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.

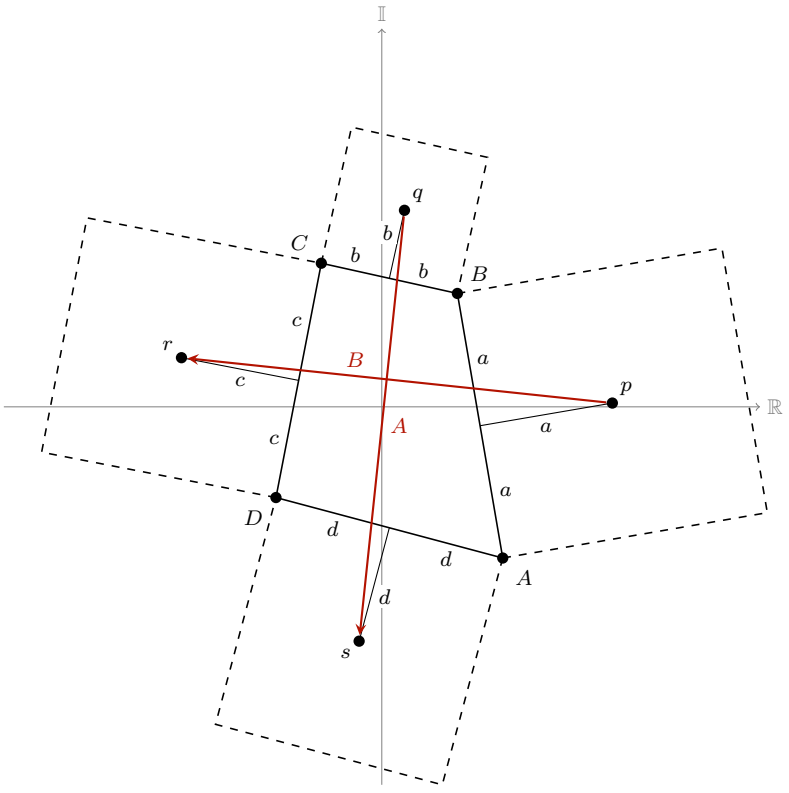

Figure 3.1: Complex polygon.

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 $a \bmod n$. *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 $\bmod n$.
- **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 $\bmod n$ of some integer a.
- **Least residue** (of $a \bmod n$): The smallest nonnegative number congruent to $a \bmod n$.
- **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 $K \subseteq H$.