2021 UChicago Math REU Notes

Steven Labalme

July 13, 2021

Weeks

List of Figures

List of Tables

Week 1

1.1 Introduction to the Program (May / Rudenko)

6/21:

- Mainly given by Peter May.
- A far broader range of mathematics than any other REU.
- Things you have to do:
  1. Soak up as much mathematics as you can.
  2. Work with a mentor to write a paper.
     - You can work with people to write a joint paper?
     - This is fairly unique to this REU.
  3. Meet with your mentors at least twice a week.
- Don't be shy and unwilling to ask questions.
- Daniil Rudenko is in charge of the apprentice program.
- Apprentice program:
  - An opportunity particularly early in one's mathematical career to explore mathematics.
  - Asynchronous video lectures.
    - Feel free to share with friends.
  - Problem solving.
    - Problems that are not merely exercises but more difficult, interesting processes.
    - Spend a couple hours a day thinking about these problems.
- Emphasis on relations between different subjects.
- They will be organizing social activities.
- Social meet and greet at 6:00 PM tonight.
- Breakout rooms:
  1. Apprentice Program.
  2. Probability.
  3. Analysis and Dynamical Systems.
  4. Algebraic Topics.
  5. Main room: Algebraic Topology.
- More on the apprentice program:

- Daniil wants us to see much more than classical analysis/calculus. He doesn't see dividing lines between fields of mathematics.
- Bijections, binomial coefficients, Catalan numbers, etc. to start.
- Group of permutations, group of isometries of the plane, what a group is, etc.
- We can solve problems individually or in groups.
  - Some problems will say not to collaborate.
- Don't try to solve every problem. Don't try to solve everything fast; it's fine if you fail, if you just think about something for a couple hours that's interesting and don't get everywhere.
- On campus classes option for participants in Chicago.
- This week 10-11 AM Wed/Fri?
- Office hours 10-11 AM on Thursday.
- He will send an email with more information.
- Be consistent in whether you want to be on or off campus.
- You may attend whatever you want, but be careful: The apprentice program is your priority, so don't spend too much time on the other stuff.
  - Follow Piazza groups to get links.
- LaTeX one solution each week.

1.2 Introduction to Complex Dynamics 1 (Calegari)

- Main focus: the Mandelbrot Set.
- Let $f_c : \mathbb{C} \to \mathbb{C}$ be the quadratic polynomial $f_c(z) := z^2 + c$ where $c \in \mathbb{C}$ is a constant and $z \in \mathbb{C}$ is a variable.
  - We study quadratics because they're the simplest nontrivial polynomial, i.e., one that displays the interesting phenomena of higher degree polynomials.
- We want to understand the dynamics of f_c, i.e., what happens as we apply f_c over and over again.
  - In other words $z \to z^2 + c \to (z^2 + c)^2 + c \to ((z^2 + c)^2 + c)^2 + c \to \cdots$.
  - Are there any special values of z that have interesting characteristics?
- **Fixed point**: A value z such that $f_c(z) = z$.
  - Fixed points of f_c are equivalent to **roots** of $f_c - z$.
- In this branch of mathematics, we don't care so much about factoring f_c as much as we care about other special entities like fixed points and **critical points**.
- **Critical point**: A point where $\mathrm{d}f_c/\mathrm{d}z = 0$.
- We denote z large by $|z| >> 1$.
- Note that $z^2 + c$ doesn't change the magnitude of z that much unless z is large.
  - Essentially, if $|z| >> 1$, then $|f_c(z)| >> |z|$.
- Introduces composition notation: $z \to f_c(z) \to {f_c}^2(z) \to {f_c}^3(z) \to \cdots$ [1].
- If z large, then the sequence $z, f_c(z), {f_c}^2(z), \ldots$ converges to infinity.

[1] Sometimes, people also use a circled number in the superscript.

- **Riemann Sphere**: The set $\hat{\mathbb{C}} := \mathbb{C} \cup \infty$.
  - Like an open set of complex numbers.
  - In this case, we can think of infinity as a fixed point.
- Any number whose absolute value is sufficiently big will converge to infinity.
- Introduces big N convergence test.
- Infinity is an **attracting fixed point**, i.e. there exists an open neighborhood U containing ∞ such that for all $z \in U$, ${f_c}^n(z) \to \infty$ as $n \to \infty$.
- **Filled Julia set**: The set $\{z : \text{the iterates } {f_c}^n(z) \text{ do not converge to } \infty\}$. *Also known as* $\boldsymbol{K(f_c)}$.
  - Equivalent to the set $\{z : \exists \text{ a constant } T \text{ s.t. } |{f_c}^n(z)| \leq T \ \forall \ n\}$.
- The points that diverge to infinity are not that interesting; their divergence is their only property.
- Much more interesting are the points that do not diverge to infinity.
- Lemma: $K(f_c)$ is closed and bounded (i.e., compact).
  - Proof: There exists T (depending on c) such that if $|z| > T$, then $z \notin K(f_c)$. Furthermore, $z \in K(f_c)$ if and only if there exists n such that $|{f_c}^n(z)| > T$. Let $U := \{z : |z| > T\}$. This is open. Thus, $z \in K(f_c) \iff z$ iterates ${f_c}^n(z) \in U$. Therefore, $K(f_c) = \mathbb{C}$, so $\bigcup_n {f_c}^n(U)$, i.e., $K(f_c)$ is closed.
  - Bounded because numbers are not arbitrarily large. *flesh out details?*
- Calegari's proofs will be somewhat informal throughout the week; he hits the main points and leaves the details as an exercise to the student.
- Question: What other topological properties does the filled Julia set have?
  - Is it possible that $K(f_c) = \emptyset$?
    - No, it is not — as a degree 2 polynomial, $f_c - z$ has at least one root, which will by necessity be a fixed point, i.e., not diverge to infinity, i.e., in the filled Julia set.
  - Could it be a finite set?
    - No — $K(f_c)$ is a **perfect set**.
    - Uncountably infinite, too.
  - Is $K(f_c)$ connected?
    - Sometimes.
- **Perfect set**: A set where every point in the set is a **nontrivial limit point** of the set.
  - Example: A closed interval, *others listed.*
- **Nontrivial limit point**: A point p in a set A such that there is a nontrivial sequence (i.e., not a constant sequence, e.g., $p, p, p, \dots$) of points in A that converge to p.
- **Not connected**: A set $X \subset \mathbb{C}$ such that there exist disjoint, open sets U, V such that $X \subset U \cup V$, $X \cap U \neq \emptyset$, and $X \cap V \neq \emptyset$.
- **Mandlebrot set**: The set of complex numbers $c \in \mathbb{C}$ such that $K(f_c)$ is connected *Also known as* $\boldsymbol{M}$.
- We can prove that $K(f_c)$ is connected if and only if the critical point of f_c is an element of $K(f_c)$.
  - Remember that critical points of f_c are equivalent to zeroes of f_c'.
- Note that critical points of $f_c := z^2 + c$ are equal to the roots of $f_c' = 2z$, i.e., the elements of $\{0\}$.

- $K(f_c)$ is connected is equivalent to the sequence $0 \to c \to c^2 + c \to (c^2 + c)^2 + c \to \cdots$ is bounded (an absolute value).
  - Thus, $c \in M$ is equivalent to the sequence $0 \to c \to c^2 + c \to (c^2 + c)^2 + c \to \cdots$ is bounded.
- The Mandelbrot set is compact, too.
- Proposition: $K(f_c)$ is connected if and only if $0 \in K(f_c)$.
  - "Proof": $\mathbb{C} - K(f_c) = \bigcup_n {f_c}^{-n}(U)$ where U is an open neighborhood of ∞, i.e., the set $\{z : |z| > T\}$.
  - Let $X_n := \mathbb{C} - {f_c}^{-n}(U)$, i.e., $X_0 = \mathbb{C} - U$, so $K(f_c) = \bigcap_n X_n$.
  - Cyclic map? X_n getting "smaller" as n increases? $X_{n+1} \subset X_n$.
  - Assume $X_n =$ little.
  - Two cases: X_n contains 0 and X_n does not contain 0.
  - Either every preimage of X_n is connected or there is a T such that for all $n \geq T$, X_n is not connected.
- Theorem (Douady-Hubbard): M is connected.

1.3 Harmonic Functions, Brownian Motion, and Analysis in the Plane 1 (Lawler)

- These topics will change week to week, so drop in at any point over the summer.
- Schedule:
  - Lectures MWF at 2:30 PM.
  - Group meeting Tuesday at 2:30 PM.
    - Anybody can attend these!
  - No Zoom on Thursday, but there will be an opportunity to talk to Greg Lawler in person at the department of mathematics outside Eckhart when the weather is good.
- Resources:
  - Piazza — look under the resources tab for lecture notes (with some exercises; these are very rough; gives you something to read with the lectures), other materials, etc.
  - There is a 180 page book draft based on his REU lectures last summer.
    - Do not share this.
- This math is at the border of analysis (basically advanced calculus) and probability.
  - Lawler thinks of these as all basically the same subject.
- We will work in $\mathbb{R}^2$.
- A lot of what Dr. Lawler does is often called Complex Analysis.
- Complex analysis allows you to get the results quicker even though they encapsulate ideas that are 100% real; we're going to take a real-function perspective.
- Harmonic function notation:
  - Domains D are connected open sets that are subsets of $\mathbb{R}^2$.
  - Mean value: $f : \mathbb{R}^2 \to \mathbb{R}$ (continuous), or $f : D \to \mathbb{R}$.

  - z, w are points in $\mathbb{R}^2$, and we write $z = (x, y)$ where x, y are the one-dimensional components.
  - $B(z, \epsilon) = \{w : |z - w| < \epsilon\}$ is an open disk and $\partial\, B(Z, \epsilon)$ is the circle of radius ϵ about z.
- If $B(z, \epsilon) \subset D$, then the (circular) mean value $MV(f; z, \epsilon)$ is the average rate of f on $\partial B(z, \epsilon)$, i.e., the quantity
$$\frac{1}{2\pi\epsilon} \int_{\{|w-z|=\epsilon\}} f(w) |\, \mathrm{d}w\, |$$
where $|\, \mathrm{d}w\, |$ is with respect to arc length.
- Let $(\cos\theta, \sin\theta) = \mathrm{e}^{i\theta}$.
- **Harmonic function**: $f : D \to \mathbb{R}$ is harmonic if f is continuous and for all $z \in D$ and every $\epsilon > 0$ with $d(z, \partial D) > \epsilon$, then $f(z) = MV(f; z, \epsilon)$.
- Many applications, notably in physics wrt. heat.
  - Consider D describing a surface with heat. Fix the temperature at the boundary. Let $U(z) =$ temperature at z (in equilibrium).
  - Then U is harmonic on D.
- We're going to understand the mean value in terms of the **Laplacian**.
- If $f : D \to \mathbb{R}$ is C^2 (the first and second derivatives exist and are continuous [either two derivatives in one variable or one derivative in both variables for $\mathbb{R}^2$]), then the Laplacian is defined by
$$\Delta f(z) = f_{xx}(z) + f_{yy}(z)$$
- Proposition: If u is C^2 in D, then $\Delta u(z) = \lim_{\epsilon\to 0} 4 \cdot \frac{MV(u;z,\epsilon)-u(z)}{\epsilon^2}$.
- For ease, let's assume that $z = 0 = (0, 0)$ and $u(z) = 0$.
- Taylor polynomial (in several variables): If $z = (x, y)$, then
$$u(z) = 0 + u_x(0)x + u_y(0)y + \frac{1}{2}u_{xx}(0)x^2 + \frac{1}{2}u_{yy}(0)y^2 + u_{xy}(0)xy + \sigma(|z|^2)^{[2]}$$
  - $u_x(0)MV(x; 0, \epsilon) + u_y(0)MV(y; 0, \epsilon) + u_{xy}(0)MV(xy; 0, \epsilon) + \sigma(\epsilon^2) + \frac{1}{2}[u_{xx}(0)x^2 + u_{yy}(0)y^2]$.
  - Note that $u_{xx}(0)x^2 = MV(x^2; 0, \epsilon)$ and $u_{yy}(0)y^2 = MV(y^2; 0, \epsilon)$.
  - You can use multivariable calculus, or you can observe that $MV(x^2; 0, \epsilon) = MV(y^2; 0, \epsilon)$, thus telling you that $MV(x^2; 0, \epsilon) + MV(y^2; 0, \epsilon) = MV(x^2 + y^2; 0, \epsilon) = \epsilon^2$.
  - Since $|z|^2 = \epsilon^2$, we have that $u(z) = \frac{1}{2}[\frac{1}{2}]$...
- Proposition: A function $f : D \to \mathbb{R}$ is harmonic if and only if it is C^2 and $\Delta f(z) = 0$ for all $z \in D$.
  - Proof: Backwards direction first. We want to show that C^2 and $\Delta f(z) = 0$ imply the mean value property. The mean value property clearly holds at $\epsilon = 0$. Consider $MV(f; z, \epsilon)$ as a function of ϵ. The derivative in ϵ ends up looking something like $\frac{1}{2\pi\epsilon} \int_{\text{circle}} \partial_n f(w) |\, \mathrm{d}w\, |$ where ∂_n is the normal direction.
  - Using the divergence theorem, we have that the above is equal to $\int_{\text{disk}} \Delta f(w)\, \mathrm{d}w$. Note that we sometimes write $\Delta f = \mathrm{d}w\, (\nabla f)$ where $\nabla f = (f_x, f_y)$. Additionally, $\operatorname{div}(\nabla f) = \partial_x(f_x) + \partial_y(f_y)$.
  - Exercise: Show that if u is harmonic, then u is C^2.
- The notion of probability comes in when we ask, "what is the 'mean value' if we are not a disk viewed from the center?"

[2] σ is pronounced "little oh."

1.4 The Mathematics of Playing Pool (Mazur)

- Main focus: Billiards in a polygon.
- The ball bounces off a side with the same angle of incidence it struck it with. If the ball hits the corner, it stops (maybe it fell into a pocket).
- **Billiards**: Start with a polygon in the plane. Shoot a billiard ball, thought of as a point mass, ...
- Rectangular tables are fully understood, but other polygons are harder. Curved sides are even more complicated.
- Connection to physics: Ehrenfest windtree model (by Paul and Tatjana Ehrenfest, 1912).
- One thing people study is the diffusion rate of a random particle. This means that if you take a random particle and follow it for a long time t, how far is it from where it started? What people know is that a typical particle is about distance $t^{2/3}$ away.
- Another example: Take two point masses with positions $0 \leq x_1 \leq x_2 \leq 1$ on the unit interval $[0, 1]$. Suppose their masses are m_1, m_2 and they move with velocities v_1, v_2, respectively. They collide with each other and with the barriers at 0 and 1. Momentum and energy are conserved.
  - We can convert this to billiards in a right triangle with the observations that energy and speed are related and momentum and angle of incidence are related.
- Billiards are important examples of **dynamical systems** where one studies behavior of objects under a deterministic system (initial position and velocity define motion for the rest of time).
- Billiards questions:
  - Are there periodic orbits?
  - How does a typical orbit behave in the long term? Is it dense? Is it equidistributed?
  - Illumination problem (can you get from any point to any other?).
- Periodic orbits:
  - There are periodic orbits in acute triangles.
  - Drop perpendiculars; use Euclidean geometry to prove.
  - It is unknown if a general obtuse triangle has a periodic orbit. This is considered to be one of the big unsolved problems in dynamics[3].
- Equidistribution and Ergodicity:
  - ...
- Rational billiards is much more well-defined. Every rational table has periodic orbits.
- Most paths equidistribute.
- Illumination problem:
  - Now imagine you put a light source at a point on your table. The walls are mirrors and a light beam bounces of the mirror with angle of incidence equal to angle of reflection. Is every point illuminated? In other words, can you get from any point to any other? Not in a Penrose unilluminable room (a region is dark in this elliptical room).
  - Polygon example from Tokarski in the 1980s (a zero-dimensional point is unilluminable).

[3] Can we consider the set of all possible initial positions and directions and see what converges to what?

  - Within the last 5 years: For any rational billiard, there are at most a finite number of unilluminable points.

- Unfolding billiards boards.
- If the slope of the line on a torus is rational, it closes up. If the slope of the line on a torus is irrational, it does not close but is equidistributed.
- For a square, when we glue the unfolded version together, we get a genus 1 surface (a torus).
- For a triangle with angles $\frac{\pi}{2}$, $\frac{\pi}{8}$, and $\frac{3\pi}{8}$, the unfolded version can be glued together into a genus 2 surface.
- Ergodicity:
  - A common notion in mathematics is that of irreducibility.
  - In our context, irreducible (or ergodic) means you cannot divide your table X nontrivially into 2 pieces $X = X_1 \cup X_2$ so that if you start with a point in X_1 and you move in a straight line, you stay in X_1 and if you start in X_2 you stay there.
  - In other words, there are no invariant sets.
- Proves the Kronecker-Weyl theorem.

1.5 Lecture 1.1: Bijections and Permutations

- Consider the statement $4 = 4$.
  - "Four is an abstraction for any set of four elements."
  - Thus, $4 = 4$ implies that $\{\text{lion}, \text{cat}, \text{tiger}, \text{cheetah}\} = \{\text{burger}, \text{pizza}, \text{pasta}, \text{borsh}\}$, for instance, but in what sense are these sets similar? They are related because there exists a bijection between them. Note, however, that there are $4! = 24$ possible bijections between these two sets.
- Let A, B be sets and $f : A \to B$ be a function (or map).

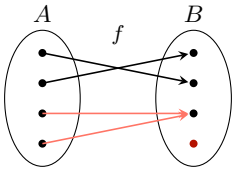


Figure 1.1: A function that is neither injective nor surjective.

  - f is **injective** if for all $a_1, a_2 \in A$, $f(a_1) = f(a_2) \implies a_1 = a_2$.
  - f is **surjective** if for every element $b \in B$, there exists an $a \in A$ such that $f(a) = b$.
  - f is **bijective** if it is surjective and injective.
    - These are one-to-one correspondances.
  - The function f in Figure 1.1 is a function because it maps every element of A to an element of B. However, it is not injective because the mappings indicated in light red map two distinct elements of A to the same element of B. Likewise, it is not surjective because the element of B drawn in dark red is not the image of any element of A under f. Because f is neither injective nor surjective, it is not bijective.
- If there exists a bijection between the set A and the nice set $[n] = \{1, 2, \ldots, n\}$, we say that $|A| = n$.

- Example:
  - Consider the sets $A = \mathbb{N}$ and $B = \{2k \mid k \in \mathbb{N}\}$.
  - Define $f : A \to B$ by $f(x) = 2x$. f is a bijection.
  - Thus, $|A| = |B|$ despite the intuitive sense that $|B|$ should be half $|A|$.
- Sets in bijection with $\mathbb{N}$ are called **countable**, and we write $|A| = \aleph_0$.
  - We can show that $|\mathbb{Q}| = \aleph_0$ and $|\mathbb{R}| \neq \aleph_0$.
- **Permutation**: A bijection $\sigma : S \to S$, where $S = \{1, \ldots, n\}$.
- Examples:
  - $n = 1$:
    - There exists a unique permutation of the set, which is an identity.
  - $n = 2$:
    - There are two different bijections here.
    - They are denoted by the following matrices.

$$\sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

  - $n = 3$:
    - Listing[4] the elements of $\mathbb{S}_3$:

$$\mathbb{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$= \left\{ \begin{array}{ccccccccccccccccc} 1 & 2 & 3 & , & 1 & 2 & 3 & , & 1 & 2 & 3 & , & 1 & 2 & 3 & , & 1 & 2 & 3 & , & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & & \searrow & & \downarrow & & \swarrow & \searrow & \downarrow & & \downarrow & & \searrow & & \swarrow & & \searrow & & \swarrow \\ 1 & 2 & 3 & & 1 & 2 & 3 & & 1 & 2 & 3 & & 1 & 2 & 3 & & 1 & 2 & 3 & & 1 & 2 & 3 \end{array} \right\}$$

    - There are different important classes of permutations — the first one listed is an identity, the next three listed are identities for one object and **cycles** of length two for the other two, and the last two are **cycles** of length three.
    - $|\mathbb{S}_3| = 6$.
- More generally, the numbers in the first row are the numbers 1 through n and the numbers in the second row are those to which the bijection maps each number:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

- We denote by $\mathbb{S}_n$ the set of permutations of $S = \{1, \ldots, n\}$.
- Exercises:
  1. Draw all permutations in $\mathbb{S}_4$.
  2. Prove that $|\mathbb{S}_n| = n!$.
     - Perhaps by induction? Trivial for the base case of 0. Then if true for n, we can map $n+1$ to $n+1$ possible numbers, so we divide into $n+1$ cases. If $\sigma(n+1) = 1$, then we know by the inductive hypothesis that we can permute the remaining n numbers in $n!$ ways. Thus, the number of permutations is $\underbrace{n! + n! + \cdots + n!}_{n+1 \text{ times}} = (n+1) \cdot n! = (n+1)!$.
- Note that in $\S_3$, permutations $\sigma(2,1,3)$, $\sigma(3,2,1)$, and $\sigma(1,3,2)$ are considered odd and the others are considered even.
  - This classification is based on the number of crossings in the function diagrams.

[4] Dr. Rudenko also shows function diagrams and directed graphs (see Figure 1.2).

1.6 Lecture 1.2: The Group of Permutations

- **Composition**: The function $g \circ f : A \to C$ defined by the map $(g \circ f)(a) = g(f(a))$, where A, B, C are sets and $f : A \to B$ and $g : B \to C$ are functions.
- The composition of two bijections is a bijection (Proposition 1.26).
- We can compose permutations to get new (or the same) permutations.
  - Example: If $\sigma = (2, 1, 3)$ and $\tau = (1, 3, 2)$, then $\tau \cdot \sigma = (3, 1, 2)$.
- This new function is known as a **product of permutations**.
- If you do this many times to the same permutation, you construct the power of a permutation.
- Example:
  - Consider $\sigma(3, 5, 1, 2, 4)$.
  - If we draw this out, then we can see that there is a cycle of length two and a cycle of length 3.
  - Thus, $\sigma^{100} = (1, 5, 3, 2, 4)$. $100\%2 = 0$, so $\sigma^{100} = i$ with respect to the $3, 1$ cycle. Additionally, $100\%3 = 1$, so $\sigma^{100} = \sigma$ with respect to the $5, 2, 4$ cycle.
  - Also note that $\sigma^{2 \cdot 3} = \sigma^6 = i$, where i is the identity permutation.
- Multiplication of permutations is associative.
- Thus, we can construct multiplication tables.
- Example:

	$\boldsymbol{e}$	$\boldsymbol{x}$
$\boldsymbol{e}$	e	x
$\boldsymbol{x}$	x	e

Table 1.1: Multiplication table for $\mathbb{S}_2$.

  - This holds where $e = (1, 2)$ and $x = (2, 1)$.
- **Identity**: The function $\mathrm{id}_A : A \to A$ defined by $\mathrm{id}_A(a) = a$, where A is a set.
  - $\mathrm{id}_{[n]} = (1, 2, \ldots, n) = e \in \mathbb{S}_n$.
    - e is also known as the **trivial permutation** or **identity permutation**.
  - For all $\sigma \in \mathbb{S}_n$, $\sigma \cdot e = e \cdot \sigma = \sigma$.
- **Inverse**: The function $f^{-1} : B \to A$ corresponding to the function $f : A \to B$ having the properties that $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.
- f^{-1} exists iff f is a bijection (Proposition 1.27).
- Note that it's often easier to check the two inverse properties than to confirm that f is bijective.
- Since permutations are bijections, all permutations have inverses.
  - If $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{smallmatrix}\right) = \sigma \in \mathbb{S}_5$, then $\sigma^{-1} = \left(\begin{smallmatrix} 3 & 4 & 1 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{smallmatrix}\right)$.
  - Note that in this case $\sigma = \sigma^{-1}$, indicating the existence of only 1- and 2-cycles.
- **Group**: A set G along with a map $G \times G \to G$.
- If the following properties hold, then a collection of objects is a group.

1. Associativity: For all $g_1, g_2, g_3 \in G$, $(g_1 g_2)g_3 = g_1(g_2 g_3)$.
2. Identity: There exists a special element $e \in G$ such that for any $g \in G$, $g \circ e = e \circ g = g$.
3. Inverse: For all $g \in G$, there exists $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = e$.

- Examples:
  - $\mathbb{S}_n$ is a group.
  - $\mathbb{Z}$ and addition is a group.
  - $\mathbb{Q}$ and multiplication is a group (notably, $\mathbb{Z}$ and multiplication is not).

1.7 Introduction to Complex Dynamics 2 (Calegari)

6/22:

- Picking up from yesterday on the proof of the proposition, $K(f_c)$ is connected iff $0 \in K(f_c)$.
  - Recall that 0 is the unique critical point.
  - Also recall that U is the set that contains only elements with sufficiently big absolute values, big enough so that $f_c(U) \subset U$.
  - Define $X_0 = \mathbb{C} - U$, $X_{n+1} = {f_c}^{-n}(X_n)$.
    - Each X_n is compact, and $K(f_c)$ is equal to the intersection of all X_n, therefore compact in and of itself.
  - Thus, $K(f_c)$ is connected iff every X_n is connected.
  - Key point: If $0 \in K(f_c)$, then each X_n is a disk; otherwise, some X_n is not a disk.
  - Fact: Every point in $\mathbb{C}$ has exactly 2 preimages under f_c except for the critical value $c = f_c(0)$ since f_c is a degree 2 polynomial.
  - Assume X_n is a disk. If X_n contains the critical value, then X_{n+1} is a disk; otherwise, not (in fact, it will be disconnected).
- Under f_c, the preimage of a circle not containing the critical value is either 2 circles, each of which maps one-to-one, or a single circle mapping two-to-one.
  - Suppose that the preimage of the boundary of the circles is two distinct circles.
  - By continuity, concentric circles narrowing down within the original set narrow down within the other two circles.
  - Each point in X_n has exactly two preimages iff $c \notin X_n$.
  - As we make smaller and smaller circles, than we can split our one-circle preimage into two disconnected subsets.
- Today: The theory of Julia sets for holomorphic functions in general.
- Let f be a **holomorphic** map from $\hat{\mathbb{C}}$ to itself.
- Every such f has finitely many 0s and poles (∞s).
- Therefore, f is a rational function, i.e., a ratio of polynomials. Symbolically, $f(z) = \frac{p(z)}{q(z)}$ for some polynomials p, q.
- To talk about Julia sets, we need some definitions.
- **Normal family**: Let U be an open subset of the Riemann sphere $\hat{\mathbb{C}}$, and let F be a family of holomorphic functions $f : U \to \hat{\mathbb{C}}$. F is **normal** if its closure (in the space of all holomorphic functions from U to $\hat{C}$) is compact.

  - In other words, if ever infinite sequence $f_n \in F$ has a subsequence that converges locally uniformly to some limit $g : U \to \hat{\mathbb{C}}$.

- Normality is local.
- Proposition: Suppose F is a family of holomorphic functions defined on U, and suppose for all $p \in U$, there exists open $p \in V \subset U$ such that $F|_V$ is normal. Then $F|_U$ is normal.
  - Proof 1: Diagonal argument.
  - Proof 2: ???
- **Julia set**: Let f be a holomorphic map from $\hat{\mathbb{C}}$ to itself. Let $\mathcal{F} := \{f^n \mid n \in \mathbb{N}\}$. The Fatou set $\Omega_f :\subset \hat{\mathbb{C}}$ is the open subset whose $\mathcal{F}$ is normal. It is equal to the union of all U where $F|_U$ is normal. Thus, Ω_f is open and $\mathcal{F}|_{\Omega_f}$ is normal. The **Julia set** $J_f :\subset \hat{\mathbb{C}}$ is $\hat{C} - \Omega_f$, i.e., $p \in J_f$ iff for all U containing p, $F|_U$ is not normal on U.
  - Hence, J_f is compact.
- Example: Let's let p be a fixed point for f.
  - p is an attracting fixed point if $|f'(p)| < 1$. p is super attracting if $|f'(p)| = 0$.
  - Example:
    - If f is a polynomial of degree at least 2, then ∞ is a super attracting fixed point.
  - If we take a sufficiently small neighborhood of p, then f shrinks and rotates the neighborhood a little bit.
  - **Basin of attraction** of p.
  - **Immediate basin of attraction** of p is the connected component of the basin of attraction of p.
- If f is a polynomial, then $K(f_c)$ is equal to the complement of the basin of infinity.
- "Most" "typical" f have $\Omega_f = \bigcup$basins of attraction of attracting periodic orbits.
  - Furthermore: every immediate basin of an attracting periodic orbit contains at least one critical point.
  - A rational map of degree d (the maximum of the degrees of polynomials p, q) has $2d - 2$ critical points.
- Theorem: The closure of the set of repelling periodic orbits (i.e., p with $f^n(p) = p$ and $|(f^n)'(p)| > 1$) is J_f.

1.8 Coambiguous Concepts 1 (May)

- Categories can inscribe things of different types.
- Categories can be interesting mathematical objects in and of themselves much like rings, groups, etc.
- Whenever you define an object, you should define a notion of a morphism (or map) between objects.
- Morphisms have compositions and identities.
- A monoid is a category with one object. A category is a monoid with many objects!
- Today: Category theory.
- **Poset**: A partially ordered set, i.e., one that is transitive, reflexive, and antisymmetric ($A \leq B$ and $A \geq B \iff A = B$).
- **Small category**: A category that has a set of objects as opposed to a class of objects. *Also known as* **kitty category**, **kittygory**.

1.9 Lecture 1.3: Cyclic Structure of a Permutation

- Let $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 4 & 2 & 6 & 5 & 1 & 8 \end{smallmatrix}\right) \in \mathbb{S}_8$.
- Consider the directed graph representation.

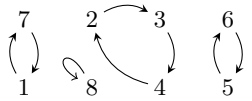


Figure 1.2: Directed graph of a permutation in $\mathbb{S}_8$.

  - Note that this is a graph because it has points connected by edges, it is directed because the edges have a direction (they are arrows/mappings), and it has some loops and some multiple edges (points with more than one edge).
  - There are four cycles in this graph (a 1-cycle, two 2-cycles, and a 3-cycle).
- **Cycle**: A permutation $\sigma = (i_1, \ldots, i_k) \in \mathbb{S}_n$, where $1 \leq i_1 \leq \cdots \leq i_k \leq n$, such that $\sigma(i_j) = i_{j+1}$, $\sigma(i_k) = i_1$, and $\sigma(s) = s$ for all $s \in [n] \setminus \{i_1, \ldots, i_k\}$.
- For example, $\sigma = (1, 3, 5) \in \mathbb{S}_5$ is the permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{smallmatrix}\right)$.
- **Length** (of a cycle): The value k in the above definition.
- **Support** (of a cycle): The set of indices $\{i_1, \ldots, i_k\}$ in the above definition.
- **Transposition**: A cycle $(i, j) \in \S_n$, where $i, j \in [n]$ are distinct.
- Thus, $\mathbb{S}_3 = \{e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$.
- Exercise:
  - Count the number of transpositions in $\mathbb{S}_n$.
  - Prove that every permutation is a product of transpositions.
    - Consider crossings in the function diagram! Relate to braids from knot theory.
    - For instance, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{smallmatrix}\right) = (1,4)(2,4)(1,3)(2,3)$.
- **Independent** (cycles): Two cycles $\sigma_1, \sigma_2 \in \mathbb{S}_n$ with disjoint supports.
- **Dependent** (cycles): Two cycles that are not independent.
- Propositions:
  1. Every permutation is a product of independent cycles.
     - In the directed graph corresponding to σ, every vertex has on incoming edge.
     - There exists a smallest k such that $\sigma^k(i) = i$.
     - *Return to this?*
  2. Independent cycles commute with each other.
     - Obvious: Consider c_1, c_2 independent. Then

$$c_1 c_2(i) = \begin{cases} c_1(i) & i \text{ is in the support of } c_1 \\ c_2(i) & i \text{ is in the support of } c_2 \\ i & i \text{ is in the support of neither} \end{cases}$$

1.10 Lecture 1.4: Binomial Coefficients

- Start with the set $S = \{1, \ldots, n\}$. Denote by 2^S the set of subsets of S.
  - If $n = 2$, then $2^S = \{\emptyset, \{1, 2\}, \{1\}, \{2\}\}$ has four elements.
- Proposition: $|2^S| = 2^{|S|}$.
  - Consider the set $S = \{1, 2, 3, 4, 5, 6\}$.
  - Identify subsets of S with a code, exemplified by $\{1, 3, 5\} \mapsto (1, 0, 1, 0, 1, 0)$.
  - Based on this, construct a map f which sends $2^S \to$ the set of sequences of $0, 1$ of length n. In other terms, map each subset $A \in 2^S$ to a sequence $(s_1, \ldots, s_n)$ where
$$s_i = \begin{cases} 0 & i \notin A \\ 1 & i \in A \end{cases}$$
  - For example, $f(\emptyset) = (0, 0, 0, 0, 0, 0)$ and $f(S) = (1, 1, 1, 1, 1, 1)$.
  - Note that f is a bijection.
  - Since the set of all sequences of $0, 1$ of length n (more commonly denoted by $\{0, 1\}^n$) clearly has 2^n elements and 2^S is in bijective correspondence with this set, we know that 2^S has $2^{|S|} = 2^n$ elements.
- Note that coding subsets by sequences is very important in computer science and mathematics.
- Geometric model: Vertices of a line segment give you subsets of a set with 1 element, vertices of a square give you subsets of a set with 2 elements, vertices of a cube give you subsets of a set with 3 elements, ...
- If $A \in 2^S$ and $f(A) = (a_1, \ldots, a_n)$, then $|A| = \sum_{i=1}^n a_i$.
- If $0 \leq k \leq n$, then $\binom{n}{k}$ is the number of subsets of size k in a set of size n.
- Proposition: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
  - $\binom{n}{k} \cdot k!$ is the number of subsets of size k and the orderings of their elements.
  - But this is the same as choosing the first element from among n elements, the second from among the remaining $n - 1$ elements and so on until $n - k + 1$, i.e.,
$$\begin{aligned} \binom{n}{k} \cdot k! &= n \cdot (n-1) \cdots (n-k+1) \\ &= \frac{n!}{(n-k)!} \end{aligned}$$
- By convention, $\binom{n}{0} = 1 = \binom{n}{n}$.
- Proposition: $\binom{n}{k} = \binom{n}{n-k}$.
  - Follows from the previous proposition.
  - Alternatively, we can seek to show that the number of subsets of size k is equal to the number of subsets of size $n - k$. But since these are inverse maps, they obviously are.
- Proposition: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
  - Follows from the factorial formula.
  - Conceptually:

- Divide the set of subsets of S of size k into those that contain n and those that do not contain n.
- The subsets of size k that do not contain n is equal to the subsets of $S \setminus \{n\}$ of size k, i.e., $\binom{n-1}{k}$.
- The subsets of size k the do contain n are in bijection with the subsets of size $k-1$ in $S \setminus \{n\}$, i.e., $\binom{n-1}{k-1}$.

- Introduces Pascal's triangle.
  - The symmetry of Pascal's triangle follows from the formula $\binom{n}{k} = \binom{n}{n-k}$.
- Theorem (Binomial Formula):

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n}b^n \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\end{aligned}$$

  - Induction proof: Left as an exercise.
  - $(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ times}}$ = a sum of monomials, e.g., $aabbaba$. We get each monomial by choosing a or b from each parentheses. Thus, $(a+b)^n = \sum_{A \subset \{1,\ldots,n\}=S} a^{|A|}b^{|S\setminus A|}$.
- Corollary: If $a = b = 1$, then $2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}1^k = \sum_{k=0}^{n}\binom{n}{k}$.

1.11 Problem Session 1

6/23:

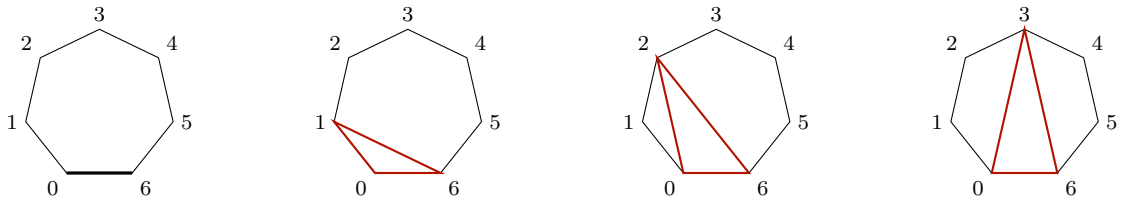
- The goal is to get you to think about math all the time. You should let problems sit in your head for a week; no expectation of solving them, but just thinking about it.
- Typo in 5a. Nobody knows what problem 4 means.
- If you're ever lost on a permutation problem, just draw out the connected graph.
- Prove any permutation is a product of adjacencies.
- 5d technically proves 5c, but there is a nicer formula for 5c that he would rather we find.

1.12 Lecture 1.5: Catalan Numbers

6/26:

- The sequence $1, 1, 2, 5, 14, 42, \ldots$.
- Discovered by Euler, who was investigating **triangulations** of a polygon.
- Let P be a **convex** polygon with $n+2$ sides.
- **Convex** (polygon): A polygon such that for all chords connecting points, the chord passes entirely through the interior of the polygon.
- **Triangulation**: A decomposition of a polygon P into triangles by nonintersecting diagonals.
- Exercise:
  - Every triangulation of P has n triangles.
- The n^{th} Catalan number C_n is the number of such triangulations.

- $C_0 := 1$.
- $C_1 = 1$.
- $C_2 = 2$.
- $C_3 = 5$ (there are 5 rotations of the "same" triangulation).
- $C_4 = 14$ (there are 6 with all three diagonals coming out of one vertex, 6 with opposite vertices having two diagonals, each, and 2 with a triangle in the center).
- Computing C_5 gets more complicated. Number the vertices of the heptagon 0-6.



(a) Original shape. (b) Term 1. (c) Term 2. (d) Term 3.

Figure 1.3: Computing C_5.

- Observe: There will always be one triangle with $\overline{06}$ as an edge (see Figure 1.3a).
- If we include $\triangle 016$, we know that there are C_4 ways to triangulate the remaining 6-gon and C_0 ways to triangulate the "triangle" to the left of $\triangle 016$, i.e., the edge $\overline{01}$. Thus, we have that $C_5 = C_0 \cdot C_4 + \cdots$ (see Figure 1.3b).
- If we consider $\triangle 026$, there are C_1 ways to triangulate the triangle to the left of $\triangle 026$ and C_3 ways to triangulate the 5-gon to the right of $\triangle 026$ (see Figure 1.3c).
- If we consider $\triangle 036$, there are C_2 ways to triangulate the 4-gons on both sides of $\triangle 026$ (see Figure 1.3d).
- Continuing, we can see that

$$C_5 = C_0C_4 + C_1C_3 + C_2C_2 + C_3C_1 + C_4C_0$$

- Proposition: The following recurrence relation holds.

$$C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}$$

  - Proof: Repeat the same argument.

- A second interpretation of Catalan numbers.
- Consider a sequence of brackets $(,)$ such as $((()))(()))($. A sequence is **admissible** if
  1. The number of opening brackets is equal to the number of closing brackets.
  2. In every initial subsequence, the number of opening brackets is greater than or equal to the number of closing brackets.
- For example, $(()))($ is not admissible but $(())()$ is.
- Note that admissible sequences are the ones that can be taken to be the parentheses to expressions, e.g., $(a + b(c + d))(e + f)$ makes sense, but we can't fill in anything in $(()))($.
- Proposition: The number of admissible sequences with $2n$ brackets equals C_n.
  - $n = 1$: $()$.

  - $n = 2$: (()), ()().
  - $n = 3$: ((())), (()()), (())(), ()(()), ()()().
  - We have to show that the number of admissible sequences satisfies the same recurrence relation.
  - Consider $n = 3$. For the first two, we have 2 sets of parentheses within the initial subsequence, and 0 outside it (C_2C_0). For the next one, we have 1 set within and 1 set outside (C_1C_1). For the last two, we have 0 sets in and 2 sets outside (C_0C_2). The number is the sum of all three.

- Exercise: Construct an explicit bijection between triangulations and parentheses.

1.13 PSet 1

1. We have discussed three ways to prove identities for binomial coefficients: induction, combinatorial bijection, and binomial formula. Try these three approaches on the following identities.

   (a) $\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}$.

   (b) $\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$.

   Proof. Combinatorial bijection: Divide the $2n$ items into two bins of n items each, which we shall refer to as the red bin and the blue bin. There are as many ways to choose n items from among both bins as there are to choose 0 items from the red bin and n items from the blue bin, plus 1 item from the red bin and $n-1$ items from the blue bin, and so on and so forth. Symbolically, $\binom{2n}{n} = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0}$. We can then apply to this identity the symmetry one (i.e., $\binom{n}{k} = \binom{n}{n-k}$) to yield the final formula. □

   (c) $\binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \cdots + \binom{n}{k}\binom{m}{0} = \binom{n+m}{k}$.

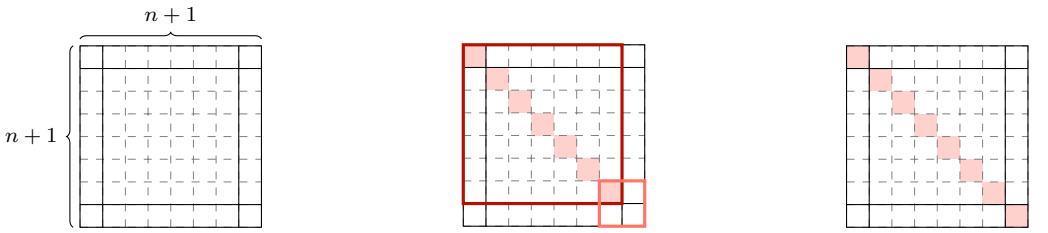
   (d) $\binom{n-1}{k-1} + \binom{n-2}{k-1} + \cdots + \binom{k-1}{k-1} = \binom{n}{k}$.

   Proof. As can be easily seen from Pascal's triangle, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. □

2. We will consider a "disease" that infects cells of a chessboard. Initially, some number of the 64 cells are infected. Subsequently, the infection spreads according to the following rule: If at least two neighbors of a cell are infected, then the cell gets infected. (Neighbors share an edge, so each cell has at most four neighbors.) No cell is ever cured. What is the minimum number of cells one can initially infect so that the whole board is eventually infected? It is easy to see that 8 is sufficient in many ways. Prove that 7 is not enough.

   Proof. To prove that 8 is the minimum number of cells one can initially infect so that the whole 8×8 board is eventually infected, it will suffice to show n is the minimum number of cells required to infect an $n \times n$ board for all natural numbers n. We induct on the the edge length of the board n using strong induction. For the base case $n = 1$, it is trivially obvious that the one cell on the board is either infected or not, so to infect the whole board, we need to infect it (i.e., infect 1 cell). Now suppose inductively that we have proven the claim for n; we now seek to prove it for $n + 1$.

   Consider an $(n+1)\times(n+1)$ board, as in Figure 1.4a. As part of infecting the board, it will be necessary to infect the $n \times n$ subgrid in the upper left-hand corner (in dark red in Figure 1.4b, and note that the n shaded cells are the initially infected ones that will infect the whole subgrid). By the inductive hypothesis, it will require a minimum of n infected cells to infect it. However, even after that whole subgrid is infected, there are still healthy cells, none of which has more than one neighbor. Thus, it will be necessary to add in at least one more infected cell. The light red subgrid at the bottom right of Figure 1.4b gives us a hint of where to put it; indeed, for the $n = 2$ case, it is necessary to have at least 2 cells infected by hypothesis, but this subgrid only contains one infected cell (one that overlaps with the other subgrid). Therefore, by placing the $(n + 1)^{\text{st}}$ infected cell in the bottom right-hand corner (see Figure 1.4c), we can infect the whole board. □



(a) An $(n+1)\times(n+1)$ chessboard. (b) Subgrids. (c) Infected cells in the beginning.

Figure 1.4: A chessboard to be infected.

3. Generators of $\mathbb{S}_n$

   (a) Prove that

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

   is a product of transpositions.

   Proof. $\sigma = (16)(23)$. □

   (b) Prove that any permutation is a product of transpositions.

   Proof. Let $\sigma = (a_1, a_2, \ldots, a_n) \in \mathbb{S}_n$ be an arbitrary permutation. Starting from $e = (1, 2, \ldots, n)$, have the first permutation be $(1a_1)$. This will set a_1 in the correct position. The second will then be (xa_2), where x is whatever is in the second position after the first transposition. This will set a_2 in the correct position. Continue down the line, always switching whatever is in the k^{th} spot with what should be there before moving on the the $(k+1)^{\text{th}}$ spot and ending at the n^{th} spot. □

   (c) Prove that any permutation in $\mathbb{S}_n$ can be written as a product of two permutations (12) and $(12\ldots n)$.

4. Two players put 25 cent coins on the round table alternately. They are allowed to put a coin on an empty spot only. The person, who cannot make a move, loses the game. Find a winning strategy for one of the players.

5. Let G be a finite group.

   (a) Prove that for $g_1, g_2, g_3 \in G$, if $g_1g_2 = g_1g_3$, then $g_2 = g_3$.

   Proof. By the inverse property of a group, there exists ${g_1}^{-1}$. Therefore, we have that

   $$\begin{aligned} {g_1}^{-1}(g_1g_2) &= {g_1}^{-1}(g_1g_3) && \text{Multiplicative POE} \\ ({g_1}^{-1}g_1)g_2 &= ({g_1}^{-1}g_1)g_3 && \text{Associativity} \\ eg_2 &= eg_3 && \text{Inverse} \\ g_2 &= g_3 && \text{Identity} \end{aligned}$$

   as desired. □

   (b) Prove that in the multiplication table of a finite group, every element appears exactly once in each row and once in each column.

   Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n. Consider the row/column defined by g_i, where i is an arbitrary natural number between 1 and n, inclusive. Suppose for the sake of contradiction that the object g appears twice in the row, such that $g_ig_j = g$ and $g_ig_k = g$, where $j \neq k$. But by part (a), $g_ig_j = g = g_ig_k$ implies that $g_j = g_k$, a contradiction, since every element of G is only listed once in the row/column headers. □

(c) Prove that for any permutation $\sigma \in \mathbb{S}_n$, there exists $N \in \mathbb{N}$ such that $\sigma^N = e$.

Proof. Decompose σ into its subcycles, i.e., if there are transpositions (2-cycles), 3-cycles, etc., identify all of these. Let A be the set of subcycle lengths. Let N be the least common multiple of every element of A.

Let a_i be the i^{th} element of σ, where i is an arbitrary natural number between 1 and n, inclusive. We want to show that the i^{th} element of σ^N is i. Suppose that i is part of a subcycle of length k. It follows that the i^{th} element of $\sigma^k, \sigma^{2k}, \sigma^{3k}, \dots$ is i. Therefore, since $N = \operatorname{lcm}(\{k, \dots\})$, the i^{th} element of σ^N is i, as desired. □

(d) Prove that for $g \in G$, we have $g^{|G|} = e$.

Proof. Something to do with part (b)? Possibly something with Lagrange's theorem, i.e., elements of subgroups hit e multiple times as the exponent increases while elements not in subgroups cycle through all elements of G before hitting e. □

6. **Erdős-Szekeres theorem**:

Prove that for any $n, m \in \mathbb{N}$, every sequence of $nm + 1$ distinct real numbers contains an increasing subsequence of length $n + 1$ or a decreasing subsequence of length $m + 1$.

Week 2

2.1 Gaussian Curvature (Neves)

6/28:

- Plan:
  1. What is a surface?
  2. What is the tangent space?
  3. What are the principal curvatures?
  4. What is the Gaussian curvature?
- In analysis:
  1. What is a function?
  2. What is the derivative?
  3. What is the Hemian of function?
  4. 2nd derivative test (determinant of Hemina).
- **Surface**: A subset $\sigma \subseteq \mathbb{R}^3$ such that for all $p \in \Sigma$, there's a neighborhood B of p in $\mathbb{R}^3$ so that $\Sigma \cap B$ "looks like a disk." More precisely, there exists an open neighborhood $U \subseteq \mathbb{R}^2$ and a map $\varphi : U \to \Sigma \cap B \subseteq \mathbb{R}^3$ such that
  i) φ is continuous and smooth.
  ii) φ is a bijection (with φ^{-1} continuous).
  iii) $\mathrm{d}\varphi_{|x} : \mathbb{R}^2 \to \mathbb{R}^3$ is injective for all $x \in U$.
- **Chart**: The quantity (φ, U) near $p \in U$.
- Examples:
  A) Plane. $\Sigma = \mathbb{R}^2 \times |0| \subseteq \mathbb{R}^3$ is a surface with chart $\varphi : \mathbb{R}^2 \to \Sigma$ where $(x, y) \mapsto (x, y, 0)$.
  B) Sphere. $\Sigma = \{\vec{u} \in \mathbb{R}^3 \mid |\vec{u}| = 1\}$.
     – Charts: Consider the sets $U = \{(x_1, x_2) \mid {x_1}^2 + {x_2}^2 < 1\} \subseteq \mathbb{R}^2$. Let $\varphi_1^+ : U \to \Sigma \cap \{(x, y, z) \mid x > 0\}$ be defined by $\varphi_1^+(u_1, u_2) = (\sqrt{1 - {x_1}^2 - {x_2}^2}, u_1, u_2)$, $\varphi_1^- : U \to \Sigma \cap \{(x, y, z) \mid x < 0\}$ be defined by $\varphi_1^-(u_1, u_2) = (-\sqrt{1 - {x_1}^2 - {x_2}^2}, u_1, u_2)$.
     – Same thing for $\varphi_2^{\pm}, \varphi_3^{\pm}$.
  C) A cone $\Sigma = \{(x, y, z) \mid z = \sqrt{x^2 + y^2}\}$ is *not* a surface because it fails property (iii).
  D) The closed unit disk $\Sigma = \{(x, y, 0) \mid x^2 + y^2 \leq 1\}$ is also not a surface.
- **Tangent space**: Let $\Sigma \subseteq \mathbb{R}^3$ be a surface and let $p \in \Sigma$. Then $T_p\Sigma \subseteq \mathbb{R}^3$ is the z-plane so that $p + T_p\Sigma$ is the affine plane that best approximates Σ near p.
  – Best linear approximation near the surface.

  - Very similar/analogous to the derivative.
- If (φ, U) is a chart near p, then $T_p\Sigma = \text{span}\{\frac{\partial\varphi}{\partial x_1}(\bar{x}_1, \bar{x}_2), \frac{\partial\varphi}{\partial x_2}(\bar{x}_1, \bar{x}_2)\}$.
- Proves linear independence of above vectors.
- Principal curvatures.
- Let $\Sigma \subseteq \mathbb{R}^3$ be a surface, $p \in \Sigma$, and $\vec{N}$ be a unit normal vector defined around p (i.e., $\vec{N}(q) \cdot \vec{v} = 0$ for all q near p and $\vec{v} \in T_q\Sigma$).
- Choose $\vec{v} \in T_p\Sigma$ such that $|\vec{v}| = 1$. Set $P_v = \text{span}\{\vec{v}, \vec{N}(p)\}$. Claim: $(\Sigma - p) \cap P_v$ is a curve near the origin.
- **Principal curvature**: The reciprocal of the radius of the circle in P_v that best approximates $(\Sigma - p) \cap P_v$ near the origin. *Also known as* $\boldsymbol{K(\vec{v})}$.
  - The sign is positive if the center of the circle is in the direction of $\vec{N}(p)$ and negative otherwise.
  - If the sign of $\vec{N}(p)$ changes, then $K(\vec{v})$ will change in sign.
- If we change $\vec{N}$ by $-\vec{N}$, then the new $K(\vec{v})$ is the opposite of the old one.
- Given $p \in \Sigma$ and $\vec{N}(p)$ a normal vector at p, we define $K_1(p)$ to have the maximum $K(\vec{v})$ over all unit vectors $\vec{v} \in T_p\Sigma$ and $K_2(p) = \min\{K(\vec{v}) \mid \vec{v} \in T_p\Sigma, |\vec{v}| = 1\}$.
- K_1, K_2 are computable quantities.

2.2 Lecture 1.6: An Explicit Formula for the Catalan Numbers

6/29:

- Theorem (discovered by Euler):

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{n!(n+1)!}$$

- Examples:
  - $C_1 = \frac{1}{2}\binom{2}{1} = 1$.
  - $C_2 = \frac{1}{3}\binom{4}{2} = 2$.
  - $C_3 = \frac{1}{4}\binom{6}{3} = 5$.
- Dyck path:
  - We'll study paths starting with $(0, 0)$, going on each stop either from (x, y) to $(x + 1, y + 1)$ or from (x, y) to $(x + 1, y - 1)$.
  - Consider the number of ways to get to each point on the integer grid $\mathbb{Z} \times \mathbb{Z}$ from $(0, 0)$.
    - Generates a rotated Pascal's triangle.
    - The number of paths from $(0, 0)$ to $(a + b, a - b)$, i.e., a moves up and b moves down is $\binom{a+b}{b}$.
- Proposition: C_n is equal to the number of paths from $(0, 0)$ to $(2n, 0)$ which are contained in the upper half-plane $(y \geq 0)$.
  - Proof: C_n is the number of sequences of brackets.
  - Transform a sequence of brackets into a path by $(\mapsto \nearrow$ and $) \mapsto \searrow$.
  - The condition $\#(= \#)$ implies that the paths start at $(0, 0)$ and end at $(2n, 0)$.
  - The condition that in every initial segment, $\#(= \#)$ implies that the path lies in the upper half plane.

- Reflection principle:
  - The number of paths from A to B in the upper half plane is equal to the number of paths from A to B minus the number of paths from A to B that intersect the line $y = -1$.
  - Symbolically, $C_n = \binom{2n}{n} - ?$
  - There exists a one-to-one correspondence between two sets: The set of all paths from A to B intersecting ℓ and the set of all paths from A to B', where B' is the reflection of B across ℓ.
- Thus, the number of paths from A to B that intersect the line $y = -1$ is equal to the number of paths from A to $(2n, -2)$.
- Therefore,

$$\begin{aligned}\binom{2n}{n} - \binom{2n}{n-1} &= \frac{(2n)!}{n!n!}\left(1 - \frac{n}{n+1}\right)\binom{2n}{n-1} \\ &= \frac{1}{n+1}\binom{2n}{n}\end{aligned}$$

  - Note that it's not obvious that $\frac{1}{n+1}\binom{2n}{n}$ is an integer unless you present it as the difference of two binomials (i.e., as $\binom{2n}{n} - \binom{2n}{n-1}$).
- Exercise:
  - Take a path from A to B intersecting ℓ and find the closest point of $P \cap \ell$ to B. Reflect the segment of the path after this point.

2.3 Introduction to Quantitative Topology (Weinberger)

7/1:

- Topological Problems:
  - Are X and Y homeomorphic?
  - $f, g : X \to Y$. Does there exist a homotopy $f_t : X \to Y$, $f_0 = f, f_1 = g$?
  - Given X, does it embed in $\mathbb{R}^n$?
- When the answer is yes, something exists.
  - But what can you tell me about the thing that exists?
  - Typically, the adjective is, "how big?"
- Suppose M is an n-dimensional triangulated manifold, i.e., $\partial(\text{tetrahedron}) = S^2$ (the boundary of M is the two dimensional sphere).
- Poincaré conjecture: if M looks like a sphere to an algebraic topologist, i.e.,
  - $\pi_1(M) = e$.
  - $\tilde{H}_i(M) = 0$, $i < n$.
  - M is homotopy equivalent to S^n.

  then it is a sphere, i.e., there exists some subdivision of M and some subdivision of $\partial(\triangle^n) = S^n$ such that $M^{\text{subdivided}}$ and $(S^n)^{\text{subdivided}}$ are combinatorially isomorphic.
- How big means how many simplicities there are.
- Another quantitative question: Suppose I triangulate the sphere with N simplicities. How much further subdivision do I need to do to make it a subdivision of the standard simplex.

- Consider S^5 (the 5-dimensional sphere).
  - Consider $\mathbb{N} \mapsto f(\mathbb{N})$, where $f(N)$ is the biggest number you need to be able to see $M \approx S^5$ combinatorially.
  - Consider the number of protons in the universe. Is it 10, $\mathbb{N}$, $N^?$, $\log\left(N^2\right)$, $2^{2^{2^{\nearrow^N}}}$? It's none of the above; $>$ all of them.

2.4 PSet 2

6/30:

1. Consider n pairs of points on the segment AB, which are symmetric with respect to its center. Half of these points are red, the other are blue. Prove that the sum of distances from the point A to the blue points equals the sum of distances from the point B to the red points.

   Proof. Let C be the midpoint of AB. Clearly, if every point is located at C, the sum of the distances from A to the blue points is $n \cdot \text{len}\,(AC)$, and similarly for B and the red points. Thus, to prove the claim, it will suffice to show that moving any pair of points located at C to two points that are symmetric with respect to C preserves the equality of the A-to-blue-points and B-to-red-points distances. We divide into three cases (both points are blue, both points are red, and one point is blue and the other red).

   If both points are blue, then moving them will not affect the B-to-red-points distance. As such, we must show that moving them symmetrically similarly does not affect the A-to-blue-points distance. But this is obviously true, as shortening the distance from A to p_1 by ℓ necessitates lengthening the distance from A to p_2 by ℓ, cancelling out any potential change.

   The proof is symmetric if both points are red.

   If one point is blue and the other red, then shortening the distance from A to p_b by ℓ necessitates shortening the distance from B to p_r by ℓ as well, preserving equality. Vice versa is true for lengthening the distance from A to p_b. □

2. Consider a set 2^S of subsets $S = \{1, 2, \ldots, n\}$. For two subsets $A, B \in 2^S$, define their symmetric difference by $A \triangle B = (A \cup B) \setminus (A \cap B)$. Prove that 2^S with this operation is a group.

   Proof. To prove tht 2^S with $\triangle$ is a group, we must verify the associativity, identity, and inverse conditions.

   To confirm that 2^S is associative, we must show that for all $A, B, C \in G$, $(A \triangle B) \triangle C = A \triangle (B \triangle C)$. Let A, B, C be arbitrary elements of 2^S. Then

$$\begin{aligned}(A \triangle B) \triangle C &= ((A \cup B) \setminus (A \cap B)) \triangle C \\ &= (((A \cup B) \setminus (A \cap B)) \cup C) \setminus (((A \cup B) \setminus (A \cap B)) \cap C) \\ &= (A \cup ((B \cup C) \setminus (B \cap C))) \setminus (A \cap ((B \cup C) \setminus (B \cap C))) \\ &= A \triangle ((B \cup C) \setminus (B \cap C)) \\ &= A \triangle (B \triangle C)\end{aligned}$$

   Note that the two big expressions are equal since we can show that they are both represented by the following picture, where the shaded area may have elements and the unshaded area cannot[1].

[1] Note that there is an alternate proof of this: Write each set as a permutation of 1s and 0s. Define a bijection f with the property that $f(A \triangle B) = (f(A) + F(B)) \bmod 2$. Then commutativity follows easily.

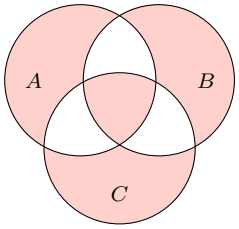


Figure 2.1: Power set group associativity.

To confirm that the identity element is the $\emptyset$, it will suffice to show that $A\triangle\emptyset = \emptyset\triangle A = A$ for all $A \in 2^S$. Let A be an arbitrary element of 2^S. Then

$$\begin{aligned} A\triangle\emptyset &= (A \cup \emptyset) \setminus (A \cap \emptyset) \\ &= A \setminus \emptyset \\ &= A \\ &= A \setminus \emptyset \\ &= (\emptyset \cup A) \setminus (\emptyset \cap A) \\ &= \emptyset\triangle A \end{aligned}$$

as desired.

To confirm $A = A^{-1}$, we must show that $A\triangle A = \emptyset$. But we have that

$$\begin{aligned} A\triangle A &= (A \cup A) \setminus (A \cap A) \\ &= A \setminus A \\ &= \emptyset \end{aligned}$$

as desired. □

3. Let G be a group.
   (a) Prove that for any $g_1, g_2 \in G$, we have $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$.
   (b) G is called **abelian** if for every two elements $g_1, g_2 \in G$, we have $g_1g_2 = g_2g_1$. In other words, G is abelian if multiplication is commutative.
   (c) Prove that the group 2^S from the previous problem is abelian.
   (d) Prove that if $g^2 = e$ for any $g \in G$, then G is abelian.

   Proof. To prove that G is abelian, part (b) tells us that it will suffice to show that for all $g_1, g_2 \in G$, we have $g_1g_2 = g_2g_1$. Let g_1, g_2 be arbitrary elements of G. Then

$$\begin{aligned} g_1g_2 &= eg_1g_2e && \text{Identity} \\ &= (g_1^{-1}g_1)(g_1g_2)(g_2g_2^{-1}) && \text{Inverse} \\ &= g_1^{-1}g_1^2g_2^2g_2^{-1} && \text{Associativity} \\ &= g_1^{-1}eeg_2^{-1} && \text{Property} \\ &= g_1^{-1}g_2^{-1} && \text{Identity} \\ &= (g_2g_1)^{-1} && \text{Part (a)} \\ &= (g_2g_1)^{-1}e && \text{Identity} \\ &= (g_2g_1)^{-1}(g_2g_1)^{-1}(g_2g_1) && \text{Inverse} \\ &= eg_2g_1 && \text{Property} \\ &= g_2g_1 && \text{Identity} \end{aligned}$$

   as desired. □

4. **The Inclusion-Exclusion Principle**

   Consider N objects and some list $P_1, P_2, \ldots, P_n$ of their properties. Let N_i be the number of objects satisfying P_i, N_{ij}, the number of objects satisfying P_i and P_j, and so on. Prove that the number of objects satisfying none of these properties is equal to

$$N - \sum N_i + \sum_{i_1<i_2} N_{i_1 i_2} - \sum_{i_1<i_2<i_3} N_{i_1 i_2 i_3} + \cdots + (-1)^n N_{123\ldots n}$$

   Proof. Induct on the number of properties. □

5. Prove that if we remove two opposite corners of a chessboard, the board cannot be covered by dominoes (each domino covers two neighboring cells of the chessboard).

   Proof. Opposite corners necessarily have the same color. However, each domino covers two squares of differing color. Therefore, since removing two opposite corners will lead to an excess of two squares of one color, there will be no way to cover every square. □

6. Define a sequence of Fibonacci numbers by formula:

$$F_0 = F_1 = 1$$
$$F_{n+2} = F_{n+1} + F_n \text{ for } n \geq 0$$

   (a) Prove that F_n gives the number of ways to present n as a sum of 1 and 2. For instance, $4 = 1+1+1+1 = 2+1+1 = 1+2+1 = 1+1 = 2 = 2+2$, so $F_5 = 4$.

   Proof. Clearly, F_0 and F_1 trivially equal 1. Then to write F_{n+2}, we can start by fixing 2 and know that there are F_n ways to write $(n+2)-2$ as a sum of 1 and 2. But 2 can also be written as $1+1$, so if we fix a 1, we know that there are F_{n+1} ways to write the sum like this. Thus, the total number of ways to write $n+2$ are $F_n + F_{n+1}$. □

   (b) Prove the **Cassini identity**:

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^{n+1}$$

   Proof. We induct on n. For the base case $n = 1$, we have

$$\begin{aligned} F_2F_0 - F_1^2 &= 2 - 1 \\ &= 1 \\ &= (-1)^{1+1} \end{aligned}$$

   Now suppose inductively that $F_{n+1}F_{n-1} - F_n^2 = (-1)^{n+1}$. It follows that

$$\begin{aligned} F_{n+1}F_{n-1} - F_n^2 &= (-1)^{n+1} \\ F_{n+1}(F_{n+1} - F_n) - F_n^2 &= (-1)^{n+1} \\ F_{n+1}^2 - F_nF_{n+1} - F_n^2 &= (-1)^{n+1} \\ -1(F_{n+1}^2 - F_n(F_{n+1} + F_n)) &= (-1)^{n+2} \\ F_{(n+1)+1}F_{(n+1)-1} - F_{n+1}^2 &= (-1)^{(n+1)+1} \end{aligned}$$

   as desired[2]. □

   (c) Prove that the sum of the elements on any diagonal of the pascal triangle is a Fibonacci number:

$$\sum_{k=0}^{n/2} \binom{n-k}{k} = F_{n+1}$$

[2] There is an alternate proof using the properties of determinants.

(d) Consider a generating function $f(x) = F_0 + F_1x + F_2x^2 + \cdots$. Prove that $f(x) = \frac{1}{1-x-x^2}$.

(e) Prove the following **Binet's Formula** for Fibonacci numbers:

$$F_n = \frac{\gamma^n - (-\gamma^{-1})^n}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Proof. We induct on n. For the base cases $n = 0, 1$, we have that

$$\begin{aligned} F_0 &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^0 - \left(\frac{1-\sqrt{5}}{2}\right)^0\right) \\ &= \frac{1}{\sqrt{5}}(1-1) \\ &= 0 \end{aligned} \qquad \begin{aligned} F_1 &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right) \\ &= \frac{1}{\sqrt{5}}\left(\frac{2\sqrt{5}}{2}\right) \\ &= 1 \end{aligned}$$

Now suppose inductively that $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ and $F_{n-1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right)$. Then

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) + \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2}+1\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{3-\sqrt{5}}{2}\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{6+2\sqrt{5}}{4}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{6-2\sqrt{5}}{4}\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+2\sqrt{5}+5}{4}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-2\sqrt{5}+5}{4}\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{(1+\sqrt{5})^2}{2^2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{(1-\sqrt{5})^2}{2^2}\right)\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right) \end{aligned}$$

as desired. □

2.5 PSet 3

7/2: 1. **Euler's function**

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n and $\varphi(n)$ be the number of integers from 1 to n which are coprime to n. Prove that

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

2. Is it possible to draw 9 segments in the plane, so that each of them intersects exactly five other segments?

   Proof. Label the segments $\ell_1, \ldots, \ell_9$. Suppose for the sake of contradiction that ℓ_1 intersects $\ell_{i_1}, \ldots, \ell_{i_5}$ where $1 \leq i_j \leq 9$. Do this for all ℓ. Then the total number of intersections is $\frac{9\times 5}{2}$, which is not a whole number, and therefore a contradiction. □

3. Consider a regular polygon with vertices $A_1, A_2, \ldots, A_n$ and center O. Prove that

$$\overrightarrow{OA_1} + \overrightarrow{OA_2} + \cdots + \overrightarrow{OA_n} = 0$$

4. Suppose that G is a group and $S \subset G$ is a finite subset, such that if $x, y \in S$, then $xy \in S$. Prove that S is a subgroup of G.

   Proof. To prove that S is a subgroup of G, it will suffice to show that it contains an identity, that inverses exist, and that multiplication is associative. Identities exist since $g^{|S|} = e$. Inverses exist since $gg^{|S|-1} = g^{|S|-1}g = e$. Multiplication is associative follows from multiplication in G is associative. □

5. (a) Prove that the composition of a parallel transport and a central symmetry (in any order) is a central symmetry.
   (b) Prove that if one reflects a point symmetrically over points O_1, O_2, O_3 and then reflects it symmetrically over the same points once again, the point returns back to its initial position.
   (c) Consider three lines a, b, c on the plane. Let $F = S_a \circ S_b \circ S_c$. Prove that $F \circ F$ is a parallel transport.

6. Prove that a bounded figure in $\mathbb{R}^2$ cannot have more than one center of symmetry. A bounded figure is any subset of $\mathbb{R}^2$, contained in a sufficiently large disc.

7. Let S be a set with operation $* : S \times S \to S$. Consider a number A_n of ways to put brackets in an expression

$$a_1 * a_2 * \cdots * a_{n+1} \tag{2.1}$$

   For instance, $A_2 = 2$ because there are just two ways: $(a_1 * a_2) * a_3$ and $a_1 * (a_2 * a_3)$.

   (a) Compute A_1, A_2, $A - 3$, and A_4.
   (b) Prove that $A_n = A_0 A_{n-1} + A_1 A_{n-2} + \cdots + A_{n-1} A_0$. Deduce that $A_n = c_n$.
   (c) Find an explicit bijection between ways to put brackets in Equation 2.1 and triangulations of a convex $(n+2)$-gon.

8. **Sylvester's theorem (*)**

   Consider n lines in the plane, not all of which pass through the same point. Prove that there exists a point in which exactly two of the lines intersect.

   Proof. Let a finite set of points lie in the plane such that they are not all collinear. Is there a configuration such that every line is through at least three points? You can prove that the answer is NO.

   Consider points p_i and lines ℓ_j. Think about $d(p_i, l_j)$. At least one of these values will be nonzero. Thus, since there's only a finite number of distances, there will be a minimum nonzero value. Suppose p' and ℓ' minimize nonzero d. □

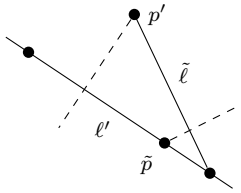


Figure 2.2: Sylvester's Theorem.

Week 3

3.1 PSet 4

7/7:

1. Consider two lines in the plane with the angle γ between them and suppose a grasshopper is jumping from one line to the other. Every jump is exactly 30 inches long, and the grasshopper jumps backwards whenever it has no other options. Prove that the sequence of its jumps is periodic if and only if $\frac{\gamma}{\pi}$ is a rational number.

2. Let $ABCD$ be a convex 4-gon and consider four squares constructed on the outside of each of its edges. Prove that the segments connecting the centers of the opposite squares are mutually perpendicular and equal in length.

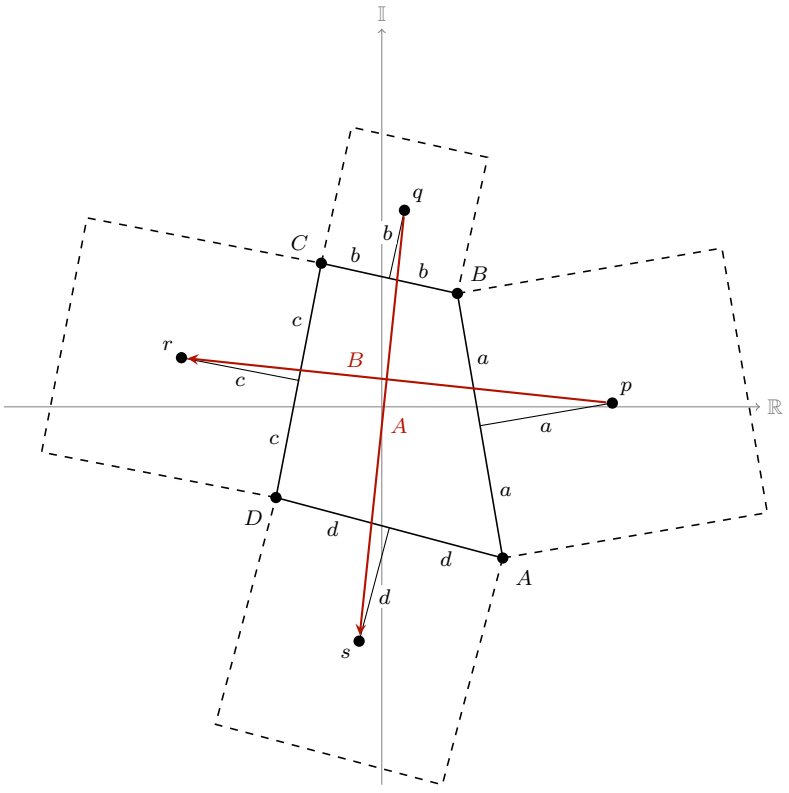


Figure 3.1: Complex polygon.

Proof. Facts:

(a) If n complex numbers add to 0, then the lines from the origin to them in the complex plane form a closed n-gon.

(b) Multiplication by i is a 90° rotation.

Let's begin. First, we define the points p, q, r, s at the center of each square in terms of the "complex numbers" from the origin at A:

$$p = (1-i)a \qquad q = 2a + (1-i)b \qquad r = 2a + 2b + (1-i)c \qquad s = 2a + 2b + 2c + (1-i)d$$

Let $A = \overrightarrow{qs}$, $B = \overrightarrow{pr}$. Then

$$\begin{aligned} A &= s - q \\ &= (1+i)b + 2c + (1-i)d \end{aligned} \qquad \begin{aligned} B &= r - p \\ &= (1+i)a + 2b + (1-i)c \end{aligned}$$

To prove that the magnitudes of A and B are the same and that they are perpendicular, Fact (a) tells us that it will suffice to show that $iB = A$, or that $A - iB = 0$. But we have that

$$\begin{aligned} A - iB &= (1+i)b + 2c + (1-i)d - i((1+i)a + 2b + (1-i)c) \\ &= (1+i)b + 2c + (1-i)d - ((i-1)a + 2bi + (i+1)c) \\ &= (1-i)a + (1-i)b + (1-i)c + (1-i)d \\ &= \frac{1-i}{2} \cdot (2a + 2b + 2c + 2d) \\ &= (1-i)0 && \text{Fact (b)} \\ &= 0 \end{aligned}$$

as desired. □

3. Prove that a composition of three symmetries is a sliding symmetry.

Proof. Each symmetry reverses the orientation of a shape. Thus, three symmetries reverse the orientation like one sliding symmetry. Symmetries also have the ability to rotate an object to any desired angle (by rotating the line of symmetry). Finally, distance from the shape to the line controls position in one orthogonal direction, and the slide can control distance in the other orthogonal direction. □

4. The points $A_1, \ldots, A_n$ form a regular polygon, inscribed in a circle with the center O. A point X lies on the same circle. Prove that the images of the point X under the symmetries with axes $OA_1, OA_2, \ldots, OA_n$ form a regular polygon.

5. Remove a corner from a 101×101 chessboard. Prove that the rest cannot be covered by triominoes. A triomino is like a domino except that it consists of three squares in a row; each cell can cover one cell on a chessboard. Each triomino can either "stand" or "lie."

6. Consider a finite collection of segments on a line so that every two of them intersect. Prove that all segments have a common point.

Proof. Let $\ell_1, \ldots, \ell_n$ be a finite collection of segments on a line (i.e., a closed interval on $\mathbb{R}$). By the hypothesis, $\ell_i \cap \ell_j \neq \emptyset$ for all $i, j \in [n]$. We induct on n. For the base case $n = 1$, we clearly have $\bigcap_{i\in[1]} \ell_i = \ell_1 \neq \emptyset$ by the definition of a closed interval. Now suppose that we have proven that $\bigcap_{i\in[n]} \ell_i \neq \emptyset$; we seek to prove the claim for $n+1$. First off, note that $\bigcap_{i\in[n]} \ell_i$ is a closed interval in its own right, and that its lower and upper bounds are the supremum of the lower bounds of all ℓ_i and the infimum of the upper bounds of all ℓ_i, respectively. Thus, to show that $\bigcap_{i\in[n+1]} \ell_i$ is nonempty, it will suffice to show that the the lower bound of ℓ_{n+1} is less than or equal to the upper bound of $\bigcap_{i\in[n+1]} \ell_i$, or vice versa. But clearly it must be, or ℓ_{n+1} would have an empty intersection with an ℓ_i, a contradiction. □

7. Let S be a set of $n+1$ integers from 1 to $2n$. Prove that at least two elements in S are coprime.

3.2 Dummit and Foote

3.2.0 Preliminaries

3.2.0.1 Basics

7/9:

- Know the basics of set theory.
- **Order** (of a set A): The cardinality of A.
- $\mathbb{Z}$ denotes the integers because the German word for numbers is "Zahlen."
- $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ denote the positive nonzero elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, respectively.
- **Fiber** (of f over b): The preimage of $\{b\}$ under f.
- **Left inverse** (of f): A function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A.
- **Right inverse** (of f): A function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

7/10:

- f is injective $\iff$ f has a left inverse.
- f is surjective $\iff$ f has a right inverse.
- f is a bijection $\iff$ f has a 2-sided inverse (or simply inverse).
- **Permutation** (of a set A): A bijection from A to itself.
- **Extension** (of g to B): The function $f : B \to C$ where $A \subset B$, $g : A \to C$, and $f|_A = g$.

3.2.0.2 Properties of the Integers

- "The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$."
- **Euclidean algorithm**: A procedure for finding the greatest common divisor of two integers a and b by iterating the division algorithm:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

  This yields $\gcd(a, b) = r_n$.

- Note that $(a, b) = ax + by$ as a consequence of the Euclidean algorithm (write r_n in terms of the other quantities iteratively).
  - x and y are not unique for any two integers a, b.
- If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.
- **Fundamental Theorem of Arithmetic**: If $n \in \mathbb{Z}$ and $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

- Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

  are their prime factorizations (we let $\alpha_i, \beta_j \geq 0$ so that we can express both as the product of the same primes). Then

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_s^{\min(\alpha_s,\beta_s)}$$
$$\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_s^{\max(\alpha_s,\beta_s)}$$

- **Euler φ-function**: The function $\varphi : \mathbb{Z}^+ \to \mathbb{N}$ defined by $\varphi(n)$ is the number of positive integers $a \leq n$ such that $(a, n) = 1$.
  - If p prime, then $\varphi(p) = p - 1$.
  - If p prime and $a \geq 1$, then $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.
  - If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.
  - If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)\end{aligned}$$

3.2.0.3 $\mathbb{Z} \setminus n\mathbb{Z}$: The Integers Modulo n

- Define $\sim$ on $\mathbb{Z}$ by $a \sim b \iff n \mid (b - a)$.
  - $\sim$ is an equivalence relation.
  - If $a \sim b$, we write $a \equiv b \bmod n$[1].
- **Congruence class** (of a): The equivalence class $\bar{a}$ of a mod n. *Also known as* **residue class**.

$$\begin{aligned}\bar{a} &= \{a + kn \mid k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}\end{aligned}$$

  - There are n distinct equivalence classes mod$n$.
- **Integers modulo n**: The set of equivalence classes $\mathbb{Z} \setminus n\mathbb{Z}$[2] under the equivalence relation $\sim$. *Also known as* **integers mod n**.
- **Reducing a mod n**: The process of finding the equivalence class mod$n$ of some integer a.
- **Least residue** (of a mod n): The smallest nonnegative number congruent to a mod n.
- **Modular arithmetic** (on $\mathbb{Z} \setminus n\mathbb{Z}$): The addition and multiplication operations defined by

$$\bar{a} + \bar{b} = \overline{a + b} \qquad \bar{a} \cdot \bar{b} = \overline{ab}$$

  for all $\bar{a}, \bar{b} \in \mathbb{Z} \setminus n\mathbb{Z}$.
- $(\mathbb{Z} \setminus n\mathbb{Z})^\times$ is the collection of residue classes which have a multiplicative inverse in $\mathbb{Z} \setminus n\mathbb{Z}$, i.e.,

$$(\mathbb{Z} \setminus n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z} \setminus n\mathbb{Z} \mid \exists\ \bar{c} \in \mathbb{Z} \setminus n\mathbb{Z} : \bar{a} \cdot \bar{c} = \bar{1}\}$$

  - It can be proven that $(\mathbb{Z} \setminus n\mathbb{Z})^\times$ is the set of residue classes whose representatives are relatively prime to n.
  - Thus, $(\mathbb{Z} \setminus n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z} \setminus n\mathbb{Z} \mid (a, n) = 1\}$.
  - Let a be an integer that is relatively prime to n. Then the Euclidean algorithm generates integers x, y such that $ax + ny = 1$. But this implies that $ax = 1 + (-y)n$, i.e., $ax \equiv 1 \bmod n$, so that $\bar{x}$ is the multiplicative inverse of $\bar{a}$.

[1] a is congruent to $b \mod n$.

[2] The motivation for this notation will become clear in the discussion of quotient groups and quotient rings.

3.2.1 Introduction to Groups

3.2.1.1 Group Theory

- "One of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof, one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised; can one determine *all* the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration."
- Motivation?

3.2.1.2 Basic Axioms and Examples

7/12:

- **Binary operation** (on a set G): A function $\star : G \times G \to G$.
- **Closed** (subset $H \subset G$ under $\star$): A subset $H \subset G$ such that $a \star b \in H$ for all $a, b \in H$, where $\star$ is a binary operation on G.
  - Alternatively, we can require that $\star|_H$ be a binary operation on H.
- If $\star$ is an associative (respectively, commutative) binary operation on G and $\star|_H$ is a binary operation on $H \subset G$, then $\star$ is associative (respectively, commutative) on H as well.
- **Group**: An ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
  (i) Associativity: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.
  (ii) Identity: There exists an element $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
  (iii) Inverse: For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
- **Abelian** (group): A group $(G, \star)$ such that for all $a, b \in G$, $a \star b = b \star a$. *Also known as* **commutative**.
- Axiom (ii) implies that G is nonempty.
- **Direct product** (of $(A, \star)$ and $(B, \diamond)$): The group $A \times B$ whose elements are those in the Cartesian product
$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$
and whose operation is defined component-wise by
$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$
- Let G be a group under the operation $\star$.

  Proposition 1.

  (1) *The identity of G is unique.*
  (2) *For each $a \in G$, a^{-1} is uniquely determined.*
  (3) $(a^{-1})^{-1} = a$ *for all* $a \in G$.
  (4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$.
  (5) *Generalized associative law: For any $a_1, \ldots, a_n \in G$, the value of $a_1 \star \cdots \star a_n$ is independent of how the expression is bracketed.*

- Let G be a group and let $a, b \in G$.

  Proposition 2. *The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,*

(1) *If $au = av$, then $u = v$;*

(2) *If $ub = vb$, then $u = v$.*

- **Order** (of an object $x \in G$): The smallest positive integer n such that $x^n = 1$. *Denoted by* $\boldsymbol{|x|}$.
  - We say x is of order n.
  - If no such n exists, the order of x is defined to be infinity and x is said to be of infinite order.
- $|g| = 1 \iff g = e$.
- Is $|\bar{x}|$ for $\bar{x} \in \mathbb{Z} \setminus n\mathbb{Z}$ equal to $\gcd(x, n)$?
- **Multiplication table** (of a finite group G): The $n \times n$ matrix whose i, j entry is the group element $g_i g_j$, where $G = \{g_1, \ldots, g_n\}$ and $g_1 = e$. *Also known as* **group table**.

Exercises

5. Prove for all $n > 1$ that $\mathbb{Z} \setminus n\mathbb{Z}$ is not a group under multiplication of residue classes.

Proof. Let n be an arbitrary natural number such that $n > 1$. Consider $\bar{0} \in \mathbb{Z} \setminus n\mathbb{Z}$. Since $\bar{x} \cdot \bar{0} = \bar{0}$ for all $\bar{x} \in \mathbb{Z} \setminus n\mathbb{Z}$, there is no element $\bar{0}^{-1} \in \mathbb{Z} \setminus n\mathbb{Z}$ such that $\bar{0} \cdot \bar{0}^{-1} = \bar{1}$. Thus, there is clearly no multiplicative inverse for $\bar{0}$ in $\mathbb{Z} \setminus n\mathbb{Z}$, contradicting axiom (iii). □

6. Determine which of the following sets are groups under addition:

(a) The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd.

Answer. Yes.
Closure: Let $\frac{a}{b}, \frac{c}{d}$ be two such rational numbers. Then since the product of two odd numbers is odd, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ is also an element of this set.
Axiom (i): As stated in the text, the associativity of a closed subset of a group under the same operation follows from the associativity of the original group.
Axiom (ii): Identity is 0.
Axiom (iii): Inverse of $\frac{a}{b}$ is $-\frac{a}{b}$, which is also clearly in the set since b is consistently odd. □

(b) The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even.

Answer. Yes.
Symmetric to (a). □

(c) The set of rational numbers of absolute value < 1.

Answer. No.
Not closed: $|\frac{2}{3} + \frac{2}{3}| = |\frac{4}{3}| \geq 1$, for instance. □

(d) The set of rational numbers of absolute value ≥ 1 together with 0.

Answer. No.
Not closed: $|\frac{3}{2} + (-\frac{1}{1})| = |-\frac{1}{2}| = \frac{1}{2} < 1$, for instance. □

(e) The set of rational numbers with denominators equal to 1 or 2.

Answer. Yes.
Closed: $\mathrm{lcm}(1, 1) = 1$, $\mathrm{lcm}(1, 2) = 2$, and $\mathrm{lcm}(2, 2) = 2$, so the denominator stays within the constraints of the set.
Axioms (i-iii): Symmetric to (a). □

(f) The set of rational numbers with denominators equal to 1, 2, or 3.

Answer. No.
Not closed: $\operatorname{lcm}(2,3) = 6 \notin \{1,2,3\}$, so $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$, for instance. □

8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of **roots of unity** in $\mathbb{C}$).

Proof. Closed: Let $z_1, z_2 \in G$ such that $z_1^n = 1$ and $z_2^m = 1$. Consider these complex numbers in the forms $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$ (note that $r_1 = r_2 = 1$ since if not, repeated exponentiation would change the magnitude of z^n vs. z^{2n}, etc.[3]). It follows that $z_1^n = e^{in\theta_1} = 1$ and $z_2^m = e^{im\theta_2} = 1$. Thus, $n\theta_1 \equiv 0 \bmod 2\pi$ and $m\theta_2 \equiv 0 \bmod 2\pi$. Consequently, $nm\theta_1 \equiv 0 \bmod 2\pi$ and $nm\theta_2 \equiv 0 \bmod 2\pi$. But this implies that $nm(\theta_1 + \theta_2) \equiv 0 \bmod 2\pi$, i.e., that nm is an integer such that $(z_1 z_2)^{nm} = e^{i(nm(\theta_1+\theta_2))} = 1$, as desired.
Axiom (i): As stated in the text, the associativity of a closed subset of a group under the same operation follows from the associativity of the original group.
Axiom (ii): Clearly, $1 = 1 + 0i \in \mathbb{C}$ and $1^1 = 1$, so $1 \in G$. Additionally, by the definition of 1, $z \cdot 1 = 1 \cdot z = z$, as desired.
Axiom (iii): Let $z \in G$ be arbitrary. Choose $z^{-1} = z^{n-1}$. Then

$$\begin{aligned} z \cdot z^{-1} &= z \cdot z^{n-1} \\ &= z^n \\ &= 1 \\ &= z^n \\ &= z^{n-1} \cdot z \\ &= z^{-1} \cdot z \end{aligned}$$

as desired. □

(b) Prove that G is not a group under addition.

Proof. By part (a), $1 \in G$. However, $1 + 1 = 2 \notin G$ since 2^n grows exponentially and never equals 1. □

15. Prove that $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

Proof. We induct on n. For the base case $n = 2$, we have by Proposition 1.4 that $(a_1 a_2) = a_2^{-1} a_1^{-1}$, as desired. Now suppose inductively that we have proven the claim for n; we now seek to prove it for $n + 1$. But we have that

$$\begin{aligned} (a_1 a_2 \cdots a_{n+1})^{-1} &= a_{n+1}^{-1}(a_1 a_2 \cdots a_n)^{-1} && \text{Proposition 1.4} \\ &= a_{n+1}^{-1} a_n^{-1} \cdots a_1^{-1} && \text{Hypothesis} \end{aligned}$$

as desired. □

24. If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

Proof. We divide into three cases ($n = 0$, $n \in \mathbb{N}$, $n \in -\mathbb{N}$).

If $n = 0$, then $(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0$, as desired.

[3] This notion can be formalized in a contradiction argument.

If $n \in \mathbb{N}$, we induct on n. For the base case $n = 1$, we have that $(ab)^1 = ab = a^1b^1$ trivially, as desired. Now suppose inductively that we've proven the claim for n; we now seek to prove it for $n+1$. But we have that

$$\begin{aligned}(ab)^{n+1} &= (ab)^n(ab)\\ &= a^nb^nab\\ &= a^nab^nb\\ &= a^{n+1}b^{n+1}\end{aligned}$$

as desired.

If $n \in -\mathbb{N}$, then $-n \in \mathbb{N}$. Therefore, by the above,

$$\begin{aligned}(ab)^n &= \frac{1}{(ab)^{-n}}\\ &= \frac{1}{a^{-n}b^{-n}}\\ &= \frac{1}{a^{-n}} \cdot \frac{1}{b^{-n}}\\ &= a^nb^n\end{aligned}$$

as desired. □

3.2.1.3 Dihedral Groups

- **Dihedral group**: A group whose elements are symmetries of geometric objects.
- D_{2n} denotes the group of symmetries of a regular n-gon.
- Note that $|D_{2n}| = 2n$.
- D_{2n} is related to S_n by labeling the vertices of the n-gon 1 through n.
- "Since symmetries are rigid modtions, one sees that once the position of the ordered pair of vertices 1,2 has been specified, the action of the symmetry on all remaining vertices is completely determined."
- Fix a regular n-gon centered at the origin in the xy-plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $\frac{2\pi}{n}$ radians. Let s be the reflection about the line of symmetry through vertex 1 and the origin. Then

  (1) $1, r, r^2, \ldots, r^{n-1}$ are distinct and $r^n = 1$, so $|r| = n$.

  (2) $|s| = 2$.

  (3) $s \neq r^i$ for any i.

  (4) $sr^i \neq sr^j$ for all $0 \leq i,\ j \leq n-1$ with $i \neq j$, so

  $$D_{2n} = \{1, \ldots, r^{n-1}, s, \ldots, sr^{n-1}$$

  In other words, each element of D_{2n} can be writen uniquely in the form s^kr^i for some $k = 0, 1$ and $0 \leq i \leq n-1$.

  (5) $rs = sr^{-1}$. Thus, r, s do not commute so D_{2n} is non-abelian.

  (6) $r^is = sr^{-i}$ for all $0 \leq i \leq n$. This indicates how to commute s with powers of r.
- Note that r, s in the above example are **generators**, which will only be rigorously introduced later but are useful now and thus used informally.
- **Generators** (of G): A subset $S \subset G$ with the property that every element in G can be written as a (finite) product of elements of S and their inverses. *Denoted by* $G = \langle \boldsymbol{S} \rangle$.

  - We write that "G is generated by S" or "S generates G."
  - Examples: $\mathbb{Z} = \langle 1 \rangle$ and $D_{2n} = \langle r, s \rangle$.

- **Relation**: An equation in a general group G that the generators satisfy.
  - Example: In D_{2n}, we have $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$.

- **Presentation** (of G): The set S of generators of G along with the relations $R_1, \ldots, R_m$, where each R_i is an equation in the elements from $S \cup \{1\}$, such that any relation among the elements of S can be deduced from these. *Denoted by* $G = \langle \boldsymbol{S \mid R_1, \ldots, R_m} \rangle$.
  - Example: $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.

- List examples and works with **collapsing** presentations, i.e., ones in which some important relations are consequences of others.

3.2.1.4 Symmetric Groups

- **Symmetric group** (on the set Ω): The group $(S_\Omega, \circ)$, where S_Ω is the set of all bijections from a nonempty set Ω to itself and $\circ$ is function composition. *Also known as* **permutations** (of Ω).
  - We write $\sigma \in S_\Omega$ and let $1 \in S_\Omega$ be the identity function defined by $1(a) = a$ for all $a \in \Omega$.
  - If $\Omega = [n]$, then we denote S_Ω by S_n.

- $|S_n| = n!$.

- **Cycle**: A string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).
  - The cycle $(a_1\ a_2\ \ldots\ a_m)$ is the permutation which sends a_i to a_{i+1} for all $1 \leq i \leq m-1$ and sends a_m to a_1.

- **Cycle decomposition** (of σ): The product of all cycles, often written in the form

$$(a_1\ a_2\ \ldots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \ldots\ a_{m_2}) \ldots (a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \ldots\ a_{m_k})$$

- Cycle decomposition algorithm:
  1. To start a new cycle, pick the smallest element of $[n]$ which has not yet appeared in a previous cycle — call it a (if you are just starting, choose $a = 1$); begin the new cycle: "$(a$".
  2. Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: "$(a\ b$".
  3. Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: "$(a\ b\ c$". Repeat this step using the number c as the new value for b until the cycle closes.
  4. Remove all cycles of **length** 1.

- Example:

$$\begin{array}{llll} \sigma(1) = 12 & \sigma(2) = 2 & \sigma(3) = 3 & \sigma(4) = 1 \\ \sigma(5) = 11 & \sigma(6) = 9 & \sigma(7) = 5 & \sigma(8) = 10 \\ \sigma(9) = 6 & \sigma(10) = 4 & \sigma(11) = 7 & \sigma(12) = 8 \end{array}$$

  becomes

$$\sigma = (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$$

- **Length** (of a cycle): The number of integers which appear in it.
- ***t*-cycle**: A cycle of length t.
- **Disjoint** (cycles): Two cycles that have no numbers in common.
- The convention of removing all cycles of length 1 makes it so that any cyclic decomposition essentially represents a function $\sigma : \mathbb{N} \to \mathbb{N}$.
- For any $\sigma \in S_n$, the cyclic decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.
  - Continuing with the above example, $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(7\ 11\ 5)(9\ 6)$.
- S_n is a non-abelian group for all $n \geq 3$.
- Disjoint cycles commute.
- The order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition.

3.2.1.5 Matrix Groups

- Since $\mathbb{Z} \setminus p\mathbb{Z}$, p prime, is a finite field, we denote it $\mathbb{F}_p$.
- **Field**: A set F together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an abelian group (call its identity 0), $(F - \{0\}, \cdot)$ is also an abeilan group, and the following distributive law holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in F$.
- $\boldsymbol{F^\times}$: The set $F - \{0\}$ where F is a field.
- **General linear group of degree $\boldsymbol{n}$**: The set of all $n \times n$ matrices, where $n \in \mathbb{Z}^+$, whose entities come from the field F and whose determinant is nonzero. *Denoted by* $\boldsymbol{GL_n(F)}$.

3.2.1.6 The Quaternion Group

- **Quaternion group**: The group

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$\begin{aligned} 1 \cdot a = a \cdot 1 = a && \text{for all } a \in Q_8 \\ (-1) \cdot (-1) = 1 && \\ (-1) \cdot a = a \cdot (-1) = -a && \text{for all } a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 && \end{aligned}$$

$$\begin{array}{lll} i \cdot j = k & j \cdot k = i & k \cdot i = j \\ j \cdot i = -k & k \cdot j = -i & i \cdot k = -j \end{array}$$

- Q_8 is a non-abelian group of order 8.

3.2.1.7 Homomorphisms and Isomorphisms

- **Homomorphism**: A map $\varphi : G \to H$ such that $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$ for all $x, y \in G$, where $(G, \star)$ and $(H, \diamond)$ are groups.
  - Intuitively, a map is a homomorphism if it respects the group structures of its domain and codomain.
- **Isomorphism**: A map $\varphi : G \to H$ such that φ is a homomorphism and a bijection.
  - If such a φ exists, we write that G and H are isomorphic, are of the same isomorphism type, and that $G \cong H$.
  - Intuitively, such a map implies that G and H are the same group; they simply have relabeled elements.
- The existence of an isomorphism between two groups implies that any property of G that can be derived from the group axioms also holds for H, and vice versa.
- $\cong$ is an equivalence relation.
- **Isomorphism class**: An equivalence class of a nonempty collection $\mathcal{G}$ of groups under $\cong$.
- $|\triangle| = |\Omega| \iff S_\triangle \cong S_\Omega \iff |S_\triangle| = |S_\Omega|$.
- **Classification theorem**: A theorem stating what properties of a structure specify its isomorphism type.
  - For example, a general classification theorem would assert that if G is an object with some structure (such as a group) and G has property $\mathcal{P}$, then any other similarly structured object (group) X with property $\mathcal{P}$ is isomorphic to G.
- If $\varphi : G \to H$ is an isomorphism, then
  1. $|G| = |H|$.
  2. G is abelian iff H is abelian.
  3. For all $x \in G$, $|x| = |\varphi(x)|$.
- Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H when each s_i is replaced by r_i. Then there is a unique homomorphism $\varphi : G \to H$ which sends $s_i \mapsto r_i$.

3.2.1.8 Group Actions

- **Group action** (of a group G on a set A): A map $\cdot : G \times A \to A$ such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and such that $1 \cdot a = a$ for all $a \in A$.
- What is a group action?
- Let G act on A, and for each $g \in G$, define $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then
  1. For each fixed $g \in G$, σ_g is a permutation of A;

     Proof. We prove that σ_g has a two-sided inverse; it follows that σ_g is a permutation. Let $g \in G$ be arbitrary. Then by Axiom (iii), there exists g^{-1}. Therefore,

     $$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} \cdot g) \cdot a \\ &= 1 \cdot a \\ &= 1\end{aligned}$$

We can prove something similar in the other direction. □

2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

   Proof. Let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$ for all $g \in G$. To prove that φ is a homomorphism, it will suffice to show that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all $g_1, g_2 \in G$. To verify the equality of functions, we must show that for all $a \in A$, $\varphi(g_1 \cdot g_2)(a) = (\varphi(g_1) \circ \varphi(g_2))(a)$. Let a be an arbitrary element of A. Then

$$\begin{aligned}
\varphi(g_1 \cdot g_2)(a) &= \sigma_{g_1 \cdot g_2}(a) \\
&= (g_1 \cdot g_2) \cdot a \\
&= g_1 \cdot (g_2 \cdot a) \\
&= g_1 \cdot \sigma_{g_2}(a) \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) \\
&= (\sigma_{g_1} \circ \sigma_{g_2})(a) \\
&= (\varphi(g_1) \circ \varphi(g_2))(a)
\end{aligned}$$

   □

- Intuitively, a group action of G on A means that every element $g \in G$ acts as a permutation on A in a manner consistent with the group operations in G.
- **Permutation representation** (associated to the group action $\cdot$): The homomorphism $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$ for all $g \in G$, defined by $\varphi(g)(a) = \sigma_g(a) = g \cdot a$ for all $a \in A$.
- Getting into what a representation is?

3.2.2 Subgroups

3.2.2.1 Definition and Examples

- Two way of unraveling the structure of an axiomatically defined mathematical object are to study subsets of the object that satisfy the same axioms, and to study quotients (which, roughly speaking, collapse one group onto a smaller one).
- **Subgroup** (of G): A subset $H \subset G$ that is nonempty and closed under products and inverses. *Denoted by* $H \leq G$.
  - In other words, we require that $x^{-1} \in H$ for all $x \in H$, and $xy \in H$ for all $x, y \in H$.
  - Alternatively, a subgroup of $(G, \cdot)$ is a subset of G that is a group in its own right under $\cdot$.
- $H \leq G$ and $H \neq G$ imply $H < G$.
- **Trivial subgroup**: The subgroup $H = \{1\}$, henceforth denoted by 1.
- $\leq$ is transitive: $K \leq H \leq G \Longleftarrow K \leq G$.
- Let G be a group.

  Proposition 3 (The Subgroup Criterion)**.** *A subset $H \subset G$ is a subgroup iff*

  (1) *$H \neq \emptyset$;*

  (2) *For all $x, y \in H$, $xy^{-1} \in H$.*

  Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Exercises

1. In each of a-e, prove that the specified subset is a subgroup of the given group.

(a) The set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition).

(b) The set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication).

(c) For fixed $n \in \mathbb{Z}^+$, the set of rational numbers whose denominators divide n (under addition).

(d) For fixed $n \in \mathbb{Z}^+$, the set of rational numbers whose denominators are relatively prime to n (under addition).

(e) The set of nonzero real numbers whose square is a rational number (under multiplication).

4. Give an explicit example of a group G and an infinite subset $H \subset G$ that is closed under the group operation but is not a subgroup of G.

5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

8. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup iff either $H \subseteq K$ or $K \subseteq H$.