MATH 9: ALGEBRA WEEK 11: EQUIVALENCE RELATIONS AND MODULAR ARITHMETIC

2020 DECEMBER 13

1. Binary Relation

Suppose we have a set, and it has a bunch of (possibly) useful objects in it. We say that some (possibly arbitrarily defined) logical relation on the elements is called a binary relation if, given any two elements, it can return True or False. Usually a binary relation is given some sort of symbol to represent its use. For example, perhaps we have the set L of all leaves on Earth, and a relation abbreviated using symbol $\sim$ which is true if the leaves are on the same plant, and false otherwise. This is a binary relation.

There is a way to define the binary relation itself as a set, which helps understand the relation itself as an object. Consider the Cartesian product $L \times L$, then $\sim \subset L$, i.e. the relation is a subset of $L \times L$. In other words, a binary relation is a collection of ordered pairs of elements from the set of interest, and the ordered pairs represent all pairs of elements for which the relation holds true. So $\sim$ in this case would be the set of all ordered pairs of leaves from the same plant, for all plants on Earth.

Note that, in general, a binary relation is not symmetric, which is why we consider ordered pairs.

There are a few properties that a binary relation can have. Some of them are familiar to you in other contexts. In the following definitions, let the set of interest be A, and the relation be denoted by X.

- right-total, if every element in A is on the right of some ordered pair in X. $\forall x \in A(\exists y \in A((y, x) \in X))$
- left-total, if every element in A is on the left of some orderd pair in X. $\forall x \in A(\exists y \in A((x, y) \in X))$
- right-definite, or right-unique, if every element in A is on the left of at most one ordered pair in X. $\forall x, y, z \in A((x, y) \in X \wedge (x, z) \in X \implies y = z)$
- left-definite, or left-unique, if every element in A is on the right of at most one ordered pair in X. $\forall x, y, z \in A((y, x) \in X \wedge (z, x) \in X \implies y = z)$
- reflexive if every element is related to itself. $\forall x \in A((x, x) \in X)$
- irreflexive if no element is related to itself. $\forall x \in A((x, x) \notin X)$
- symmetric if a relation one way means the relation holds the other way. $\forall x, y \in A((x, y) \in X \implies (y, x) \in X)$
- antisymmetric if a relation one way means the relation does not hold the other way. $\forall x, y \in A((x, y) \in X \implies (y, x) \notin X)$
- transitive, if $\forall x, y, z \in A(((x, y) \in X \wedge (y, z) \in X) \implies (x, z) \in X)$

Here are some examples.

Example 1. Leaves. Given the set L of all leaves on Earth and the relation $\sim_L$ of all ordered pairs of leaves on the same plant, this relation is right-total, left-total, reflexive, symmetric, and transitive. I is not righ-definite, left-definite, irreflexive, or antissymetric.

Example 2. Tomorrow. Let D be the set of all days to ever exist. Let T be the relation *tomorrow*: given two days d_1 and d_2, we have $d_1 T d_2$ if d_2 is the day after d_1. This relation is right-definite, left-definite, irreflexive, and antisymmetric. It is not reflexive, symmetric, or transitive. Assuming there was a first day to ever exist, it is not right-total; assuming there will be no last day to exist, it is left-total.

Example 3. Greater. Let $\mathbb{Z}$ be the set of integers, and $>$ be the relation *greater than*, which holds true if the element on the left is a greater integer than the element on the right, i.e. $x > y$ if x is greater than y. This relation is right-total, left-total, irreflexive, antisymmetric, and transitive. It is not right-definite, left-definite, reflexive, or symmetric.

Example 4. Square. Let S be the relation on the set $\mathbb{Z}$ given by $xSy \leftrightarrow x^2 = y$. This relation is left-total and right-definite. It is not right-total, left-definite, reflexive, irreflexive, symmetric, antisymmetric, or transitive.

Relations are sometimes also given the following attributes. Filling them in (except the last one) will be a homework exercise (see the homework).

- function, a relation is a function if...
- injective, a relation is injective if...

- surjective, a relation is surjective if...
- bijective, a relation is bijective if...
- order, a relation is an order relation if...
- equivalence, a relation is an equivalence relation if... (see below)

2. Equivalence Relations

A relation is an equivalence relation if it is reflexive, symmetric, and transitive.

The first, and motivating, example, is equality. Consider $\mathbb{Z}$ for example. The relation $=$, where $x = y$ if x is equal to y, is an equivalence relation.

But there are many other examples. Consider this: on the set $\mathbb{Z}$, $x \sim y$ if $|x| = |y|$. This relation is reflexive, symmetric, and transitive, and therefore it is an equivalence relation. Another example is having the same area: given the set P of all polygons on some given plane, let $a \sim b$ if a and b have the same area, then this is an equivalence relation.

Here is a collection of example relations. Consider each one and determine whether it is an equivalence relation.

1. On the set of all lines in a plane: the relation of being parallel
2. On the set of all lines in a plane: the relation of being perpendicular
3. On $\mathbb{R}$, the relation $x \sim y$ if $x + y \in \mathbb{Z}$
4. On $\mathbb{R}$, the relation $x \sim y$ if $x - y \in \mathbb{Z}$
5. On $\mathbb{R}$, the relation $x \sim y$ if $x > y$
6. On $\mathbb{R} - \{0\}$, the relation $x \sim y$ if $xy > 0$

After you've thought about them and made your determinations, read the following to see the answers and explanations.

1. On the set of all lines in a plane: the relation of being parallel ; this is an equivalence relation: every line is parallel to itself, lines being parallel is a symmetric relation, and parallelism is an equivalence relation as long as Euclid's parallel postulate is assumed.
2. On the set of all lines in a plane: the relation of being perpendicular ; this is not an equivalence relation, it is not reflexive, no line is perpendicular to itself.
3. On $\mathbb{R}$, the relation $x \sim y$ if $x + y \in \mathbb{Z}$; this is not an equivalence relation, it is not reflexive, consider $0.4 \in \mathbb{R}$, we have $0.4 + 0.4 = 0.8 \notin \mathbb{Z}$.
4. On $\mathbb{R}$, the relation $x \sim y$ if $x - y \in \mathbb{Z}$; this is an equivalence relation, it is reflexive because $x - x = 0 \in \mathbb{Z}$ for all x, it is symmetric because $y - x = -(x - y)$ and any integer's negation is also an integer, and it is transitive because if $x - y$ and $y - z$ are integers, then their sum $(x - y) + (y - z)$ is an integer, which simplifies to $(x - z) \in \mathbb{Z}$, thus $x \sim z$.
5. On $\mathbb{R}$, the relation $x \sim y$ if $x > y$; this is not an equivalence relation, it is not reflexive, $x \not> x$, in fact it's also not symmetric.
6. On $\mathbb{R} - \{0\}$, the relation $x \sim y$ if $xy > 0$; this is an equivalence relation, it is reflexive because squares of nonzero numbers are always positive, and it is symmetric because multiplication is commutative, and it is transitive because $(xy > 0) \wedge (yz > 0) \implies (xyyz > 0) \implies (xzy^2 > 0) \implies (xz > 0)$ (the last step is possible because y^2 is positive).

Now for the following definition: given an equivalence relation, an equivalence class is a maximal set of mutually related elements. That is, a set of elements which are all equivalent to each other, and which contains every element equivalent to something in the set.

Theorem 1 (Equivalence Class)**.** *Given a set A, equivalence relation E, and element $a \in A$, the set $[a] = \{x \in A | aEx\}$ is an equivalence class.*

Proof. To prove that $[a]$ is a maximal set of equivalent elements, first one must prove that any pair of elements in $[a]$ is equivalent. Given $x, y \in [a]$, we know $aEx \wedge aEy$, applying symmetry we get $xEa \wedge aEy$, and applying transitivity we get xEy, thus x and y are equivalent.

To prove the set is maximal, suppose we have some $x \in [a]$ and some $u \in A$ such that xEu. Then we know $aEx \wedge xEu$, therefore by transitivity we have aEu, therefore $u \in [a]$. Thus there is no element in $A - [a]$ that can be added to $[a]$ to make it a bigger set of mutually equivalent elements. □

For this reason, we often talk about the equivalence class of an element. The notation $[a]$ is read "the equivalence class of a".

Here is another definition. A partition of a set is a set of subsets of the set, which are mutually disjoint, and whose union is the whole set. In other words, given a set A, and a set $B = \{a_1, a_2, a_3, ...\}$ (possibly infinite), if $a_i \cap a_j = \delta_{ij} a_i$ (i.e. is equal to a_i if $i = j$ and is equal to the empty set otherwise), and $\bigcup a_i = A$, then B is a partition of A.

Time for another theorem!

Theorem 2 (Equivalence Class Partition)**.** *Given a set A and equivalence relation E, the set F of equivalence classes of E is a partition of A.*

Proof. First, the sets are mutually disjoint. In order to show this, suppose we have two equivalence classes $f, g \in F$, such that $f \neq g$. Because $f \neq g$, we have $\exists q \in g(q \notin f)$. If $f \cap g$ is nonempty, then the intersection contains some element $p \in (f \cap g)$. I claim that q is equivalent to everything in f; if this is the case, then f would not be a maximal set of mutually equivalent elements, because $f \cup \{q\}$ would be a bigger set of mutually equivalent elements, contradicting the hypothesis that $f \in F$. To show that q is equivalent to everything in f, note first that $p \in g$, therefore pEq. Next, take some arbitrary $x \in f$, then we have xEp. Put together, we have $xEp \wedge pEq$, therefore xEq.

Now that that's done, to prove $\bigcup F = A$, it is enough to show that every element in A is in some equivalence class in F. Let $a \in A$ be an arbitrary element of A. Then $[a]$ is an equivalence class, therefore $[a] \in F$, but we also know $a \in [a]$ by reflexivity. Therefore $a \in [a] \in F$. □

A corollary of this theorem is that, given any equivalence class f and an element $a \in f$, we have $[a] = f$. This follows from the fact that $a \in ([a] \cap f)$, thus $[a] \cap f$ is nonempty, therefore we must have $[a] = f$.

3. Modular Arithmetic

One of the famous examples of the use of equivalence classes in a practical setting is modular arithmetic. (Another great example is days of the year, for example a person's birthday is an equivalence class of days that are each one year apart; but I won't spend too much time on that exmaple.) Take the set of integers $\mathbb{Z}$ and some natural number $n \in \mathbb{N}$, then the relation $\sim_n$ defined as $a \sim_n b \leftrightarrow n|(a - b)$ is an equivalence relation (recall that $x|y$ means $y = kx$ for $k \in \mathbb{Z}$). Typically this is written $a \equiv b \mod n$. Any integer $r \in \mathbb{Z}$ forms an equivalence class under this relation, which we can write as $[r]_n$.

The *arithmetic* part comes from the following theorem. To state it, first have the following definitions:
Let the sum of two sets $f + g$ denote the set of all sums of elements from the respective sets, i.e. $f + g := \{x + y | x \in f, y \in g\}$.
Similarly define the product of two sets, $fg := \{x \cdot y | x \in f, y \in g\}$.
Lastly define $f^p := \{x^p | x \in f\}$, for some $p \in \mathbb{N}$.

Theorem 3 (Modular Arithmetic)**.** *Given a modular equivalence relation $\sim_n$ on $\mathbb{Z}$ as described above, let f, g be equivalence classes of $\sim_n$. Then $f + g$, fg, and f^p are all equivalence classes of $\sim_n$.*

Because of this theorem, we can define the following arithmetic on equivalence classes of $\sim_n$.

$$[a]_n + [b]_n := [a + b]_n$$
$$[a]_n \cdot [b]_n := [ab]_n$$
$$([a]_n)^p := [a^p]_n$$

These all make sense because $a \in [a]_n$ and $b \in [b]_n$ therefore by definition $a + b \in [a]_n + [b]_n$, but $[a]_n + [b]_n$ is an equivalence class, therefore it is an equivalence class that contains $a + b$, therefore it must be equal to the equivalenec class $[a + b]_n$. Similarly for the product and power.

The arithmetic is referred to as modulo n, written $\mod n$. When we write $\mod n$, it is assumed we are working with equivalence classes, so the equivalence classes are written without the brackets. Related

to this, have a useful vocab word: an equivalence class of a modular equivalence relation is called a residue. Anyways, here are some examples:

$$0 \equiv 6 \mod 6$$
$$1 \equiv 7 \mod 6$$
$$2 + 3 \equiv 5 \mod 6$$
$$2 + 4 \equiv 0 \mod 6$$
$$3 + 4 \equiv 1 \mod 6$$
$$5 \equiv -1 \mod 6$$
$$2 \cdot 3 \equiv 0 \mod 6$$
$$2 \cdot 4 \equiv 2 \mod 6$$
$$2^5 \equiv 2 \mod 6$$

It is not hard to show that these arithmetic operations satisfy the usual arithmetic operations of commutativity, associativity, distributivity (of multiplication over addition), and that 0 and 1 are additive and multiplicative identities, respectively. We also have additive inverses, i.e. given any integer r, there is an integer $-r$ such that $r + (-r) \equiv 0$. Therefore we can use the symbols and operations for addition, multiplication, subtraction, and exponentiation, in essentially the same way as we use them for integers normally.

What we don't have is division. However, there are special cases that can work. In order to divide, one needs multiplicative inverses. Given an integer r, and a modulo n, there may or may not be an integer s such that $r \cdot s \equiv 1 \mod n$. If this integer s exists, then it is called the multiplicative inverse of r, abbreviated as r^{-1}. In order to find a multiplicative inverse, we have to solve $rs \equiv 1 \mod n$, which is equivalent to solving $rs - 1 = kn$ (for some integer value of k), according to the definition of the modular equivalence relation. Based on a famous and ancient result in number theory, this equation is solvable if and only if the greatest common divisor of r and n is 1, written $(r, n) = 1$, also known as "r is mutually prime to n". To solve the equation explicitly, use Euclid's algorithm - this is something you should know how to do.

A number r that has an inverse modulo n is said to be invertible modulo n. Thus r is invertible modulo n iff $(r, n) = 1$.

Examples:

- 3 is invertible mod 10, and its inverse is 7. $3 \cdot 7 = 21 \equiv 1 \mod 10$.
- 3 is not invertible mod 9. The greatest common divisor of 3 and 9 is 3.
- 2 is invertible mod 9. The inverse is 5. $2 \cdot 5 = 10 \equiv 1 \mod 9$.
- The equivalence classes that are invertible mod 6 are 1 and 5.
- The equivalence classes that are invertible mod 5 are 1, 2, 3, and 4.

One last definition and theorem.

A zero-divisor modulo n is a number that is a factor of 0 mod n with nonzero quotient. In other words, if you can multiply two nonzero numbers to get zero, then those two numbers are zero-divisors mod n. An example is $2 \cdot 3 \equiv 0 \mod 6$, here 2 and 3 are zero-divisors mod 6.

Theorem 4 (Finite Integral Domain)**.** *An equivalence class mod n is invertible if and only if it is not a zero-divisor.*

The name is an allusion to a more general result, that finite integral domains are fields - ask if you are curious, but it's not part of this course.

4. Final Note

If any of the notation here is confusing or unclear to you, or is new to you, please ask. You can take notes about questions you want to ask in future classes. In any case, there are some conventions here that are common in a more modern math perspective: for example, sets of sets is common, and the union $\bigcup F$ is the union of all sets inside F. There is no need to distinguish sets of sets from sets of other types of objects, since mostly any type of object can be defined as a set anyways.