Homework 2

Math 25a

Due September 21, 2018 at 5pm

Topics covered (lectures 3-4): equivalence relations, modular arithmetic, cardinality

Instructions:

- The homework is divided into one part for each CA. You'll submit each part to the corresponding CA's mailbox on the second floor of the science center.
- If your submission to any one CA takes multiple pages, then staple them together. A stapler is available in the Cabot library in the science center. Failure to staple your homework could result in loss of points.
- If you collaborate with other students, please mention this near the corresponding problems.
- For the first two assignments, we would like you to keep track of how long it takes you to complete the entire assignment. Please write that somewhere on your solutions, so we can adjust the difficulty accordingly.
- Some problems from this assignment come from Simmon's book *Introduction to topology and modern analysis*. I've indicated this next to the problems (e.g. Simmons 1.2.3 means problem 3 from the exercises to Section 2 of Chapter 1). You can find a digital copy of Simmons' book on the course website.

1 For Joey

An *abelian group* is a set A with an operation $\star : A \times A \to A$ that satisfies the following properties:

1. (Commutativity) $a \star b = b \star a$ for every $a, b \in A$.
2. (Associativity) $(a \star b) \star c = a \star (b \star c)$ for every $a, b, c \in A$.
3. (Identity) There exists an element $e \in A$ so that $a \star e = a$ for every $a \in A$.
4. (Inverses) For each $a \in A$, there is an element $a' \in A$ so that $a \star a' = e$.

Example: the integers $\mathbb{Z}$ with addition as the operation is an abelian group. Non-example: $\mathbb{Z}$ with multiplication as the operation is not an abelian group because $\frac{1}{2}$, the multiplicative inverse of 2, is not in $\mathbb{Z}$.

Problem 1. *Let X be a nonempty set and let $P(X)$ be the power set. Which of the abelian group axioms hold for the union operation $\cup : P(X) \times P(X) \to P(X)$.*

Solution. □

Problem 2. *Let X be a set. For subsets $A \subset X$ and $B \subset X$ the symmetric difference is defined as*

$$A \Delta B = (A - B) \cup (B - A).$$

We can view this as an operation $\Delta : P(X) \times P(X) \to P(X)$. Which of the abelian group axioms does this operation satisfy? (Hint: for associativity, draw a picture first.)

Solution. □

Problem 3 (Simmons 1.5.6)**.** *Let X be a nonempty set with a relation $\sim$. Consider the following argument.*

Claim: If $\sim$ is symmetric and transitive, then it is also reflexive.

Proof: $x \sim y \Rightarrow y \sim x$; also $x \sim y$ and $y \sim x \Rightarrow x \sim x$. Therefore $x \sim x$ for every $x \in X$.

This argument is at odds with a problem from HW1. Where is the flaw?

Solution. □

2 For Laura

Problem 4. *Define an injection $(0,1)^2 \to (0,1)$. Is your function surjective? Explain. Hint: use decimal expansions.*[1]

Solution. □

Problem 5. *Let $U \subset V$ be a subspace. Suppose $u \in U$ and $v \in V \setminus U$. Is it possible that $u+v \in U$?*

Solution. □

Problem 6. *Fix an an integer $n \geq 2$. Consider the relation on $\mathbb{Z}$ defined by*

$$a \sim b \text{ if } n \text{ divides } (a-b).$$

Show that $\sim$ is an equivalence relation. Let $[a]$ denote the equivalence class of an integer a, and let $\mathbb{Z}/n\mathbb{Z}$ denote the set of equivalence classes. Prove that the equivalence classes $[0], [1], \ldots, [n-1]$ are distinct and that $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$.

Solution. □

[1] This can be improved to show there is an injection $\mathbb{R}^2 \to \mathbb{R}$. Later in the course we'll show there is no *linear* injection $\mathbb{R}^2 \to \mathbb{R}$. In 25b we'll show there is no *differentiable* injection $\mathbb{R}^2 \to \mathbb{R}$.

3 For Beckham

Problem 7 (Simmons 1.5.2)**.** *Define an equivalence relation $\sim$ on $\mathbb{R}$ by $x \sim y$ if $x - y \in \mathbb{Z}$. Show that this is an equivalence relation, and describe the set $\mathbb{R}/\mathbb{Z}$ of equivalence classes. Is the addition $[x] + [y] = [x + y]$ well-defined on $\mathbb{R}/\mathbb{Z}$? Is the multiplication $[x] \cdot [y] = [xy]$ well-defined?*

Solution. □

Problem 8. *Define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by the rules*

$$[a] + [b] = [a + b] \quad \textit{and} \quad [a] \cdot [b] = [ab].$$

In class we proved that addition is well-defined on $\mathbb{Z}/n\mathbb{Z}$. Conclude that $[0]$ is the additive identity (i.e. $[a] + [0] = [a]$ for each $[a]$), and that the additive inverse to $[a]$ is $[n - a]$. Prove that multiplication is well-defined and that $[1]$ is the multiplicative identity and that the distributive law holds $[a]([b] + [c]) = [a][b] + [a][c]$.

Solution. □

Problem 9. *(a) Find all the elements of $\mathbb{Z}/6\mathbb{Z}$ that don't have a multiplicative inverse.*

(b) Show that every $[a] \neq [0]$ in $\mathbb{Z}/7\mathbb{Z}$ has a multiplicative inverse. Find each inverse explicitly.

Solution. □

4 For Davis

Problem 10. *Let a and b be positive integers. The greatest common divisor d of a and b is defined as the largest positive integer that divides both a and b. For example, if $b = p$ is a prime that does not divide a, then the greatest common divisor of a and b is 1. By the Euclidean algorithm[2] if d is the greatest common divisor of a and b, then $d = ax + by$ for some integers x and y.*

Use this to show that every nonzero element $[a]$ of $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $n = p$ is prime.

Solution. □

Problem 11. *Use congruences to show*

(a) 3 divides $k \in \mathbb{N}$ if and only if 3 divides the sum of the digits of k.

(b) $a^2 + b^2 = c^2$ cannot hold for a, b odd and c even.

Solution. □

Problem 12 (Existence of transcendental numbers)**.** *A number $z \in \mathbb{R}$ is called algebraic if it is a root of a polynomial with integer coefficients, i.e. there is a polynomial $p(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ such that $p(z) = 0$. For example, $\frac{a}{b} \in \mathbb{Q}$ is algebraic because it's a root of $p(x) = bx - a$ and $\sqrt{2}$ is algebraic because it's a root of $p(x) = x^2 - 2$. A number that's not algebraic is called transcendental, e.g. the number π is transcendental.[3] Here you prove that there are uncountably many transcendental numbers!*

(a) Prove there are countably many polynomials with coefficients in $\mathbb{Z}$. Hint: Express this set as $X = \bigcup X_k$, where X_k is the set of polynomials $p = a_n x^n + \cdots + a_1 x + a_0$ such that $a_0 + \cdots + a_n + n \leq k$.

(b) Conclude there are countably many algebraic numbers. You may use the fact that a polynomial of degree n has at most n roots.[4]

(c) Conclude there are uncountably many transcendental numbers.[5]

Solution. □

[2] We might prove this at some point. See also Math 122.
[3] This is not easy to prove.
[4] We'll prove this eventually. The proof relies on the Fundamental Theorem of Algebra.
[5] Note how *non-constructive* this argument is!