January 8, 2023

Algebra.

Equivalence relations and partitions.

Definition. A **binary relation** on a set A,

$$x \sim y, \qquad x, y \in A$$

is a collection of ordered pairs of elements of A, $\{(x, y)\}$, $x, y \in A$. In other words, it is a subset of the Cartesian product $A^2 = A \times A$.

More generally, a binary relation between two sets A and B is a subset of $A \times B$. The terms correspondence, dyadic relation and 2-place relation are synonyms for binary relation.

Example 1. A binary relation $>$ ("is greater than") between real numbers $x, y \in \mathbb{R}$ associates to every real number all real numbers that are to the left of it on the number axis.

Example 2. A binary relation "is the divisor of " between the set of prime numbers P and the set of integers $\mathbb{Z}$ associates every prime p with every integer n that is a multiple of p, but not with integers that are not multiples of p. In this relation, the prime 3 is associated with numbers that include -6, 0, 6, 9, but not 2 or -8; and the prime 5 is associated with numbers that include 0, 10, and 125, but not 6 or 11.

Injections, surjections, bijections between the sets are established by defining the corresponding (injective, surjective, or one-to-one) binary relations between the elements of these sets. A relation $x \sim y$ is,

- **left-total**: $\forall x \in X, \exists y \in Y, x \sim y$, a relation is left-total when it is a function, or a multivalued function;
- **surjective** (right-total, or onto): $\forall y \in Y, \exists x \in X, x \sim y$;
- **injective** (left-unique): $\forall (x_1, x_2, \in X, y \in Y), \big((x_1 \sim y) \wedge (x_2 \sim y) \Rightarrow (x_1 = x_2)\big)$
- **functional** (right-unique, also called univalent, or right-definite): $\forall (x \in X, y_1, y_2, \in Y), \big((x \sim y_1) \wedge (x \sim y_2) \Rightarrow (y_1 = y_2)\big)$, such a binary relation is also called a partial function;

- **one-to-one**: injective and functional.

A binary relation $x \sim y$ is

- **reflexive** if $\forall x \in A$, we have $x \sim x$
- **symmetric** if $\forall x, y \in A$, we have $(x \sim y) \Rightarrow (y \sim x)$
- **transitive** if $\forall x, y, z \in A$, we have $(x \sim y) \wedge (y \sim z) \Rightarrow (x \sim z)$

Definition. An **equivalence relation** is a binary relation that is reflexive, symmetric, and transitive.

Given an equivalence relation on A, we can define, for every $a \in A$, its **equivalence class** $[a]$ as the following subset of A:

$$[a] = \{x \in A, (x \sim a)\}$$

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

$$A = A_1 \cup A_2 \dots \cup A_n \dots$$

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

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

Example. Define the equivalence relation on $\mathbb{Z}$ by congruence mod 3: $a \equiv b \; mod$ 3 if $a - b$ is a multiple of 3. This defines a partition, $[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$, $[1] = \{\dots, -2, 1, 4, 7, \dots\}$, $[2] = \{\dots, -1, 2, 5, 8, \dots\}$.

Exercise 1. Present examples of binary relations that are, and that are not equivalence relations. For each of the following relations, check whether it is an equivalence relation.

- On the set of all lines in the plane: relation of being parallel
- On the set of all lines in the plane: relation of being perpendicular
- On $\mathbb{R}$: relation given by $x \sim y$ if $x + y \in \mathbb{Z}$
- On $\mathbb{R}$: relation given by $x \sim y$ if $x - y \in \mathbb{Z}$
- On $\mathbb{R}$: relation given by $x \sim y$ if $x > y$
- On $\mathbb{R} - \{0\}$: relation given by $x \sim y$ if $xy > 0$

Exercise 2. Let $\sim$ be an equivalence relation on A.

- Prove that if $a \sim b$, then $[a] = [b]$: $\forall x \in A, x \in [a] \Rightarrow x \in [b]$
- Prove that if $a \nsim b$, then $[a] \cap [b] = \emptyset$.

Exercise 3. Let $f: A \xrightarrow{f} B$ be a function. Define a relation on A by $a \sim b$ if $f(a) = f(b)$. Prove that it is an equivalence relation.

Exercise 4. For a positive integer number $n \in \mathbb{N}$, define relation $\equiv$ on $\mathbb{Z}$ by $a \equiv b$ if $a - b$ is a multiple of n

- Prove that it is an equivalence relation;
- Describe equivalence class $[0]$;
- Prove that equivalence class of $[a + b]$ only depends on equivalence classes of a, b, that is, if $[a] = [a']$, $[b] = [b']$, then $[a + b] = [a' + b']$.

Exercise 5. Define a relation $\sim$ on $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ by $(x_1, y_1) \sim (x_2, y_2)$ if $x_1 + y_1 = x_2 + y_2$. Prove that it is an equivalence relation and describe the equivalence class of $(1, 2)$.

Exercise 6. Is it possible to partition the set of all integers, $\mathbb{Z}$, into equivalence classes using the binary relation $p \sim q$: $p \equiv 0 mod(q)$ ("p is a multiple of q"), which was defined in Example 2.

Recap: Elements of number theory. Modular arithmetics.

Definition. For $a, b, n \in \mathbb{Z}$, the congruence relation, $a \equiv b \bmod n$, denotes that, $a - b$ is a multiple of n, or, $\exists q \in \mathbb{Z}, a = nq + b$.

All integers congruent to a given number $r \in \mathbb{Z}$ with respect to a division by $n \in \mathbb{Z}$ form congruence classes, $[r]_n$. For example, for $n = 3$,

$$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

$$[1]_3 = \{\dots, -2, 1, 4, 7, \dots\}$$

$$[2]_3 = \{\dots, -1, 2, 5, 8, \dots\}$$

$$[3]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\} = [0]_3$$

There are exactly n congruence classes mod n, forming set Z_n. In the above example $n = 3$, the set of equivalence classes is $Z_3 = \{[0]_3, [1]_3, [2]_3\}$. For general n, the set is $Z_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$, because $[n]_n = [0]_n$.

One can define addition and multiplication in Z_n in the usual way,

$$[a]_n + [b]_n = [a + b]_n$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

$$([a]_n)^p = [a^p]_n, p \in \mathbb{N}$$

Here the last relation for power follows from the definition of multiplication.

Exercise. Check that so defined operations do not depend on the choice of representatives a, b in each equivalence class.

Exercise. Check that so defined operations of addition and multiplication satisfy all the usual rules: associativity, commutativity, distributivity.

In general, however, it is impossible to define division in the usual way: for example, $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$, but one cannot divide both sides by $[3]_6$ to obtain $[2]_6 = [0]_6$. In other words, for general n an element $[a]_n$ of Z_n could give $[0]_n$ upon multiplication by some of the elements in Z_n and therefore would not have properties of an algebraic inverse, so there may exist elements in Z_n

which do not have inverse. In practice, this means that if we try to define an inverse element, $[r^{-1}]_n$, to an element $[r]_n$ employing the usual relation, $[r]_n \cdot [r^{-1}]_n = [1]_n$, there might be no element $[r^{-1}]_n$ in class Z_n satisfying this equation. However, it is possible to define the inverse for some special values of r and n. The corresponding classes $[r]_n$ are called invertible in Z_n.

Definition. The congruence class $[r]_n \in Z_n$ is called invertible in Z_n, if there exists a class $[r^{-1}]_n \in Z_n$, such that $[r]_n \cdot [r^{-1}]_n = [1]_n$.

Theorem. Congruence class $[r]_n \in Z_n$ is invertible in Z_n, if and only if r and n are mutually prime, $(r, n) = 1$. Or, $\forall [r]_n, (\exists [r^{-1}]_n \in Z_n) \Leftrightarrow \big((r, n) = 1\big)$.

To find the inverse of $[a] \in Z_n$, we have to solve the equation, $ax + ny = 1$, which can be done using Eucleadean algorithm. Then, $ax \equiv 1 \bmod n$, and $[a]^{-1} = [x]$.

Examples.

3 is invertible mod 10, i. e. in Z_{10}, because $[3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10}$, but is not invertible mod 9, i. e. in Z_9, because$[3]_9 \cdot [3]_9 = [0]_9$.

7 is invertible in Z_{15}: $[7]_{15} \cdot [13]_{15} = [91]_{15} = [1]_{15}$, but is not invertible in Z_{14}: $[7]_{14} \cdot [2]_{14} = [14]_{14} = [0]_{14}$.