Week 1

Motivating Group Theory

1.1 Groups as Shuffles

9/28:

- Office hours will be pooled between the two sections.
  - Our section's TA is Abhijit Mudigonda (abjihitm@uchicago.edu). His office hours will always be in JCL 267[1]. The times are...
    - Monday: 12:30-2:00 (OH).
    - Wednesday: 1:30-2:30 (PS).
    - Thursday: 12:30-2:00 (OH).
  - The other section's TA is Ray Li (rayli@uchicago.edu). His office hours will always be in Eck 17[2]. The times are...
    - Tuesday: 5:00-7:00 (OH).
    - Thursday: 4:00-5:00 (OH).
    - Thursday: 5:00-6:00 (PS).
- Textbook: Abstract Algebra. Download the PDF from LibGen.
- Weekly HW due on Monday at the beginning of class. Submit online or in person. There is a webpage w/ all the homeworks, but don't do them all at once because they're subject to change.
- Notes on math and math pedagogy.
  - There's a tendency to say here's an object, here's its properties, etc.
  - But this is not historically accurate or motivated. Calegari really gets it! Math is motivated by abstracting examples.
  - Let's not just define a group, but start with an example. This week, we will give examples of groups. In later weeks, we will establish the axiomatic framework that is really only there to understand these examples.
  - Don't stare at the page blankly waiting for inspiration when doing homework; think of examples first and test out your intuition on them to actually understand what the question means.
  - There are some hard problems; work with each other, but acknowledge our collaborators.
  - In-class midterm; final will be take-home. Calegari doesn't like timed exams.
- Today's example: Shuffling.
  - 52 cards; can be shuffled.

[1] JCL is John Crerar Library.

[2] Eckhart basement.

- Number of shuffles:

$$|\text{shuffles}| = 52! \approx 8 \times 10^{67}$$

- Properties of shuffles.
  - **Distinguished shuffle**: e, the identity shuffle, where you do nothing.
  - Shuffle once; shuffle again. The composition of two shuffles is another shuffle.
  - If you repeat the *same* shuffle enough times, the cards will come back to the same order.
    - ➢ Let σ be a shuffle, and $n \in \mathbb{N}$. Does there exist n such that

$$\sigma^n = \underbrace{\sigma \circ \cdots \circ \sigma}_{n \text{ times}} = e$$

    - ➢ Proving this: By the piegeonhole principle, if you have $\sigma^1, \ldots, \sigma^{52!+1}$, then we have repeats a, b with $52! + 1 \geq a > b \geq 1$ such that $\sigma^a = \sigma^b$. This statement is weaker than we want, though.
    - ➢ We need more tools. A shuffle is a bijection/permutation. Thus, for every σ, there exists σ^{-1}. This allows us to do this:

$$\begin{aligned} \sigma^a &= \sigma^b \\ \sigma^{-b} \circ \sigma^a &= \sigma^{-b} \circ \sigma^b \\ \sigma^{a-b} &= e \end{aligned}$$

    - ➢ This implies a bound! We get that $n \leq 52!$, so $a - b \leq 52!$.
- Define two shuffles: A and B.
  - A splits the deck into two halves (cards 1-26 and 27-52) and stacks (from the top down) the first card off of the 1-26 pile, then the first card off of the 27-52 pile, then the second card off of the 1-26 pile, then the second card off of the 27-52 pile, etc. The final order is $1, 27, 2, 28, \ldots, 26, 52$.
  - B does the same thing as A but with the first card off of the 27-52 pile. The final order is $27, 1, 28, 2, \ldots, 52, 26$.
- Computation shows that $A^8 = e$ and $B^{52} = e$.
  - For A, $2 \to 3 \to 5 \to 9 \to 17 \to 33 \to 14 \to 27 \to 2$.
  - For B, we can do the same thing but obviously the cycle is much longer.
- We shouldn't necessarily have an intuition for this right now, but in doing more examples, Calegari certainly believes we can develop it.
- First HW problem (due Friday). Can, just by using combinations of A and B, we generate any possible shuffle? Hint: Develop your intuition on a smaller value of 52.

- I really like Calegari. Very nice, relatable, not demeaning.
- **Binary operation** (on G): A map from $G \times G \to G$.
- **Group**: A mathematical object consisting of a set G and a binary operation $*$ on G satisfying the following properties.
  1. There exists an identity element $e \in G$ such that $e \times g = g \times e = g$ for all $g \in G$.
  2. For any $g \in G$, there exists $h \in G$ such that $h * g = g * h = e$.
  3. (Associativity) For any $g_1, g_2, g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.

  Denoted by $(\boldsymbol{G}, \boldsymbol{*})$.
- In the cards example, the elements of G are the shuffles and $*$ is the composition operation between two shuffles.

- Aside on shuffles: For bijections, $h(g(x)) = x$ implies $g(h(y)) = y$.
  - Proof: Let $x = h(y)$ — we can do this since h is a bijection. Then since $h(g(h(y))) = h(y)$ and h is injective, $g(h(y)) = y$. This works for all y.
- The set of shuffles, together with composition, does form a group.
- Theorem: If G is a group such that $|G| < \infty$, then any $g \in G$ has finite **order**, i.e., there exists n such that $g^n = e$.
- Lemma:
  1. The identity e is unique.
     - Let e_1, e_2 be identities. Then
     $$e_1 = e_1 * e_2 = e_2$$
  2. Inverses are unique.
     - Let h, h' be inverses of g. Then
     $$h = e * h = (h' * g) * h = h' * (g * h) = h' * e = h'$$
- Proving examples is easier, but these aren't that hard.
- If you understand everything about S_5, you'll understand everything about this course.

1.2 Blog Post: What is Group Theory About?

From Calegari (2022).

10/24:
- Many great ideas on how mathematics should be taught.
  - Example: "A natural mathematical question is: How do we quantify this symmetry? This is unlike mathematical questions you might be used to, like 'what is 2^{10}' or 'what is $\int_{-1}^{1} \sqrt{1 - x^2}$,' but it is actually reflective of what real mathematicians do."
- A terrific intuitive motivation for group theory.
- Using symmetry to put constraints on physical laws.
  - Suppose we want to understand the gravitational attraction between two particles $\mathbf{x}, \mathbf{y}$ in $\mathbb{R}^3$.
  - The gravitation pull F has a certain magnitude which depends on the positions of the two particles, i.e.,
  $$F(\mathbf{x}, \mathbf{y}) = F(x_1, x_2, x_3, y_1, y_2, y_3)$$
  - However, "our conception of this force is that it shouldn't depend on how we are labeling the coordinates," i.e., the force should be invariant under translation. Thus,
  $$F(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} - \mathbf{y}, \mathbf{0}) = F(x_1 - y_1, x_2 - y_2, x_3 - y_3, 0, 0, 0)$$
  - Going further, the force should not depend on the direction, but only the distance between the two particles. Thus,
  $$F(\mathbf{x}, \mathbf{y}) = H(|\mathbf{x} - \mathbf{y}|)$$
  - Thus, we see that through only consideration of symmetry, we have put strong constraints on how the force of gravity may behave.
- Review of the riffle shuffle stuff from class.

1.3 Blog Post: The Axioms of a Group

From Calegari (2022).

- Relevant section from Dummit and Foote (2004): 1.1.
- Review of the content covered in class, plus the cancellation lemma (from the 10/3 lecture).
- Note that the cancellation lemma for groups is stronger than the one for the real numbers.
  - In $\mathbb{R}$, we have $xy = xz$ implies $y = z$ or $x = 0$, but the latter case doesn't happen in groups.
  - One consequence of this observation is that $\mathbb{R}$ under numerical multiplication does not form a group.

1.4 The Cube Group

9/30:

- Can't download `.tex` file for homework?
  - Calegari will check it.
- Detail on the homework?
  - Up to your level of confidence in what you think is clear to be true.
  - The problem is not about doing linear algebra; it's about finding some facts about linearly algebraic objects.
  - Concentrate on the new geometry of the situation.
  - Project confidence to the grader that you know what you're doing.
- The symmetries of the cube.
  - Rotational symmetries.
  - Rigid transformation.
  - Preserves lengths, angles, and lines.
  - A map from the cube to itself, i.e., ϕ : cube $\to$ cube.
  - No scaling allowed.
  - Reflectional symmetries are *not* going to be allowed for today; we will insist that the orientation is also preserved for now.
  - We want the set of all rotations and compositions of rotations. (Are compositions of rotations also rotations? We'll answer later. Yes they are.)
- Symmetries should be composable: If you compose two symmetries, you should get a third one.
  - In other words, we want the symmetries to form a group.
- We want to fix the center of the cube at the origin. Thus, a symmetry can be a linear map $M : \mathbb{R}^3 \to \mathbb{R}^3$.
  - We want it to preserve angles, i.e., orthogonality. Thus, we should assert $MM^T = I$.
  - We also want it to preserve orientation. Then we should have $\det(M) = 1$.
- **Cu**: The cube group.
- Does the permutation of faces determine M?
  - Yes.
  - Furthermore, if we know where e_1, e_2 go, then the fact that orientation and orthogonality are preserved implies that we know where e_3 goes. Thus, M is determined by two (adjacent) faces.

- An upper bound on $|\text{Cu}|$.
  - Send e_1 to one of 6 faces and send e_2 to one of the 5 remaining faces (so $|\text{Cu}| \leq 6 \cdot 5 = 30$).
  - Send e_1 to one of 6 faces and send e_2 to one of the four remaining *adjacent* faces (so $|\text{Cu}| \leq 6 \cdot 4 = 24$).
  - And, in fact, $|\text{Cu}| = 24$.
- Moreover, since the rotations of the cube are determined by permutations of the faces, we can map $\text{Cu} \hookrightarrow S_6$. Additionally, composing any permutations of the faces is the same as composing any permutations of S_6, i.e., ϕ is an **injective homomorphism** to a **subgroup** of S_6.
- We can also think about permuting the vertices.
  - 3 vertices (chosen correctly) form a basis of $\mathbb{R}^3$.
  - Thus, since there are 8 vertices, we have another map from $\text{Cu} \hookrightarrow S_8$.
  - Since we can map the first vertex to any of eight and the second to only one of three adjacent vertices, the order is $8 \cdot 3 = 24$[3].
- We now have both Cu and S_4 with order 24. Are they isomorphic?
  - One characteristic of a cube that numbers four are its four diagonals. This induces a function from $\text{Cu} \to S_4$. We now just need to prove it's bijective.
  - Let v_1, v_2, v_3, v_4 be the vertexes of one face. Then $-v_1, \dots, -v_4$ are the vertexes of the opposite face, and the line from each v_i to $-v_i$ is a diagonal of the cube. To prove that the function is bijective, we will show that different elements of Cu map to different elements of S_4.
  - Let A and B be actions on the cube group such that

$$\begin{aligned} Bv_1 &= \pm Av_1 \\ Bv_2 &= \pm Av_2 \\ Bv_3 &= \pm Av_3 \\ Bv_4 &= \pm Av_4 \end{aligned}$$

  - Taking $C = A^{-1}B$ means that

$$\begin{aligned} Cv_1 &= \pm v_1 \\ Cv_2 &= \pm v_2 \\ Cv_3 &= \pm v_3 \\ Cv_4 &= \pm v_4 \end{aligned}$$

  - If $Cv_1 = v_1$, it implies that $Cv_i = v_i$ for $i = 2, 3, 4$.
  - Thus, A and B are distinct?

1.5 Blog Post: Symmetries of the Cube

From Calegari (2022).

10/24:

- Motivating the definition of symmetries of the cube.
- From our intuition, symmetries can be of the form...
  1. Rotations in lines passing through the origin.
  2. Linear maps which preserve distances, angles, and orientation.

[3] We have gotten the order a different way. Deep connection to prime factorization? Edges would be $2 \cdot 12$!

- Claim: These two sets are the same.

  Proof. From HW1, the first set is SO(3). Thus, we need only prove that the second set is exactly SO(3). To begin, we will concentrate only on distances and angles.

  Let $\langle x,y\rangle$ denote the Euclidean inner product of $x,y\in\mathbb{R}^3$. Since $\langle x,y\rangle=|x||y|\cos(\theta)$, the set of all linear maps that preserve distances and angles is equal to the set of all linear maps M satisfying

  $$\langle Mx,My\rangle=\langle x,y\rangle$$

  Since $\langle x,y\rangle=x^Ty$, this means we want

  $$\begin{aligned}(Mx)^T(My)&=x^Ty\\ x^TM^TMy&=x^Ty\\ M^TM&=I\end{aligned}$$

  It follows that we want all $M\in\mathrm{O}(3)$.

  Without going into detail, the orientation issue further restricts us to SO(3). □

- Calegari subtly gives away the $f(n)+f(53-n)=53$ from the homework in this post!

1.6 Chapter 0: Preliminaries

From Dummit and Foote (2004).

Basics

12/4:
- Frequently used notation defined at the beginning of the textbook.
- Know the basics of set theory.
  - Definitions given for: **Subset**, **Cartesian product**, $\mathbb{Z}$[4], $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
  - Additional important terms are defined below.
- **Order** (of a set A): The number of elements of A (provided A is a finite set). *Also known as* **cardinality**. *Denoted by* $|\boldsymbol{A}|$.
- $\mathbb{Z}^+,\mathbb{Q}^+,\mathbb{R}^+$ denote the positive nonzero elements of $\mathbb{Z},\mathbb{Q},\mathbb{R}$, respectively.
- **Function** (from A to B). *Also known as* **map**. *Denoted by* $\boldsymbol{f:A\to B}$, $\boldsymbol{A\xrightarrow{f}B}$.
  - Additional function-adjacent definitions not defined below: **Domain**, **codomain**, **composition**, **injection**, **surjection**, **bijection**, **bijective correspondence**, and **restriction**.
- **Value** (of f at a): *Denoted by* $\boldsymbol{f(a)}$.
  - Implication: We apply functions on the left throughout the book.
- $\boldsymbol{f:a\mapsto b}$, $\boldsymbol{a\mapsto b}$, $\boldsymbol{f(a)=b}$ are all used interchangeably to describe the action of f on **elements**.
  - The middle one is used only when f is understood from the context.
- If f is not specified on elements but defined by a rule, we must check that it is **well-defined** for each element in its domain.

[4] The German word for numbers is "Zahlen."

- **Image** (of A under f): The following subset of B (the codomain of f). *Also known as* **range**. *Denoted by* $\boldsymbol{f(A)}$. *Given by*
$$f(A) = \{b \in B \mid b = f(a),\ a \in A\}$$
- **Preimage** (of $C \subset B$ under f): The following subset of A (the domain of f). *Also known as* **inverse image**. *Denoted by* $\boldsymbol{f^{-1}(C)}$. *Given by*
$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$
- **Fiber** (of f over b): The preimage of $\{b\}$ under f.
  - f^{-1} is not, in general, a function since the fibers of f generally contain many elements, i.e., many elements of A in general map to the same B.
- **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.
- **2-sided inverse** (of f): A function $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A. *Also known as* **inverse**.
  - Implied to be unique by part (3) of Proposition 1.
- Relating properties of functions.

  Proposition 1. Let $f : A \to B$.

  1. f is injective iff f has a left inverse.
  2. f is surjective iff f has a right inverse.
  3. f is a bijection iff f has a 2-sided inverse.
  4. If A, B satisfy $|A| = |B|$, then $f : A \to B$ is bijective iff f is injective iff f is surjective.
- **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 $f|_A = g$.
  - Extensions need not exist nor be unique.
- **Representative** (of an equivalence class): Any element of the equivalence class.
  - Additional relation-adjacent terms: **Binary relation**, **reflexive**, **symmetric**, **transitive**, **equivalence relation**, **equivalence class**, **equivalent** (elements), and **partition**.
- The notions of an equivalence relation and a partition of A are the same.

  Proposition 2. Let A be a nonempty set.

  1. If $\sim$ defines an equivalence relation on A, then the set of equivalence classes of $\sim$ form a partition of A.
  2. If $\{A_i \mid i \in I\}$ is a partition of A, then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i, $i \in I$.
- Assumed familiarity with induction proofs.

Properties of the Integers

- Many of the properties stated herein will be familiar from elementary arithmetic.
  - We state them now because we will need them in Part I (Group Theory).
  - However, we delay proofs until Chapter 8, when we prove them in the more general context of ring theory.
  - To avoid circular reasoning, the proofs in Chapter 8 will not rely on any result from Part I, so the full logical structure of this book is Ring Theory and then Group Theory, but it is presented the other way around for pedagogical purposes.
- **Well Ordering** (of $\mathbb{Z}$): Any nonempty subset $A \subset \mathbb{Z}^+$ contains a **minimal element** m satisfying $m \leq a$ for all $a \in A$.
- ***a* divides *b***: Two numbers $a, b \in \mathbb{Z}$ with $a \neq 0$ such that $b = ac$ for some $c \in \mathbb{Z}$. *Denoted by* $\boldsymbol{a \mid b}$.
  - If a doesn't divide b, then we write $\boldsymbol{a \nmid b}$.
- **Greatest common divisor** (of $a, b \in \mathbb{Z} \setminus \{0\}$[5]): The unique positive integer d satisfying
  1. $d \mid a$ and $d \mid b$. (d is a *common* divisor of a, b.)
  2. If $e \mid a$ and $e \mid b$, then $e \mid d$. (d is the *greatest* common divisor of a, b.)

  Also known as **g.c.d.** *Denoted by* $\boldsymbol{(a, b)}$.
- **Relatively prime** (numbers): Two numbers $a, b \in \mathbb{Z} \setminus \{0\}$ for which $(a, b) = 1$.
- **Least common multiple** (of $a, b \in \mathbb{Z} \setminus \{0\}$): The unique positive integer l satisfying
  1. $a \mid l$ and $b \mid l$. (l is a *common* multiple of a, b.)
  2. If $a \mid m$ and $b \mid m$, then $l \mid m$. (l is the *least* common multiple of a, b.)

  Also known as **l.c.m.**
- "The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$" (Dummit & Foote, 2004, p. 4).
- **Division Algorithm**: If $a, b \in \mathbb{Z} \setminus 0$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \qquad\qquad 0 \leq r < |b|$$

- **Quotient**: The number q in the above definition.
- **Remainder**: The number r in the above definition.
- **Euclidean Algorithm**: A procedure for finding the greatest common divisor of two integers a and b by iterating the Division Algorithm. *Given by*

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

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

[5] Dummit and Foote (2004) prefers the notation $\mathbb{Z} - \{0\}$ for set differences, but I will stick with what I know.

Proof. Existence of r_n: $|b| > |r_0| > |r_1| > \cdots |r_n|$ is a decreasing sequence of strictly positive integers and such a sequence cannot continue indefinitely.

The rest of the proof comes later. □

- Example of applying the Euclidean Algorithm given.
- (a,b) is a $\mathbb{Z}$-linear combination of a,b: In particular, there exist $x,y \in \mathbb{Z}$ such that

$$(a,b) = ax + by$$

Proof. Exploit the Euclidean Algorithm. Use the second-to-last line to write (a,b) in terms of r_{n-1}, r_{n-2}:

$$r_n = r_{n-2} - q_n r_{n-1}$$

Then use $r_{n-1} = r_{n-3} - q_{n-1}r_{n-2}$ to express r_n in terms of r_{n-2}, r_{n-3}. Go back and back until we express r_n in terms of a,b, and then combine terms. □

- Notes on the above result.
  - Previous example expanded to apply here.
  - Either x or y will be negative.
  - x and y are not unique. The general solution is known, though (see Exercise 0.2.4 and Chapter 8).
- **Prime** (number $p \in \mathbb{Z}^+$): A number $p \in \mathbb{Z}^+$ for which $p > 1$ and the only positive divisors of p are 1 and p.
- **Composite** (number $n \in \mathbb{Z}^+$): A number $n \in \mathbb{Z}^+$ for which $n > 1$ and n is not prime.
- Examples given.
- If p is a prime and $p \mid ab$ for some $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.
  - This property can be used to define the primes (see Exercise 0.2.3).
- **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 $p_1, p_2, \dots, p_s$ and positive integers $\alpha_1, \alpha_2, \dots, \alpha_s$ such that

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

  - This decomposition is unique.
- Let a, b be positive integers such that

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

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

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

- **Euler φ-function**: The function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $\varphi(n)$ is defined to be 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

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

  - φ is used for many functions throughout the text, so when we wish to indicate the Euler φ-function, we do so explicitly.

Exercises

3. Prove that if n is composite, then there are integers a,b such that $n\mid ab$ but $n\nmid a$ and $n\nmid b$.

4. Let a,b,N be fixed integers with a,b nonzero, and let $d=(a,b)$. Suppose x_0,y_0 are particular solutions to $ax+by=N$ (i.e., $ax_0+by_0=N$). Prove that for any integer t, the integers

$$x=x_0+\frac{b}{d}t \qquad\qquad y=y_0-\frac{a}{d}t$$

are also solutions to $ax+by=N$ (this is, in fact, the general solution).

$\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

- Fix $n\in\mathbb{Z}^+$.
- Define $\sim$ on $\mathbb{Z}$ by $a\sim b\iff n\mid(b-a)$.
  - We can prove that $\sim$ is an equivalence relation.
  - If $a\sim b$, we write $a\equiv b\pmod{n}$[6].
- **Congruence class** (of a mod n): The equivalence class of a mod n. *Also known as* **residue class**. *Denoted by* $\bar{\mathbf{a}}$. *Given by*

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

  - There are n distinct equivalence classes mod n, namely $\bar{0},\bar{1},\dots,\overline{n-1}$, and collectively referred to as the **integers modulo n**.
  - The congruence classes differ for different n, so always be sure to fix n before discussing them.
- **Integers modulo n**: The set of equivalence classes under this equivalence relation. *Also known as* **integers mod n**. *Denoted by* $\mathbb{Z}/n\mathbb{Z}$[7]
- **Reducing a mod n**: The process of finding the equivalence class mod n of some integer a.
  - Also frequently refers to finding the **least residue** of a mod n.
- **Least residue** (of a mod n): The smallest nonnegative number congruent to a mod n.
- **Modular arithmetic** (on $\mathbb{Z}/n\mathbb{Z}$): The addition and multiplication operations defined by

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

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

[6] "a is congruent to b mod n."

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

  - In other words, take a representative element of both residue classes, add or multiply them, and then take the class containing the product to be the sum (resp. product).

- Example given to hint at the well-definedness of modular arithmetic.
- Proof that modular arithmetic is well-defined.

  Theorem 3. The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined above are both well-defined, that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., if

  $$a_1 \equiv b_1 \pmod{n} \qquad\qquad a_2 \equiv b_2 \pmod{n}$$

  then

  $$a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \qquad\qquad a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

  Proof. Given. □

- Further comments on equivalence classes and the integers mod n.
  - Preview: Adding equivalence classes by their representatives is a special case of a more general construction (that of a **quotient**).
  - We should be familiar with manipulating equivalence classes from studying $\mathbb{Q}$ rigorously.
  - We should be familiar with modular arithmetic from timekeeping: 8 hours after 5:00 AM? Must be 13h00, but $13 \equiv 1 \pmod 1$2 so 1:00 PM.
  - We do need to be able to think of equivalence classes as elements that can be manipulated in their own right. But it is important to remember that these *are* still equivalence classes at the end of the day.
  - Useful application of modular arithmetic: Computing the last two digits of 2^{1000} using the integers modulo 100.
- $\boldsymbol{(\mathbb{Z}/n\mathbb{Z})^\times}$: The collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. *Given by*

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

- An alternate form for $(\mathbb{Z}/n\mathbb{Z})^\times$.

  Proposition 4. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

  Proof. See Exercises 0.3.10-0.3.14. □

- Further comments on $(\mathbb{Z}/n\mathbb{Z})^\times$.
  - The set given in Proposition 4 is well-defined since if $(a, n) = 1$, then we clearly have $(a+qn, n) = 1$ as well.
  - Explicit example given: $(\mathbb{Z}/9\mathbb{Z})^\times$.
  - Computing the multiplicative inverse of $\bar{a}$: Let $(a, n) = 1$. Then the Euclidean algorithm generates integers x, y such that $ax + ny = 1$. But this implies that $ax = 1 + (-y)n$, i.e., $ax \equiv 1 \bmod n$. Therefore, $\bar{a} \cdot \bar{x} = \bar{1}$, so $\bar{x}$ is the multiplicative inverse of $\bar{a}$.

Exercises

10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ-function.

11. Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

12. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$, $1 \leq a \leq n$. Prove that if a, n are not relatively prime, then there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

13. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$, $1 \leq a \leq n$. Prove that if a, n are relatively prime, then there exists an integer c with such that $ac \equiv 1 \pmod{n}$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers].

14. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence probe Proposition 4. Verify this directly in the case $n = 12$.