to be the set of orthogonal matrices $A \in \mathrm{GL}_n(\mathbf{R})$. Similarly define $\mathrm{SO}(n) \subset \mathrm{O}(n)$ to be the collection of orthogonal matrices A such that $\det A = 1$.*

[65] i.e., a basis such that each basis element is of unit length and any two distinct elements of the basis are orthogonal

In words, $\mathrm{O}(n)$ is called the **orthogonal group** (of order n) and $\mathrm{SO}(n)$ the **special orthogonal group** (also of order n). That these sets actually form subgroups of $\mathrm{GL}_n(\mathbf{R})$ follows from prop 10.8. From example 10.6 we know that any matrix $A \in \mathrm{O}(n)$ is represented by some orthonormal basis of $\mathbf{R}^n$. If furthermore $A \in \mathrm{SO}(n)$ then A is *orientation preserving*: that is, the standard orientation[66] on the basis of coordinate axis in $\mathbf{R}^n$ is preserved under A.

10.8 Proposition. *Let $n \geq 1$ then $\mathrm{O}(n)$ and $\mathrm{SO}(n)$ are groups. Moreover,*

$$\mathrm{SO}(n) \trianglelefteq O(n) \leq \mathrm{GL}_n(\mathbf{R})$$

10.9 Proposition. $\mathrm{O}(2)$ *and* $\mathrm{SO}(2)$ *are given by the following:*

- $\mathrm{O}(2) = \left\{ \pm \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbf{R} \right\}$
- $\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbf{R} \right\}$

10.10 Corollary. $\mathrm{SO}(2) \cong \mathbf{R}/2\pi\mathbf{Z}$

10.11 Rotations of real space

When you think of a rotation of space, what really is happening is an orientation preserving change of orthonormal basis for $\mathbf{R}^n$. That is to say, the group $\mathrm{SO}(n)$ captures the rotational structure of $\mathbf{R}^n$.

For instance, the following propositions tells us what *finite rotational symmetries* look like in $\mathbf{R}^2$ and $\mathbf{R}^3$.

10.12 Proposition. *Let $H \leq \mathrm{SO}(2)$ be a finite subgroup. Then H is isomorphic to $\mathbf{Z}_n$ for some $n \geq 1$.*

In particular H is generated by a matrix of the form

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

10.13 Proposition. *Let $H \leq \mathrm{SO}(3)$ be a finite subgroup. Then H is isomorphic to one of the following groups*

- $\mathbf{Z}_n$ *(for some $n \geq 1$)*
- D_n *(for some $n \geq 1$)*
- A_4, S_4 *or* A_5

In particular, these symmetries can be realized as group actions as follows:

- $\mathbf{Z}_n$ acts on a (thickened) n-gon in $\mathbf{R}^3$ by rotation

[66] For instance, in $\mathbf{R}^3$ this is the *right-hand rule*

- D_n acts on a (thickened) n-gon in $\mathbf{R}^3$ by rotations and reflections
- A_4 acts on the tetrahedron as orientation preserving symmetries
- S_4 acts on the cube and octahedron as orientation preserving symmetries
- A_5 acts on the icosahedron and dodecahedron as orientation preserving symmetries

A precise proof is a bit beyond the scope of our class. But, here's a heuristic argument: if $H \leq \mathrm{SO}(3)$ were some finite subgroup not from this list, then H would be the rotational symmetry of some shape. If this were a 3D shape it would have be a (finite) regular polyhedron. But, we've already enumerated all of the regular polyhedra (the Platonic solids) and their symmetry groups.

10.14 Remark. A question I get a lot from students is "What is the fourth dimension". The (cheap) but "correct" answer of the "fourth dimension is just $\mathbf{R}^3$ with another axis" does not really satisfy. What you really want is to understand the structure of SO(4): Our intuition about 3-dimensional space is built off of interacting (i.e., rotating) actual 3D objects all our life, we implicitly understand the group structure of SO(3) even if we don't know it by name.

Meaning, if you want to get a better understanding of 4D space, you can start by understanding what SO(4) looks like: What kind of subgroups does it have? For instance, the quaternion group Q_8 is (isomorphic to) a subgroup of SO(4) (and notably Q_8 is not a subgroup of SO(3)), so is a "new" type of rotational symmetry unlocked with the additional dimension. What's nice, is that with some understanding of matrix operations, and our newly acquired language of group theory, we can begin to understand how to answer this question (and the same questions for higher dimensional spaces still).

Another thing to point out is that these matrix groups are *manifolds* (essentially, "shapes" that have geometry). Meaning, you can talk about *paths of rotations* as just parametrized curves in the space $\mathrm{SO}(n)$. Even in $\mathbf{R}^3$ some bizarre things[67] happen that are not immediately obvious, but give us deep insight to the geometry of space (and also show up when, e.g., describing certain types of symmetries in particle physics)

10.15 Exercises

1. Prove proposition 10.2. Then prove that $A \mapsto A^T$ describes an action by $\mathbf{Z}_2$ on $\mathrm{GL}_n(\mathbf{R})$.
2. Let $E(n) = \{(A, x) : A \in \mathrm{O}(n), x \in \mathbf{R}^n\}$. Define a binary operation on $E(n)$ by
$$(A, x) \cdot (B, y) = (AB, Ay + x)$$
Prove that $E(n)$ is a group.
3. Let $\theta \in \mathbf{R}$. Prove that the following matrices are all elements of SO(3)
$$R_x(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \quad R_y(\theta) = \begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix} \quad R_z(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[67] For instance, the Plate trick

and then prove that $R_x(\theta), R_y(\theta), R_z(\theta)$ denote (counterclockwise) rotations by θ of the x-, y- and z-axes in $\mathbf{R}^3$.

4. Let θ, ψ be real numbers. Prove that SO(4) contains the following matrix

$$R_{\theta,\psi} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 & 0 \\ \sin\theta & \cos\theta & 0 & 0 \\ 0 & 0 & \cos\psi & -\sin\psi \\ 0 & 0 & \sin\psi & \cos\psi \end{pmatrix}$$

Use this show that $\mathrm{SO}(2) \oplus \mathrm{SO}(2) \leq \mathrm{SO}(4)$. Is there an n such that $\mathrm{O}(2) \oplus \mathrm{O}(2) \leq \mathrm{SO}(n)$?

Follow up: Does SO(4) contain the following matrix?

$$\widetilde{R_{\theta,\psi}} = \begin{pmatrix} 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & \sin\theta & \cos\theta \\ \cos\psi & -\sin\psi & 0 & 0 \\ \sin\psi & \cos\psi & 0 & 0 \end{pmatrix}$$

5. Let Δ_n be a regular n-gon centered at the origin in $\mathbf{R}^2$ and let O(2) act on $\mathbf{R}^2$ by $(A, x) \mapsto Ax$. Prove that $\mathrm{Stab}_{\mathrm{O}(2)}(\Delta_n) \cong D_n$ the n-th dihedral group.

6. Let SO(3) act on $\mathbf{R}^3$ by $(A, x) \mapsto Ax$. Is this action transitive? Determine the set of orbits from this action.

7. Let $A \in \mathrm{GL}_n(\mathbf{R})$ be a symmetric matrix. Prove that the eigenvalues of A are always real numbers and that any two nonparallel eigenvectors of A are perpendicular.

8. Let A be a symmetric $n \times n$ matrix, i.e., a matrix such that $A^T = A$ and $x, y \in \mathbf{R}^n$ be column vectors. Let $\langle x, y \rangle_A$ be given by

$$\langle x, y \rangle_A = x^T A y$$

Prove that the following hold:

   a. $\langle x, y \rangle_A = \langle y, x \rangle_A$

   b. $\langle x, y + z \rangle_A = \langle x, y \rangle_A + \langle x, z \rangle_A$

   c. $\langle kx, y \rangle_A = k \langle x, y \rangle_A$ for any scalar k

Such an operation $(x, y) \mapsto \langle x, y \rangle_A$ is called an *bilinear form*. Prove further that if $A = \mathrm{Id}$ then $\langle x, y \rangle_{\mathrm{Id}} = x \cdot y$ the *dot product* of vectors x, y.

9. True or False: There is an $n \geq 1$ such that $\mathrm{O}(n)$ has an abelian subgroup of infinite cardinality.

10. Let $n \leq m$. Show that $\mathrm{O}(n) \leq \mathrm{O}(m)$ and $\mathrm{SO}(n) \leq \mathrm{SO}(m)$.

11. Let $n \geq 1$. Prove that $S_n \leq \mathrm{O}(n)$. Is it also the case that $S_n \leq \mathrm{SO}(n)$?

12. *Challenge.* (Follow up to problem 3.). Let v be some vector in $\mathbf{R}^3$ and $\theta \in \mathbf{R}$. Write $R_v(\theta)$ for the element in SO(3) given by rotation about the axis produced by v in the counterclockwise direction. Denote by L_v the following matrix

$$L_v = \frac{d}{d\theta}\left[R_v(\theta)\right]_{\theta=0}$$

Note that L_v is the *instantaneous rotation* through axis v when $\theta = 0$. Let $x = (1,0,0), y = (0,1,0), z = (0,0,1)$ denote the vectors in the positive x-, y-, and z-axes respectively.

a. Prove that for any (column) vector u, $L_v u = v \times u$.

b. Prove that

$$L_x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \quad L_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix} \quad L_z = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

c. Prove that $L_xL_y - L_yL_x = L_z$, $L_yL_z - L_zL_y = L_x$ and $L_zL_x - L_xL_z = L_y$

d. For a vector $v = (a,b,c)$, show that L_v is given by

$$L_v = aL_x + bL_y + cL_z.$$

e. Prove that for vectors u, v, the cross product $u \times v$ satisfies

$$L_{u\times v} = L_uL_v - L_uL_v.$$

The (real) vector space with basis L_x, L_y, L_z is (an isomorphic form) of the associated *Lie algebra* to the *Lie group* SO(3). It's usually written $\mathfrak{so}(3)$. Though this may look intimidating (and it is), what you've just shown is that $\mathfrak{so}(3)$ is isomorphic (as algebras) to $\mathbf{R}^3$ equipped with the cross-product.

13. *Challenge.* (Follow up to problem 8.). You may recall the *second-derivative test*[68] from multivariable calc. If $f\colon \mathbf{R}^3 \to \mathbf{R}$ is a differentiable function of three variables, write H for the Hessian matrix

$$H = \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{pmatrix}$$

Here, f_{xy} denotes the partial derivative $\partial^2 f/\partial x \partial y$, etc. Note H is a function of the variables x, y, z.

a. Prove that H is symmetric

b. Prove that for a column vector $v \in \mathbf{R}^3$, that $\langle v, v\rangle_H$ is equal to the concavity of f in the direction v.

c. Prove that if (at a point $P \in \mathbf{R}^3$ such that $\nabla f(P)$ is the zero vector) that if all eigenvalues of H are positive, then P is a local minimum of f.

[68] That is, if (a,b) is a point such that $\nabla f(a,b) = 0$ then the Hessian determinant $D = f_{xx}f_{yy} - f_{xy}^2$ evaluated at (a,b) can be used to determine if (a,b) is a max/min or saddle point.

A Mathematical induction

Induction, or **mathematical induction**, is a useful tool for proving (or in many cases "confirming") the existence of some pattern, usually dependent on the natural numbers. Rather than give a general description of what induction is, it's better to look at the following example and see how to use induction.

A.1 Example. A classic example is proving the sum formula

$$1 + 2 + 3 + \cdot + n = \frac{n(n+1)}{2} \tag{A.1.1}$$

holds for all $n \geq 1$. It goes as follows: let's first show that the formula holds for $n = 1$. Since

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

this is indeed true. Here's the trick: we show that *if* the formula is true for some value of n, then it *must* be true for $n + 1$ as well. Let's see

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

So, by induction, (A.1.1) must hold for all n.

It's important to note what we've just shown. Let's let $P(n)$ be the statement that the formula (A.1.1) holds for n. In the first step we showed $P(1)$ is true. Then we showed that $P(n)$ implies $P(n+1)$. At this point it's like watching a bunch of dominoes topple over. We get that $P(1)$ is true, so $P(2)$ must be. But then $P(3)$ must be, and $P(4)$, and $P(5)$, and so on. If we give ourselves an arbitrary n and ask the question "is $P(n)$ true?" the answer must be "yes" as we can work our way back to its truth value being tied to $P(1)$, which was already shown. Note as well that induction doesn't tell us "what" the formula (A.1.1) should be. It only allows us to prove that the formula is correct.

A.2 Using induction

Induction is typically used to prove statements like (A.1.1) which can be phrased as a set of propositions $\{P(n) : n \in \mathbf{N}\}$ which have a decent "regularity" to them. A general approach to using induction is then:

- Show that there is a "starting value" $k \in \mathbf{N}$ such that $P(k)$ is true. Typically this is $k = 1$, but it doesn't have to be. This is called the **base case**.
- Show that given an arbitrary $n \geq k$, that if $P(n)$ is true, then $P(n+1)$ must be true. This is called the **inductive step**.

A good proof by induction will then end by justifying why and how induction has been used, but the above steps are where the work goes in.

A.3 Well-orderings

What induction relies on is that the set $\mathbf{N}$ is well-ordered[69]. A complete definition is given below for your entertainment, but we won't really need to go any deeper into well-orderings than understanding how to use theorem A.5.

A.4 Definition. *Let X be a set. An **ordering** on X is a relation $\leq$ on X such that*

- *For each pair of elements $x, y \in X$ either $x \leq y$ or $y \leq x$*
- *$x \leq x$ for all $x \in X$*
- *If $x, y, z \in X$ such that $x \leq y$ and $y \leq z$, then $x \leq z$.*
- *If $x \leq y$ and $y \leq x$, then $x = y$.*

A set X with ordering $\leq$ is called **well-ordered** if each nonempty subset $Y \subset X$ has a least-element for this ordering (that is, there is $y \in Y$ such that $y \leq z$ for all $z \in Y$). You can convince yourself that $\mathbf{N}$ is well-ordered, but $\mathbf{Z}$ is not (at least with the typical ordering of integers). A fun, but somewhat controversial, fact in mathematics is that *any* set can be well-ordered.

For us, it's enough to use the following as a black-box statement (which is true more or less by definition).

A.5 Theorem ($\mathbf{N}$ is well-ordered)**.** *Any nonempty subset $X \subset \mathbf{N}$ has a smallest element.*

A.6 Exercises

1. Use induction to prove for $n \geq 1$ that
$$1^2 + 2^2 + 3^3 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$
2. Use induction to prove that $n! > 2^n$ for $n \geq 4$.
3. Use induction to prove for $n \geq 2$ that
$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n-1)n} = \frac{n-1}{n}$$
4. You may know about the Fibonacci numbers: $a_1 = 1, a_2 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$. Prove for $n \geq 1$ that
$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

   Challenge. What is the limit $\lim_{n \to \infty} a_{n+1}/a_n$ of the ratio of successive Fibonacci numbers?

[69] And in fact this is a sufficient condition *do* induction, meaning you can "do induction" over any well-ordered set, even those with uncountably many elements, it's just harder to intuit what is happening

5. With respect to the usual ordering, are the sets $\mathbf{Q}$ or $\mathbf{R}$ well-ordered?

6. Prove that for any $n \geq 1$ there is an integer k such that

$$10^{n+1} + 10^n - 1 = 3k$$

7. *Challenge.* Let $n \geq 1$ and let $a_1, a_2, \cdots, a_n$ be real numbers. Prove that

$$\sqrt[n]{a_1 a_2 a_3 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k$$

This is known as the AM-GM inequality.

8. *Challenge.* Let $S = \{0, 1\} \times \mathbf{N}$ and give S the order that $(a, b) \leq (c, d)$ if either (i) $a = c, b \leq d$ or (ii) $a < c$[70]. Show that S is well-ordered. Show as well that there is no bijection $f \colon S \to \mathbf{N}$ that preserves this ordering $\leq$ (that is, such that if $a \leq b$ in S then $f(a) \leq f(b)$ in $\mathbf{N}$).

[70] This is sometimes called the *lexicographic order*