MATH 9
ASSIGNMENT 21: PARTITIONS, EQUIVALENCE CLASSES AND MODULAR ARITHMETIC

MARCH 27, 2022

Partitions

A *partition* of a set A is decomposition of it into non-intersecting subsets:

$$A = A_1 \cup \dots A_n \dots$$

with $A_i \cap A_j = \varnothing$. It is allowed to have infinitely many subsets A_i.

Now, let $\sim$ be an equivalence relation on a set A. Recall that we have defined, for an element $a \in A$, its equivalence class by

$$[a] = \{x \in A \mid x \sim a\}$$

Theorem. *If $\sim$ is an equivalence relation on a set A, then it defines a partition of A into equivalence classes.*

Example: if $A = \mathbb{Z}$ and the equivalence relation is defined by congruence mod 3:

$$a \equiv b \mod n \text{ if } a - b \text{ is a multiple of } 3$$

then

$$\begin{aligned}
[0] &= \{\dots, -6, -3, 0, 3, 6, \dots\}\\
[1] &= \{\dots, -2, 1, 4, 7, \dots\}\\
[2] &= \{\dots, -1, 2, 5, 8, \dots\}\\
[3] &= \{\dots, -6, -3, 0, 3, 6, \dots\} = [0]
\end{aligned}$$

and thus we have a partition of $\mathbb{Z}$:

$$\mathbb{Z} = [0] \cup [1] \cup [2]$$

Define

$$A/{\sim} = \text{set of equivalence classes for } \sim$$

so elements of $A/{\sim}$ are equivalence classes. Informally, $A/{\sim}$ is the set obtained from A by identifying all equivalent elements from A with each other.

Examples:

- Vectors: the set of vectors is defined as the set of equivalence classes

  $$\{\text{directed segments in the plane}\}/\sim$$

  where the equivalence relation is given by $\vec{AB} \sim \vec{A'B'}$ if $ABB'A'$ is a parallelogram.
- rational numbers: $\mathbb{Q} = \{(a, b) \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}/\sim$, where $\sim$ is given by

  $$(a, b) \sim (c, d) \text{ if } ad = bc$$

  (this is obtained from $a/b = c/d$ by cross-multiplying).
- Remainders, or residues, modulo m (here $m > 1$):

  $$\mathbb{Z}_m = \mathbb{Z}/(\equiv \mod m)$$

  where $\equiv \mod m$ was defined by $a \equiv b \mod m$ if $a - b$ is a multiple of m (or, equivalently, if a, b give the same remainder upon division by m). In this case, there are exactly m equivalence classes: $[0]$, $[1]$, …, $[m - 1]$ (because $[m] = [0]$); thus, $\mathbb{Z}_m$ is a finite set with m elements.

  Moreover, $\mathbb{Z}_m$ is more than a set: one can define addition and multiplication in it in the usual way:

  $$\begin{aligned}
  [a] + [b] &= [a + b]\\
  [a] \cdot [b] &= [ab]
  \end{aligned}$$

  (note that one needs to check that this definition does not depend on the choice of representatives a, b in each equivalence class – we discussed this.) So defined addition and multiplication satisfy all the usual rules: associativity, commutativity, distributivity (we skip discussion of this). Note, however, that in general it is impossible to divide: for example, $[2][3] = [0]$ in $\mathbb{Z}_6$, but one can not divide both sides by $[3]$ to get $[2] = [0]$.

When doing the homework, the following result (which we had discussed last year) will be helpful:

Theorem. *An congruence class $[a]$ modulo m is invertible (i.e., there exists some $[b]$ such that $[a][b] = [1]$) if and only if $\gcd(a, n) = 1$. In particular, if n is prime, then any non-zero congruence class is invertible.*

To construct the inverse of $[a]$ mod n, one uses Euclid's algorithm which allows us to find integer x, y such that

$$ax + ny = 1$$

Thus, $ax \equiv 1 \mod n$, so $[a]^{-1} = [x]$.

Homework

1. Let relation $\sim$ on the set $\mathbb{R}^2$ be defined by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Describe equivalence classes and show that $\mathbb{R}^2/\sim$ can be identified with $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$.

2. Let $\sim$ be the relation on the set of all directed segments in the plane defined by

$$\vec{AB} \sim \vec{A'B'} \qquad \text{if } ABB'A' \text{ is a parallelogram.}$$

Prove that it is an equivalence relation.

3. Consider the equivalence relation on $\mathbb{R}$ given by

$$x \sim y \text{ if } x - y = n \cdot 360 \text{ for some } n \in \mathbb{Z}$$

Show that this is an equivalence relation, and construct a bijection between the set of equivalence classes and the unit circle.

4. Recall the equivalence relation from last homework: consider the set $A = \mathbb{R}^2 - \{(0, 0)\}$ (coordinate plane with the origin removed). Define a relation $\sim$ on A by

$$(x_1, x_2) \sim (y_1, y_2) \text{ if there exists } t > 0 \text{ such that } x_1 = ty_1, x_2 = ty_2$$

Can you describe all equivalence classes for this relation? can you describe the set $A/\sim$ of equivalence classes?

5. Compute the following inverses:
— inverse of $[2]$ mod 5
— inverse of $[5]$ mod 7
— inverse of $[7]$ mod 11

6. Let $n > 1$ and let a be an integer such that $\gcd(a, n) = 1$. Recall that in this case, $[a]$ has an inverse in $\mathbb{Z}_n$: there exists b such that $[a][b] = [1]$.

(a) Show that one can divide both sides of equality in $\mathbb{Z}_n$ by $[a]$: if $[ax] = [ay]$, then $[x] = [y]$. [Hint: $[ax] = [ay]$ means that $a(x - y) \equiv 0 \mod n$.] Note that it fails without the assumption $\gcd(a, n) = 1$.

(b) Prove that the function $\mathbb{Z}_n \to \mathbb{Z}_n \colon [x] \mapsto [ax]$ is injective. (Recall that a function $f \colon A \to B$ is injective if for every $y \in B$, the equation $f(x) = y$ has at most one solution.)

(c) Prove that this function is bijective. Can you describe the inverse function?

(d) Deduce that for any $y \in \mathbb{Z}$, equation $ax \equiv y \mod n$ has an integer solution, and any two solutions differ by a multiple of n.