Math/CS 120: Intro. to Math	Professor: Padraic Bartlett

Lecture 4: Constructing the Integers, Rationals and Reals

Week 5 *UCSB 2014*

1 The Integers

Normally, using the natural numbers, you can easily define the **integers** as follows:

Definition. The **integers**, denoted $\mathbb{Z}$, are all of the positive and negative whole numbers: i.e.

$$\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, 3, \ldots\}.$$

However, the definition above can readily be seen to be suspect, for precisely the same reasons that our earlier attempts to make the natural numbers were sketchy. What do we mean by -3? How does -3 interact with addition and multiplication, and does it do so in a way that "plays nicely" with our recursive definitions from earlier? How do we even **form** this set using our axioms — we don't have any rules that amount to "you can make a second copy of your first set but with special symbols in front of all of those elements," and it's not clear how our axioms might adapt to making such rules in any place.

We present a rigorous construction of $\mathbb{Z}$ in this section! This will involve less work than our earlier constructions, but will require one very deep and useful concept: the idea of an **equivalence class**.

1.1 Equivalence Classes

Definition. Take any set S. A **relation** R on this set S is a map that takes in ordered pairs of elements of S, and outputs either true or false for each ordered pair.

You know many examples of relations:

- Equality ($=$), on any set you want, is a relation; it says that $x = x$ is true for any x, and that $x = y$ is false whenever x and y are not the same objects from our set.
- "Mod n" ($\equiv \mod n$) is a relation on the integers: we say that $x \equiv y \mod n$ is true whenever $x - y$ is a multiple of n, and say that it is false otherwise.
- "Less than" ($<$) is a relation on many sets, for example the real numbers; we say that $x < y$ is true whenever x is a smaller number than y (i.e. when $y - x$ is positive,) and say that it is false otherwise.
- "Beats" is a relation on the three symbols (rock, paper, scissors) in the game Rock-Paper-Scissors. It says that the three statements "Rock beats scissors," "Scissors beats paper," and "Paper beats rock" are all true, and that all of the other pairings of these symbols are false.

In this class, we will study a specific class of particularly nice relations, called **equivalence relations**:

Definition. A relation R on a set S is called an **equivalence relation** if it satisfies the following three properties:

- **Reflexivity**: for any $x \in S$, xRx.
- **Symmetry**: for any $x, y \in S$, if xRy, then yRx.
- **Transitivity**: for any $x, y, z \in S$, if xRy and yRz, then xRz.

It is not hard to classify our example relations above into which are and are not equivalence relations:

- Equality $(=)$ is an equivalence relations on any set you define it on – it trivially satisfies our three properties of reflexivity, symmetry and transitivity.
- "Mod n" ($\equiv \mod n$) is an equivalence relation on the integers. This is not hard to check:
  - **Reflexivity**: for any $x \in \mathbb{Z}$, $x - x = 0$ is a multiple of n; therefore $x \equiv x \mod n$.
  - **Symmetry**: for any $x, y \in S$, if $x \equiv y \mod n$, then $x - y$ is a multiple of n; consequently $y - x$ is also a multiple of n, and thus $y \equiv x \mod n$.
  - **Transitivity**: for any $x, y, z \in S$, if $x \equiv y \mod n$ and $y \equiv z \mod n$, then $x - y$, $y - z$ are all multiples of n; therefore $(x - y) + (y - z) = x - y + y - z = x - z$ is also a multiple of n, and thus $x \equiv z \mod n$.
- "Less than" $(<)$ is not an equivalence relation on the real numbers, as it breaks reflexivity: $x \not< x$, for any $x \in \mathbb{R}$.
- "Beats" is not an equivalence relation on the three symbols (rock, paper, scissors) in the game Rock-Paper-Scissors, as it breaks symmetry: "Paper beats rock" is true, while "Rock beats paper" is false.

Equivalence relations are remarkably useful because they allow us to work with the concept of equivalence classes:

Definition. Take any set S with an equivalence relation R. For any element $x \in S$, we can define the **equivalence class** corresponding to x as the set

$$\{s \in S \mid sRx\}$$

Again, you have worked with lots of equivalence classes before. For $\mod 3$ arithmetic on the integers, for example, there are three possible equivalence classes for an integer to belong to:

$$\{\ldots - 6, -3, 0, 3, 6 \ldots\}$$
$$\{\ldots - 5, -2, 1, 4, 7 \ldots\}$$
$$\{\ldots - 4, -1, 2, 5, 8 \ldots\}$$

Every element corresponds to one of these three classes.

The concept of equivalence classes is useful largely because of the following observation:

Observation. Take any set S with an equivalence relation R. On one hand, every element x is in some equivalence class generated by taking all of the elements equivalent to x, which is nonempty by reflexivity. On the other hand, any two equivalence classes must either be completely disjoint or equal, by symmetry and transitivity: if the sets $\{s \in S \mid sRx\}$ and $\{s' \in S \mid s'Ry\}$ have one element t in common, then tRx and tRy implies, by symmetry and transitivity, that xRy; therefore, by transitivity, any element in one of these equivalence relations must be in the other as well.

Consequently, these equivalence classes **partition** the set S: that is, if we take the collection of all distinct equivalence classes, every element of S is in exactly one such set!

1.2 Defining $\mathbb{Z}$

Using this concept, we define the integers as follows:

Definition. Construct $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$, the Cartesian product of the natural numbers with themselves. Create an equivalence relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ as follows: write $(a, b) \sim (c, d)$ if and only if $a - b = c - d$. (If you're concerned about the fact that subtraction isn't formally defined yet, simply set $(a, b) \sim (c, d)$ if and only if $a + d = b + c$; this is equivalent.)

Take the collection of all of the equivalence classes of $\mathbb{N}^2$ under this relation. We call this set the **integers**, and write it as $\mathbb{Z}$.

It may be hard at first to see how this corresponds with our normal notion of "integer." The idea, roughly, is that a pair (a, b) corresponds to the integer $a-b$, where our equivalence relation is a way of saying that (a, b) and $(a + k, b + k)$ both represent the same "integer."

This might seem weird, but this has the advantage of being a set we can construct with our axioms (it's a collection of subsets of $\mathbb{N}^2$, all expressible via formulas!) Moreover, while it looks weird, it's actually a really easy set to define all of our operations on:

- Suppose we want to add two equivalence classes X, Y together. To do this, pick out a representative $(x_1, x_2) \in X, (y_1, y_2) \in Y$ from its equivalence class. Add these pairwise, to get the pair $(x_1 + y_1, x_2 + y_2)$. There is an equivalence class Z containing this pair, because equivalence classes partition $\mathbb{N}^2$! Define $X + Y = Z$. Notice that it doesn't matter what representative we picked for X or Y above, as picking any other representatives $(x_1 + c, x_2 + c), (y_1 + d, y_2 + d)$ would result in $(x + 1 + y + 1_c + d, x_2 + y_2 + c + d)$, which is equivalent to $(x_1 + y_1, x_2 + y_2)$ and thus does not change our equivalence class Z. Consequently, this is a well-defined operation!

- Multiplication is still iterated addition.

- For ordering: to compare any two equivalence classes X, Y, pick out a representative $(x_1, x_2) \in X, (y_1, y_2) \in Y$. We say that $X < Y$ if and only if $x_1 - x_2 < y_1 - y_2$, or equivalently $x_1 + y_2 < y_1 + x_2$. Again, you can check that this property does not depend on the representatives chosen from X, Y's equivalence classes, so this too is well-defined. We leave as an exercise for the homework the observation that this ordering $<$ is still a total ordering, but that it no longer satisfies the well-ordering property.

1.3 Properties of $\mathbb{Z}$

The integers satisfy all of the properties listed earlier for $\mathbb{N}$, with the exception of well-ordering:

- **Closure(+)**: $\forall a, b \in \mathbb{Z}$, we have $a+b \in \mathbb{Z}$.
- **Identity(+)**: $\exists 0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}$, $0 + a = a$.
- **Commutativity(+)**: $\forall a, b \in \mathbb{Z}, a + b = b + a$.
- **Associativity(+)**: $\forall a, b, c \in \mathbb{Z}, (a + b) + c = a + (b + c)$.
- **Closure(·)**: $\forall a, b \in \mathbb{Z}$, we have $a \cdot b \in \mathbb{Z}$.
- **Identity(·)**: $\exists 1 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}$, $1 \cdot a = a$.
- **Commutativity(·)**: $\forall a, b \in \mathbb{Z}, a \cdot b = b \cdot a$.
- **Associativity(·)**: $\forall a, b, c \in \mathbb{Z}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Antireflexivity(<)**: $\forall a \in \mathbb{Z}, a \not< a$.
- **Antisymmetry(<)**: $\forall a, b \in \mathbb{Z}$, exactly one of ($a < b$, $a = b$,$b < a$) holds.
- **Transitivity(<)**: $\forall a, b, c \in \mathbb{Z}$, if $a < b$ and $b < c$, we have $a < c$.
- **Add. Order(<, +)**: $\forall a, b, c \in \mathbb{Z}$, if $a < b$, then $a + c < b + c$.
- **Distributivity**: $(+, \cdot)$: $\forall a, b, c \in \mathbb{Z}, (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

As well, it satisfies the following extra two properties:

- **Inverses**$(+) : \forall a \in \mathbb{Z}, \exists$ a unique $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0$.
- **Mult.Order**$(<, \cdot) : \forall a, b, c \in \mathbb{Z},$ if $a < b, 0 < c$ then $ac < bc$.

Again, you can rigorously prove that the integers satisfy these properties. Instead of doing this, our focus for this class is going to be showing how we can use these relatively few properties to prove other statements about these number systems! For example, a property that we didn't list above, but that seems pretty important, is the following:

- **New property**?$(+) : \forall a \in \mathbb{Z}, 0 \cdot a = 0.$

Another also-true property, that we also omitted above, is the following:

- **Other new property**?$(+) : \forall a \in \mathbb{Z}. (-a) = (-1) \cdot a.$

A question we could ask, given these properties, is the following: should we have listed it above? Or, if we already have the properties we've listed earlier, are these additional properties superfluous: i.e. can we prove that they're true just using the properties we have above, without having to look at the definitions of $\mathbb{Z}$?

As it turns out, we can simply use our earlier properties to prove that these are true! We do this here:

Claim.

- **New property?(+)** : $\forall a \in \mathbb{Z}, 0 \cdot a = 0$.

Proof. Take any $a \in \mathbb{Z}$. Because of the closure($\cdot$) property, we know that $0 \cdot a$ is also a natural number. Trivially, we know that

$$0 \cdot a = 0 \cdot a.$$

We also know that 0 is an additive identity: therefore, in specific, we know that $0 = 0 + 0$, and therefore that

$$0 \cdot a = (0 + 0) \cdot a.$$

Applying the distributive property then tells us that

$$0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a).$$

Now, we can use the inverse(+) property to tell us that because $0 \cdot a$ is a natural number, we also know that there is some other natural number $-(0 \cdot a)$ such that $(0 \cdot a) + (-(0 \cdot a)) = 0$. Then, if we add this to both sides of our equality above (which we can do and still get integers because of closure,) we get

$$(0 \cdot a) + (-(0 \cdot a)) = ((0 \cdot a) + (0 \cdot a)) + (-(0 \cdot a)).$$

Applying the inverse property to the left hand side tells us that it's 0; applying the associative property to the right side tells us that

$$0 = ((0 \cdot a) + (0 \cdot a)) + (-(0 \cdot a)) = (0 \cdot a) + ((0 \cdot a) + (-(0 \cdot a))) = (0 \cdot a) + 0 = (0 \cdot a),$$

by applying first the inverse property and then the additive identity property to make the $+0$ go away. Therefore, we've proven that for any $a \in \mathbb{Z}$, we have

$$0 = 0 \cdot a.$$

□

We continue to our second proof:

Claim.

- **Other new property?(+)** : $\forall a \in \mathbb{Z}, (-a) = (-1) \cdot a$.

Proof. By the multiplicative identity property, we know that $1 \in \mathbb{Z}$; by the additive inverse property, we then also know that $-1 \in \mathbb{Z}$ and that

$$0 = 1 + (-1).$$

Using closure, distributivity, and the multiplicative identity property, we can take any a and multiply it by the left and right hand sides above:

$$0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a).$$

Using our result above, we know that $0 \cdot a = 0$, and therefore that

$$0 = a + (-1) \cdot a).$$

Using the additive inverse property and closure, we know that $-a$ is an integer and that we can add it to the left and right hand sides above:

$$(-a) + 0 = (-a) + (a + (-1) \cdot a).$$

Using the additive identity property at left and associativity/inverses/the additive identity at right gives us

$$(-a) = ((-a) + a) + (-1) \cdot a = 0 + (-1) \cdot a = (-1) \cdot a,$$

which is what we claimed. $\square$

These proofs should hopefully persuade you of two things: one, that it's possible to do an awful lot with the properties listed above, and two that it can be really fussy to do so. Throughout most of your CCS courses, we'll generally assume that things like arithmetic work how we think they do, and not bother too much with citing these properties; usually, we'll keep our focus on the stranger/weirder definitions that each class specializes in, rather than these basic arithmetical definitions.

However, it does bear noting that the proofs above is cool in a few ways that aren't immediately obvious, as well. Specifically, we showed that $0 \cdot a = 0$, and that $(-a) = (-1) \cdot a$, using **only** these properties, and not anything special to $\mathbb{Z}$. Therefore, we know that the same result will be true for **anything**[1] that also satisfies these properties! This illustrates another thing that it's always worth paying attention to in your proofs: what facts are you specifically using in a proof? Do you need all of them? Can you extend your proof to covering many other situations, because you only care about a few properties and not the details of the object you're studying? (Keeping this in mind is one of the bigger leaps I made when switching from undergrad to graduate mathematical research.)

2 Defining $\mathbb{Q}$ and $\mathbb{R}$

2.1 The Rational Number System

One particularly useful use of the concept of equivalence classes is in our definition of the rational numbers themselves! In particular, ask yourself: what is the set of the rational numbers?

Most people will quickly say something equivalent to the following:

$$\left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

[1] Things that satisfy the list of properties with respect to $+, \cdot$ (but ignore the $<$ ones) that we listed above are called **rings**; you will see them in many CCS courses.

The issue with this as a set is that it has **lots** of different entries for numbers that we usually think are not different objects! I.e. the set above contains

$$\frac{-1}{-2}, \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}, \ldots,$$

all of which we think are the same number! People usually then go back and change our definition above to the following:

$$\left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b > 0, GCD(a,b) = 1 \right\}.$$

This fixes our issue from earlier: we no longer have "duplicated" numbers running around. However, it has other issues: suppose that you wanted to define addition on this set! Naively, you might hope that the following definition would work:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

However, for many fractions, the output of this operation is not an element of our new set!

$$\frac{2}{5} + \frac{8}{5} = \frac{40 + 10}{25} = \frac{50}{25} \notin \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b > 0, GCD(a,b) = 1 \right\}.$$

These difficulties that we're running into with the rational numbers come from the fact that, practically speaking, **they aren't a set** in most contexts that we work with them! Rather, they are a **set with an equivalence relation**:

- The underlying set for the rational numbers: $\mathbb{Z} \times \mathbb{N}$, the set of all pairs of numbers of the form (z, n), where z is an integer and n is a natural number.

- The equivalence relation: we say that $(a, b) \sim (c, d)$ if and only if $\frac{a}{b} = \frac{c}{d}$. This might seem like it's referring to the rationals to define the rationals! To avoid this, use the following equivalent definition: $(a, b) \sim (c, d)$ if and only if $ad = bc$. (Check that this is an equivalence relation!)

- A **rational number** is any equivalence class of our set above under the above equivalence relation. This is the idea we have when we think of

  $$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}, \ldots$$

  as all representing the "same number" $1/2$: we're identifying $1/2$ with its equivalence class!

- In this setting, we define addition, multiplication, and all of our other properties just how we would normally. That is: suppose we have two equivalence classes X, Y of $\mathbb{Z} \times \mathbb{N} / \sim$ that we want to add. To do this, we do the following:

  - Take any element $(a, b) \in X$ and any $(c, d) \in Y$.

– Find the pair corresponding to what we think addition should be: i.e. because

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

we should send $(a, b) + (c, d)$ to $(ad + bc, bd)$.

– Find the equivalence class Z containing $(ad + bc, bd)$.

– Set $X + Y = Z$.

If this process is well-defined, then it shouldn't matter what $(a, b) \in X$ and $(c, d) \in Y$ we pick here: because our algorithm had us pick any such pairs, it should give us the same output no matter what we pick! And indeed, this happens: consider what would occur if we picked any other elements from X, Y; if $(a, b) \sim (w, x)$ and $(c, d) \sim (y, z)$, then we have $ax = bw, cz = dy$ and therefore that

$$\begin{aligned}
(a, b) + (c, d) &= (ad + bc, bd) \\
&\sim (adxz + bcxz, bdxz) \\
&= (bwdz + bxdy, bdxz) \\
&\sim (wz + xy, xz) \\
&= (w, x) + (y, z).
\end{aligned}$$

So addition is well-defined! Ordering and multiplication have similar sorts of definitions; we leave them to the reader to check that they're also well-defined.

The rational numbers satisfy all of the properties listed for the integers, along with the following new properties:

- **Inverses($\cdot$)** : $\forall a \in \mathbb{Q}, a \neq 0, \exists$ a unique $\frac{1}{a} \in \mathbb{Q}$ such that $a \cdot \frac{1}{a} = 0$.
- **Archimedean($<$)** : $\forall p > 0 \in \mathbb{Q} \exists n \in \mathbb{N}$ such that $0 < \frac{1}{n} < p$.

2.2 The Real Number System

Finally, we move to the real number system:

Definition. The real numbers, denoted $\mathbb{R}$, have a lot of different definitions. The most common is probably the "infinite decimal sequence" definition, which we give below:

$$\mathbb{R} = \{a_0.a_1a_2a_3a_4 \ldots : a_0 \in \mathbb{Z}, a_i \in \{0, \ldots 9\}, i \geq 1\}$$

In the above definition, we regard infinite strings of 9's, like $.999999999\ldots$, to be equivalent to a $+1$ in the next highest decimal place and replacing all of the 9's with 0's: for example, we ask that $.9999999\ldots = 1.000000\ldots$. Once again, this is a notion you can make formal with the concept of **equivalence relations**.

Instead of proceeding in this way, however, we adopt a different approach for defining the real numbers. Consider the following leading question: what, actually, do you think of when you think about a specific real number? Take π, for example: what do you think of when this comes to mind?

Typically, people associate π with its decimal sequence: i.e.

$$\pi = 3.14159265\ldots$$

This is why we went with the decimal approximation above. However, I would claim that the important part of this description is not the "decimal" part: it's the "approximation" part! For example, we can express numbers in lots of different ways: i.e. we could write

$$\begin{aligned}\sqrt{2} &= 1.4142135623\ldots\\ &= 1.0110101000_{\text{binary}}\ldots\\ &= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}\end{aligned}$$

All of these expressions are correct! Furthermore, we want to think of all of these expressions as denoting the same real number.

Consequently, I would claim that our definition for a real number should not be something that talks about decimal strings. Instead, it should be something that talks about approximations! We do this here:

Definition. Cauchy: We say that a sequence $\{a_n\}_{n=0}^{\infty}$ is **Cauchy** if "the terms of $\{a_n\}_{n=0}^{\infty}$ get close to each other as n gets large." Formally, we say

$$\{a_n\}_{n=0}^{\infty} \text{ is Cauchy} \Leftrightarrow \forall \epsilon > 0, \exists N \forall m, n > N, |a_n - a_m| < \epsilon.$$

Essentially, for any amount of "close to L" we want, there is some N past which if we pick a_m, a_n's with $m, n > N$, we have that a_n is as close to a_m as we wanted. It's *like* having a limit, except that you don't actually know where the sequence is going; just that the terms are getting close to each other!

These are the "approximations" that we talked about. To determine when two approximations are **equivalent**, then, we use the following definition:

Definition. Limits: We say that a sequence $\{a_n\}_{n=0}^{\infty}$ has the limit L as n approaches infinity if "the terms of $\{a_n\}_{n=0}^{\infty}$ go to L as n gets large." Formally, we say

$$\lim_{n\to\infty} a_n = 0 \Leftrightarrow \forall \epsilon > 0, \exists N \forall n > N, |a_n - L| < \epsilon.$$

Essentially, for any amount of "close to L" we want, there is some N past which if we pick a_n's with $n > N$, we have that a_n is as close to L as we wanted.

With this machinery, we define the real numbers as follows:

Definition. Take the collection of all Cauchy sequences of rational numbers: call it S. Define a relation $\sim$ on Cauchy sequences, defined as follows: we say that $\{x_n\}_{n=1}^{\infty} \sim \{y_n\}_{n=1}^{\infty}$ if and only if $\lim_{n\to\infty} x_n - y_n = 0$. In other words, we declare two Cauchy sequences to be equivalent if and only if they go to the same place!

This is an equivalence relation. To see why, simply check the three properties:

- **Reflexive**: We want to show that for any $\{x_n\}_{n=1}^{\infty}$, $\{x_n\}_{n=1}^{\infty} \sim \{x_n\}_{n=1}^{\infty}$. By definition, this happens if and only if the limit $\lim_{n\to\infty} x_n - x_n = \lim_{n\to\infty} 0 = 0$, which is true!

- **Symmetry**: We want to show that if $\{x_n\}_{n=1}^{\infty} \sim \{y_n\}_{n=1}^{\infty}$, then $\{y_n\}_{n=1}^{\infty} \sim \{x_n\}_{n=1}^{\infty}$. This is also pretty quick: if we have $\{x_n\}_{n=1}^{\infty} \sim \{y_n\}_{n=1}^{\infty}$, then we have that $\lim_{n\to\infty} x_n - y_n = 0$. But this limit is just $-1 \cdot \lim_{n\to\infty} y_n - x_n$, which consequently is also 0; therefore $\{y_n\}_{n=1}^{\infty} \sim \{x_n\}_{n=1}^{\infty}$, as claimed.

- **Transitivity**: We want to show that if $\{x_n\}_{n=1}^{\infty} \sim \{y_n\}_{n=1}^{\infty} \sim \{z_n\}_{n=1}^{\infty}$, then $\{x_n\}_{n=1}^{\infty} \sim \{z_n\}_{n=1}^{\infty}$.

  This is similar. If we have $\{x_n\}_{n=1}^{\infty} \sim \{y_n\}_{n=1}^{\infty} \sim \{z_n\}_{n=1}^{\infty}$, then we have that $\lim_{n\to\infty} x_n - y_n = \lim_{n\to\infty} y_n - z_n = 0$.

  By some theorems that we'll talk about in a week or two, the sum of two limits is equal to the limit of their sums, provided all of the individual limits exist[2] and are finite. Therefore, we can combine these two limits to get that $\lim_{n\to\infty} x_n - z_n = 0$, as claimed!

Look at $S/\sim$: i.e. the collection of all equivalence classes of Cauchy sequences under this relation $\sim$. (Less formally: this is the collection of all approximations, with two approximations called equivalent if they approximate the same thing!) We define the real numbers as $S/\sim$.

As before, we can define addition and other operations on this set with little difficulty:

- To add two equivalence relations X, Y, pick two representatives $\{x_n\}_{n=1}^{\infty} \in X, \{y_n\}_{n=1}^{\infty} \in Y$.

- Form the Cauchy sequence $\{x_n + y_n\}_{n=1}^{\infty}$, and let Z be the equivalence class containing this sequence.

- Set $X + Y = Z$.

As before, you can check that this is well-defined!

Just to explore this concept of the real numbers a bit further, let's consider a few examples of Cauchy sequences.

Example. The sequence $\{a_n\}_{n=0}^{\infty}$, where each $a_n = 0$, is Cauchy.

[2] If they don't, then this can go horribly wrong. Consider $\lim_{n\to\infty} 0$, which is 0, and which is definitely not equal to $(\lim_{n\to\infty} n) + (\lim_{n\to\infty} -n) = \infty - \infty =$undefined!

Proof. This might seem like a trivial example, but let's start with it because it will give us practice with our definitions. As a first step: we want to show that some object (namely, $\{a_n\}_{n=0}^{\infty}$) has some property (is Cauchy.)

How do we do this? Well: we **use the definition of the property!** This is the only approach we can take to this problem, in fact — if we want to show that something satisfies a given property, we **must** look up the definition of that property, and then show[3] that our object satisfies that definition!

Let's do this here. Our definition for Cauchy was the following:

$$\forall \epsilon > 0, \exists N \forall m, n > N, |a_n - a_m| < \epsilon.$$

How do we prove such a statement? Well; once again, our first move here is predetermined without any thought. To prove a claim that starts with a $\forall$ quantifier, our first step must be to consider **all** possible values that satisfy that claim! So: the first words on our paper should be

"Take any $\epsilon > 0$."

What does the rest of our definition ask us for? Well, we're trying to find **some** N such that for all $n, m > N$, we have $|a_n - a_m| < \epsilon$. This may look difficult to understand, so let's actually plug in what the a_n's are into this expression:

$$\exists N \forall n, m > N, |0 - 0| < \epsilon.$$

Now this is less scary! In particular: can you find a value of N such that $0 < \epsilon$? Sure! Any N works, in fact, because $\epsilon > 0$ by assumption! So: can you find a value of N such that for all (things you don't care about here), you have $0 < \epsilon$? Again, sure! Any N works.

But what does this mean? We've shown that for any ϵ greater than zero, there is a value of N such that for all n, m greater than N, $|a_n - a_m| = 0 < \epsilon$. In other words, we proved that this sequence is Cauchy! $\square$

Hopefully the above example illustrated a bit of how to prove some sequence $\{a_n\}_{n=0}^{\infty}$ is Cauchy. We give a skeleton version of the general process here, along with a less-trivial example:

- Write "Take any $\epsilon > 0$."
- Take the expression $|a_n - a_m|$, and substitute in whatever the a_n's are defined to be.
- Stare at the expression $|a_n - a_m| < \epsilon$, and try to find out how big n, m have to be to make that expression true. Often, you will need to refer to ϵ in this "big enough" value; this is OK, because our first step in this proof was to pick ϵ, and so this is a defined quantity we can refer to.

  Often, to do this, we will replace $|a_n - a_m|$ with some simpler and larger expression that is easier to work with, and yet still goes to zero (and thus will be smaller than our ϵ for big enough values of n, m!)

[3] When we go to show that our object has a given property, this is where our cleverness can come in / we can pull in other theorems or results or tricks; but our first step is **always** to think about the definitions.

- Set N to that "big enough" value.
- Then, for any $\epsilon > 0$, we have that if n, m are bigger than N, they are "big enough" so that $|a_n - a_m| < \epsilon$. So we're Cauchy!

Example. The sequence $\{a_n\}_{n=1}^{\infty}$, where each $a_n = \frac{1}{n}$, is Cauchy.

Proof. We proceed by the skeleton above. Take any $\epsilon > 0$. Our goal is to find out conditions on n, m such that if they are "large enough," then the expression

$$\left|\frac{1}{n} - \frac{1}{m}\right| < \epsilon$$

holds.

To do this, think about how we typically deal with inequalities! Instead of directly working with the LHS and RHS and showing that one is greater than the other, a typically more productive approach is to **approximate** one side by something simpler! In particular, for the inequality above, suppose that we could replace $\left|\frac{1}{n} - \frac{1}{m}\right|$ with something **larger**[4], but still less than ϵ. Then, logically, we would know that

$$\begin{gathered}(\text{larger thing}) < \epsilon \\ \Rightarrow \left|\frac{1}{n} - \frac{1}{m}\right| < \epsilon,\end{gathered}$$

and therefore that we would have our desired claim!

So: what's larger than $\left|\frac{1}{n} - \frac{1}{m}\right|$? Well, lots of things. Most of them aren't too useful to us, though: i.e. while $\left|\frac{1}{n} - \frac{1}{m}\right| \leq 2$, that 2 isn't going to be less than our arbitrary ϵ. A better question, then: what's larger than $\left|\frac{1}{n} - \frac{1}{m}\right|$ that's still small (or if you prefer, goes to 0 as n, m go to infinity?)

There are many good answers! The one we use here is the triangle inequality, which tells us that for any x, y, we have $|x - y| \leq |x| + |y|$, and therefore that

$$\left|\frac{1}{n} - \frac{1}{m}\right| \leq \frac{1}{n} + \frac{1}{m}.$$

Better! However, we don't necessarily get to pick n, m : we just get to pick N such that $N < n, m$. So it's going to make our lives easier if we can get N in here as well. But this is easy! Just notice that because $N < n, m$, we have

$$\left|\frac{1}{n} - \frac{1}{m}\right| \leq \frac{1}{n} + \frac{1}{m} < \frac{1}{N} + \frac{1}{N} = \frac{2}{N}.$$

[4]When doing this trick, always make sure that your logic is in the right order. A common mistake that I see students make in their first year is replacing the smaller side of an inequality with something even smaller, and then claiming that this proves their original inequality! This clearly doesn't work: i.e. if x, y are positive integers, you can't prove that $x < y$ by showing that $0 < y$. As always: when you're done with a proof, read it through! Ask yourself if every juncture makes sense! Find friends and ask them to proofread your proofs!

Therefore, we can solve our original problem by solving the following much easier one: given an arbitrary $\epsilon > 0$, can we find a value of N such that

$$\frac{2}{N} < \epsilon?$$

The answer is yes: set $N > \frac{2}{\epsilon}$! This expression is equivalent to the one above, and thus proves that claim.

In total, what have we shown? Well: for any $\epsilon > 0$, we've shown that if we choose $N > \frac{2}{\epsilon}$, we will have for any $n, m > N$,

$$\left| \frac{1}{n} - \frac{1}{m} \right| \leq \frac{2}{N} < \epsilon.$$

So our sequence is Cauchy! $\square$