Math 4310 Handout - Equivalence Relations

Dan Collins

In class, we've been talking about the integers, which we've denoted $\mathbb{Z}$. We started off talking about *equality* in $\mathbb{Z}$, but then moved on to talking about *congruences*, which is a weaker notion. This handout explains how "congruence modulo n" is something called an *equivalence relation*, and we can use it to construct a set $\mathbb{Z}/n\mathbb{Z}$ that's a "quotient" of $\mathbb{Z}$. The key point is that a congruence modulo n in $\mathbb{Z}$ becomes an equality in $\mathbb{Z}/n\mathbb{Z}$ (and in abstract algebra, we really like to phrase things in terms of equalities).

To start off, we need to say what we mean by a *binary relation* R on a set A. The idea is that any two elements a, b should be able to be compared, and either are "related" (which we might write aRb) or "not related" (which we can write aRb). To formalize this, we can define a binary relation to be any subset $R \subseteq A \times A$, i.e. R can be any set of ordered pairs in A. If R is our relation, we say a and b are related if $(a, b) \in R$ and they're not related otherwise. To make it clearer what we mean, we usually use some symbol like $\sim$ to denote the relation, since $a \sim b$ looks much better than aRb to denote "a and b are related."

So, if $\equiv \pmod{n}$ or $\equiv_n$ denotes congruence modulo n, we can formalize this being a relation by saying it consists of pairs of integers $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that n divides $a - b$. In fact, $\equiv_n$ is a particularly nice type of relation called an *equivalence relation*:

Definition 1. An *equivalence relation* on a set A is a relation $\sim$ on A satisfying the following conditions:

- Reflexivity: If $a \in A$ then $a \sim a$.
- Symmetry: If $a, b \in A$ satisfy $a \sim b$, then we also have $b \sim a$.
- Transitivity: If $a, b, c \in A$ satisfy $a \sim b$ and $b \sim c$, then we also have $a \sim c$.

It's easy to see that $\equiv_n$ satisfies these three axioms. Certainly any number is congruent to itself, and that if $a \equiv_n b$ then $b \equiv_n a$. Finally, if $a \equiv_n b$ and $b \equiv_n c$ we have that n divides both $a - b$ and $b - c$, so it divides $(a - b) + (b - c) = a - c$ and thus $a \equiv_n c$.

Definition 2. Let $\sim$ be an equivalence relation on a set A. We define the *equivalence class* of A, which we denote $[a]$, to be the set of all things equivalent to A under $\sim$:

$$[a] = \{b \in A : a \sim b\}.$$

Using the equivalence relation axioms we can prove that equivalence classes behave pretty nicely:

Lemma 3. *Let $\sim$ be an equivalence relation on a set A. Then:*

1. *For any $a \in A$, a is an element of its own equivalence class $[a]$.*
2. *For any $a, b \in A$ with $a \sim b$, we have $[a] = [b]$.*
3. *For any $a, b \in A$ with $a \not\sim b$, we have that $[a]$ and $[b]$ are disjoint (i.e. contain no common elements).*

Proof. (1) This follows from reflexivity; since $a \sim a$ we have $a \in [a]$ by definition.

(2) To prove equality, it's enough to show the two containments of sets $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

To prove $[b] \subseteq [a]$, i.e. that $[b]$ is a subset of $[a]$, we need to show that whenever $c \in [b]$ we also have $c \in [a]$. But by definition, $c \in [b]$ means $b \sim c$, and by our assumption we have $a \sim b$. Using transitivity for these two relations we conclude $a \sim c$, which means $c \in [a]$ by definition.

To prove $[a] \subseteq [b]$, we can use the same argument as in the previous paragraph, swapping all of the a's and b's. We need to be a little careful, though - our assumption is still $a \sim b$, so we can't swap the letters in the phrase "by our assumption we have $a \sim b$"! Fortunately, we *can* modify the argument a bit using symmetry, and replace it with "by our assumption we have $a \sim b$, and by symmetry we have $b \sim a$."

(3) Suppose not; then there is an element c with $c \in [a]$ and $c \in [b]$. By definition this means $a \sim c$ and $b \sim c$. Using symmetry on the second relation we get $c \sim b$ and then transitivity gives $a \sim b$, which contradicts our assumption. $\square$

We can then define the *quotient set* $A/\sim$ of A by an equivalence relation $\sim$ as the set of equivalence classes:

$$A \sim = \{[a] : a \in A\}.$$

Note that we're defining this as a *set*, so it doesn't contain any element "multiple times"! So if $a \sim b$ and thus $[a] = [b]$, this common equivalence class is considered to be a *single element* of the set $A/\sim$.

So $A/\sim$ is a set of sets, which might be a bit hard to get your head around at first! For a concrete example, we can consider $\mathbb{Z}/\equiv_3$. One element of $\mathbb{Z}/\equiv_3$ is the equivalence class 0, of all elements congruent to 0 mod 3 - so it is the set

$$[0] = \{\cdots, -6, -3, 0, 3, 6, 9, \cdots\}.$$

Note that this means $[0] = [3] = [-3] = [9000]$ and so on - we can "represent" this equivalence class by any of its elements, but they are all different names for the same set. Similarly, we have equivalence classes

$$[1] = \{\cdots, -5, -2, 1, 4, 7, 10, \cdots\} \qquad [2] = \{\cdots, -4, -1, 2, 5, 8, 11, \cdots\}.$$

These are actually all of the equivalence classes - we can see that every element of $\mathbb{Z}$ is in one of them (corresponding to its remainder after division by 3), and then the quotient space

$$\mathbb{Z}/\equiv_3 = \{[0], [1], [2]\}$$

is a three-element sets (with each *element* itself an infinite set of integers). In fact the three sets [0], [1], and [2] are disjoint subsets of $\mathbb{Z}$ and they have union equal to all of $\mathbb{Z}$; this is true in general:

Corollary 4. *Let A be a set and $\sim$ an equivalence relation. Then $A/\sim$ is a* partition *of A: it is a set of subsets of A satisfying:*

- *Any two distinct elements in $A/\sim$ are disjoint subsets of A.*
- *Every element of A is in some element of $A/\sim$ (i.e. the union of all sets in $A/\sim$ is equal to A).*

Proof. The first statement follows from items (2) and (3) of the previous proposition - two equivalence classes $[a]$ and $[b]$ are either equal or disjoint, depending on whether $a \sim b$ or not. The second statement follows from item (1), since any a is in the equivalence class $[a]$ in $A/\sim$. □

So we can think of $A/\sim$ as being constructed by starting with A and "gluing together" elements of A to make single elements of $A/\sim$. Accordingly we have a natural function (sometimes called the "projection map") $\pi : A \to A/\sim$ which takes an element a to its equivalence class $[a]$. (I'm not entirely sure why this construction got the name "quotient" but it's all over mathematics).

Example 5. The main example we're interested in right now (and why we're doing this) is to consider the quotient set $\mathbb{Z}/\equiv_n$ for any $n \geq 1$. This is a finite set with exactly n elements, the "congruence classes" $[0], [1], \ldots, [n-1]$. We call this set the *integers modulo* n, and usually denote it $\mathbb{Z}/n\mathbb{Z}$ rather than $\mathbb{Z}/\sim_n$ (this notation will make more sense later). In this case the projection map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ maps any integer a to its equivalence class $[a]$, which is equal to the equivalence class $[r]$ where $0 \leq r < n$ is the remainder of dividing a by n.

Example 6. This idea of "gluing" comes up often in more geometric settings. For instance we can take the interval $I = [0, 1] \subseteq \mathbb{R}$ and define an equivalence relation on it by $x \sim x$ for every x (which we need for reflexivity) and also $0 \sim 1$ and $1 \sim 0$. Here the equivalence classes are the sets $\{x\}$ for $0 < x < 1$, and $\{0, 1\}$. So all we're doing when we build $I/\sim$ is taking the two ends of the interval and gluing them together, which should give us a circle! (If you want to see how to really make sense of the geometry of this situation, you should take Math 4530).

Example 7. For our purposes in this course we're just assuming that the rational numbers $\mathbb{Q}$ exist and form a field. If you want to formally *construct* $\mathbb{Q}$, though, you might proceed by starting with pairs (a, b) with $a, b \in \mathbb{Z}$ and $b \neq 0$, and interpreting this pair as representing the fraction a/b. But different pairs can give the same fraction, e.g. $(1, 2)$ and $(2, 4)$ both represent the fraction $1/2$. To fix this you need to define an equivalence relation by $(a, b) \sim (c, d)$ if $ad = bc$ (exactly what you get by clearing denominators in the equation $a/b = c/d$).

Example 8. Later on in the course, we'll come back to talking about equivalence relations when we talk about *quotient vector spaces.*

Now that we've defined equivalence relations, we need to talk about how to define functions on them. Since we have the projection map $\pi : A \to A/\sim$, it's easy to define functions *into* $A/\sim$ - we can define a function into A and then do the projection. But what about functions *out of* $A/\sim$? If we can explicitly use the elements of $A/\sim$ then this is easy, of course, but what if we only really have a handle on the elements of A?

Example 9. Consider the rational numbers $\mathbb{Q}$, which we talked about above as coming from equivalence relations for equivalent fractions. Of course we already know how define functions directly with rational numbers: for instance we can define a function $f : \mathbb{Q} \to \mathbb{Q}$ by $f(q) = q + 3/2$. But what if we want to define something using the numerator and denominator of the fraction expression a/b? For instance can try to define $g, h : \mathbb{Q} \to \mathbb{Q}$ by

$$g\big(a/b\big) = \frac{a^2 + b^2}{ab} \qquad\qquad h\big(a/b\big) = \frac{a}{b^2}.$$

Some testing (or algebraic manipulations) should convince you that g is "well-defined" and should give us an actual function. On the other hand, you should also be able to see that h doesn't make sense - you can represent the same rational number as two different fractions and have our "function" h give you different answers!

So how do we know when we can define a function on $A/\sim$ by first defining its value on $[a]$ in terms of a representative a of the equivalence class? We just need to check that if $a \sim b$ and thus $[a] = [b]$, the value we're trying to assign to $f([a])$ is the same as the value we're trying to assign to $f([b])$.

Example 10. There is a well-defined function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ specified by $f([a]) = [1 - a]$. To see this, suppose $a \equiv b \pmod{n}$ are two representatives of the same equivalence class; our rules for working with congruences let us conclude that $1 - a \equiv 1 - b \pmod{n}$ as well, and thus $[1 - a] = [1 - b]$.

Non-Example 11. There is *not* a well-defined function $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ given by $f([a]) = [a]$. In the domain of $\mathbb{Z}/5\mathbb{Z}$ we have $1 \sim 6 \pmod{5}$, for instance, so we'd be trying to set $f([1]) = [1]$ and $f([6]) = 6$. But in the codomain of $\mathbb{Z}/10\mathbb{Z}$, $[1] \neq [6]$ because $1 \not\equiv 6 \pmod{10}$.

Example 12. There is a well-defined function $f : \mathbb{Z}/32\mathbb{Z} \to \mathbb{Z}$ defined by

$$f([a]) = \begin{cases} 0 & a \text{ is even} \\ 1 & a \text{ is odd} \end{cases},$$

because if $[a] = [b]$ then $a \equiv b \pmod{32}$ and thus a, b have the same parity. On the other hand there is not a function $\mathbb{Z}/33\mathbb{Z} \to \mathbb{Z}$ defined this way, because we'd be trying to set $f([0]) = 0$ and $f([33]) = 1$, but $[0] = [33]$.

Example 13. If we take the interval $I = [0, 1]$ with $0 \sim 1$ as discussed above, then $f : I/\sim \to \mathbb{R}$ defined by $f([x]) = \sin(2\pi x)$ is well-defined because we just need to check that $f([0])$ and $f([1])$ agree (which is true because $\sin(0) = 0 = \sin(2\pi)$). On the other hand, $g([x]) = \sin(x)$ is not well-defined because $\sin(1) \neq \sin(0)$.

For working with the sets $\mathbb{Z}/n\mathbb{Z}$, the most important thing we need to do is check that addition and multiplication are well-defined.

Proposition 14. *There are well-defined addition and multiplication maps* $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})$ *given by* $[a] + [b] = [a + b]$ *and* $[a] \cdot [b] = [ab]$.

Proof. To verify well-definedness we need to check that if $[a] = [a']$ and $[b] = [b']$ then $[a + b] = [a' + b']$ and $[ab] = [a'b']$. But this falls out of what we talked about in class, that if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$. $\square$

So we now have a set $\mathbb{Z}/n\mathbb{Z}$ (consisting of n equivalence classes $[0], [1], \ldots, [n - 1]$) with addition and multiplication defined on it. In the language of abstract algebra, this gives $\mathbb{Z}/n\mathbb{Z}$ the structure of a *commutative ring*, and if p is a prime number it actually gives $\mathbb{Z}/p\mathbb{Z}$ the structure of a *field*. Fields are one of the underlying concepts we'll be using in linear algebra, and $\mathbb{Z}/p\mathbb{Z}$ is an important concrete example of them that we'll look at often!