MODERN ALGEBRA I GU4041

Homework 2, due February 6: Equivalence relations, modular arithmetic

1. In each of the following situations, X is a set and R is a relation. Determine whether it is an equivalence relation by checking whether it satisfies each of the necessary conditions (reflexive, symmetric, transitive). Justify your answer. If R is an equivalence relation, give a simple description of the set of equivalence classes.

(a) $X = \mathbb{Z}$, aRb if $a + b$ is even.

(b) $X = \mathbb{Z}$, aRb if $a + b$ is odd.

(c) $X = \mathbb{R}^3$, vRw if there is a rotation of X centered at the origin that takes v to w.

(d) $X = \mathbb{R}$, aRb if $a - b$ is the square of a real number.

2. Continuing problem 1, let X be the set of continuous real-valued functions on the interval $[0, 1]$. If $f, g, \in X$, say fRg if

$$\int_0^1 f(x)dx = \int_0^1 g(x)dx.$$

Prove that R is an equivalence relation and define a bijection between the set of equivalence classes for R and the set $\mathbb{R}$ of real numbers.

3. Let n and m be integers greater than 1. We define a function $f : \mathbb{Z}_{nm} \to \mathbb{Z}_m$: if $a \in \mathbb{Z}$, $[a]_{nm}$ is its residue class in $\mathbb{Z}_{nm}$, and $[a]_m$ is its residue class in $\mathbb{Z}_m$, we set $f([a]_{nm}) = [a]_m$.

(i) Show that this is a *well-defined* function: if $[a]_{nm} = [b]_{nm}$ for $a, b \in \mathbb{Z}$, show that

$$f([a]_{nm}) = [a]_m = [b]_m = f([b]_{nm}).$$

Explain why this is important.

(ii) Show that f is a surjective function.

(iii) Here we denote elements of $\mathbb{Z}_{nm}$ by the letters x, y. Define the relation $\sim_f$ on $\mathbb{Z}_{nm}$ by

$$x \sim_f y \Leftrightarrow f(x) = f(y).$$

Show that this is an equivalence relation. Determine the partition of $\mathbb{Z}_{nm}$ associated to the relation $\sim_f$. How many elements are in each equivalence class?

4. Represent the elements of $\mathbb{Z}_7$ by the residue classes $[0], [1], [2], [3], [4], [5], [6]$. Then we can write addition and multiplication with these representatives:

$$[5] + [5] = [3]; \; [5] \cdot [5] = [4].$$

(a) What residue classes in $\mathbb{Z}/7\mathbb{Z}$ can be obtained as squares of integers?

(b) Using similar notation for the set $\mathbb{Z}_{41}$, work out the following expressions; the answer should be of the form $[a]$ with $0 \leq a \leq 40$.

$$[14] + [33] =? \; ; \; [7] \cdot [8] =?.$$

(c) As in (b), but for the set $\mathbb{Z}_{10}$; the answer should be of the form a with $0 \leq a \leq 9$.

$$a \equiv 12 \cdot 12 \pmod{10}; \; a = 107 + 413 \pmod{10}.$$

5. Let X be the set of triangles in the euclidean plane and let $\cong$ be the relation $A \cong B$ if A and B are congruent triangles.

(a) Explain why $\cong$ is an equivalence relation.

(b) Let $f : X \to \mathbb{R}$ be the function that to a triangle A associates its area. Show that f *factors through* a function

$$\tilde{f} : X/\cong \; \to \mathbb{R}.$$

In other words, if $p : X \to X/\cong$ is the map taking a triangle A to its equivalence class $[A]$, then we have

$$\tilde{f} \circ p = f.$$

6. Use the Euclidean algorithm to determine the GCD and LCM for each of the following pairs of integers. (i) $n = 104$, $m = 950$. (ii) $n = 18$, $m = 207$.

Recommended reading

Gallagher's notes, sections 1 and 2, at `https://www.math.columbia.edu/~khovanov/modAlgSpring2017/Gallagher/`.