Equivalence Classes

Ryan C. Daileda

Trinity University

Intro to Abstract Mathematics

Equivalence Classes

Recall: An *equivalence relation* on a set A is a relation $R \subset A^2$ that is *reflexive*, *symmetric* and *transitive*.

Definition

Let R be an equivalence relation on A and let $a \in A$. The *equivalence class of* a is the set

$$[a] = \{b \in A \mid bRa\},$$

the set of all elements of A that are R-related to a.

Remark. By reflexivity of R, for all $a \in A$ one has aRa, which implies $a \in [a]$. This has two consequences:

1. No equivalence class is empty.
2. Every $a \in A$ belongs to an equivalence class.

Example

Example 1

Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Compute the equivalence class of a under congruence modulo m.

Solution. Recall that $b \equiv a \pmod{m}$ if and only if $m|b-a$.

Thus:

$$\begin{aligned} b \in [a] &\iff b \equiv a \pmod{m} \\ &\iff m|b-a \\ &\iff b-a = mk, \text{ some } k \in \mathbb{Z} \\ &\iff b = a+mk, \text{ some } k \in \mathbb{Z} \\ &\iff b \in \{a+mk \mid k \in \mathbb{Z}\} := a+m\mathbb{Z}. \end{aligned}$$

We conclude that the equivalence class of a is the *arithmetic progression*

$$\boxed{[a] = a + m\mathbb{Z} = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}}$$

□

For instance, if $m = 3$ then:

$$[5] = 5 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\} = [2] = [8] = \cdots$$

$$[-2] = -2 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, 10, 13, \ldots\} = [1] = [7] = \cdots$$

$$[0] = 0 + 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\} = [3] = [-3] = \cdots$$

Preliminary Observations

Notice. In our final example:

1. Distinct classes do not overlap, i.e. they are disjoint.
2. Multiple elements can share the same equivalence class.
3. Every integer belongs to some class (the classes *cover* $\mathbb{Z}$), as expected.

We will generalize all three of these statements to arbitrary equivalence relations.

We will also explain why there are exactly $m = 3$ equivalence classes, by generalizing to C_m.

Quotient Sets

Definition

Let R be an equivalence relation on a set A. The set

$$A/R = \{[a] \mid a \in A\} \subset \mathcal{P}(A)$$

is called the *quotient of A by R*.

Remark. A/B is commonly read as A *modulo* B, or just A *mod* B.

Example 2

Our example above shows that under congruence modulo 3 (C_3):

$$\mathbb{Z}/C_3 = \{[5], [-2], [0]\}.$$

Structure of A/R

It is easier to understand specific examples if we first analyze the general structure of A/R.

Theorem 1

Let A be a set with an equivalence relation R. Then:

1. *For all $a, b \in A$, $[a] = [b]$ if and only if aRb.*
2. *For all $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \varnothing$.*
3. *A is the (disjoint) union of the set of equivalence classes:*

$$A = \bigsqcup_{C \in A/R} C.$$

Remark. Parts **2** and **3** say that A/R is a *partition* of A.

Proof

1. ($\Rightarrow$) If $[a] = [b]$, then $b \in [b] = [a]$, so that bRa.

Since R is symmetric, this implies aRb, as claimed.

($\Leftarrow$) Suppose aRb.

Let $c \in [a]$. Then cRa and aRb, so that transitivity implies cRb.

Thus, $c \in [b]$. This proves $[a] \subset [b]$, for any pair $a, b \in A$.

By reversing the roles of a and b we therefore obtain $[b] \subset [a]$, and hence $[a] = [b]$.

2. Let $a, b \in A$.

It is easy to see that $P \vee Q$ is logically equivalent to $\neg P \rightarrow Q$.

So we assume $[a] \cap [b] \neq \varnothing$ and show that $[a] = [b]$.

Let $c \in [a] \cap [b]$.

Then cRa and cRb, so that $[c] = [a]$ and $[c] = [b]$ by part **1**.

Thus $[a] = [c] = [b]$, as needed.

3. We have already proven that every $a \in A$ belongs to $[a] \in A/R$. The result follows. □

Example

Example 3

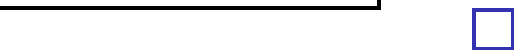
Let $m \in \mathbb{N}$. Determine the quotient set $\mathbb{Z}/C_m$, the equivalence classes in $\mathbb{Z}$ under congruence modulo m.

Solution. Let $a \in \mathbb{Z}$ and write $a = qm + r$ with $0 \leq r < m$.

Then $qm = a - r$ so that $m|a - r$ and $a \equiv r \pmod{m}$.

By Theorem 1, $[a] = [r]$.

Thus $\boxed{Z/C_m = \{[r] \,|\, 0 \leq r < m\} = \{[0], [1], [2], \ldots, [m-1]\}}$.



Uniqueness

It is worth noting that the uniqueness of remainders in the division algorithm implies that if $r, s \in \{0, 1, 2, \ldots, m-1\}$ and $[r] = [s]$, then $r = s$.

Thus, in the expression $\mathbb{Z}/C_m = \{[0], [1], [2], \ldots, [m-1]\}$ there are *no repeats*. Consequently:

Theorem 2

There are exactly *m equivalence classes in $\mathbb{Z}$ under congruence modulo m, and they are given by the classes of the remainders upon division by m: $\mathbb{Z}/C_m = \{[0], [1], [2], \ldots, [m-1]\}$.*

Remark. In practice one usually writes $\mathbb{Z}_m$ or $\mathbb{Z}/m\mathbb{Z}$ instead of $\mathbb{Z}/C_m$.

Example

Example 4

Determine $\mathbb{R}/C_Z$, where $C_Z = \{(x, y) \in \mathbb{R}^2 \mid x - y \in \mathbb{Z}\}$.

Remark. Instead of xC_Zy one writes $x \equiv y \pmod{\mathbb{Z}}$.

Solution (Sketch). For $x \in \mathbb{R}$ Let

$$\lfloor x \rfloor = \max\{n \mid n \in \mathbb{Z} \text{ and } n \leq x\},$$

the *floor* of x.

Since $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, we have $0 \leq \underbrace{x - \lfloor x \rfloor}_{(x)} < 1$. We call (x)

the *fractional part of* x.

So $(x) \in [0,1)$ and

$$x - (x) = x - (x - \lfloor x \rfloor) = \lfloor x \rfloor \in \mathbb{Z} \;\Rightarrow\; x \equiv (x) \pmod{\mathbb{Z}}$$
$$\Rightarrow\; [x] = [(x)].$$

It follows that $\mathbb{R}/C_Z = \{[y] \,|\, y \in [0,1)\}$.

And one can show that if $y, z \in [0,1)$ and $[y] = [z]$, then $y = z$.

So each equivalence class is *uniquely* represented by a $y \in [0,1)$.

These are the *remainders mod* $\mathbb{Z}$. □

We can rephrase the results of preceding example as follows.

Theorem 3

For every $x \in \mathbb{R}$, there exist unique $n \in \mathbb{Z}$ and $\epsilon \in [0, 1)$ so that $x = n + \epsilon$. In fact, $n = \lfloor x \rfloor$ and $\epsilon = (x)$.

For example,

$$\pi = 3.141592\ldots = 3 + 0.141592\ldots \quad \Rightarrow \quad [\pi] = [0.141592\ldots],$$
$$\sqrt{5} = 2.236067\ldots = 2 + 0.236067\ldots \quad \Rightarrow \quad \left[\sqrt{5}\right] = [0..236067\ldots],$$

whereas

$$-1.75 = -2 + 0.25 \quad \Rightarrow \quad [-1.75] = [0.25].$$

Example

Recall the equivalence relation Q on $\mathbb{Z} \times \mathbb{N}^+$ given by

$$(a, b)Q(c, d) \iff ad - bc = 0.$$

The equivalence classes of Q are called *fractions*. We write

$$\frac{a}{b} := [(a, b)].$$

The *rational numbers* are the set of all fractions:

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{N}^+)/Q.$$

This is the standard way to construct $\mathbb{Q}$ from $\mathbb{Z}$.