Saul Youssef
Boston University
2013

Numbers

Let's define the natural numbers

$$0, 1, 2, 3, 4, \ldots$$

to be the isomorphism classes of finite sets in the category of finite sets. If we do that, the categorical product and sum lets us define

$$2 \times 6 \cong 12$$

$$2 \oplus 6 \cong 8 \quad \ldots \text{etc.}$$

$\mathbb{N}$ is thus a commutative monoid with both $\times$ and $\oplus$ ("+" from now on). You can also check that in the category of finite sets, we have

$$A \times (B \oplus C) \cong (A \times B) \oplus (A \times C)$$

so that $a \cdot (b+c) = a \cdot b + a \cdot c$ in $\mathbb{N}$.

$\mathbb{N}$ is, thus, ~~an~~ a rng, meaning a ring without inverses.

Q: What other rngs and/or rings can we construct starting with $\mathbb{N}$?

- Try $\mathbb{N} \times \mathbb{N}$ with component-wise addition and multiplication

$$(a, b) + (a', b') \equiv (a + a', b + b')$$

$$(a, b) \cdot (a', b') \equiv (a \cdot a', b \cdot b')$$

Check that

(a) $+$ is a commutative monoid ✓

(b) $\cdot$ makes a commutative monoid also ✓

(c) The distributive law works:

$$(a,b) \cdot ((a', b') + (a'', b''))$$
$$\stackrel{?}{=} (a,b) \cdot (a', b') + (a, b) \cdot (a'', b'') \quad ✓$$

Thus, $(\mathbb{N} \times \mathbb{N}, +, \cdot)$ is a rng also.

OK. Now let's try some quotients...

- In $\mathbb{N} \times \mathbb{N}$ again, try

$$(a, b) \, E \, (a+x, b+x) \quad \text{for all } x \in \mathbb{N}.$$

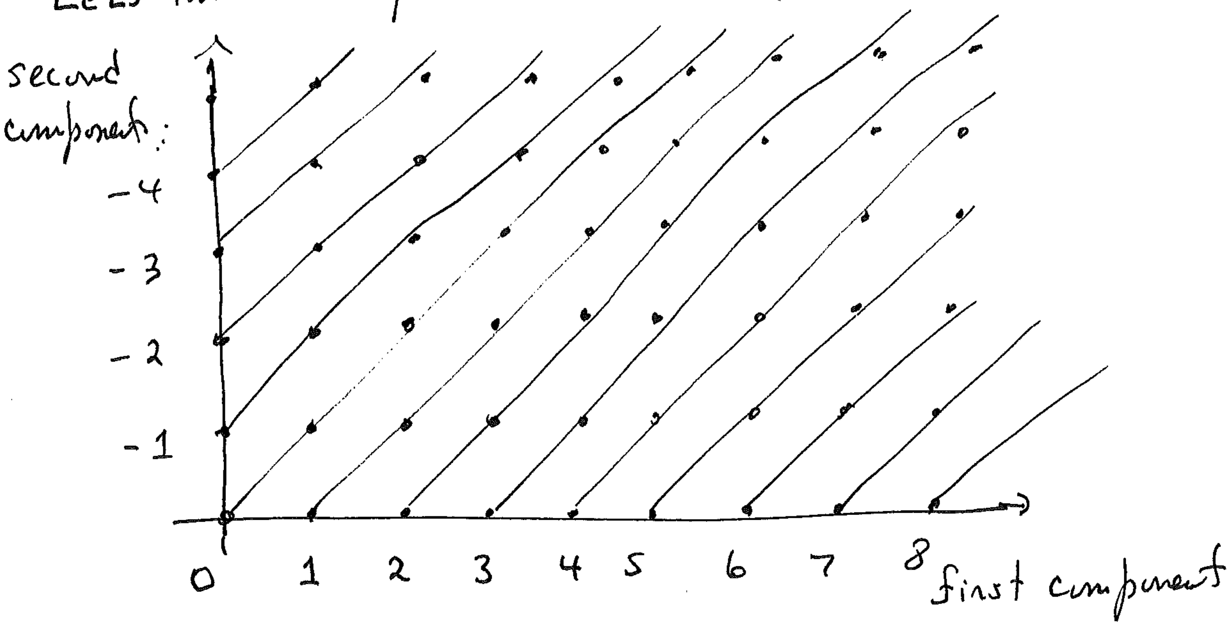
Define a sum and product on $\mathbb{N} \times \mathbb{N} / E$.

$$[a, b] + [a', b'] \equiv [a+a', b+b'] \quad \checkmark \text{ OK}$$

$$[a, b] \cdot [a', b'] \equiv [aa', bb'] \; \times \leftarrow \text{doesn't work anymore}$$

$$[a, b] \cdot [a', b'] \equiv [aa' + bb', ab' + ba'] \quad \checkmark \text{ OK!}$$

Let's make a picture of the equivalence classes



<u>Notation</u> $\quad [3,0] + [0,3] = [3,3] = [0,0]$

$$\text{"}3\text{"} + \text{"}-3\text{"} = \text{"}0\text{"}$$

We have invented <u>the integers</u> $\mathbb{Z} \equiv \mathbb{N} \times \mathbb{N} / E$.

This is a <u>ring</u> not just a rig.

Try the same idea with $\cdot$ instead of $+$:

- In $\mathbb{N} \times \mathbb{N}$, let

$$(a,b) \mathrel{E} (a \cdot x, b \cdot x) \quad \text{for all } x \neq 0.$$

We're excluding $x = 0$, otherwise we get one giant useless equivalence class.

$$[a,b] \cdot [a', b'] \equiv [a \cdot a', b \cdot b'] \checkmark$$ Easy this time

$$[a,b] + [a', b'] \equiv [a + a', b + b'] \times$$ doesn't work

$$[a,b] + [a', b'] \equiv [ab' + ba', bb'] \checkmark$$ OK!

Check distributivity:

$$[a_1, b_1] \cdot ([a_2, b_2] + [a_3, b_3])$$

$$= [a_1, b_1] \cdot [a_2 b_3 + b_2 a_3, b_2 b_3]$$

$$= [a_1 a_2 b_3 + a_1 b_2 a_3, b_1 b_2 b_3] \stackrel{?}{=}$$

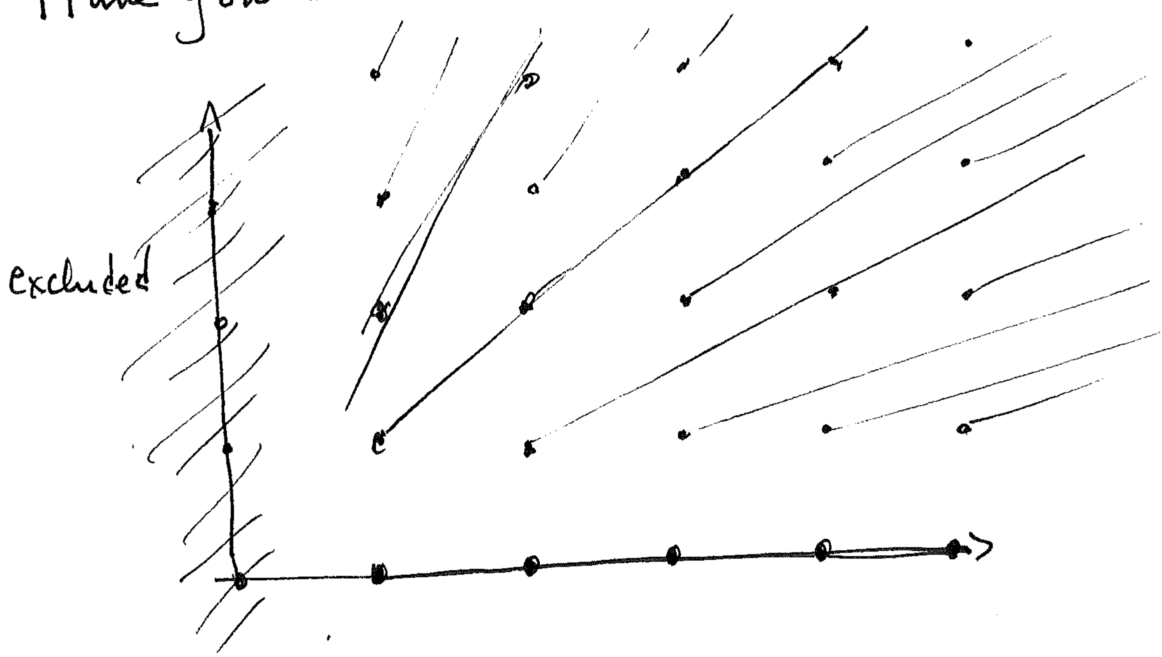
$$[a_1 a_2, b_1 b_2] + [a_1 a_3, b_1 b_3]$$

$$= [a_1 a_2 b_1 b_3 + b_1 b_2 a_1 a_3, b_1 b_2 b_1 b_3]$$

This works, but only if $b_1 \neq 0$. $\Rightarrow$ we can ~~remove~~ exclude points with the second component $= 0$.

$$\mathbb{N} \times (\mathbb{N} - \{0\}) / E \quad \text{is an rng.}$$

Have you seen $\mathbb{N} \times (\mathbb{N} - \{0\}) / E$ before?



Notation: $[a, b] \equiv \frac{a}{b}$

Yes! We have invented the rational numbers

$\mathbb{Q} \equiv \mathbb{N} \times (\mathbb{N} - \{0\}) / E$.

Besides being a ring, $\mathbb{Q}$ has a new property:

Every nonzero $q \in \mathbb{Q}$ has a multiplicative inverse.

Proof: Let $q = [a, b]$ be nonzero. $\Rightarrow a \neq 0$

$\Rightarrow [a, b] \cdot [b, a] = [ab, ba] = [1, 1] = 1$.

def: Redefine $\mathbb{Q} \equiv \mathbb{Z} \times (\mathbb{Z} - \{0\}) / E$ as the same thing works. $\mathbb{Q}$ is then a ring.

def: A commutative ring where every nonzero element has a multiplicative inverse is called a field.

Remember from the group theory homework that $\mathbb{Z}_6 \equiv \mathbb{Z}/6\cdot\mathbb{Z}$ is a group. You can easily check that $\mathbb{Z}_6$ is also a ring with

$$(a + 6\mathbb{Z})\cdot(b + 6\mathbb{Z}) \equiv (a\cdot b + 6\mathbb{Z}).$$

More generally, $\mathbb{Z}_n$ are rings for all $n \geq 0$.

<u>Extra</u>: $\mathbb{Z}_p$ is a field if p is prime.

<u>Proof</u>: Given any nonzero $x \in \mathbb{Z}_p$, the sequence $x, x^2, x^3, \dots$ must repeat and so $x^m = x^n$ for some $m < n$. $\Rightarrow$ $x^m(1 - x^{n-m}) = 0$. Since $\mathbb{Z}_p$ is an integral domain, one of these two factors must be zero. x^m cannot be zero because p is prime. $\Rightarrow$ $1 = x^{n-m} = x\cdot(x^{n-m-1})$ $\Rightarrow$ x has a multiplicative inverse $\Rightarrow$ $\mathbb{Z}_p$ is a field.

Can we make rings from sequences in $\mathbb{Z}$?

- For infinite sequences of integers, you can just add and multiply component-wise to get a new ring.
- Strangely enough, if you consider "ultimately zero" sequences such as

$$6 \quad 0 \quad -4 \quad 7 \quad 4 \quad 0 \quad 0 \quad 0 \ldots$$

$$2 \quad -1 \quad 0 \quad 5 \quad 0 \quad 0 \quad 0 \quad 0 \ldots$$

there is a new, second way to multiply. Let

$n \equiv n_0, n_1, n_2, \ldots$ ultimately zero

$m \equiv m_0, m_1, m_2, \ldots$ ultimately zero

$$(n+m)_k \equiv n_k + m_k$$

$$(n * m)_k \equiv \sum_{i+j=k}' n_i m_j \qquad \text{"convolution product".}$$

This is also a ring which is already known to you:

<u>Notation</u>: $2 \quad -1 \quad 0 \quad 5 \quad 0 \quad 0 \quad 0 \ldots$

" $2 - 1 \cdot x + 5x^3$ "

These are <u>polynomials</u> " $\mathbb{Z}[x]$ ".

It's pretty clear that the same thing works in any ring, so, for example, ultimately zero sequences of rationals gives us the polynomial ring $\mathbb{Q}[x]$ with rational coefficients.

Let's look at infinite sequences of rationals

$$r = r_0, r_1, r_2, \ldots$$

that "settle down":

<u>def</u>: r <u>settles down</u> if $|r_i - r_j|$ remains below any chosen $\epsilon > 0$ for all i, j greater than some N.

<u>def</u>: r <u>settles down to $q \in \mathbb{Q}$</u> if $|r_i - q|$ remains below any chosen $\epsilon > 0$ for all i greater than some N.

It's easy to check that with

$$(r+s)_i \equiv r_i + s_i$$

$$(r \cdot s)_i \equiv r_i \cdot s_i,$$

rational sequences that settle down [Settling $(\mathbb{Q})$] are a ring [to check $r \cdot s$, it helps to notice that settling sequences are bounded].

<u>def</u>: A rational sequence is <u>insignificant</u> if it settles down to 0.

It's easy to see that the subset of insignificant sequences is a subring of Settling($\mathbb{Q}$) and, further, that $\epsilon \cdot r$ is insignificant for any $r \in$ Settling($\mathbb{Q}$).

Using this, it is easy to check that

$$r E s \iff r - s \text{ is insignificant}$$

is an equivalence relation and

$$[r] + [s] \equiv [r+s]$$

$$[r] \cdot [s] \equiv [r \cdot s]$$

makes Settling($\mathbb{Q}$)/E into a ring.

<u>Terminology</u>:

r "settles down" $\longleftrightarrow$ r is a <u>Cauchy sequence</u>

r "settles down to q" $\longleftrightarrow$ $\underline{\lim_{n\to\infty} r_n = q}$

insignificant sequences $\longrightarrow$ An "ideal" in Settling($\mathbb{Q}$) [analogous to a normal subgroup in group theory]

Settling($\mathbb{Q}$)/E $\longleftrightarrow$ $\mathbb{R}$, the <u>real numbers</u>.

Example :

$$3.1415926\ldots$$

$$\equiv [3, 3.1, 3.14, 3.141, 3.1415, \ldots].$$

From our quotient, we have

$$0.9999\ldots = 1.000\ldots$$

since their difference is insignificant.

When we were looking at $\mathbb{N} \times \mathbb{N}$ (or $\mathbb{Z} \times \mathbb{Z}$) before, we actually had some options that we didn't try:

$\underline{\mathbb{Z} \times \mathbb{Z}}$

$$(a, b) + (a', b') \equiv (a + a', b + b')$$

$$(a, b) \cdot (a', b') \equiv (aa' - bb', ab' + ba')$$

This also works, making a ring called the <u>Gaussian integers</u>.

Notation: $(a, b) \Leftrightarrow a + ib$

- If you do the same thing starting with $\mathbb{R} \times \mathbb{R}$, you get $\mathbb{C}$, the field of <u>complex numbers</u>.

The "Cayley-Dickson" construction

This works for a not-necessarily commutative ring with a linear involution "$*$" satisfying

$$(a+b)^* = a^* + b^*$$

$$a^{**} = a$$

$$(a\,b)^* = b^* a^*$$

Given that, define a new algebra on pairs as

$$(a_1, b_1) + (a_2, b_2) \equiv (a_1 + a_2,\ b_1 + b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) \equiv (a_1 a_2 - b_2 b_1^*,\ a_1^* b_2 + a_2 b_1)$$

$$(a, b)^* \equiv (a^*, -b)$$

Starting with the reals with $a^* \equiv a$, this gives the complex numbers ~~as~~ as we had them before.

$\mathbb{R} \overset{c.n.}{\Longrightarrow} \mathbb{C}$

As before.

$\mathbb{C} \overset{c.n}{\Longrightarrow} \mathbb{H}$

Gives the quaternions represented as pair of complex numbers. Note that $\mathbb{H}$ is no longer commutative.

$\mathbb{H} \overset{c.n}{\Longrightarrow} \mathbb{O}$

Gives the octonions represented as pair of quaternions. Note that $\mathbb{O}$ is no longer even associative.

You can keep going, but this gets into unknown territory, at least for me.

The category of Finite Sets

$\downarrow$ isomorphism classes

$\mathbb{N}$

$\downarrow$

$\mathbb{N} \times \mathbb{N}$

$\downarrow$ $(a,b) E (a+x, b+x)$

$\mathbb{Z} \longrightarrow$ ∞ sequences

$\mathbb{Z} \longrightarrow$ ultimately zero sequences : $\mathbb{Z}[x]$

$\mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z} \longrightarrow$ Gaussian integers

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$

$\mathbb{Z} \longrightarrow \mathbb{Z}_n$

$\mathbb{Z} \longrightarrow \mathbb{Z} \times (\mathbb{Z} - \{0\})$

$\downarrow$ $(a,b) E (a\cdot x, b \cdot x)$ $x \neq 0$

$\mathbb{Q} \longrightarrow$ ∞ sequences

$\mathbb{Q} \longrightarrow$ ultimately zero sequences : $\mathbb{Q}[x]$

$\mathbb{Q} \longrightarrow$ Cauchy sequences

$\downarrow$ $r E s$ if $r - s$ is insignificant

$\mathbb{R}$

$\mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R} \xrightarrow{C.D.} \mathbb{C} \xrightarrow{C.D.} \mathbb{H} \xrightarrow{C.D.} \mathbb{O} \xrightarrow{C.D.}$?

?

?

?