150A: Modern Algebra
Notes

Melissa Zhang
UC Davis

Winter 2024

Contents

These notes are for a course based on Artin's *Algebra*. As such, we generally follow the conventions in that book, but also introduce common terminology and vocabulary not used in the book.

Important terms are either *italicized* or **bolded**. In general, a bolded term indicates that I am introducing to you right now and that you should learn right now. An italicized term might just be an emphasis, or a term that we will seriously introduce later in the course.

1 Prerequisite material

Mathematics is in general cumulative (as with many fields). I am assuming you already know topics such as the unit circle, the division algorithm, how to solve an equation, etc., and will not list everything that is prerequisite material. Instead, let's focus on two very important college courses that this course relies on.

1.1 Proofs

First, in order to succeed in this course, you **must be able to read, write, and evaluate proofs.** If you aren't feeling too confident about proofs yet after taking MAT 108, that's ok, but be aware that you must work extra hard on getting used to reading and writing proofs as soon as possible. This means that you should pay extra attention to how I structure my proofs in class and in the homework solutions, and give yourself extra time to write out clean proofs on homeworks.

There are also other topics from MAT 108 that will be needed in this class, such as the concept of equivalence relations and partitions. We will still go over these concepts in an accelerated fashion, but I will assume you have seen them before.

1.2 Typing

You are also expected to typeset your homework on LaTeX. This is not a skill that I expect you to already have; my goal is for you to learn this skill in this course. However, you should not try to learn how to typeset while simultaneously thinking about how to structure your proofs; the result of this multi-tasking will be a waste of your valuable time. You must first (on paper, or whatever you normally use) work out your solution, and clarify your argument; you should even write down your proof with the variables you intend to use while typing it up. Only after you have a full argument written down should you start typing up your solution; at this point, the only task you have is to figure out the commands for math symbols you already wrote on paper. Start your homeworks early!

1.3 Writing with proper grammar

Part of the reason for asking you to type up your homework is that you will (hopefully) be forced to write in full sentences and to organize your work more clearly. You are expected to be able to write mathematics in full sentences with proper grammar and **punctuation**! If you submit a sub-par homework solution or exam solution, style points may be deducted. I cannot stress enough how fundamental writing proofs *well* is to your mathematics background.

1.4 Linear algebra

Finally, as this is an algebra class, your background knowledge in linear algebra will be extremely important. If you don't remember basic topics in linear algebra, please go back and review them. In particular, sections 1.1, 1.3, and 1.4 in the book are very relevant to the material we will cover. Here's a non-comprehensive list of concepts off the top of my head that you will need to know:

- matrix addition, multiplication, scalar multiplication, identity
- determinant, invertible matrix, inverse of a 2×2 matrix
- vectors, basis of a vector space
- matrix transpose
- block matrices, block multiplication, diagonal matrix, scalar matrix

2 Introduction to Groups

In algebra, we use symbols to represent quantities, objects, relations, etc. This translates a specific problem into an abstract problem. We develop methods to solve this problem in more generality (i.e. abstractly, or algebraically) and then translate the solution back to the specific problem.

When I first saw algebra in middle school, this is the kind of problem I would solve:

Example 2.1. Tamara has 35 coins in nickels and quarters. In all, she has $4.15. How many of each type of coin does she have? [1]

Different subfields of algebra are used to solve different parts or types of problems.

Example 2.2. One of the nicest and most pervasive types of algebra is **linear algebra**:

- All relationships between variables are *linear*, as opposed to quadratic, exponential, non-algebraic, etc.
- We often simplify nonlinear problems using linear approximations, then obtain approximate solutions.
- *Matrix groups* are used *represent* more complicated abstract groups.

Example 2.3. *Modern* or *abstract* algebra is a more general term referring to all algebra beyond, say, solving single-variable equations or basic linear algebra. For example, topics in abstract algebra include

- algebraic structures: groups, rings, fields, lattices, representations, group actions, etc.
- relations between them: homomorphisms, isomorphisms, sub- and quotient objects, products, etc.

Our course focuses on the most fundamental algebraic structure among those listed: groups. Below, we will discuss groups from two related points of view. This serves both as a bit of a review, as well as an overview of the structure of this course.

2.1 Groups by axiomatic definition

Definition 2.4. A **group** is a set G together with a **law of composition** $\circ$ that has the following properties:

- $\circ$ is associative: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$
- G contains an identity element $1 = 1_G$ such that $1 \circ a = a$ and $a \circ 1 = a$ for all $a \in G$.
- Every element $a \in G$ has an **inverse**, i.e. an element b such that $a \circ b = 1 = b \circ a$.

[1] from https://www.chilimath.com/lessons/algebra-word-problems/coin-word-problems/

Other terms for *law of composition* include **group law**, **multiplication in the group**, **composition rule**, **group operation**, etc.

Exercise 2.5. (a) What happens if we drop the requirement that $a \circ 1 = a$ and just assume that $1 \circ a = a$?

(b) What happens if we drop the requirement that $b \circ a = 1$ and just assume that $a \circ b = 1$?

Remark 2.6. Note that commutativity of $\circ$ is not required in the definition of a group. A group where $\circ$ is indeed commutative, i.e. $a \circ b = b \circ a$ for all $a, b \in G$ is called a **commutative** or **abelian** (or **Abelian**) group.

To describe a group, we have to provide both the *underlying set* G and the composition rule $\circ$. So, we might write something like $(G, \circ)$ to be super clear, but just write G if it's clear what group we're talking about.

Also, we don't need to use the symbol $\circ$.

Exercise 2.7. Which of the following are groups? Why or why not?

(a) $(\mathbb{N}, +)$

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{Z}, -)$

(d) $(\mathbb{Z}, \cdot)$

(e) $(\mathbb{R}, +)$

(f) $(\mathbb{R}, \cdot)$

(g) $(\mathbb{R} - \{0\}, \cdot)$

(h) $(\mathbb{C}, +)$

(i) $(\mathbb{C}, \cdot)$

(j) $(\mathbb{C} - \{0\}, \cdot)$

(k) $(\mathbb{Q}, +)$

(l) $(\mathbb{Q}, \cdot)$

(m) $(\mathbb{Q} - \{0\}, \cdot)$

After doing this exercise, you might realize that $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all very similar. This is because they are all **fields**, which are another type of algebraic structure that we will discuss in this course.

Example 2.8. Let $M_{2\times 2}\mathbb{R}$ denote the set of 2×2 matrices with real entries. This is a group under addition, but is *not* a group under matrix multiplication, because some matrices are not invertible (e.g. the zero matrix).

Example 2.9. The **general linear group** of 2×2 matrices is

$$GL_2(\mathbb{R}) = \{A \in M_{2\times 2}(\mathbb{R}) \mid \det A \neq 0\}.$$

By definition[2], everything in $GL_2(\mathbb{R})$ has a multiplicative inverse. Matrix multiplication is indeed associative. We write either I or I_2 for the identity matrix.

[2] review determinants if this isn't clear!

2.2 Groups as sets of symmetries

Historically, groups came up naturally from *group actions*. The action corresponding to the identity element is "do nothing".

To me, the most concrete way to understand and see a group action is to think about symmetries of 2D regular polygons.

Question 2.10. What are the *symmetries* of a square? How many different symmetries are there?

If we think of a square as a rigid object, we can rotate it by angles that are multiples of $\pi/2$, and also reflect across vertical, horizontal, and diagonal (angle $\pm\pi/4$) lines.

Suppose we are building a video game where you need to be able to manipulated a square with only two buttons. We might choose to assign our buttons to the following actions:

- $\rho =$ rotate by $\pi/2$ CCW (counterclockwise)
- $\tau =$ reflect across the x-axis

We think about actions like we think about functions (hence the $\circ$ symbol).

Question 2.11. Can you write down a sequence of button presses to achieve all the symmetries of the square?

There are obviously many different sequences of button presses that would achieve the same result. One important but perhaps non-obvious way to do absolutely nothing is $\rho \circ \tau \circ \rho \circ \tau = (\rho \circ \tau)^2$. (Try it!)

Definition 2.12. The **dihedral group** D_n is the group of symmetries of a regular n-gon. [3]

One way we will use to describe groups is called **group presentation**, which is written in the form

$$\langle \text{generators} \mid \text{relations} \rangle.$$

The generators are the buttons you implement. The relations are a set of button presses that do nothing. Once we understand *normal subgroups*, we will be able to formalize this definition rigorously. However, it's still useful to us right now, for intuition. For example, we can describe the set of symmetries of a square now as

$$D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = \rho\tau\rho\tau = 1 \rangle.$$

Remark 2.13. Notice that I've been eliding the composition symbol $\circ$ in favor of *multiplicative notation*. We will talk more about conventions later, but for now you should just think back to how you used to write $2 \times 2 = 4$, then you started writing $a \cdot b = c$, and even later on you would just write $AB = I$.

Exercise 2.14. Write down a group presentation for the symmetries of a triangle: define what your generators do, and then write down some obvious relations. Then, think about how you would prove that your presentation uniquely determines your symmetry group D_3.

2.3 Cyclic groups C_n

Definition 2.15. A group G is **cyclic** if it is generated by a single element, i.e. there exists an element $\rho \in G$ such that every $g \in G$ can be written in the form $g = \rho^k$ for some $k \in \mathbb{Z}$.

Example 2.16. The cyclic group C_{12} has the presentation

$$C_{12} = \langle \rho \mid \rho^{12} = 1 \rangle.$$

Question 2.17. Is $\mathbb{Z} = (\mathbb{Z}, +)$ a cyclic group?

Definition 2.18. The **order** of a group G is the number of elements that it contains, and is denoted $|G|$.

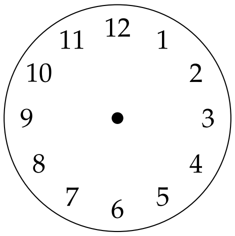
[3] Warning: There are other conventions; some people write D_{2n} instead.

- If $|G|$ is finite, then G is a *finite group*.
- If $|G|$ is infinite, then G is an *infinite group*.

Question 2.19. What is the order of the group $C_n = \{\rho \mid \rho^n = 1\rangle$?

Exercise 2.20. Prove that every cyclic group is abelian.

Example 2.21. While we used multiplicative notation above to define C_{12}, this group is basically the same as the additive group we use when we look at analog clocks:



The group $\mathbb{Z}/12\mathbb{Z}$ is the additive group of integers **mod 12**. (We will talk more about this notation later.)

The group operation, addition, works exactly as you'd expect while looking at a 12-hour analog clock. For example, 8 am + 6 hours = 2 pm, so 8 + 6 = 2.

This brings us to an important point about additive and multiplicative notation.

Remark 2.22. (Notation Conventions)

So far in this class we've used a couple different notations for the **composition law / group operation** in a group G:

1. An abstract symbol, such as $\circ$.
   - Permutations $p, q \in S_n$ are set maps $[n] \to [n]$. We can compose them in two ways: $p \circ q$ or $q \circ p$.
   - When $n \geq 3$, S_n is **nonabelian**, so in general $p \circ q \neq q \circ p$.
2. **Additive notation**, where $+$ is a **commutative** group operation:
   - e.g. $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$
   - Use 0 to represent the **additive identity**.
3. **Multiplicative notation**, where $b \circ a = b \cdot a$ is written ba:
   - If $x, y \in \mathbb{R}^\times = (\mathbb{R} - \{0\}, \cdot)$, we write xy as their product.
   - If $p, q \in S_n$, we write pq or qp. In general, $pq \neq qp$.
   - Use 1 to represent the **multiplicative identity**.

2.4 Permutations of sets and the symmetric groups S_n

Question 2.23. There are five seats in a classroom, and five students. How many different ways are there to seat the students?

Definition 2.24. Let S be a set. A **permutation** of S is a bijective map

$$p : S \to S.$$

Example 2.25. Let $[5] = \{1, 2, 3, 4, 5\}$.
Here is an example of a permutation p of [5]:

i	1	2	3	4	5
$p(i)$	3	5	4	1	2

Notation 2.26. For any $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \ldots, n\}$.

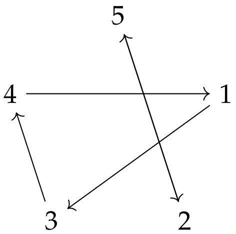
Definition 2.27. The group of *all* permutations of $[n]$ is called the **symmetric group** and is denoted S_n.

Do not confuse this with *permutation groups* in general, which are *subgroups* of symmetric groups.

Exercise 2.28. Consider our permutation $p \in S_5$ above.

(a) How does the permutation p^2 act on $[5]$?

(b) Recall that $p^2 = p \circ p$. Write down a similar chart.



To write down the **cycle notation** for a permutation, we start with an arbitrary index, such as 3, and then write down $p(3)$, and repeat until we get back to 3:

$$3 \mapsto 4 \mapsto 1 \mapsto 3$$

For p above, this gives us a 3-cycle $(3\ 4\ 1)$. Then, we choose an index that we haven't seen yet, and do the same thing: $(2\ 5)$.

If an index is fixed by a permutation, then by convention, we omit writing the 1-cycle. For example,

$$q = (12)(34) \in S_5$$

is cycle notation for the permutation given by the following chart:

i	1	2	3	4	5
$q(i)$	2	1	4	3	5

Example 2.29. There are many equivalent ways to write p in cycle notation:

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

Disjoint cycles can be written in any order, and cycles need only have their cyclic order preserved.

Exercise 2.30. Cycle notation allows us to compose permutations easily. Let

$$p = (3\ 4\ 1)(2\ 5) \qquad q = (1\ 2)(3\ 4).$$

(a) Write down p^2, p^3, and p^4 in cycle notation.

Solution: $p^2 = (3\ 1\ 4)$, $p^3 = (2\ 5)$, $p^4 = (3\ 4\ 1)$

(b) Write down qp and pq in cycle notation. (Remember, qp means $q \circ p$.)

Solution: $qp = (1\ 2)(3\ 4) \circ (3\ 4\ 1)(2\ 5) = (1\ 4\ 2\ 5)$, $pq = (3\ 4\ 1)(2\ 5) \circ (1\ 2)(3\ 4) = (1\ 5\ 2\ 3)$

Definition 2.31. A **transposition** is a 2-cycle. We usually denote them by $\tau_{ij} = (i\ j)$.

Theorem 2.32. The set of all transpositions τ_{ij} (where $i \neq j$ are indices in $[n]$) generate S_n.

Proof. (Proof idea) Any permutation is a product (i.e. composition) of cycles, so One way to prove this is by exhibiting an algorithm for constructing cycles from transpositions.

For example, observe that

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

(Note once again that we first apply the transposition at the far right, and work out way left, because we are actually just composing set maps.) This reasoning works in general:

$$(i_1\, i_2\, \cdots\, i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \cdots (i_1\, i_3)(i_1\, i_2).$$

□

Example 2.33. How can we write $p = (3\,4\,1)(2\,5)$ as a composition of transpositions?

We can represent permutations using **permutation matrices**. The key observation is that there is an obvious set bijection

$$[n] \cong \{e_1, e_2, \ldots, e_n\}.$$

Example 2.34. Let $\sigma = (1\ 3\ 2) \in S_3$. We can represent σ as the linear transformation that sends each $e_i \mapsto e_{\sigma(i)}$:

$$\sigma \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Recall from linear algebra the following two facts:

- The determinant of the $n \times n$ identity matrix $I_n \in M_{n\times n}(\mathbb{R})$ is 1.
- If M' is obtained from M by interchanging two different rows, then $\det A' = -\det A$.

Definition 2.35 (Sign of a permutation)**.** Let $p \in S_n$ be a permutation. The **sign** of p is equal to the determinant of the permutation matrix P representing p:

$$\operatorname{sgn}(p) := \det(P).$$

The following exercise shows we could equivalently define $\operatorname{sgn}(p)$ to be $(-1)^k$, where k is the number of transpositions in any composition of transpositions equal to p. If $\operatorname{sgn}(p) = +1$, we say that p is **even**; otherwise, if $\operatorname{sgn}(p) = -1$, we say that p is **odd**.

Exercise 2.36. (a) Prove that the transpose of a permutation matrix is its inverse.

(b) Prove that the determinant of a permutation matrix is always ±1.

(c) Let $p \in S_n$, and write p as a composition (or equivalently, product) of k transpositions:

$$p = \tau_{i_1} \circ \tau_{i_2} \circ \ldots \circ \tau_{i_k}$$

Prove that p is even if and only if k is even, and that p is odd if and only if k is odd.

2.5 Complex numbers

The complex numbers $\mathbb{C}$ are is pervasive in mathematics and will provide us with many interesting examples of groups.

Let i be a variable satisyfing the relation $i^2 = -1$. The underlying set of $\mathbb{C}$ is $\{a + bi \mid a, b \in \mathbb{R}$. In other words, the complex numbers are just polynomials (with real coefficients) in the variable i, except that any time you see i^2, you can replace it with $-1 \in \mathbb{R}$.

This tells us how to add and multiply complex numbers. Addition is the same as vector addition in $\mathbb{R}^2$:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Multiplication is the same as for polynomials:

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac-bd) + (ad+bc)i$$

What's more interesting is that one can also divide complex numbers. That is, every nonzero complex number has a *multiplicative inverse*:

$$\frac{1}{a+bi} = (a+bi)^{-1} = \frac{1}{a^2+b^2}(a-bi)$$

The variable of choice for complex numbers is usually z, followed by w. The **complex conjugate** of $z = a+bi$ is $\bar{z} = a - bi$.[4]

When we view z as a vector $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$, its length is given by $||z|| = \sqrt{a^2+b^2}$. When we view z as a complex number, we call this the **absolute value** or **modulus** of z, and write

$$|z| = \sqrt{a^2+b^2}.$$

Exercise 2.37. Verify that $z\bar{z} = |z|^2 = a^2+b^2$, and observe that

$$z^{-1} = \frac{\bar{z}}{|z|^2}.$$

It is often easier to work with polar coordinates (r,θ) rather than rectangular coordinates (x,y). We can write any complex number $z = x+iy$ in polar coordinates (r,θ) where

- $r = |z|$, the length of the vector z
- θ is the angle the vector z makes with the real axis (which is identified with the x-axis in $\mathbb{R}^2$).

Recall from precalculus that to translate from (r,θ) to (x,y), we compute

$$x = r\cos\theta \qquad y = r\sin\theta.$$

For Taylor series reasons, we can write

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

Euler's formula says that $e^{\pi i} = -1$, and therefore $e^{2\pi i} = 1$.

Therefore if $z = x+iy$, and (x,y) in rectangular coordinates translates to (r,θ) in polar coordinates, we can write

$$z = x+iy = re^{i\theta}.$$

We will use this notation *extensively*, because it makes complex multiplication very simple. Let $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$. Then

$$z_1z_2 = \left(r_1e^{i\theta_1}\right)\left(r_2e^{i\theta_2}\right) = (r_1r_2)e^{(\theta_1+\theta_2)i}.$$

Geometrically, multiplication by i represents rotating by $\pi/2$ counterclockwise (CCW). That is, the vector iz is just the vector z rotated by $\pi/2$.

Example 2.38. The unit circle S^1 inside $\mathbb{C}$ is the set of complex numbers of modulus 1:

$$S^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}.$$

Note that I could have also written $\theta \in [0, 2\pi)$, or any other interval of this shape of length 2π, because $e^{2\pi i} = 1$.

This is a group under complex multiplication. (See HW01 for the same group described in a different way.)

Exercise 2.39. Prove that the **circle group** S^1 (under complex multiplication) is *not* cyclic.

Exercise 2.40. Prove that $\mathbb{C}^\times = \mathbb{C} - \{0\}$ is a group under complex multiplication.

Exercise 2.41. Find a *representation* of $\mathbb{C}^\times$ in $GL_2(\mathbb{R})$. That is, assign every element $z \in \mathbb{C}^\times = \mathbb{C} - \{0\}$ to a 2×2 invertible matrix so that matrix multiplication agrees with multiplication in $\mathbb{C}^\times$.

[4] This is in analogy with the conjugates we learn about in precalculus: $a \pm b\sqrt{k}$.

2.6 Aside: Real algebras

Here's an interesting nonabelian group.

Definition 2.42. The **quaternion group** H is the group consisting of elements

$$\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}.$$

where ± 1 commutes with all elements, and multiplication is determined by

$$\begin{aligned} &\pm 1\mathbf{i} = \pm\mathbf{i}, \qquad \pm 1\mathbf{j} = \pm\mathbf{j}, \qquad \pm 1\mathbf{k} = \pm\mathbf{k} \\ &\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \\ &\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}. \end{aligned}$$

Remark 2.43. This construction of $\mathbb{C}$ from polynomials with real coefficients makes $\mathbb{C}$ into a real *algebra*[5]. We can keep going, and define the quaternions $\mathbb{H}$ and the octonions $\mathbb{O}$. However, the quaternions aren't commutative, and the octonions aren't even associative.

Exercise 2.44. (Advanced)

1. Define the *Hamiltonian quaternions* $\mathbb{H}$ as polynomials in $\mathbf{i}, \mathbf{j}, \mathbf{k}$ with real coefficient, subject to the relations in the group H. This makes $\mathbb{H} = \mathbb{R}[H]$, the *group ring* built from $\mathbb{R}$ and H. (We will talk more about rings later in the course.)
2. Define $\mathbb{H}$ differently, now using $\mathbb{C}$ as the coefficients. (This describes $\mathbb{H}$ as an algebra over $\mathbb{C}$.)
3. Use the description of $\mathbb{H}$ as an algebra over $\mathbb{C}$ to find a representation of $\mathbb{H}$ by 2×2 matrices with complex entries.

2.7 Subgroups

Definition 2.45. A subset H of a group G is a **subgroup** (written $H \leq G$) if it has the following properties:

- *Closure*: If $a, b \in H$, then $ab \in H$ as well.
- *Identity*: $1 = 1_G \in H$
- *Inverses*: If $a \in H$, then $a^{-1} \in H$ as well.

Example 2.46. The *even integers* $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$ is a proper subgroup of $\mathbb{Z}$.

Similarly, for any $n \in \mathbb{N}$, the set of multiples of n, denoted $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$, is a subgroup of $\mathbb{Z}$. (Note that $1\mathbb{Z} = \mathbb{Z}$ is not a proper subgroup.)

Warning The book writes $\mathbb{Z}n$ instead of $n\mathbb{Z}$, and hence writes the group $\mathbb{Z}/12\mathbb{Z}$ as $\mathbb{Z}/\mathbb{Z}12$. Either notation is mathematically reasonable, since $\mathbb{Z}$ is commutative. However, I prefer the more common notation $\mathbb{Z}/12\mathbb{Z}$.

Exercise 2.47. Convince yourself that for natural numbers $n, m \in \mathbb{N}$, $(nm)\mathbb{Z}$ is a subgroup of both $m\mathbb{Z}$ and $n\mathbb{Z}$. It may help to start with an example, e.g. $n = 2, m = 3$.

Example 2.48. The **trivial group** is the group with one element, the identity. Any nontrivial group G automatically has at least two subgroups:

1. the **trivial subgroup** $H = \{1\} \leq G$
2. $H = G$, the whole group itself.

A subgroup $H \leq G$ where $H \neq G$ (as a set) is called a **proper subgroup.**

A group G that has no nontrivial, proper subgroups is called a **simple group.**

[5] This is a term we haven't defined yet.

Example 2.49. Here are some more examples of subgroups.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, where the group operation is $+$
2. $S^1 \leq (\mathbb{C}, \cdot)$
3. $S_k \leq S_n$ where $k \leq n$ $(k, n \in \mathbb{N})$

The following proposition gives a potentially easier way to check whether a subset $H \subset G$ is a subgroup.[6]

Proposition 2.50. (The Subgroup Criterion) A subset H of a group G is a subgroup if and only if $H \neq \emptyset$ and for all $a, b \in H$, $ab^{-1} \in H$.

Exercise 2.51. Prove Proposition 2.50. HW02

2.8 Order of a group

We now introduce the *order* of a group, which is a description of its size. Finite and infinite groups behave quite differently!

Definition 2.52. The **order** of a group G is the number of elements that the set G contains, and is denoted $|G|$.

- If $|G|$ is finite, then G is a *finite group*. In this case, we write $|G| = n$.
- If $|G|$ is infinite, we don't usually make any further distinctions about the cardinality of G. We just write $|G| = \infty$, and say that G is an infinite group.

Exercise 2.53. What is the order of C_n? D_n? $\mathbb{Z}$?

2.9 Order of an element

Given an element x in a group G, we can also define the *order of the element*, which is related to the notion of the order of a group.

Definition 2.54. Let $x \in G$. The **cyclic subgroup generated by** x is

$$\langle x \rangle := \{g \in G \mid g = x^k \text{ for some } k \in \mathbb{Z}\}.$$

Exercise 2.55. Prove that $\langle x \rangle$ really is a subgroup of G.

Notice that we use the notation $\langle \cdot \rangle$ to mean *generated by*. This is similar to the notation we use for generators and relations in a group presentation. We will continue to use this notation. For example, if we want to describe the subgroup generated by a subset $X \subset G$, we can write $\langle X \rangle$.

Definition 2.56. The **order** of an element $x \in G$, denoted $|x|$, is the order of the cyclic subgroup $\langle x \rangle$ generated by x.

If $|x| = n \in \mathbb{N}$, then we say x *has order* n or *is of order* n. If $|x| = \infty$, then x is an element of *infinite order.*

Example 2.57. The order of $1_G \in G$ (the element) is always 1 (the natural number).

Exercise 2.58. Convince yourself that if $x \in G$, then $|x| \leq |G|$. When would $|x| = |G|$?

Exercise 2.59. In $\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$, what are the elements of finite order? What is the order of the element i?

[6] However, I often still just check the conditions in the definition.

Exercise 2.60. (The Klein four group ♫) Recall that $GL_2(\mathbb{R})$ is the group of invertible 2×2 matrices with real coefficients. Inside $GL_2(\mathbb{R})$, there is a subgroup called the **Klein four group** V:

$$V = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right\}$$

Use the concept of *order of an element* to prove that V is *not* cyclic.
Solution: By inspection, every element has order either 1 or 2. If V were cyclic, then it would be generated by a single element g; since $\langle g \rangle = 4$, the order of g would be 4.

Exercise 2.61. Let $a, b \in G$. Prove that $|ab| = |ba|$. HW02

Exercise 2.62. Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian? HW02

2.10 Subgroups of $\mathbb{Z}$

At this point you might already have some guesses for what the subgroups of $\mathbb{Z}$ are.

Theorem 2.63. Let S be a subgroup of $(\mathbb{Z}, +)$. Then S is either

- the trivial subgroup $\{0\}$ or
- of the form $n\mathbb{Z}$, where n is the smallest positive integer in the set S.

Proof.

- Since 0 is the additive identity, $0 \in S$. If $S \neq \{0\}$, then there exist integers $n, -n \neq 0$ in S. So S contains a positive integer.
- Let a be the smallest positive integer in S. We want to show that $a\mathbb{Z} = S$, so we need to show that $a\mathbb{Z} \leq S$ and $S \leq a\mathbb{Z}$.
- To check that $a\mathbb{Z} \leq S$, observe that (1) closure and induction imply $ka \in S$, (2) $0 = 0a \in S$, and (3) S contains inverses, so $-ka \in S$.
- To show $S \subseteq a\mathbb{Z}$, pick any $n \in S$. Use division with remainder to write $n = qa + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < a$.
  - Since S is a *subgroup*, $r = n - qa \in S$.
  - Since a is the smallest positive integer in S, r must $= 0$.
  - Therefore $n = qa \in a\mathbb{Z}$.

□

The argument in this proof is very useful, and we will see it again in this course.

Proposition 2.64. Let $x \in G$, and let S denote the *set* of integers k such that $x^k = 1$:

$$S = \{k \in \mathbb{Z} \mid x^k = 1\}.$$

(a) S is a subgroup of $\mathbb{Z}$

(b) If $x^r = x^s$ (say, $r \geq s$), then $x^{r-s} = 1$, i.e. $r - s \in S$.

(c) Suppose that S is not the trivial subgroup $\{0\} \leq \mathbb{Z}$. Then $S = n\mathbb{Z}$ for some positive integer n. The powers $\{1, x, x^2, \ldots, x^{n-1}\}$ are the distinct elements of the subgroup $\langle x \rangle$, and so the order of $\langle x \rangle$ is n.

Proof. (a) Let's use the subgroup criterion. Since $0 \in S$, $S \neq \emptyset$. If $k, \ell \in S$, then $x^{k-\ell} = x^k(x^\ell)^{-1} = 1 \cdot 1 = 1$. (You can also just check the three subgroup conditions.)

(b) This follows from the Cancellation Law (i.e. manipulating the algebraic equation).

(c) Suppose $S \neq \{0\}$. Then by Theorem 2.63, $S = n\mathbb{Z}$, where n is the smallest positive integer in S.

Now let x^k be an arbitrary power of x. We can write $k = qn + r$ with $0 \leq r < n$. Then $x^{qn} = 1^q = 1$, so $x^k = x^{qn}x^r = x^r$. Therefore every x^k is equal to one of the elements x^r where $0 \leq r < n$.

It remains to check that the powers $\{1, x, x^2, \dots x^{n-1}\}$ are all distinct. If $x^p = x^q$ with $0 \leq p < q < n-1$, then by (b), $q - p$ is a positive multiple of n; this is impossible.

□

Part (c) therefore gives an equivalent definition of the order of an element in a group:

Corollary 2.65. If $|g| \neq \infty$, then $|g| = \min\{n \in \mathbb{N} \mid g^n = 1$.

Exercise 2.66. Prove that every subgroup of a cyclic group is cyclic. *Hint: Work with exponents and use the description of the subgroups of* $\mathbb{Z}^+$. HW03

3 A bit of review + generalizations

3.1 Fields and Vector Spaces

Definition 3.1. A **field** is a set $\mathbb{F}$ equipped with two associative and commutative binary operations $+$ and $\cdot$ such that

- $(\mathbb{F}, +)$ is an abelian group, with identity 0
- $(\mathbb{F}^\times = \mathbb{F} - \{0\}, \cdot)$ is an abelian group, with identity 1
- $a(b + c) = ab + ac$ (distributivity of $\cdot$ over $+$).

In other words, a field is a set where you can add, subtract, multiply, and divide just as you do with the real numbers.

Example 3.2. Here are some examples of fields:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ where p is prime (see next section)

Definition 3.3. A **vector space** over a field $\mathbb{F}$ is a set V with the two operations

- addition: $v + w$ for $v, w \in V$ and
- scalar multiplication: cv for $c \in \mathbb{F}$, $v \in V$

where

- $(V, +)$ is an abelian group with identity the *zero vector* $\vec{0}$
- $(ab)v = a(bv)$ for $a, b \in \mathbb{F}$ and $v \in V$ (associativity of scalar multiplication)
- $1v = v$
- $a(v + w) = av + aw$ and $(a + b)v = av + bv$ for $a, b \in \mathbb{F}$, $v, w \in V$ (distributivity).

Exercise 3.4. Note that if $0 = 0_{\mathbb{F}}$, then for any $v \in V$, $0v = \vec{0}$ (use distributivity). We usually just write the symbol 0 for both zeroes, because of this relationship.

Example 3.5. Here are some examples of vector spaces over a field $\mathbb{F}$. These are all probably quite familiar if you let $\mathbb{F} = \mathbb{R}$.

- $V = \mathbb{F}$
- $V = \mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F}$

- $V = M_{n\times n}(\mathbb{F})$, the set of all $n \times n$ matrices with entries in $\mathbb{F}$
- $V = \mathbb{F}[x]$, the set of polynomials in x with coefficients in $\mathbb{F}$

Definition 3.6. A **subspace** W of a vector space V over a field $\mathbb{F}$ is a *nonempty* subset closed under the operations of addition and scalar multiplication.

A subspace W is **proper** if it is neither $\{0\} \subset V$ nor $V \subset V$.

Example 3.7. The set of all continuous functions $\mathbb{R} \to \mathbb{R}$, denoted $C^0(\mathbb{R})$, is a vector space over $\mathbb{R}$. Observe that $\mathbb{R}[x]$ is a vector **subspace** of $C^0(\mathbb{R})$. [7]

Definition 3.8. Let V, W be vector spaces over a field $\mathbb{F}$. A **linear map** (which is short for "$\mathbb{F}$-linear map") is a function $\phi : V \to W$ that preserves the structure of vector spaces:

- $\phi(\vec{0}_V) = \vec{0}_W$
- $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ for $v_1, v_2 \in V$
- $\phi(cv) = c\phi(v)$ for $v \in V, c \in \mathbb{F}$

Remark 3.9. In general, the word **linear** indicates that a map behaves like a linear function $f(x) = ax + b$, in the sense that if we have two coefficients c_1, c_2 and two elements x_1, x_2, then

$$f(c_1x_1 + c_2x_2) = c_1f(x_1) + c_2f(x_2).$$

This will come up in 150B when you talk about modules over rings, which are generalizations of vector spaces over fields.

Example 3.10. Let $A \in M_{n\times m}(\mathbb{R})$. (That is, n rows, m columns.) View A as a linear map $A : \mathbb{R}^m \to \mathbb{R}^n$. (Here, the **domain** of the function A is $\mathbb{R}^m$ and the **codomain** of the function A is $\mathbb{R}^n$.)

- The **nullspace** of A is the set of all vectors in the domain that are sent to 0 by A:

$$\mathrm{null}(A) = \{v \in \mathbb{R}^m \mid Av = 0 \in \mathbb{R}^n\}.$$

- The **range** of A is the set of all output vectors in the codomain of A:

$$\mathrm{range}(A) = \{Av \in \mathbb{R}^n \mid v \in \mathbb{R}^m\}.$$

Check that $\mathrm{null}(A)$ is a subspace of $\mathbb{R}^m$, and $\mathrm{range}(A)$ is a subspace of $\mathbb{R}^n$.

Exercise 3.11. How many elements are there in the vector space $\mathbb{F}_p^2$? How many different *proper* subspaces of $\mathbb{F}_p^2$ are there? HW04

3.2 Equivalence classes and partitions

A **partition** P of a set S is a subdivision of S into nonoverlapping, nonempty subsets. Here is a precise definition.

Definition 3.12. Let S be a set. A **partition** $P = \{P_i\}_{i\in I}$ is a set of subsets of S such that the following conditions hold:

- For all i, $P_i \neq \emptyset$.
- If $i \neq j$, then $P_i \cap P_j = \emptyset$.
- $P = \bigcup_{i\in I} P_i$.

[7] We write $C^r(\mathbb{R})$ for the set of all r-times differentiable functions from $\mathbb{R} \to \mathbb{R}$. Notice that $\mathbb{R}[x] \subset C^\infty(\mathbb{R}) \subset \cdots \subset C^r(\mathbb{R}) \subset C^{r-1}(\mathbb{R}) \subset \cdots \subset C^1(\mathbb{R}) \subset C^0(\mathbb{R})$.

In other words, a partition $P = \{P_i\}_{i \in I}$ is a collection of nonempty subsets of S such that for all $s \in S$, $s \in P_i$ for *exactly one* $i \in I$.

In this case, S is the *disjoint union* of the subsets in P:

$$S = \coprod_{i \in I} P_i.$$

Exercise 3.13. What are all the partitions of the set $[4]$?

Recall that a **relation** R on a set S is a subset of $S \times S$. (This is more general than a *function*.) If $(a, b) \in R$, we usually write $a \sim b$; however, note that a priori, we don't know if this relationship is symmetric, since $(a, b) \neq (b, a)$ in $S \times S$.

We care more about equivalence relations, though:

Definition 3.14. An **equivalence relation** on a set S is a relation $\sim$ that is

- **reflexive**: $a \sim a$
- **symmetric**: if $a \sim b$ then $b \sim a$
- **transitive**: if $a \sim b$ and $b \sim c$, then $a \sim c$

for all $a, b, c \in S$.

Definition 3.15. Let $\sim$ be an equivalence relation on S. Let $a \in S$. The **equivalence class of** a, denoted $[a]$ or $\bar{a}$, is the subset of S consisting of all elements that are related to a by $\sim$:

$$[a] = \{b \in S \mid a \sim b\}.$$

We say that a is a **representative** of its equivalence class.

Exercise 3.16. Let a, b be elements in a group G. We say a is **conjugate** to b if there exists $g \in G$ such that $b = gag^{-1}$. Prove that **conjugacy** is an equivalence relation. HW03

The following proposition states that *equivalence relations* and *partitions* are actually one and the same.

Proposition 3.17. An equivalence relation $\sim$ on a set S determines a partition P, and vice versa.

Proof. HW03 □

Remark 3.18. Let P denote the partition given by the equivalence relation $\sim$ on S. By the Axiom of Choice, no matter how large the cardinality of P is, we are able to choose a representative from each subset in P. That is, if $P = \{P_\alpha\}_{\alpha \in I}$ where I is an indexing set, it is possible to pick out a collection $\{s_\alpha\}_{\alpha \in I}$.

Remark 3.19. If S is empty, then the only partition is $P = \{\}$, i.e. P itself is the empty set. Then the conditions that make P a partition are vacuously true.

Example 3.20. (Equivalence relations defined by maps) A set map $f : S \to T$ defines an equivalence relation on S, indexed by the elements of the image of f, $\text{img}(f) \subset T$:

$$P = \{P_t = f^{-1}(t) \mid t \in \text{img}(f)\}$$

- Here $f^{-1}(t)$ is the **inverse image** or **preimage** of $t \in T$. (We also sometimes say that $f^{-1}(t)$ is the *fiber* of f over $t \in T$.)
- If $t \notin \text{img}(f)$, then $f^{-1}(t) = \emptyset$ and is not included in the partition P.

Please be warned that f^{-1} here is symbolic notation, and is in particular not indicating an inverse function. If f is not bijective, there is no inverse function f^{-1}.

3.3 Modular arithmetic

We have talked a bit about $\mathbb{Z}/n\mathbb{Z}$ as well as the fields $\mathbb{F}_p$. Let's review their construction now using the ideas of equivalence classes / partitions, and discuss what it means for a function (i.e. set map) to be *well-defined*.

Two integers $a, b \in \mathbb{Z}$ are **congruent mod** n if $a - b \in n\mathbb{Z}$. In this case, we write $a \equiv b \mod n$.

Exercise 3.21. Check that $\equiv$ is an equivalence relation.

Let $\bar{a}$ denote the equivalence class of a under the equivalence relation $\equiv$. Observe that by the division algorithm, the set of numbers $\{0, 1, \ldots, n-1\}$ is a complete set of representatives (i.e. we have one representative from every equivalence class). So, the partition corresponding to $\equiv$ is

$$P = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\},$$

and we really think of $\bar{k}$ as the subset

$$\bar{k} = k + n\mathbb{Z} \subset \mathbb{Z}.$$

Proposition 3.22. Addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$, induced by $+, \cdot$ on $\mathbb{Z}$, are **well-defined.**

Proof. Check that if $a \equiv a'$ and $b \equiv b'$, then

1. $(a + b) \equiv (a' + b')$ and
2. $ab \equiv a'b'$.

□

The concept of "well-definedness" doesn't come from cold, hard mathematics, but rather our human tendency to make errors when trying to define a function (i.e. a set map).

Sometimes mathematicians ask whether a function is well defined. What they mean is this: "Does the rule you propose really assign to each element of the domain one and only one value in the codomain?"

- *The Art of Proof*, by Matthias Beck and Ross Geoghegan.

Example 3.23. If I try to define a function $f : \mathbb{N} \to \mathbb{R}$ by saying "$f(n)$ is the real number that squares to n", then I have not succeeded in defining a function, because, for example, it's ambiguous what $f(4)$ should be. You would then tell me, "f is not a well-defined function." By saying this you are not saying that f was ever actually a mathematical function at all; you are saying that this rule doesn't define a function.

Exercise 3.24. HW03 This exercise will show you an example of an assignment that is actually not well-defined, and is therefore not a function, as well as an example where a function is actually defined successfully.

(a) Prove that the following assignment is **not** a well-defined function between sets:

$$\begin{aligned} \varphi : \mathbb{Z}/10\mathbb{Z} &\to \mathbb{Z}/7\mathbb{Z} \\ \bar{k} &\mapsto \bar{k}. \end{aligned}$$

(Recall that $\bar{k}$ denotes the equivalence class of k in $\mathbb{Z}/n\mathbb{Z}$.)

(b) Prove that the following assignment **is** a well-defined function between sets:

$$\begin{aligned} \varphi : \mathbb{Z}/10\mathbb{Z} &\to \mathbb{Z}/5\mathbb{Z} \\ \bar{k} &\mapsto \bar{k}. \end{aligned}$$

4 Maps between groups

4.1 Homomorphisms

Definition 4.1. Let $(S, \Box)$ and $(T, \blacktriangle)$ be groups. A **homomorphism**

$$\varphi : (S, \Box) \to (T, \blacktriangle)$$

is a (set) map $\varphi : S \to T$ such that for all $a, b \in S$,

$$\varphi(a \,\Box\, b) = \varphi(a) \blacktriangle \varphi(b).$$

Here's a more standard-looking definition of a group homomorphism:

Definition 4.2. Let G, G' be groups, written with multiplicative notation. A **homomorphism**

$$\varphi : G \to G'$$

is a map from G to G' such that for all $a, b \in G$,

$$\boxed{\varphi(ab) = \varphi(a)\varphi(b).}$$

This homomorphism condition is probably the most important equation in this class.

Example 4.3. Here are some familiar examples of homomorphisms.

- $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$
- $\text{sgn} : S_n \to \{\pm 1\}$
- $i : S_n \to S_m$ where $n \leq m$
- $\exp : \mathbb{R}^+ \to \mathbb{R}^\times$, where $x \mapsto e^x$
- $\varphi : \mathbb{Z}^+ \to G$ where $\varphi(n) = a^n$ for a fixed element $a \in G$
- $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$

Example 4.4. Some important homomorphisms:

- Let G, G' be groups. The **trivial homomorphism** is the map $g \mapsto 1_{G'}$ for all $g \in G$.
- Let G be a group. The **identity homomorphism** is $\text{id}_G : G \to G$ given by $g \mapsto g$ for all $g \in G$.
- Let H be a subgroup of G. The **inclusion map** is $i : H \hookrightarrow G$ where $h \mapsto h$ for all $h \in H$.

Exercise 4.5. Let $\varphi : G \to G'$ be a group homomorphism. Prove the following facts.

(a) If $a_1, a_2, \ldots, a_n \in G$, then
$$\varphi(a_1 a_2 \cdots a_k) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_k).$$

(b) $\varphi(1_G) = 1_{G'}$

(c) If $a \in G$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Definition 4.6. Let $\varphi : G \to G'$ be a group homomorphism.

- The **kernel** of φ is
$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_{G'}\}.$$

- The **image** of φ is
$$\operatorname{img}\varphi = \{g' \in G' \mid g' = \varphi(g) \text{ for some } g \in G\}.$$
Note that this is the same as
$$\varphi(G) = \{\varphi(g) \mid g \in G\}.$$
We use both notations for the image.

Exercise 4.7. HW03 Let $\varphi : G \to G'$ be a homomorphism.

(a) Prove that $\ker\varphi$ is a subgroup of G.

(b) Prove that $\operatorname{img}\varphi$ is a subgroup of G'.

(c) Prove that $\ker\varphi = \{1_G\}$ if and only if φ is injective (as a set map).

Example 4.8. Here are some examples of kernels:

- The kernel of $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ is the subgroup of all matrices with determinant 1; this is called the *special linear group* $SL_n(\mathbb{R})$.
- The kernel of the sign homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$ is called the **alternating group** A_n. This is the subgroup of all the *even* permutations.

Exercise 4.9. Demonstrate in class Let U denote the group of invertible upper triangular 2×2 matrices

$$\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{R},\ ad \neq 0 \right\} \subset GL_n(\mathbb{R})$$

and let $\varphi : U \to \mathbb{R}^\times$ be the map that sends $A \mapsto a^2$. Prove that φ is a homomorphism, and determine its kernel and image.

Exercise 4.10. Let $f : \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.

Definition 4.11. Here are some more important vocabulary words:

- A homomorphism $\varphi : G \to G'$ is an **isomorphism** if it is also a set bijection.
- A homomorphism from G to itself ($\varphi : G \to G$) is called an **endomorphism**.
- An *isomorphism* from G to itself is called an **automorphism.**

Remark 4.12. Recall from MAT 108 that there are a couple ways to show that a set map $f : A \to B$ is a bijection.

One way to show that f is bijective is to show that it is both injective and surjective.

- To show that f is injective, you need to show that if $f(a) = f(a')$, then $a = a'$.
- To show that f is surjective, you need to show that for all $b \in B$, there is some $a \in A$ such that $f(a) = b$.

The other way is to exhibit an inverse function $f^{-1} : B \to A$ for f. You need to check that $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

Exercise 4.13. Let $\varphi : G \to H$ be an *isomorphism*. Prove that for all $g \in G$, the order of g is the same as the order of $\varphi(g)$: $|g| = |\varphi(g)|$.

Exercise 4.14. Let G be a group. Prove that the map $\varphi : G \to G$, $x \mapsto x^2$, is an endomorphism of G if and only if G is abelian.

Exercise 4.15. HW03

(a) Let p be a prime number. How many automorphisms does the cyclic group C_p have?

(b) How many automorphisms does C_{24} have?

4.2 Cosets

Before discussing cosets, review equivalence relations/partitions and modular arithmetic.

Definition 4.16. Let H be a subgroup of G, and let $a \in G$. The **left coset** of H containing a is the set

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}.$$

Some remarks:

- The set of all left cosets of H in G is $\{bH \mid b \in G\}$. (There are probably repeats!)
- Note that every element $h \in H$ is in the same (left) coset (of H), the **identity** coset, which is the (left) coset of H containing 1. This coset is the set $H \subset G$.

We can also make the same definition for **right cosets**. The right coset of H containing a is

$$Ha = \{g \in G \mid g = ha \text{ for some } h \in H\}.$$

Example 4.17. It's useful to keep a concrete example in mind as a reference. In this example, let $G = \mathbb{Z}$, and let H be the subgroup $3\mathbb{Z}$. Note that the group operation is $+$. We can visualize the cosets of $3\mathbb{Z}$ as the three rows below:

$3\mathbb{Z}$	$\cdots$	-9	-6	-3	0	3	6	9	12	15	$\cdots$
$1+3\mathbb{Z}$	$\cdots$	-8	-5	-2	1	4	7	10	13	16	$\cdots$
$2+3\mathbb{Z}$	$\cdots$	-7	-4	-1	2	5	8	11	14	17	$\cdots$

I like to think of this as an infinite corn-on-the-cob, with the integers spiraling around the cob. In this example, if you break the corn and look at a cross-section, there will be three kernels going around the circle.

Proposition 4.18. Let $H \leq G$. The left cosets of H form a partition of G. (The right cosets of H also form a partition of G.)

Proof. By the definition of the set of left cosets, each coset is nonempty, and the union of all the cosets is G. It remains to check that if two cosets have nonempty intersection, then they are the same coset. It suffices to show that if $a \in bH$, then $aH = bH$.

Suppose $a \in bH$, i.e. there is some $h_a \in H$ such that $a = bh_a$, and therefore also $b = ah_a^{-1}$. Since we want to show a set equivalence, we should check double inclusion:

- $(aH \subseteq bH)$ If $ah \in aH$, then $ah = (bh_a)h = b(h_ah) \in bH$.
- $(bH \subseteq aH)$ If $bh \in bH$, then $bh = (ah_a^{-1})h = a(h_a^{-1}h) \in aH$.

(The proof for right cosets is nearly identical.) □

Because partitions and equivalence relations are logically the same thing, you can also try proving Proposition 4.18 in terms of equivalence relations.

Exercise 4.19. Prove Proposition 4.18 by defining an equivalence relation on the elements of G such that the equivalence classes agree with the set of left cosets.

Notation 4.20. We will sometimes write G/H to denote the set of left cosets of H. You will see later in this course why this notation both makes sense and also is unfortunate. This is why I keep just writing "the set of left cosets of H in G".

The proof of the following proposition should hopefully give a better sense of how cosets relate to each other.

Proposition 4.21. Let $H \leq G$. All cosets of H (left or right!) have the same cardinality.

Proof. We first show that every left coset has the same cardinality as the identity coset H. Let gH be a left coset of H, and consider the *set map* given by left multiplication by g:

$$\begin{aligned}(g\cdot) : H &\to gH \\ h &\mapsto gh\end{aligned}$$

Because g lives in a group, we automatically get an obvious inverse *set map*

$$\begin{aligned}(g^{-1}\cdot) : gH &\to H \\ x &\mapsto g^{-1}x\end{aligned}$$

(Note that x must necessarily be of the form gh_x for a unique $h_x \in H$, since because if $gh_x = gh'_x$, then by cancellation $h_x = h'_x$. So this map is well-defined.)

Check for yourself that these two maps really are inverse set maps. Therefore g is a bijection, and so H and gH have the same cardinality (by definition of cardinality).

To show that all right cosets have the same cardinality as H (which is both a left and right coset!), use the same trip, but with the set map $(\cdot g) : H \to Hg$, right multiplication by g. □

The following example is a great one to keep in your pocket. Recall that S_3 is the smallest nonabelian group; this makes the cosets behave different from those in abelian groups. Also, S_3 is written multiplicatively, unlike our previous concrete examples.

Example 4.22. *The set of right cosets isn't always the same as the set of left cosets!* As an example, consider $H = S_2 = \langle(12)\rangle$ and $G = S_3$. The left cosets of H are

- $1H = \{1, (12)\}$
- $(13)H = \{(13), (13)(12)\} = \{(13), (123)\}$
- $(23)H = \{(23), (23)(12)\} = \{(23), (132)\}$

whereas the right cosets are

- $1H = \{1, (12)\}$
- $H(13) = \{(13), (12)(13)\} = \{(13), (132)\}$
- $H(23) = \{(23), (23)(13)\} = \{(23), (123)\}$

A group homomorphism $\varphi : G \to G'$ is in particular a set map. Recall from Example 3.20 that the set of subsets $\{\varphi^{-1}(t) \subset G \mid t \in \operatorname{img}(\varphi)\}$ form a partition of G. Because of how well structured groups are, these subsets turn out to exactly be the cosets of the kernel $K = \ker \varphi$!

Remark 4.23. If you were paying attention, you'll notice that I didn't specify whether these were left or right cosets. It turns out that for a special type of subgroup, called a *normal subgroup*, left and right cosets agree. You will also later prove that kernels of homomorphisms are normal.

Proposition 4.24. Let $\varphi : G \to G'$ be a homomorphism, and let $a, b \in G$. Let $K = \ker \varphi$. The following conditions are equivalent (TFAE):

(a) $\varphi(a) = \varphi(b)$

(b) $a^{-1}b \in K$

(c) $b \in aK$

(d) $bK = aK$

Proof. To prove a 'TFAE' statement, it suffices to prove implications in a cycle. We will show that (a) $\implies$ (b) $\implies$ (c) $\implies$ (d) $\implies$ (a).

(a) $\implies$ **(b)** If $\varphi(a) = \varphi(b)$, then $1 = \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b)$ so $a^{-1}b \in K$.

(b) $\implies$ **(c)** If $a^{-1}b \in K$, then $a^{-1}b = k$ for some $k \in K$. Therefore $b = ak \in aK$.

(c) $\implies$ **(d)** This follows from the fact that the set of left cosets of K form a partition of G.

(d) $\implies$ **(a)** If $bK = aK$, then there exist $k_a, k_b \in K$ such that $bk_b = ak_a$. Since $\varphi(k_a) = \varphi(k_b) = 1$, we have

$$\varphi(b) = \varphi(b)\varphi(k_b) = \varphi(bk_b) = \varphi(ak_a) = \varphi(a)\varphi(k_a) = \varphi(a).$$

□

4.3 Index of a subgroup, the Counting Formula

Let H be a subgroup of a group G.

Notation 4.25. The **set** of left cosets of H in G is denoted G/H. (The set of right cosets of H in G is denoted $H\backslash G$.)

Remark 4.26. *Warning:* In general, G/H is a just a set, not a group. We will see that if $G/H = H\backslash G$, then the group operation on G induces a group operation on the set G/H. In this case, H is a *normal subgroup*, and G/H, with the induced operation, is a *quotient group*.

Proposition 4.27. The subgroup $H \leq G$ has the same number of left and right cosets.

Proof. (Proof idea) From each left coset of H, choose a representative. [8] This gives us a fixed set of representatives $\{r_\alpha\}_{\alpha \in G/H}$. Define $\varphi : G/H \to H\backslash G$ by $r_\alpha H \mapsto Hr_\alpha$.

This is well-defined because we made all our choices at the beginning. This is also clearly a bijection, with inverse $\varphi^{-1} : H\backslash G \to G/H$ taking $Hr_\alpha \mapsto r_\alpha H$. □

Definition 4.28. The **index** of H in G, denoted $[G : H]$, is the number ($\in \mathbb{N} \cup \{\infty\}$) of left cosets of H in G.

By Proposition 4.27, we could equally define $[G : H]$ to be the number of right cosets of H in G.

Theorem 4.29. (The Counting Formula) Let $H \leq G$. Then $|G| = |H| \cdot [G : H]$.

Proof. First consider the case where $|G| < \infty$. Since G/H forms a partition of G, and every coset aH contains $|H|$ elements, there are $|G|/|H|$ left cosets in total.

Now suppose $|G| = \infty$. We will check that either $|H|$ or $[G : H]$ must be infinite too. (Note first that $|H|, [G : H]$ are both natural numbers, i.e. ≥ 1.) By way of contradiction, suppose that both $|H|$ and $[G : H] = k$ were finite. From each of the $k = [G : H]$ left cosets of H, we can pick a representative; this gives us a set of representatives $\{a_1, a_2, \ldots, a_k\}$, with each from a different coset. Then $G = \bigcup_{i=1}^{k} a_i H$ contains $k \cdot |H| < \infty$ elements, which is a contradiction. □

Corollary 4.30.

- For $H \leq G$, $|H|$ divides $|G|$, i.e. $|H| \mid |G|$.
- For $g \in G$, $|g|$ divides $|G|$, i.e. $|g| \mid |G|$.

This is useful when classifying groups of a particular finite order.

Example 4.31. Let $|G| = p$ where p is a prime number. For any non-identity $a \in G$. $G = \langle a \rangle$. Therefore there is only one isomorphism (equivalence) class of groups of order p prime.

Corollary 4.32. Let $\varphi : G \to G'$ be a homomorphism.

- $[G : \ker\varphi] = |\operatorname{img}\varphi|$ (Therefore $|G| = |\ker\varphi||\operatorname{img}\varphi|$.)
- $|\ker\varphi| \mid |G|$
- $|\operatorname{img}\varphi| \mid |G|$ and $|\operatorname{img}\varphi| \mid |G'|$.

[8] Using the Axiom of Choice here!

Exercise 4.33. HW04 Let $\varphi : G \to G'$ be a group homomorphism. Suppose that $|G| = 18$ and $|G'| = 15$, and that φ is not the trivial homomorphism. What is the $|\ker \varphi|$?

Example 4.34. Recall that $A_n = \ker \operatorname{sgn}$, where $\operatorname{sgn} : S_n \to \{\pm 1\}$ is the sign homomorphism. Therefore the order of $A_n = \frac{|S_n|}{2} = \frac{n!}{2}$.

Proposition 4.35. If $K \leq H \leq G$, then $[G : K] = [G : H][H : K]$.

Proof. (Proof sketch.) First consider the case where both indices on the right side are finite, and consider partitions of G and H by cosets of H and K, respectively. Then consider the case where at least one of the indices on the right is infinite, and show that $[G : K]$ has to be infinite as well. □

Proposition 4.36. If $\varphi : G \to G'$ is an isomorphism, then the inverse *set* map is also an isomorphism.

Proof. HW05 □

4.4 Conjugation, Normal subgroups

Here is a very important definition:

Definition 4.37. Let $g \in G$.

- **Conjugation** by $g \in G$ is the automorphism $c_g : G \to G$ that sends $x \mapsto gxg^{-1}$. (See Exercise **??**.)
- If $y = gxg^{-1}$, then x and y are **conjugates** of each other. Note that $x = g^{-1}yg$ is obtained by conjugating y by the element g^{-1}.

Exercise 4.38. (Exercise 3.16) HW03 Show that conjugacy is an equivalence relation. The equivalence classes are called **conjugacy classes.**

Exercise 4.39. HW05 Let G be a group, and let $a, b \in G$. Prove that ab and ba are conjugate elements.

Here's another very important definition in this course:

Definition 4.40. A subgroup $H \leq G$ is **normal** if for all $h \in H$, and all $g \in G$, $ghg^{-1} \in H$. If H is a normal subgroup of G, we write $H \trianglelefteq G$.

In other words, a subgroup $H \leq G$ is normal it is closed under conjugation by any element in the whole group G. There are many equivalent ways to say that a subgroup is normal:

Proposition 4.41. Let $H \leq G$. The following are equivalent (TFAE):

(a) H is a normal subgroup of G, i.e. for all $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$.

(b) For all $g \in G$, $gHg^{-1} = H$.

(c) For all $g \in G$, $gH = Hg$.

(d) Every left coset of H in G is also a right coset.

Note: As usual, gHg^{-1} means $\{ghg^{-1} \mid h \in H\}$.

Proof. This is an abridged proof. Make sure you understand the notation gH, Hg, and gHg^{-1} first. Once you are able to work with this kind of notation, the proof of this proposition is quite short.

(a) $\implies$ (b): Suppose $H \trianglelefteq G$. Then for $gHg^{-1} \subset H$ by definition. But $H \subset gHg^{-1}$ as well because $g^{-1}Hg \subset G$.

(b) $\implies$ (a): Now suppose $gHg^{-1} = H$ for all $g \in G$. Let $g \in G$ and $h \in H$. Then $ghg^{-1} \in gHg^{-1} \in H$.

(b) $\iff$ (c) is clear, and (c) $\implies$ (d) is clear.

(d) $\implies$ (c): Suppose every left coset of H is also a right coset, and let $g \in G$. Then gH contains g, and so does Hg, so gH must be the right coset Hg.

□

Remark 4.42. Notice that the proof above was not hard. However, it was important for us to state the proposition as four equivalent statements because we will encounter normal subgroups in a lot of different contexts. Different characterizations will be useful in different contexts.

Exercise 4.43. HW04 Prove that every subgroup of index 2 is a normal subgroup. Show that a subgroup of index 3 need not be normal by exhibiting a counterexample.

Remark 4.44. Here are some immediate observations.

(a) If G is abelian, then any $H \leq G$ is normal.

(b) $\{1\}$ and G are normal in G.

Definition 4.45. The **center** of G, denoted $Z(G)$, is the set of all the elements that commute with every element in G:

$$Z(G) = \{z \in G \mid gz = zg \text{ for all } g \in G\}.$$

We could equivalently define the center to be all the elements that are fixed by conjugation by all elements of G:

$$Z(G) = \{z \in G \mid gzg^{-1} = z \text{ for all } g \in G\}.$$

Kernels of homomorphisms are normal, and this allows us to prove various *isomorphism theorems* later:

Proposition 4.46. If $\varphi : G \to G'$ is a homomorphism, then $\ker \varphi \trianglelefteq G$.

Proof. HW05 □

Exercise 4.47. On the other hand, $\operatorname{img} \varphi$ need not be normal. Prove this by exhibiting a counterexample.

Proposition 4.48.

(a) If $H \leq G$ and $g \in G$, then the set gHg^{-1} is also a subgroup of G.

(b) If G has exactly one subgroup H of order r, then $H \trianglelefteq G$.

Exercise 4.49. Let G be a group of order $|G| = p^r$ where p is prime, and $r \in \mathbb{N}$. Show that G contains a subgroup of order p.

4.5 Aside: Conjugacy classes in S_n

For a permutation $p \in S_n$, the **cycle type** of p is basically the shape of the partition of n that the cycle notation for p creates. This is best described by example:

Example 4.50. The cycle type of $(1\,2)(3\,4\,5)$ in S_7 is $1+1+2+3$, because there are two indices that are fixed (6 and 7), one cycle of size 2, and one cycle of size 3. We usually write the sizes of the blocks in (weakly) ascending order.

Proposition 4.51. The conjugacy classes of S_n are in bijection with the **cycle types**.

Proof. Here is the idea of the proof. Observe that if p sends $i \mapsto j$, then qpq^{-1} sends $q(i) \mapsto q(j)$. So if p has a cycle that looks like

$$(i_1\; i_2\; \cdots\; i_k),$$

then qpq^{-1} has the cycle

$$(q(i_1)\; q(i_2)\; \cdots\; q(i_k)).$$

□

Remark 4.52. Conjugation, whether in the symmetric group or by change-of-basis matrices in linear algebra, is really the algebraic way of describing a *change of perspective.* When we conjugated p by q, all we did was replace the indices in the cycles with their images under q.

Exercise 4.53. Let p and q be permutations in S_n. Prove that pq and qp have cycles of equal sizes.

Exercise 4.54. For each of the following, determine whether σ_1 and σ_2 are conjugate to each other in S_9. If they are conjugate, find a permutation $\tau \in S_9$ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.

(a) $\sigma_1 = (1\ 2)(3\ 4\ 5)$ and $\sigma_2 = (1\ 2\ 3)(4\ 5)$

(b) $\sigma_1 = (1\ 3)(2\ 4\ 6)$ and $\sigma_2 = (3\ 5) \circ (2\ 4)(5\ 6)$

(c) $\sigma_1 = (1\ 5)(7\ 2\ 4\ 3)$ and $\sigma_2 = \sigma_1^{2023}$

Exercise 4.55. Let q be a 5-cycle in S_n, where $n \geq 6$.

(a) What is the cycle type of q^{17}? HW05

(b) In terms of n, how many permutations are there such that $pqp^{-1} = q$?

4.6 Quotient groups

Let $N \trianglelefteq G$. Then $G/N = N\backslash G$, so let's just say *cosets of* N rather than specifying left/right cosets.

Notation 4.56. Let C be a coset of N in G, and say $C = aN$. When we think of C as an element of the set G/N, we may write on of the following:

- $[C] \in G/N$
- $\bar{a} \in G/N$ (i.e. the *equivalence class* of a under the partition by cosets
- $[a]$ (also standard notation for the equivalence class of a)
- abuse notation and write aN, while remembering that we are talking about aN as a single element of a partition, and forgetting about the fact that it's a set itself.

Remark 4.57. Remember that in additive notation, the coset containing a would be written $[C] = \bar{a} = [a] = a + N$.

Just as we have been writing $aN = \{an \mid n \in N\}$, we use similar notation for the product of two subsets of a group G:

Notation 4.58. Let $A, B \subset G$. Then

$$AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\} = \{ab \mid a \in A, b \in B\}.$$

Proposition 4.59. *G/N inherits a group structure from G.*

Proof. Define multiplication in G/N by $(aN)(bN) = (ab)N$. Check that this is well-defined, and observe that this is precisely why we need N to be normal. Check that identity and inverses are also preserved. □

Notation 4.60. Let $\overline{G}$ denote the quotient group G/N under the induced multiplication from G. Let $\pi : G \to \overline{G}$ be the obvious map $G \to G/N$. This is called the **canonical map**.

Theorem 4.61. $\pi : G \to \overline{G}$ *is a surjective homomorphism whose kernel is* N.

Corollary 4.62. *Let $a_1, a_2, \ldots, a_k \in G$ such that $\prod_i a_i = 1$. Then $\prod_i \bar{a}_i = \bar{1}$.*

Exercise 4.63. Suppose $H \leq G$ is not a normal subgroup. Prove that there exist left cosets aH and bH such that their product $(aH)(bH)$ is not a coset of H.

Quotient groups are intimately related to group homomorphisms via the First Isomorphism Theorem below. This is the first of three *Isomorphism Theorems*, and is the most important one for us.

Theorem 4.64. Let $\varphi : G \to G'$ be a surjective group homomorphism with kernel N. The quotient group $\overline{G} = G/N$ is isomorphic to the image G'. In other words, there is a unique isomorphism $\bar{\varphi} : \bar{G} \to G'$ such that the following diagram *commutes:*

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \\
\overline{G} \arrow[ur, "\bar{\varphi}"] &
\end{tikzcd}$$

Corollary 4.65. Let $\varphi : G \to G'$ be *any* group homomorphism with kernel N and image $H' \leq G'$. Then the quotient group $\overline{G} = G/N$ is isomorphic to t he image H'.

One way we use the First Isomorphism Theorem is to identify quotient groups with more familiar groups that we already know about.

Example 4.66. In the following examples, our groups are abelian, and so every subgroup is normal. For the subgroups-group pairs listed, identify the quotient group as a more familiar group.

(a) $3\mathbb{Z} \leq \mathbb{Z}$, more generally $n\mathbb{Z} \leq \mathbb{Z}$

(b) $\mathbb{R}e_1 \leq \mathbb{R}^2$

(c) $S^1 \subset \mathbb{C}^\times$

(d) $\mathbb{R}^+ \subset \mathbb{C}^\times$

Example 4.67. Do the same for these nonabelian groups:

(a) $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

(b) $A_n \leq S_n$

Exercise 4.68. Let $H = \{\pm 1, \pm i\} \leq \mathbb{C}^\times$.

(a) Prove that H is normal in $\mathbb{C}^\times$.

(b) Describe explicitly the cosets of H.

(c) Identify the quotient group $\mathbb{C}^\times/H$. (*Hint:* If you're stuck, first play around with the map $\psi : S^1 \to S^1$ given by $e^{i\theta} \mapsto (e^{i\theta})^2$.)

Exercise 4.69. In the general linear group $GL_3(\mathbb{F})$, consider the subsets

$$H = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{and} \qquad K = \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where $*$ represents an arbitrary element of a field $\mathbb{F}$.

(a) Show that H is a subgroup of $GL_3(\mathbb{F})$. *Hint: First, compute the product*

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}.$$

(b) Show that K is a *normal* subgroup of H.

(c) For $\mathbb{F} = \mathbb{R}$, identify the quotient group H/K (up to isomorphism). *Hint: Let $A, B \in H$. Under what conditions are A and B in the same coset of K? Use this to construct a surjective homomorphism from H.*

Remark 4.70. The subgroup H discussed here is called the *Heisenberg group*, and we can actually define it using elements of commutative rings, not just fields. This version of this group with $\mathbb{F} = \mathbb{R}$ was used by Weyl to give an algebraic interpretation of Heisenberg's Uncertainty Principle.

Exercise 4.71. Recall that the Klein four group is $V = \{1, a, b, ab\} = \langle a, b \mid a^2 = b^2 = [a, b] = 1\rangle \cong C_2 \times C_2$ (see page 47 in the book).

(a) Prove that the subgroup $N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ in S_4 is isomorphic to the Klein four group.

(b) Prove that N is normal in S_4. *Hint: Use a theorem from lecture on Wednesday; do not use brute force!*

(c) Prove that the subgroup $H = \langle(1\ 2), (3\ 4)\rangle \leq S_4$ is also isomorphic to V, but is not a normal subgroup of S_4.

(d) Identify the quotient group S_4/N by computing the cosets. *Hint: Recall that $|S_4| = 4! = 24$; use the counting formula. Either define an isomorphism between S_4/N and your candidate group, or define a surjection from S_4 to your candidate group. You do not need to show me that your map is a homomorphism; just check for yourself that it really is.*

(e) How many subgroups are there in S_4 that contain N? (*Do not solve this by brute force!*)

Exercise 4.72. Let $G = (\mathbb{R}^2, +)$ and let $D \leq G$ denote the set of points on the diagonal:

$$D = \{(x, y) \in \mathbb{R}^2 \mid y = x\}.$$

(a) Briefly explain why $D \trianglelefteq G$.

(b) Use the First Isomorphism Theorem to identify the quotient group G/D with a familiar group.

4.7 Product groups

Here are some harder exercises involving normal subgroups that will become useful when we discuss product groups:

Exercise 4.73. HW05 Let K and H be subgroups of a group G.

(a) Prove that the intersection $K \cap H$ is a subgroup of G.

(b) Prove that if $K \trianglelefteq G$, then $K \cap H \trianglelefteq H$.

Exercise 4.74. HW05 Let H and K be subgroups of G.

(a) Prove that if $HK = KH$, then HK is a subgroup of G.

(b) Prove that if H and K are both *normal* subgroups of G, then their intersection $H \cap K$ is also a *normal* subgroup of G.

Definition 4.75. Let $(A, \star)$ and $(B, \diamond)$ be groups. Then $(A \times B, \cdot)$ is a group under the multiplication rule defined by

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

for $a_i \in A$, $b_i \in B$, $i = 1, 2$.

Exercise 4.76. In this exercise, you will verify all the group axioms for $A \times B$.

(a) Prove that multiplication is associative.

(b) What's the identity element $A \times B$?

(c) What's the inverse of $(a, b) \in A \times B$?

Exercise 4.77. Prove that $A \times B$ is abelian if and only if both A and B are abelian.

The relationships among the groups A, B, and $A \times B$ is captured by the following maps:

$$\begin{tikzcd}
A \arrow[dr, "i_A"] & & A \\
& A \times B \arrow[ur, "p_A"] \arrow[dr, "p_B"] & \\
B \arrow[ur, "i_B"] & & B
\end{tikzcd}$$

Here i_A and i_B are *injections*; p_A and p_B are *projections*.

(You can look up the definition of these terms, but let's not focus on the nuanced definition of injections and projections in general, for now.)

Example 4.78. $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

The argument for $C_6 \cong C_2 \times C_3$ also works for arbitrary cyclic groups of order rs where $\gcd(r, s) = 1$:

Proposition 4.79. Let r and s be relatively prime integers. A cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.

On the other hand, $C_2 \times C_2$ is not a cyclic group; this is the Klein four group.

While building product groups is easy, it's harder to detect whether a given group is a product of two groups. The last part of the following proposition *characterizes* product groups.

Remark 4.80. Pay attention to the techniques used in the proof; the proof of each statement serves as good practice with normal groups.

Proposition 4.81. Let $H, K \leq G$. let $\mu : H \times K \to G$ be the multiplication map $\mu(h, k) = hk$. Its image is the subset

$$HK = \{hk \mid h \in H, k \in K\} \subset G.$$

(a) μ is injective if and only if $H \cap K = \{1\}$.

(b) μ is a homomorphism from the product *group* $H \times K$ to G if and only if elements of K commute with elements of H: $hk = kh$.

(c) If $H \trianglelefteq G$, then $HK \leq G$.

(d) $\mu : H \times K \to G$ is an isomorphism if and only if

- $H \cap K = \{1\}$
- $HK = G$
- $H, K \trianglelefteq G$.

Proof. See Page 65 in the book, Proposition 2.11.4. □

Remark 4.82. The multiplication map is a set map, a priori. It can even be bijective without being a homomorphism. For example, consider the subgroups $\langle(1\ 2)\rangle$ and $\langle(1\ 2\ 3)\rangle$ inside S_3.

Remark 4.83. If $G = H \times K$, what is the quotient group G/K?

Exercise 4.84. HW06 Let G be a group of order 21. Suppose it contains two *normal* subgroups K and N, where $|K| = 3$ and $|N| = 7$. Prove that $G \cong K \times N$.

4.8 Correspondence Theorem

Let $\varphi : G \to \mathcal{G}$ be a group homomorphism, and let $H \leq G$.

We may **restrict** φ to a homomorphism

$$\begin{aligned} \varphi|_H : H &\to \mathcal{G} \\ h &\mapsto \varphi(h) \end{aligned}$$

- $\ker(\varphi|_H) = (\ker \varphi) \cap H$
- $\operatorname{img}(\varphi|_H) = \varphi(H)$

Remark 4.85. Since $\varphi|_H$ is a homomorphism, the order of the image $\varphi(H)$ divides both $|H|$ and $|\mathcal{G}|$. If $|H|$ and $|\mathcal{G}|$ have no common factors, then $H \leq \ker \varphi$.

Example 4.86. Recall A_n is the kernel of the sign homomorphism $\sigma : S_n \to \pm 1$.

Let q be a permutation with odd order, and let $H = \langle q \rangle$. Then $H \leq A_n$.

Proposition 4.87. Let $\varphi : G \to \mathcal{G}$ be a homomorphism with kernel K. Let $\mathcal{H} \leq \mathcal{G}$, and let $H = \varphi^{-1}(\mathcal{H})$.

1. Then $K \leq H \leq G$. *(A chain of subgroups.)*
2. If $\mathcal{H} \trianglelefteq \mathcal{G}$, then $H \trianglelefteq G$.
3. If φ is surjective and $H \trianglelefteq G$, then $\mathcal{H} \trianglelefteq \mathcal{G}$.

Proof.
1. *Check carefully; note that φ^{-1} means* preimage.
2. Suppose $\mathcal{H} \trianglelefteq \mathcal{G}$. Let $x \in H, g \in G$. Then $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in \mathcal{H}$ because $\mathcal{H} \trianglelefteq \mathcal{G}$.
3. Suppose φ is surjective and $H \trianglelefteq G$. Let $a \in \mathcal{H}, b \in \mathcal{G}$. Since φ is surjective, there exist elements $x \in H, y \in G$ such that $\varphi(x) = a$, $\varphi(y) = b$. Since H is normal, $yxy^{-1} \in H$, so $\varphi(yxy^{-1}) = bab^{-1} \in \mathcal{H}$.

□

Example 4.88. Consider $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$. Since $\mathbb{R}^\times$ is abelian, $\mathbb{R}^\times_{>0} \trianglelefteq \mathbb{R}^\times$. The preimage under $\det$ of the positive reals is the set of invertible matrices with positive determinant, and is therefore a normal subgroup of $GL_n(\mathbb{R})$.

Theorem 4.89. (The Correspondence Theorem) Let $\varphi : G \to \mathcal{G}$ be a *surjective* group homomorphism with kernel K. Then there is a bijective correspondence

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow \{\text{subgroups of } \mathcal{G}\}.$$

The correspondence is given by

$$\mathcal{H} \rightsquigarrow \varphi^{-1}(\mathcal{H}).$$

Suppose H and $\mathcal{H}$ are corresponding subgroups. Then:

- $H \trianglelefteq G$ if and only if $\mathcal{H} \trianglelefteq \mathcal{G}$.
- $|H| = |\mathcal{H}||K|$.

Proof. Here are the things to check:

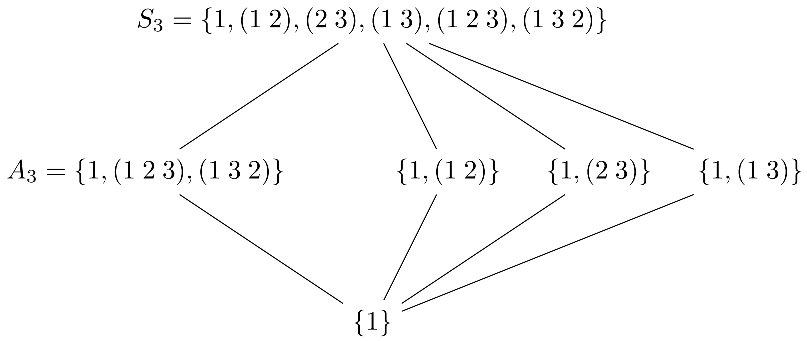
1. $\varphi(H)$ is a subgroup of $\mathcal{G}$
2. $\varphi^{-1}(\mathcal{H})$ is a subgroup of G, and it contains K
3. $\mathcal{H} \trianglelefteq \mathcal{G}$ if and only if $\varphi^{-1}(\mathcal{H}) \trianglelefteq G$
4. *Bijectivity of the correspondence:* $\varphi(\varphi^{-1}(\mathcal{H})) = \mathcal{H}$ and $\varphi^{-1}\varphi(H) = H$.
5. $|\varphi^{-1}(\mathcal{H})| = |\mathcal{H}||K|$.

□

Exercise 4.90. Let $\varphi : G \to G'$ be a surjective homomorphism between finite groups. Suppose $H \leq G$ and $H' \leq G'$ correspond to each other under the bijection in the Correspondence Theorem. Prove that $[G : H] = [G' : H']$.

Exercise 4.91. Let C_{12} be generated by x and let C_6 be generated by y. Consider the surjective homomorphism $\varphi : C_{12} \to C_6$ determined by $x \mapsto y$. Explicitly write down the correspondence between subsets given by the Correspondence Theorem. *If you are claiming a group G has k subgroups, you must explain (briefly) why you've found all of them.*

Example 4.92. Here's a diagram of the subgroup structure of S_3:


$S_3 = \{1, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$
$A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$
$\{1, (1\,2)\}$
$\{1, (2\,3)\}$
$\{1, (1\,3)\}$
$\{1\}$

5 Symmetries of plane figures

5.1 Distance in $\mathbb{R}^2$

We can think of the additive group $\mathbb{R}^2$ as a group of vectors or a group of points in the plane. In any case, Euclidean distance gives us a notion of distance between two elements $\vec{x}, \vec{y} \in \mathbb{R}^2$:

$$d(\vec{x}, \vec{y}) = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2}.$$

This distance function is actually induced by the dot product, as follows.
Recall that for $\vec{v}, \vec{w} \in \mathbb{R}^2$, the *dot product* of $\vec{v}$ and $\vec{w}$ is

$$\vec{v} \cdot \vec{w} = v_1 w_1 + v_2 w_2.$$

The length of the vector $\vec{v}$, or the *norm* of $\vec{v}$ is given by

$$\|\vec{v}\| = \sqrt{v \cdot v} = \sqrt{v_1^2 + v_2^2}.$$

Given vectors $v, w \in \mathbb{R}^2$ (thought of as points in $\mathbb{R}^2$), the distance between v and w is

$$d(v, w) = \|w - v\| = \|v - w\|.$$

Now consider a linear map $A : \mathbb{R}^2 \to \mathbb{R}^2$. If we choose choose a basis for the domain and codomain, we can write A as a matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Let $\vec{a}_1$ denote the first column vector and let $\vec{a}_2$ denote the second column vector.

Exercise 5.1. Check that $Ae_i = a_i$ for $i = 1, 2$.

Any vector $\vec{v} \in \mathbb{R}^2$ can be written as a linear combination of the standard basis vectors e_1 and e_2 (because $\{e_1, e_2\}$ is a *basis*):

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = v_1 e_1 + v_2 e_2.$$

Since A is a *linear map*, we have

$$A\vec{v} = A(v_1 e_1 + v_2 e_2) = v_1 A e_1 + v_2 A e_2 = v_1 a_1 + v_2 a_2.$$

In other words, the linear map A is determined by its value on the basis vectors e_1 and e_2.

5.2 The Orthogonal Group $O(2)$

When does a linear map $A : \mathbb{R}^2 \to \mathbb{R}^2$ preserve distances, i.e.

$$d(x, y) = d(Ax, Ay)?$$

Intuitively, this should be the linear maps that rigidly rotate or reflect the plane, without any squeezing or stretching. In particular, this means that the standard basis vectors e_1 and e_2 are sent to vectors a_1 and a_2 which are still unit vectors that are orthogonal to each other.

Definition 5.2. Two vectors $a_1, a_2 \in \mathbb{R}^2$ are orthonormal if

- $a_1 \cdot a_2 = 0$ (i.e. $a_1 \perp a_2$)
- $\|a_1\| = \|a_2\| = 1$ (i.e. a_1 and a_2 are *unit vectors*, i.e. vectors of length 1)

Definition 5.3. A matrix $A = [a_1\ a_2]$ is **orthogonal** if its columns $\{a_1, a_2\}$ are orthonormal.

Definition 5.4. The **orthogonal group** $O(2)$ is the group of orthogonal 2×2 matrices.

Exercise 5.5. Prove that if A is orthogonal, then A preserves distances.

It turns out that the converse is also true: 2×2 matrices that preserve distance are orthogonal.

We now discuss what $O(2)$ looks like as a group. Let

$$\rho_\theta := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

denote rotation by θ about the origin (counter-clockwise, of course). Let

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

denote reflection across the e_1-axis.

Fact 5.6. Any matrix in $O(2)$ is either of the form ρ_θ or $\rho_\theta \tau$.

- The set of orthogonal matrices that are just simple rotations $\{\rho_\theta \mid \theta \in [0, 2\pi)$ is the set of *orientation-preserving* orthogonal matrices. In other words, the matrix takes the "front" of the plane to the "front".
- On the other hand, the set of orthogonal matrices that are rotations composed with a reflection are *orientation-reversing*; they take the "front" of $\mathbb{R}^2$ to the "back".

This fact tells us that orthogonal actions such as reflection about a line that is *not* the e_1-axis can be written as the product of a rotation and the reflection τ.

Here are two important subgroups of $O(2)$:

- $S^1 \cong$ the set of rotations = $\{\rho_\theta \mid \theta \in [0, 2\pi)$ (We originally defined S^1 as a subgroup of $\mathbb{C}^\times$; notice that there is an isomorphism between this group of rotation matrices and S^1 the subgroup of $\mathbb{C}^\times$.)
- $\mathbb{Z}/2\mathbb{Z} \cong \langle \tau \rangle$, the order 2 cyclic subgroup generated by the reflection τ. (Notice that $\tau = \tau^{-1}$.)

Exercise 5.7. Prove that $S^1 \trianglelefteq O(2)$. Solution: S^1 has index 2.

5.3 $O(2)$ is a semi-direct product

Temporarily write $N = S^1$ and $H = \mathbb{Z}/2\mathbb{Z}$. Even though Fact 5.6 tells us that $G = NH$ as a set, $O(2)$ is **not** the direct product of the subgroups N and H. This is because the elements of N and H don't commute! We already saw this when we looked at dihedral groups, which are themselves subgroups of $O(2)$: for any rotation ρ,

$$\rho\tau\rho\tau = 1 \implies \tau\rho\tau = \rho^{-1}.$$

Therefore if $\rho \neq \rho^{-1}$, then conjugation by τ does not fix ρ.

However, all is not lost, because $N \trianglelefteq O(2)$. It turns out that $O(2)$ is a *semi-direct product* of S^1 and $\mathbb{Z}/2\mathbb{Z}$.

Definition 5.8. Let G be a group, and let $N, H \leq G$. If $N \trianglelefteq G$, $G = NH$, and $N \cap H = \{1\}$, then G is a **semi-direct product** of N and H. This is written

$$G = N \rtimes H.$$

Remark 5.9. This is not a definition I necessarily want you to memorize; I just want to show you how similar the conditions are to those in the proposition characterizing product groups.

The underlying set of $N \rtimes H$ is still the Cartesian product $N \times H$; however, multiplication is *twisted* by conjugation. Let $(n, h), (m, k) \in N \times H$ (as a set). Then their product in the semi-direct product $N \rtimes H$ is

$$(n, h) \cdot (m, k) = (nc_h(m), hk)$$

where $c_h(m) = hmh^{-1} \in N$ is the conjugation of m by h. (This is where we need N to be normal in G.)

The multiplication formula might seem unnatural, but the following computation should hopefully convince you that, if you already know N, H were subgroups of a bigger group G where we already have multiplication, then the formula above is very natural.

Recall that $G = NH$, so every element can be written in the for nh for $n \in N$, $h \in H$. Let $n_1h_1, n_2h_2 \in NH = G$. Their product in G is

$$(n_1h_1)(n_2h_2) = n_1h_1n_2h_2.$$

We wish to move the n_2 to the left of the h_1 in order to write the product in the form nh. To do this, we can rewrite our product:

$$n_1h_1n_2h_2 = n_1h_1n_2(h_1^{-1}h_1)h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1c_{h_1}(n_2)h_1h_2 \in NH.$$

In other words, **the cost of commuting n_2 past h_1 is conjugation by h_1.**

Fact 5.10. $O(2) = S_1 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Let $\rho_\alpha a$ and $\rho_\beta b$ be two elements in $O(2)$, where $\rho_\alpha, \rho_\beta \in S_1$ and $a, b \in \{1, \tau\} = \mathbb{Z}/2\mathbb{Z}$. Then multiplication in $O(2)$ is given by

$$(\rho_\alpha a)(\rho_\beta b) = \rho_\alpha c_a(\rho_\beta)ab.$$

Notice that if $a = 1$, then conjugation by a does nothing (and we might as well have written $\rho_\alpha a\rho_\beta b$ as $\rho_\alpha\rho_\beta b$, which is already in the form we like).

On the other hand, if $a = \tau$, then $c_a(\rho_\beta) = \rho_\beta^{-1} = \rho_{-\beta}$.

Example 5.11. To drive this idea home, let's compute the product of these two orientation-reversing elements of $O(2)$:

$$\begin{aligned}(\rho_\alpha\tau)(\rho_\beta\tau) &= \rho_\alpha(\tau\rho_\beta\tau^{-1})(\tau\tau)\\ &= \rho_\alpha\rho_{-\beta}\tau^2\\ &= \rho_{\alpha-\beta}.\end{aligned}$$

The result is a rotation by an angle $\alpha - \beta$. (Try it!)

5.4 Isometries of the plane

Definition 5.12. A function $f : \mathbb{R}^2 \to \mathbb{R}^2$ is an **isometry** if it preserves distances:

$$d(p,q) = d(f(p), f(q)) \quad \text{for all points } p, q \in \mathbb{R}^2$$

Let $\mathrm{Isom}(\mathbb{R}^2)$ denote the group of isometries of $\mathbb{R}^2$.

We think of isometries of $\mathbb{R}^2$ as **symmetries** of the plane. In particular, we can study the symmetries of the plane by studying symmetries of **plane figures**. These are subsets of the plane, such as the drawing of a stick figure. (See the book for pictures of various symmetries of plane figures.)

Fact 5.13. $\mathrm{Isom}(\mathbb{R}^2)$ is *generated* by the following elements. Let x be a point in $\mathbb{R}^2$:

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

- **Translations**: for a translation vector $v \in \mathbb{R}^2$, and a point $x \in \mathbb{R}^2$,

$$t_v(x) = x + v.$$

- **Rotations**: for an angle $\theta \in S^1$ and a point $x \in \mathbb{R}^2$,

$$\rho_\theta(x) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

- **Reflection across the e_1-axis**: for a point $x \in \mathbb{R}^2$,

$$\tau(x) = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$$

Remark 5.14. Warning: The points in $\mathbb{R}^2$ are those being moved around by the isometries. The translations vectors $v \in \mathbb{R}^2$ are **not** the same as the points in the plane. You should think of them as velocity vectors.

Proposition 5.15. The subgroup of translations $T = \{t_v \mid v \in \mathbb{R}^2\} \leq \mathrm{Isom}(\mathbb{R}^2)$ is normal.

Proof. For any $g \in \mathrm{Isom}(\mathbb{R}^2)$, we need to show that $g t_v g^{-1}$ is also a translation. It suffices to just check the cases where g is a generator, since every isometry is a composition of these.

First check that T is a subgroup; then the conjugation of t_v by any translations is necessarily also a translation.

Next, let $g = \rho_\theta$, and let $c = \cos\theta$ and $s = \sin\theta$. The rotation matrix for ρ_θ and $\rho_\theta^{-1} = \rho_{-\theta}$ are

$$\rho_\theta = \begin{bmatrix} c & -s \\ s & c \end{bmatrix} \qquad \text{and} \qquad \rho_{-\theta} = \begin{bmatrix} c & s \\ -s & c \end{bmatrix}$$

respectively. (Use the fact that cosine is an even function, and sine is an odd function.) Compute that

$$\rho_\theta t_v \rho_{-\theta} = t_{\rho_\theta v}.$$

Third, let $g = \tau$. Compute that

$$\tau t_v \tau = t_{\tau v}.$$

□

Exercise 5.16. HW07 We used $\mathbb{R}^2$ to describe the points on the plane. We could equivalently use $\mathbb{C}$, the complex plane. Since we use the same notion of distance for points in the complex plane, as metric spaces, $\mathbb{R}^2$ is the same as $\mathbb{C}$. Write formulas for the generators of $\mathrm{Isom}(\mathbb{C})$ in terms of the complex variable $z = x+iy$.

5.5 Connecting the geometry with the algebra

Question 5.17. Let ℓ be the line of reflection of the isometry $\rho_\theta\tau \in O(2)$. What is the the angle the line ℓ makes with the e_1-axis?

Let's use polar coordinates; we will represent points in the plane as points in the complex plane. Let $re^{i\alpha} \in \mathbb{C}$. Then

$$\rho_\theta\tau(re^{i\alpha}) = \rho_\theta(re^{i\alpha}) = re^{-i\alpha} \cdot e^{i\theta} = re^{i(\theta-\alpha)}.$$

In other words, the reflection $\rho_\theta\tau$ swaps the positions of the two points

$$re^{i\alpha} \leftrightarrow re^{i(\theta-\alpha)}.$$

Hence the angle that the mirror line ℓ makes an angle of

$$\frac{\alpha + (\theta - \alpha)}{2} = \frac{\theta}{2}$$

with the e_1-axis.

Exercise 5.18. Check that the points on the line ℓ are indeed fixed by the reflection $\rho_\theta\tau$.

Question 5.19. Let $g = t_a\rho_\alpha\tau$ be a glide reflection.

(a) What is the angle that the line of reflection makes with the e_1-axis?

(b) What is the **glide vector** v?

Notice that translations do not affect the angle that the line of reflection makes with the horizontal axis. To answer (a), let $\bar{g} = \rho_\alpha\tau$ be the part of g in $O(2)$. *(We will talk more about g vs. $\bar{g}$ when we talk about discrete subgroups of* $\mathrm{Isom}(\mathbb{R}^2)$*.)* By the previous exercise, we know the line of reflection makes an angle of $\alpha/2$ with the e_1-axis.

To answer (b), we first observe that g^2 *is just a translation*, specifically by *twice the glide vector*, $2v$. So we first compute g^2, using our knowledge of the semi-direct product structures of $\mathrm{Isom}(\mathbb{R}^2)$ and $O(2)$:

$$g^2 = (t_a\rho_\alpha\tau)(t_a\rho_\alpha\tau) = t_a(\rho_\alpha\tau)t_a(\rho_\alpha\tau) = t_a t_{\rho_\alpha\tau(a)}(\rho_\alpha\tau)(\rho_\alpha\tau) = t_{a+\rho_\alpha\tau(a)}.$$

Therefore the glide vector for g is $v = \frac{1}{2}(a + \rho_\alpha\tau(a))$.

Exercise 5.20. HW07 Prove that a conjugate of a glide reflection in $\mathrm{Isom}(\mathbb{R}^2)$ is also a glide reflection, and that the glide vectors have the same length.

5.6 Discrete subgroups of $\mathrm{Isom}(\mathbb{R}^2)$

Let $H \le \mathrm{Isom}(\mathbb{R}^2)$.

- H contains an arbitrarily small translation if, for any $\varepsilon > 0$, there is a translation $t_v \in H$ such that $0 < |v| < \varepsilon$.
- Similarly, H contains arbitrarily small rotations if, for any $\varepsilon > 0$, there is a rotation $\rho_\theta \in H$ such that $0 < |\theta| < \varepsilon$.

Definition 5.21. A group G of isometries of the plane (i.e. $G \le \mathrm{Isom}(\mathbb{R}^2)$) is **discrete** if it does not contain arbitrarily small translations or rotations.

In other words, G is **discrete** if there exists a real number ε such that

- if $t_v \in G$ and $v \neq 0$ (i.e. $t_v \neq \mathrm{id}$), then $|v| > \varepsilon$, and
- if $\rho_\theta \in G$, where $\theta \in [-\pi, \pi)$, then $|\theta| \ge \varepsilon$.

Given a discrete group of isometries $G \le \mathrm{Isom}(\mathbb{R}^2)$, we will study the following subgroups:

- the **translation group** $L \leq G$, a subgroup of the group of translations $T \leq \mathrm{Isom}(\mathbb{R}^2)$
- the **point group** $\overline{G}$, a subgroup of the orthogonal group $O(2) \leq \mathrm{Isom}(\mathbb{R}^2)$.

Exercise 5.22. Explain why, in the setup above, $G \cong L \rtimes \overline{G}$.

The following theorem classifies all possible translation groups:

Theorem 5.23. Every discrete subgroup $L \leq T \cong \mathbb{R}^2$ is one of the following:

- the zero group: $L = \{0\}$
- the set of integer multiples of a nonzero vector a: $L = \mathbb{Z}a$
- the set of integer combinations of two linearly independent vectors a and b: $L = \mathbb{Z}a + \mathbb{Z}b$. *Groups of this type are called **lattices**.*

Proof. We will use the following Lemma, which describes some fairly intuitive geometric properties of discrete sets of points/vectors in the plane.

Lemma 5.24. Let D be a discrete set of points in the plane, i.e. there is some $\varepsilon > 0$ such that, for all points $p \neq q$ in D, $d(p, q) \geq \varepsilon$.

(A) A bounded region of the plane contains only finitely many points in D.

(B) If $D \neq \{0\}$, then it contains a non-origin point of minimal distance from the origin.

Recall the difference between infimum and minimum from Mat 108.

Remark 5.25. When we say *minimal length* vector in $L \leq \mathbb{R}^2$, we mean a *nonzero* vector of minimal length.

We now work in cases, at times describing the elements of L as points or as vectors, as needed in context.

Case 0: L is the trivial subgroup Let L be a discrete subgroup L of $\mathbb{R}^2$. If $L = \{0\}$, then we are done.

Case 1: L lies on a line through the origin Now suppose L is not just the trivial subgroup, and all points lie on a line ℓ. (This line must necessarily go through the origin, which is the identity element in L.) Let a be a minimal length vector in L; we want to show that $L = \mathbb{Z}a$. Suppose by way of contradiction that there is some vector b that is not an integer multiple of a. Let ka be a multiple of a that is closest to b. Then $b - ka$ is a nonzero vector of length shorter than a. This is a contradiction to the minimality of a.

Case 2: L is none of the above We now use the same idea we used in Case 1, but obtain two "short" vectors that are linearly independent. First let a be a minimal length vector. Since L does not lie on a line, $L - \mathbb{Z}a$ is nonempty and still discrete, so we can find a vector b that is minimal length in $L - \mathbb{Z}$. We want to show that $L = \mathbb{Z}a + \mathbb{Z}b$. Suppose there is some vector $c \in L$ that is not a linear combination of a and b. Then c lies inside a parallelogram whose vertices are the lattice $\mathbb{Z}a + \mathbb{Z}b$. Let $ia + jb$ be a lattice point closest to c. Then the vector $c - (ia + jb)$ is shorter than b, which contradicts the minimality of b in $L - \mathbb{Z}a$. *(Draw a picture!)*

□

The following proposition basically tells us that if we view $p \in L$ as the result of translating the origin by t_p, that if $\bar{g}$ is in the point group, the point $\bar{g}(p)$ will also be a point in the lattice L (i.e. a translation of 0 by something in L).

Proposition 5.26. Let G be a discrete subgroup of $\mathrm{Isom}(\mathbb{R}^2)$. Let a be an element of its translation group L, and let $\bar{g}$ be an element of its point group $\overline{G}$. Then $\bar{g}(a) \in L$.

Proof. To show that $\bar{g}(a) \in L$, we just need to show that $t_{\bar{g}(a)} \in G$. Indeed, we showed previously that $t_{\bar{g}(a)} = g t_a g^{-1} \in G$. □

It's worth taking some time to really absorb what the above proposition is saying, while looking at a wallpaper pattern. They key to fully understanding the proposition is to make sure you're clear on the separation between *isometries* of $\mathbb{R}^2$ (which are symmetries of the wallpaper) and the points in the plane themselves (which we get from picking a particular point on the wallpaper and moving it around).

With the above proposition, we can now describe point groups of discrete subgroups $G \le \mathrm{Isom}(\mathbb{R}^2)$ by studying symmetries of lattices Λ that take the form of a rotation or reflection in $O(2)$.

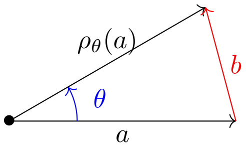
The following theorem classifies all possible point groups:

Theorem 5.27 (Crystallographic Restriction)**.** Let Λ be a **discrete** subgroup of $\mathbb{R}^2$, and let $\mathrm{Sym}(\Lambda) \le \mathrm{Isom}(\mathbb{R}^2)$ denote the group of symmetries of Λ.

Let $H \le O(2) \cap \mathrm{Sym}(\lambda)$, and suppose that $\Lambda \ne \{0\}$. Then

1. every rotation in H has order 1,2,3,4, or 6, and
2. H is one of the groups C_n or D_n, where $n \in \{1, 2, 3, 4, 6\}$.

Proof. It suffices to prove (a). Let ρ_θ be a rotation in H. Let $a \in \Lambda$ be a *minimal length* translation vector $t_a \in \mathrm{Sym}(\Lambda)$. Then $\rho_\theta t_a = t_{\rho_\theta(a)} \in \mathrm{Sym}(\Lambda)$, so $\rho_\theta(a) \in \Lambda$. Let $b = \rho(a) - a$:

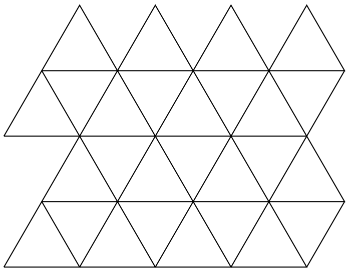


From the figure, we see that $\|b\| < \|a\|$ if $\theta < \pi/3$. So by minimality of a, we must have $\theta \ge \pi/3$. Therefore $|\rho_\theta| \le 6$.

We can easily construct lattices Λ with symmetries ρ_θ of order $1, 2, 3, 4, 6$. *Try this yourself.*

It remains to show that $\theta = 2\pi/5$ is *impossible*. Let $\phi = 2\pi/5$. If $\rho_\phi \in H$, then $b = \rho_\phi^2(a) + a \in \Lambda$ as well. But then b is shorter than a, which again contradicts the minimality of a. *Use trigonometric functions to prove this for yourself!* $e^{\frac{4\pi i}{5}} \approx -.81 + .59i$ □

Exercise 5.28. HW08 Let G denote the group of symmetries of the following **infinite** wallpaper pattern P constructed from equilateral triangles of side length 1:



(a) Determine the point group $\overline{G}$ of G, and find the index in G of the subgroup of translations L.

(b) Find translation vectors $a, b \in \mathbb{R}^2$ realizing L as the lattice $\mathbb{Z}a + \mathbb{Z}b$.

6 Group actions

Definition 6.1. A **group action** (or **group operation**) is a map $G \times S \to S$, $(g, s) \mapsto g * s$, where G is a group and S is a set, satisfying the following axioms:

(a) $1 * s = s$ for all $s \in S$

(b) (*associative law*) $(gg') * s = g * (g' * s)$ for all $g, g' \in G$ and $s \in S$.

A few remarks:

- We say G *acts on* S, and write $G \curvearrowright S$.
- We often omit the $*$ notation and just write gs for $g * s$. With this notation, the axioms are $1s = s$ and $(gg')s = g(g's)$.
- For each $g \in G$, we get a map $m_g : S \to S$ given by $s \mapsto gs$.

Example 6.2. Let $[n]$ denote the set of indices $\{1, 2, \cdots, n\}$. Then the symmetric group S_n acts on $[n]$.

Here is a more visual example. Let S^2 be the surface of a globe (a *sphere*). We can let $G = S^1, \mathbb{Z}/n\mathbb{Z}$ act on S^2 by rotation about the axis of the globe. Keep this example in mind as we discuss the rest of this section.

Definition 6.3. Let $G \curvearrowright S$, and fix $s \in S$. The **orbit** of s is

$$O_s = \{s' \in S \mid s' = gs \text{ for some } g \in G\} = \{gs \mid g \in G\}.$$

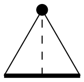
- The orbit of s is the set of elements in S that we can get to by acting on s by an element of g.
- The orbits for a group action are equivalences for the equivalence relation $s \sim s'$ if $s' = gs$ for some $g \in G$.
- Thus, the orbits of the action $G \curvearrowright S$ partition the set S.
- The group acts independently on each orbit.

Example 6.4. Let $G = \text{Isom}(\mathbb{R}^2)$, and let S be the set of triangles in $\mathbb{R}^2$. The orbit of a given triangle T is the set of all triangles congruent (same angles and same side lengths).

Definition 6.5. Let $G \curvearrowright S$, and fix $s \in S$. The **stabilizer** of s is teh set of group elements that leave s fixed:

$$G_s = \{g \in G \mid gs = s\}.$$

This is a subgroup of G. Check this yourself!

Example 6.6. Consider the action of D_3 on an equilateral triangle. Stabilizer of a vertex, an edge, and a perpendicular bisector are all C_2:  The stabilizer of the center of the triangle is the rotation subgroup C_3.

Definition 6.7. Let $G \curvearrowright S$.

- If S consists of one orbit, then the action of G on S is **transitive**.
- If $gs = s$ implies that $g = 1$, then the action of G on S is **free**.

Remark 6.8. An action $G \curvearrowright S$ is called **faithful** if the only $g \in G$ such that $gs = s$ *for all* s is $g = 1$. Notice that **free** $\implies$ **faithful**.

Example 6.9.
- (not free, not transitive) rotation action of $\mathbb{Z}/3\mathbb{Z}$ on the globe
- (not free, transitive) defining action of $\text{Isom}(\mathbb{R}^2)$ on $\mathbb{R}^2$
- (free, not transitive) $H =$ subgroup of $T \leq \text{Isom}(\mathbb{R}^2)$ of horizontal translations
- (free, transitive) action of G on G by left multiplication: $\mu : G \times G \to G$

Remark 6.10. Make sure you're very clear about what set your group is acting on.

Exercise 6.11. It's obvious that the action of G is transitive on each orbit of the action $G \curvearrowright S$. Why?

Exercise 6.12. Suppose a group G **acts freely** on a set S (i.e. the group action $G \curvearrowright S$ is free). Prove that for any $s \in S$, the stabilizer G_s is the trivial subgroup of G.

Proposition 6.13. Let $G \curvearrowright S$, $s \in S$, and $G_s =$ stabilizer of s.

(a) If $a, b \in G$, then $as = bs$ iff $a^{-1}b \in G_s$, iff $b \in aG_s$.

(b) Suppose $s' = as$. Then $G_{s'}$ is a **conjugate subgroup** to G_s:

$$G_{s'} = aG_sa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in G_s\}$$

Proof. (a) Clear: $as = bs$ iff $a^{-1}bs = s$.

(b) Show double inclusion.

($G_{s'} \supseteq aG_sa^{-1}$) If $g \in aG_sa^{-1}$, then $g = aha^{-1}$ for some $h \in G_s$. Then $gs' = (aha^{-1})(as) = ahs = as = s'$.

($G_{s'} \subseteq aG_sa^{-1}$) Since $s = a^{-1}s'$, $a^{-1}G_{s'}a \subseteq G_s$ by the same argument.

□

Exercise 6.14. HW09 Does the rule $P * A = PAP^{\top}$ define an operation of GL_n on $M_{n\times n}$, the set of $n \times n$ matrices? *Here, $P^{\top}$ is the transpose of the matrix $P \in GL_n$.*

Exercise 6.15. HW09 Let $G = GL_n(\mathbb{R})$ act on the set $V = \mathbb{R}^n$ by left multiplication.

(a) Describe the decomposition of V into orbits for this action.

(b) What is the stabilizer of e_1?

(c) Is this action of G on $V - \{0\}$ free, transitive, both, or neither?

6.1 The action of G on cosets of $H \leq G$

Let H be a subgroup of G (not necessarily normal). Then G acts on the set of left cosets G/H of H in a *natural* way, i.e. in an obvious or canonical way:

$$g * [aH] = [gaH].$$

Observe that

- This action is transitive. Why?
- The stabilizer of the coset $[H]$ is the subgroup H. Why?

Example 6.16. Let $G = D_3 = \{1, \rho, \rho^2, \tau, \rho\tau, \rho^2\tau\}$, and let $H = \langle\tau\rangle = \{1, \tau\}$.
The left cosets of H are

$$H = \{1, \tau\} \qquad \rho H = \{\rho, \rho\tau\} \qquad \rho^2 H = \{\rho^2, \rho^2\tau\}$$

To understand how G acts on G/H, we just need to know how the generators ρ and τ act on G/H. (Why?)

- $\rho*$ sends $H \mapsto \rho H \mapsto \rho^2 H \mapsto H$
- $\tau*$ sends $H \mapsto H$, $\rho H \leftrightarrow \rho^2 H$

In other words, if we label the three cosets $H, \rho H, \rho^2 H$ as C_1, C_2, C_3 respectively, then the action of ρ is $(1\ 2\ 3)$ on the indices, and the action of τ is $(2\ 3)$ on the indices.

6.2 Orbit-stabilizer theorem

Proposition 6.17. Suppose a group G acts on a set S. Let $s \in S$. Let G_s denote the stabilizer of s, and let O_s denote the orbit of s.

There is a bijective map (of sets!)

$$\begin{aligned} \varepsilon : G/G_s &\to O_s \\ [aG_s] &\mapsto as \end{aligned}$$

that respects the action of G on both sides, i.e.

$$\varepsilon(g[C]) = g\varepsilon([C])$$

for every coset C and every element $g \in G$. (We say that the map ε is G-**equivariant**.)

Proof. For the purposes of this proof, we let $H = G_s$.

First, we need to show that ε is well-defined. Suppose $aH = bH$; we need to show that $as = bs$. Since $a \in bH$, there is some $h \in H$ such that $a = bh$. Since $h \in H = G_s$ fixes s, $as = bhs = bs$.

Second, we show that ε is injective. If $\varepsilon(aH) = \varepsilon(bH)$, then $as = bs$, so $b^{-1}as = b^{-1}bs = 1s = s$. Then $b^{-1}a \in H$, so $aH = bH$ indeed.

Third, we show that ε is surjective. If $s' \in O_s$, then there is some $g \in G$ such that $s' = gs$. Then $\varepsilon(gH) = gs = s'$.

Finally, we need to check that ε is G-equivariant. Let $g \in G$, and let $[aH] \in G/H$. Then

$$\varepsilon(g[aH]) = \varepsilon([gaH]) = gas = g(as) = g\varepsilon([aH]).$$

□

Example 6.18. Here are some examples illustrating the Orbit-Stabilizer Theorem for transitive actions.

1. Consider the action of D_5 on the vertices V of a regular pentagon. Let $v \in V$ and let H be the stabilizer of v. Then thre is a bijection
$$\varepsilon : D_5/H \to V$$
since the orbit of v is all of V.

2. Consider $\mathrm{Isom}(\mathbb{R}^2) \curvearrowright \mathbb{R}^2$. The stabilizer of the origin is O_2. The orbit of the origin is the entire plane. So there is a bijection between $T \cong \mathrm{Isom}(\mathbb{R}^2)/O(2)$ and $\mathbb{R}^2$. (Recall that T was the normal subgroup of translations.)

3. Let $\mathcal{L}$ denote the set of all lines in $\mathbb{R}^2$. There is an induced action by $\mathrm{Isom}(\mathbb{R}^2)$. For $L \in \mathcal{L}$, let H_L denote the stabilizer of L. Then $\mathrm{Isom}(\mathbb{R}^2)/H_L \leftrightarrow \mathcal{L}$.

Exercise 6.19. On the other hand, consider the non-transitive action of $H = \langle \tau \rangle \leq D_5$ on the vertices V of a pentagon. There are three orbits. Exhibit the bijective map ε for all three of these orbits.

Exercise 6.20. Exhibit the bijective map ε from the orbit-stabilizer theorem explicitly, for the case where G is the dihedral group D_4 and S is the set of vertices of a square.

The Orbit-Stabilizer Theorem is very often used to count things. Recall that the Counting Formula tells us

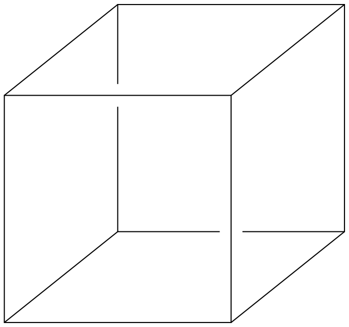
$$|G| = |H||G/H|.$$

In terms of group actions, we have yet another version of the counting formula.

Observation 6.21 (Counting Formula)**.** Let S be a finite set on which G acts. Let $s \in S$. By the Orbit-Stabilizer Theorem,

$$|G| = |G_s||O_s|.$$

Here is an example that illustrates we can use this formula to determine the size of a symmetry group. Consider a cube:



Question 6.22. How big is the set of orientation-preserving symmetries of the cube?

First, a couple of remarks:

1. To rephrase this in terms of abstract algebra, we first note that the set of symmetries is actually a group. So, we can rephrase this question as follows. Let G be the group of orientation-preserving symmetries of the cube. What is $|G|$, the order of the group G?
2. This the 3D analogue to the symmetries of plane figures, such as a square. The symmetries must be isometries of $\mathbb{R}^3$.
3. **Orientation-preserving** means that you can't reflect the cube through a plane; we really want to only consider symmetries that you can physically perform on a real-life cube, such as a die.
4. If we're looking at a solid object in real life (i.e. not an infinite 3D object), then the group of orientation-preserving symmetries consists only of rotations. So, the book will call these **rotational symmetries**

In order to answer this, one could try to count all the symmetries. Or, one could focus on, say, the set of faces. That is, there is clearly a natural action of G on the set of 6 faces of a cube. Let f be a particular face. The only actions I can perform that preserve a given face are the four rotations about the line normal to that face. Therefore $|G_f| = 4$. The orbit of f is all six faces of the cube, so $|O_f| = 6$. Then by the Orbit-Stabilizer Theorem and Counting Formula, we know $|G| = 24$.

Exercise 6.23. Let G be the set of rotational symmetries of a regular dodecahedron. This is a solid with 12 faces that are all regular pentagons. What is $|G|$?

We can also use algebra to figure out the size of a set that a group acts on, by using the following observation.

Observation 6.24 (Decomposition of S into orbits)**.** Let S be a finite set on which G acts, and let $O_1, O_2, \ldots, O_k$ be the set of orbits. Then

$$|S| = |O_1| + |O_2| + \cdots + |O_k|.$$

More interestingly, by the Counting Formula, for each $i = 1, 2, \ldots, k$, we know that $|O_i|$ **must divide** $|G|$.

This observation is also very useful in many contexts. We'll see this again when we talk about conjugacy classes in groups later on.

Example 6.25. Let G be the set of **rotational symmetries** of a tetrahedron T. (We are only looking at orientation-preserving rigid motions.) Let V, E, F be the set of vertices, edges, and faces, respectively. Observe that $|V| = 6$, $|E| = 4$, and $|F| = 6$.

Pick a vertex v and consider the stabilizer G_v. We can **restrict** the action $G \curvearrowright T$ to an action $G \curvearrowright V$, because we observe that any symmetry of T will necessarily take a vertex to another vertex.

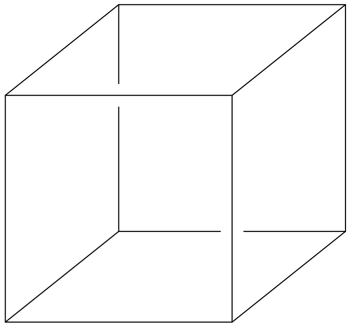
Using geometric reasoning, we see that $G_v \cong \mathbb{Z}/3\mathbb{Z}$ is generated by rotation about the axis going through the vertex v that is normal to the face opposite to v. The action $G_v \curvearrowright V$ has two orbits: v is fixed by G_v, so it's in an orbit on its own; the other three vertices are taken to each other under the action, so they form an orbit. We summarize this by the equation

$$|V| = 4 = 1 + 3.$$

Similarly, any symmetry of T must take an edge to an edge, so we get an induced action $G_v \curvearrowright E$. View T with v at the top of the pyramid with a flat base. The three sloped edges form an orbit, and the three flat edges form another orbit. The orbit decomposition of the set of edges can be summarized as

$$|E| = 6 = 3 + 3.$$

Exercise 6.26. A *cube* is a 3D solid with 6 square faces of equal size:



One example of the cube is the set of points $Q = [0,1]^3 \subset \mathbb{R}^3$.

Let G be the group of **rotational symmetries** of the cube. This is a subgroup of $O(3)$ consisting of *orientation-preserving* symmetries of the cube. [9]

Let V, E, and F denote the sets of vertices, edges, and faces of the cube, respectively. Check for yourself that the size of these sets are

$$|V| = 8 \quad |E| = 12 \quad |F| = 6.$$

(a) Use the counting formula to determine the order of G.

(b) Let G_v, G_e, G_f be the stabilizers of a vertex v, and edge e, and a face f of the cube. Determine the formulas of the form

$$|S| = |O_1| + |O_2| + \cdots + |O_k|$$

(formula 6.9.4 in the text) that represent the decomposition of each of the three sets V, E, F into orbits for each of the subgroups. *Your solution should contain* $9 = 3 \times 3$ *formulas, one for each (group, set) pair. First make sure you are clear on what the group and set in the group action is, in each case!*

We've already talked a bunch about actions *induced* by other actions. Here are two more ways to get induced actions: we can take a subgroup the acting group, or modify the set being acted on.

1. Let $G \curvearrowright S$, and let U be a subset of S. The **stabilizer of the subset** $U \subset S$ is the set H of elements where $gU = U$. Check that H is indeed a subgroup.
   - Observe that then we get an induced action of H on U.
   - We also get an action of G on the orbit of U in the *set of subsets* of S. (See example below.)
2. Let $G \curvearrowright S$, and let $H \leq G$. Then $H \curvearrowright S$.

Example 6.27. Let G be the group of rotational symmetries of the cube. We already computed that there are 24 such symmetries, by considering the action of G on F, the set of 6 faces. From $G \curvearrowright F$, we also get an action of G on *pairs of* faces. There are $\binom{6}{2}$ unordered pairs of faces.

[9] The group of orientation-preserving isometries of $\mathbb{R}^3$ is called $SO(3)$.

6.3 Action of $G \curvearrowright G$ by left multiplication

Recall that we can define an action of G on $S = G$ itself by left multiplication:

$$\begin{aligned} \mu : G \times G &\to G \\ (g, x) &\mapsto gx. \end{aligned}$$

In other words, we are putting group multiplication into the framework of a group action.
This action is both transitive and free:

- (Transitive) It suffices to show that there is just one orbit, so we will show that every $g \in G$ is in the orbit of the identity. Indeed, $\mu(g, 1) = g \cdot 1 = g$.
- (Free) If $gx = x$, then by cancellation we have $g = 1$.

Observation 6.28. For any group action $G \curvearrowright S$, we can view the map

$$\begin{aligned} G \times S &\to S \\ (g, s) &\mapsto g * s \end{aligned}$$

satisfying the identity and associativity axioms equivalently as a map

$$\begin{aligned} G &\to \mathrm{Perm}(S) \\ g &\mapsto [g* : S \to S] \end{aligned}$$

where $\mathrm{Perm}(S)$ is the group of permutations of the elements of S. (For example, $\mathrm{Perm}(\{1, 2, \ldots, n\}) = S_n$; this is the more general construction.)

We can view the action $G \curvearrowright G$ by left multiplication as a map

$$\begin{aligned} G &\to \mathrm{Perm}(G) \\ g &\mapsto m_g \end{aligned}$$

where m_g is "multiply by g on the left", i.e. $m_g(h) = gh$.

- This map is an injective group homomorphism: $m_g(x) = x$ for all $x \in G$ iff $g = 1$. In other words, this action is *faithful*. But we already knew this, since we showed that the action was in fact *free*. See Remark 6.8.

Using this action, can prove that every finite group lives inside a symmetric group S_n; this is another reason why it's so important to understand symmetric groups.

Theorem 6.29 (Cayley's Theorem)**.** Every finite group G is isomorphic to a subgroup of some symmetric group S_n.

Proof. Let $n = |G|$. Then $\mathrm{Perm}(G) \cong S_n$. The homomorphism $\varphi : G \to \mathrm{Perm}(G) \cong S_n$ is injective, so $G \cong \mathrm{img}(\varphi)$. □

Note that it's an entirely different question to ask for the *smallest* n such that $G \hookrightarrow S_n$.

6.4 Action of $G \curvearrowright G$ by conjugation

We can define a different action of G on itself by conjugation; this will tell us more about the structure of the group.

The action of G on itself by conjugation is given by $(g, x) \mapsto gxg^{-1}$. In this section, we will write $g * x := gxg^{-1}$ to emphasize the action.

Definition 6.30. Let $x \in G$. The **centralizer** of x, denoted $Z(x)$, is the stabilizer of x under the conjugation action $G \curvearrowright G$:

$$Z(x) = \{g \in G \mid gxg^{-1} = x\}.$$

These are precisely the elements of G that commute with x.

Exercise 6.31. Prove that $Z(G)$ is a subgroup of G.

Remark 6.32. Recall that the **center** $Z(G)$ of a group G is the set of elements that commute with *all* $x \in G$. Therefore $Z(G) = \bigcap_{x \in G} Z(x)$.

If G is abelian, then for all $x \in G$, $Z(x) = G$. (And $Z(G) = G$.)

Definition 6.33. The **conjugacy class** of $x \in G$ is the orbit of x under the conjugation action of $G \curvearrowright G$.

We will write $C(x)$ for the conjugacy class of x, though I don't believe there is standard notation for this. Here are some immediate observations:

- The Counting Formula tells us that

$$|G| = |G_x||O_x| = |Z(x)||C(x)|$$

- For any $x \in G$, $\langle x \rangle \subseteq Z(x)$.
- $Z(G) \leq Z(x)$
- An element $x \in G$ is in $Z(G)$ iff $Z(x) = G$ iff $C(x) = \{x\}$. Think through this.

Definition 6.34. For a finite group G, the **class equation of** G is the equation describing how the group G is decomposed into conjugacy classes:

$$|G| = \sum_{\text{conj. classes } C} |C| = |C_1| + |C_2| + \ldots + |C_k|.$$

By convention, we let $C_1 = C(1) = \{1\}$ (the conjugacy class of the identity element).

Some more quick observations:

- For all $x \in Z(G)$, $C(x) = \{x\}$, so there will be $|Z(G)|$ ones in the class equation for G.
- For every conjugacy class C_i, by the counting formula we know $|C_i| \mid |G|$.

Example 6.35. The class equation of $S_3 \cong D_3$ is $6 = 1 + 2 + 3$, because

$$S_3 = \{1\} \cup \{(123), (132)\} \cup \{(12), (23), (13)\}.$$

Observe that since A_3 is a *normal* subgroup of S_3, it must be a union of conjugacy classes. Indeed, A_3 is the union of the first two conjugacy classes shown above.

Exercise 6.36. Determine the class equation of $D_4 = \langle \rho, \tau \mid \rho^4 = \tau^2 = \rho\tau\rho\tau = 1 \rangle$. Solution: Instead of directly computing conjugacy classes, you can instead compute the size of centralizers; this way, you can use the counting formula to know when you've found all the elements in the conjugacy class. For example, consider ρ. We know $\rho \notin Z(D_4)$ since $\tau\rho\tau = \rho^{-1}$ (i.e. ρ^{-1} is in the conjugacy class of ρ). Then $Z(\rho) = \langle \rho \rangle$, which contains 4 elements. So $|C(\rho) = 2$. This means we've already found the entire conjugacy class of ρ: $C(\rho) = \{\rho, \rho^{-1}\}$. There are many different ways to arrive at the final answer, which is that $8 = 1+1+2+2+2$.

6.5 p-groups

The conjugation action of $G \curvearrowright G$ is one tool that mathematicians have used to classify finite groups. We will now discuss the simplest cases, which are groups of order a prime power.

Let p be a prime number. Recall that we were able to completely classify groups of order p: they are all isomorphic to C_p. Review exercise: Can you prove this now?

Definition 6.37. A **p-group** is a group of order p^r where $r \geq 1$.

Proposition 6.38. The center of a p-group is not the trivial group.

Proof. Suppose $|G| = p^r$ and consider the class equation. All conjugacy classes must be of order p, but we know $|C_1| = 1$. So there must be at least p one's, i.e. at least p elements in the center. □

Exercise 6.39. Use a similar argument to prove the following theorem:

Theorem 6.40. Let G be a p-group, and suppose G acts on a finite set S. If the order of S is not divisible by p, then there is a **fixed point** of the action $G \curvearrowright S$, i.e. an element $s \in S$ where $G_s = G$.

Proposition 6.41. Every group of order p^2 is abelian.

Proof. Let $|G| = p^2$. By Proposition 6.38, $Z(G) \neq \{1\}$. A priori there are two possibilities: $|Z(G)|$ is either p^2 or p. If $|Z(G)| = p^2$, then we are done. We will now show that $|Z(G)|$ *cannot* be p.

By way of contradiction, suppose that $|Z(G)| = p$. Now let $x \in G - Z(G)$. Then $Z(x)$ contains $\langle x \rangle$ and also $Z(G)$, so the order of $Z(x)$ must be p^2. But then $x \in Z(G)$, which is a contradiction. □

Corollary 6.42. A group of order p^2 is either cyclic, or the product of two cyclic groups of order p.

Proof. Pick an element $x \neq 1$ in G. Then $|x| \in \{p, p^2\}$. If $|x| = p^2$, then $G = \langle x \rangle \cong C_{p^2}$.

If $|x| = p$, then pick some $y \notin \langle x \rangle$. Now observe: Can you prove each of these?

- $\langle x \rangle, \langle y \rangle \trianglelefteq G$
- $\langle x \rangle \cap \langle y \rangle = \{1\}$
- $\langle x \rangle \langle y \rangle = G$

Therefore $G \cong \langle x \rangle \times \langle y \rangle$. □

Remark 6.43. We don't have the tools to prove the following fact, but it's an important theorem in algebra:

Theorem 6.44 (Classification of finite abelian groups)**.** If G is a finite abelian group, then it is isomorphic to a product of finite cyclic groups.

More generally, there is a related theorem for *finitely generated* abelian groups. The proof relies on thinking about abelian group as $\mathbb{Z}$-*modules*, which you'll learn about later in the 150 series.