Discrete Mathematics lecture notes 8-1

October 24, 2013

24. Equivalence classes and constructing number systems

Last time we introduced the notion of an equivalence relation $\sim$ on a set X and showed that this was really the same notion of a partition on X. We also noted that we can construct a new set from an equivalence relation:

Definition 1. We denote by $X/\sim$ the set of $\sim$-equivalence classes of X. If we think of an equivalence relation in terms of partitions of X, then $X/\sim$ is the set of subsets of X that make up the partition. Elements of $X/\sim$ are called *equivalence classes*, and denote by $[x]$ the equivalence class containing $x \in X$.

Recall that if $x, y \in X$, then either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

Exercise. Reprove the above claim, being sure to make note of which properties of equivalence relations you use where.

Let us see how equivalence relations can be used to construct new sets of interest in some specific examples.

$\mathbb{Z}/\mathbf{n}$,

Pick $n \in \mathbb{N}$ and let $\sim$ be the equivalence relation on $\mathbb{Z}$ given by $a \sim b$ iff $a \mod n = b \mod n$ iff $n|(b-a)$.

Exercise. Show that $\sim$ is an equivalence relation, and $\mathbb{Z}/\sim$ has n elements, namely $[0], [1], \ldots, [n-1]$.[1]

From this exercise, and also from the suggestive notation, we might guess that $\mathbb{Z}/\sim$ is actually $\mathbb{Z}/n$ in disguise. If so, the disguise is a beaglepuss; comparing the constructions of $\mathbb{Z}/\sim$ and $\mathbb{Z}/n$ show them to be exactly the same, if phrased slightly differently.

That said, $\mathbb{Z}/n$ came equipped with an algebraic structure that $\mathbb{Z}/\sim$ doesn't yet have.[2] Luckily, the addition and multiplication on $\mathbb{Z}/n$ are easy to reproduce for $\mathbb{Z}/\sim$:

Definition 2. Define an addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}/\sim$ by

$$[a] \oplus [b] := [a+b] \qquad \text{and} \qquad [a] \odot [b] := [a \cdot b],$$

where $+$ and $\cdot$ are the standard addition and multiplication of $\mathbb{Z}$.

There is a potential problem with this definition, in that it may not be *well-defined.* In other words, it may not actually make sense, because the addition in $\mathbb{Z}/\sim$ is defined in terms of *representatives* of the equivalence classes. What happens if we change the representative? In other words, since (for example) $[1] = [1+n]$ and $[0] = [n]$, we should be able to compute $[1] + [0]$ as either $[1+0]$ or $[(1+n)+n]$. Note that even though $1 \neq 1+2n$, the *classes* of these two integers are in fact equal, so the addition $\oplus$ is well-defined *on the level of equivalence classes*, i.e., in $\mathbb{Z}/\sim$.

Exercise. Show in general that if $[a] = [a']$, $[b] = [b']$, then $[a+b] = [a'+b']$ and $[a \cdot b] = [a \cdot b']$, and conclude that $\oplus$, $\otimes$ are well-defined in general.

$\mathbb{Z}$,

Let us see how to construct the integers from the natural numbers. Up until this point we've simply made some noises about "adjoining additive inverses" and left it at that; of course this isn't really good enough. Let's see how we can make this more precise.

Set $X := \mathbb{N} \times \mathbb{N}$, and define a relation $\sim$ on X by $(a, b) \sim (a', b')$ if $a + b' = a' + b$.[3]

[1] Note that $[i]$ here means the equivalence class containing i, *not* the set $\{1, 2, \ldots, i\}$. Write out explicitly what the set $[i]$ means in this new context.

[2] Note that in the definition of $\mathbb{Z}/\sim$ we take it to be the *set* of equivalence classes of $\sim$; saying that there is an addition or multiplication is *extra structure* that we must specify.

[3] Morally, what's going on is that we want to write something like "$a - b$" for the class $[a, b]$, except that subtraction isn't something that makes sense in $\mathbb{N}$. Instead, we define our equivalence relation in such a way that two pairs are equivalent if their imagined differences would be equal, but stated in such a way so as to never make use of the notion of subtraction.

Exercise. Show that $\sim$ is indeed an equivalence relation.

We *define* $\mathbb{Z} := X \sim$.[4]

Exercise. Show that if $[a, b] \in \mathbb{Z}$, then there is some in $n \in \mathbb{N}$ such that $[a, b] = [n, 0]$ or $[a, b] = [0, n]$.

Exercise. Use the previous exercise to define a bijection from the ordinary[5] set of integers to what we're now defining to be $\mathbb{Z}$. Call this bijection φ.

Again, $\mathbb{Z}$ should come equipped with an addition and multiplication, which should be built out of that of $\mathbb{N}$.

Definition 3. Define an addition $\oplus$ and a multiplication $\odot$ on $\mathbb{Z}$ by

$$[a, b] \oplus [c, d] := [a + c, b + d] \qquad \text{and} \qquad [a, b] \odot [c, d] := [a \cdot c + b \cdot d, a \cdot d + b \cdot c],$$

where $+$ and $\cdot$ are the already-defined addition and multiplication of $\mathbb{N}$.[6]

Exercise. Show that $\oplus$ and $\odot$ are well-defined.

Exercise. Show that $[0, 0]$ is an identity for $\oplus$, and that $[1, 0]$ is an identity for $\odot$. Moreover, show that for any $[a, b] \in \mathbb{Z}$, we have $[a, b] \oplus [b, a] = [0, 0]$, so that every element has an additive inverse. Finally, show that $\oplus$ and $\odot$ are associative, commutative, and obey the distributive law.

Exercise. If $\varphi : Z \to \mathbb{Z}$ is the bijection from the naive integers $\mathbb{Z}$ that you constructed a few exercise ago, show that $\varphi(x + y) = \varphi(x) \oplus \varphi(y)$ and $\varphi(x \cdot y) = \varphi(x) \odot \varphi(y)$.

The content of the previous exercise is often rephrased: φ is an *isomorphism.* This means not only that it is a bijection, but that the bijection respects all the algebraic structure in sight (here, multiplication and addition). From the point of view that we recognize mathematical objects by their properties,[7] the existence of an isomorphism means that we should think of the naive and formal integers as being "the same" in a very fundamental sense: As they have the same structure and satisfy the same properties, we have no reasonable way of distinguishing one from the other. So we won't.

$\mathbb{Q}$,

The whole idea behind creating $\mathbb{Z}$ from $\mathbb{N}$ was that we should be able to undo addition–i.e., subtract–and that we could arrange this through a clever choice of equivalence class on pairs on natural numbers. Similarly, the process of going from $\mathbb{Z}$ to $\mathbb{Q}$ is based on our desire to undo multiplication–to divide. Luckily, we have a template we can follow: Repeat the above construction, with multiplication in place of addition.

Set $Y := \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$,[8] and define a relation $\sim$ on Y by setting $(a, b) \sim (c, d)$ if $ad = bc$, understood to mean multiplication in $\mathbb{Z}$.[9]

Exercise. Show that $\sim$ is an equivalence relation on Y.

Define $\mathbb{Q} := Y / \sim$. Show that there is an injection $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q} : a \mapsto [a, 1]$.

Definition 4. Define an addition and multiplication on $\mathbb{Q}$ by

$$[a, b] \oplus [c, d] := [a \cdot d + b \cdot c, b \cdot d] \qquad \text{and} \qquad [a, b] \odot [c, d] := [a \cdot d, b \cdot d],$$

where again $+$ and $\cdot$ are the already-defined addition and multiplication on $\mathbb{Z}$.

[4] Of course, the previous section already made reference to $\mathbb{Z}$; it was included first because it was an easier example. If you prefer to be rigorous, read this section before the previous one.

[5] I.e., our earlier naive notion.

[6] To motivate this definition, go to a small corner of your notebook and work out: "If $[a, b] = a - b$ and $[c, d] = c - d$, then $(a - b) + (c - d) = (a + c) - (b + d)$ and $(a - b)(c - d) = (ac + bd) - (ad + bc)$." Then turn this intuition into a definition.

[7] Look back on the first few lectures where a great deal of emphasis was placed on the axioms that govern $\mathbb{N}$, for instance.

[8] Do I mean $\mathbb{Z}$ the naively defined set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, or the set of equivalence classes on $\mathbb{N} \times \mathbb{N}$ defined above? Because you've shown there is an isomorphism between these two objects, *it doesn't matter*!

[9] Again, we secretly think of an equivalence class $[a, b]$ as the fraction $\frac{a}{b}$. In this context the idea that one number could have many names is actually something that you're quite familiar with: $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \ldots$ just reflects that we've set up or relation so that $(1, 2) \sim (2, 4) \sim (3, 6) \sim \ldots$.

Exercise. Show that $\oplus$ and $\odot$ are well-defined.

Exercise. Show that $[0,1]$ is an additive identity for $\mathbb{Q}$ and $[1,1]$ is a multiplicative identity. Show that every element $[a,b]$ of $\mathbb{Q}$ has an additive inverse, and if $[a,b] \neq [0,1]$, then $[a,b]$ has a multiplicative inverse. Finally, show that any element of $\mathbb{Q}$ can be written as the product of something in the image of ι and the multiplicative inverse of something else in the image of ι.

Exercise. Show that $\oplus$ and $\odot$ are associative, commutative, and satisfy the distributive law.

Exercise. If Q is the naive version of the rationals, i.e., symbols of the form $\frac{a}{b}$, construct a bijection $\varphi : Q \to \mathbb{Q}$, check that it is well-defined, and show that $\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{a}{b}) \oplus \varphi(\frac{c}{d})$ and $\varphi(\frac{a}{b} \cdot \frac{c}{d}) = \varphi(ab) \odot \varphi(\frac{c}{d})$. Conclude that our naive and formal versions of the rationals are isomorphic.

and beyond. . .

Hopefully you're becoming convinced that looking at equivalence relations is a good way of getting new sets out of old, or even new sets with additional structure. We will not do so in this course, but one can also construct the real numbers $\mathbb{R}$ out of equivalence classes of (certain infinite sequences of) rational numbers, or the complex numbers as a set of equivalence classes of polynomials with coefficients in $\mathbb{R}$.[10] To call equivalence relations ubiquitous would understate their importance, especially as (as I'm trying to convince you) we often make extensive use of them without even realize that we are doing so.

[10] Constructing $\mathbb{R}$ from $\mathbb{Q}$ is a fairly involved process, but constructing $\mathbb{C}$ from $\mathbb{R}$ is relatively straightforward to state: Recall that $\mathbb{R}[x]$ denotes the set of polynomials with real coefficients, and define a relation $\sim$ on $\mathbb{R}[x]$ by setting $f \sim g$ if $(x^2+1)|(f-g)$. Then, as a set, $\mathbb{C} := \mathbb{R}[x]/\sim$, and moreover the addition and multiplication on $\mathbb{R}[x]$ induce a multiplication on $\mathbb{C}$. If we regard $r \in \mathbb{R}$ as a constant polynomial, then $r \mapsto [r]$ is an injection $\mathbb{R} \hookrightarrow \mathbb{C}$, and one can show that any element of $\mathbb{C}$ can be written $[a+bx]$ for some $a, b \in \mathbb{R}$. Finally, the obvious definition of multiplication gives $[x] \cdot [x] = [x^2]$; since $(x^2+1)|((x^2)-(-1))$, we conclude that $[x]^2 = [-1]$. And away we go.