Slawomir Chodnicki Follow
Jan 2, 2020 · 11 min read ★ · Listen

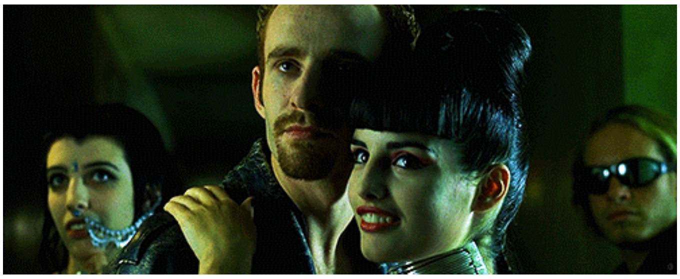
Why a·0=0 and Other Proofs of "the Obvious"

How "obvious" becomes "interesting" when we go back to first principles.

Let's find out what we can prove about real numbers starting from humble beginnings. We're going to prove a couple of things you may not think of as even needing a proof, such as `a·0=0`

Constructing proofs from simple premises, we'll learn something about the structure of numbers, and why things are the way they are. If that sounds interesting to you, grab a hot beverage and join me.

It's going to be fun. I promise.



Let's follow the white rabbit.

The truths we start with

Everything accepted as true must follow from axioms and definitions. Our axioms effectively establish that our numbers form a Field. Let's go.

Addition

Addition is our most familiar operation. The axioms establish some basic properties.

$$
\begin{array}{rcr}
\forall a, b, c \in \mathbb{R}: & (a+b)+c = a+(b+c) & \text{A1} \\
\exists 0 \in \mathbb{R}\ \forall a \in \mathbb{R}: & a+0 = a & \text{A2} \\
\forall a \in \mathbb{R}\ \exists (-a) \in \mathbb{R}: & a+(-a) = 0 & \text{A3} \\
\forall a, b \in \mathbb{R}: & a+b = b+a & \text{A4}
\end{array}
$$

A1 tells us addition is associative: evaluation order of sums does not matter.

A2 ensures us there is a neutral element with regards to addition. We call that element 0. When adding 0 to something, nothing changes.

A3 ensures that every number 'a' has an additive inverse that we call '-a'. When a number and its inverse are added together, we get 0.

A4 tells us addition is commutative: we're allowed to swap a and b when summing them up, and the result is the same.

> *Note that we have not defined any notion of subtraction. As far as we're concerned subtracting a number means adding the additive inverse of that number.*

Multiplication

Multiplication looks remarkably similar to addition with regard to its formal properties. Let's dig into it.

> *About notation:*
> *— we're often omitting the multiplication dot*
> *— we're using `1/a` and `a^-1` interchangeably*
> *— `a/b` means `a(1/b)`*

Let's look at our axioms:

$$
\begin{array}{rcr}
\forall a, b, c \in \mathbb{R}: & (ab)c = a(bc) & \text{A5} \\
\exists 1 \in \mathbb{R}\ 1 \neq 0\ \forall a \in \mathbb{R}: & 1 \cdot a = a & \text{A6} \\
\forall a \in \mathbb{R} \setminus \{0\}\ \exists a^{-1} \in \mathbb{R}: & a \cdot a^{-1} = 1 & \text{A7} \\
\forall a, b \in \mathbb{R}: & ab = ba & \text{A8}
\end{array}
$$

A5 tells us multiplication is associative: the evaluation order of products does not matter.

A6 ensures there is a neutral element with regards to multiplication. We call that element 1. When multiplying something with 1, nothing changes.

Note that the axiom explicitly states 1≠0. So at least two distinct elements 1 and 0 are guaranteed to exist.

A7 ensures every number except 0 has a multiplicative inverse that we call a^(-1) or 1/a. When any number and its multiplicative inverse are multiplied together, we get 1.

A8 tells us multiplication is commutative: we’re allowed to swap a and b when multiplying, and the result is the same.

> *Note that we have not defined any notion of division. As far as we’re concerned dividing by a number means multiplying by the multiplicative inverse of that number. Every number except zero is guaranteed to have an inverse, so we’re good.*

How Addition and Multiplication are related

$$\forall a, b, c \in \mathbb{R}: \qquad a(b+c) = ab + ac \qquad \text{A9}$$

A9 tells us that multiplication distributes over addition. The product of a sum is the sum of the products.

Warming up

Now that we have something to work with, let’s flex our reasoning muscles. This is where we’re asked to “prove the obvious”, and it’s not necessarily always clear how to go about this.

Let’s go.

Zero and One are unique

The first task is to prove that there are no other neutral elements with respect to addition and multiplication.

What does that mean? It means there can’t be another number that happens to be neutral with respect to addition and multiplication. If an element has that property, it must be 0 or 1 respectively.

Turns out that is a consequence of commutativity. Let’s assume some number E is neutral with regards to addition.

$$\begin{aligned} E + 0 &= E && \text{(i - 0 neutral)} \\ 0 + E &= 0 && \text{(ii - E neutral)} \\ E + 0 &= 0 + E && \text{(A4)} \\ E &= 0 && \text{(per i and ii)} \end{aligned}$$

Turns out if an element is neutral, it’s got to be 0. We can’t be commutative otherwise.

The exact same reasoning applies to products. Let’s assume some number E is neutral with regards to multiplication.

$$
\begin{aligned}
E \cdot 1 &= E && \text{(i - 1 neutral)}\\
1 \cdot E &= 1 && \text{(ii - E neutral)}\\
E \cdot 1 &= 1 \cdot E && \text{(A8)}\\
E &= 1 && \text{(per i and ii)}
\end{aligned}
$$

Again, if an element is neutral, it’s got to be 1. Commutativity demands it.

Inverses are unique

Next, we’ll establish that additive and multiplicative inverses are unique.

That is to say, if I have a number **a** there’s only one **-a** that is the additive inverse. Similarly, if I have a number **a** — with the exception of 0 — there is only one **1/a** that is the multiplicative inverse.

The axioms guarantee that inverses exist. They don’t tell us that there’s exactly one inverse per number.

> *Why is that important? Say you want to solve* `a + x = b` *for x and you say: I add* `-a` *on both sides. So far it’s not clear that* `-a` *is uniquely determined, so you’d have to worry about which one to pick and whether the solution for x turns out to be different depending on your choice.*

Let’s assume we have a number V that is the additive inverse of a, that is `a + V = 0`

$$
\begin{aligned}
a - a &= 0 && \mid +V\\
V + a - a &= V\\
-a &= V && \text{(V + a = 0)}
\end{aligned}
$$

Turns out that we need associativity to prove this fact. Associativity looks like an innocent and quaint condition in our definitions. But make no mistake, it is imposing remarkable structural properties on our numbers.

Since multiplication is associative as well, the proof for multiplication is exactly the same. Let’s look at a number V that is the multiplicative inverse of a, that is `Va = 1`

$$
\begin{aligned}
aa^{-1} &= 1 && \mid \cdot V\\
Vaa^{-1} &= V\\
a^{-1} &= V && \text{(Va = 1)}
\end{aligned}
$$

Now we have established that every number has exactly one unique corresponding inverse. We can confidently speak of *the* number -x or 1/x as opposed to just some -x or 1/x.

Rules for sums

Let’s look at some things we can prove about addition.

The unknown in a+x=b has a unique solution

One “obvious” thing to prove about addition is that when you know the sum and one of the numbers going into it, you can tell what the other number was.

Let’s contrast that with another operation involving two arguments that doesn’t have this property: exponentiation. Say we know $x^4 = 16$. What’s x? Could be 2, could be -2. Can’t be sure. Addition does not have that uncertainty. If we know the result and one operand, we can establish what the other operand was.

Let’s assume a and b as fixed, and x is unknown. We’re proving that `a + x = b` has a unique solution for x.

$$\begin{aligned} a + x &= b && \mid -a \\ a - a + x &= b - a \\ x &= b - a && \text{(A3)} \end{aligned}$$

Adding our — uniquely determined — `-a` on both sides gives us a solution for x, the number: `b+(-a)`.

-(-a) = a

Our next “obvious” thing to prove is that inverting an inverted number gives us back the original: `-(-a) = a`

All we know about `-(-a)` is its defining property: being the inverse of `-a`. Let’s begin with that.

$$\begin{aligned} -a + (-(-a)) &= 0 && \mid +a \\ a - a + (-(-a)) &= a \\ -(-a) &= a && \text{(a - a = 0)} \end{aligned}$$

Associativity is enough to prove our case. Associativity not only establishes inverses as uniquely determined, but it also establishes symmetry between them. Nice.

`(-a) + (-b) = -(a+b)`

The next thing on the list is proving that the sum of inverses is the inverse of the sum. In symbols: `(-a) + (-b) = -(a+b)`

Let’s start with what we know: `a+b` and its inverse `-(a+b)` add up to `0`

$$\begin{aligned} a+b-(a+b) &= 0 && \mid -a \\ -a+a+b-(a+b) &= -a \\ b-(a+b) &= -a && \mid -b && (\text{-a + a} = 0) \\ -b+b-(a+b) &= (-a)+(-b) \\ -(a+b) &= (-a)+(-b) && && (\text{-b + b} = 0) \end{aligned}$$

Let’s leave addition, and focus on multiplication instead.

Rules for Products

Everything we’ve proven about sums and additive inverses applies to products and multiplicative inverses. The only interesting difference is that the axioms don’t guarantee the existence of a multiplicative inverse for 0. Whenever we’re using 1/a, we assume a ≠ 0.

Let’s run through the proofs quickly. They are entirely symmetrical to the cases for addition.

The unknown in ax=b has a unique solution

For any a ≠ 0 `ax = b` has a unique solution for x. Similar to a sum, where we had to add the additive inverse of a, now we multiply with the multiplicative inverse of a.

$$\begin{aligned} a \cdot x &= b && \mid \cdot a^{-1} \quad a \neq 0 \\ a^{-1}a \cdot x &= ba^{-1} \\ x &= ba^{-1} && && \text{(A7)} \end{aligned}$$

1/(1/a) = a

We want to show that `1/(1/a) = a:` the inverse of a multiplicative inverse is the original. As always with multiplicative inverses: a≠0. Let’s look for the multiplicative inverse of `1/a`. All we know about it is that when multiplied with `1/a` we get `1`.

$$\begin{aligned} a^{-1} \cdot a^{-1^{-1}} &= 1 && \mid \cdot a \quad a \neq 0 \\ aa^{-1} \cdot a^{-1^{-1}} &= a \\ a^{-1^{-1}} &= a && && (aa^{-1} = 1) \end{aligned}$$

`1/a · 1/b = 1/ab`

Multiplying inverses gives the inverse of their product. We want to show that `1/a · 1/b = 1/ab` . As always when taking multiplicative inverses: a≠0 and b≠0.

Let’s start with `ab` and its inverse.

$$\begin{aligned} ab \cdot (ab)^{-1} &= 1 && \mid \cdot a^{-1} \\ a^{-1}ab \cdot (ab)^{-1} &= a^{-1} \\ b \cdot (ab)^{-}1 &= a^{-1} && \mid \cdot b^{-1} && (a^{-1}a = 1) \\ b^{-1}b \cdot (ab)^{-1} &= a^{-1}b^{-1} \\ (ab)^{-1} &= a^{-1}b^{-1} && && (b^{-1}b = 1) \end{aligned}$$

Linking sums and products

Our rule about the distributive properties of products across sums implies some interesting propositions.

There’s some interplay between 0 — the neutral element of *addition* — and multiplication. Also, -1 — which is the *additive* inverse of 1 — has an interesting relationship with multiplication.

Let’s dig into it.

Multiplying by zero produces zero

This is an interesting proposition because 0 has been introduced as an element with properties with regards to *addition*. The rules for multiplication mention it only insofar as to not guarantee the existence of a multiplicative inverse.

Proving anything about multiplication with 0 will probably include the distributive law. Let’s rewrite `a·0` using the distributive law, and see what happens. Let’s look at `a(0+0)`

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0) \\ a \cdot 0 &= a \cdot 0 + a \cdot 0 && \mid -(a \cdot 0) && \text{(A9)} \\ 0 &= a \cdot 0 \end{aligned}$$

Turns out the distributive law makes it necessary that multiplication by 0 produces 0. This is also why 0 can’t have a multiplicative inverse. Multiplying that inverse with 0 would be 1 by definition, not 0.

Suppose for a moment there was some number v such that `v·0 = 1` . It would be in contradiction to the distributive law, and lead to things such as:

```
1 = v·0 = v(0+0) = v·0+v·0 = 1+1
```

Any number multiplied by 0 must be 0 or we have to ditch the distributive law. But we‘re keeping it. It’s good. We just recognize that the multiplicative inverse of 0 does not exist. There is no way to divide by 0 and still be consistent with our axioms. Simple as that. Moving on.

`a(-b) = -(ab)`

Multiplying by an additive inverse gives the additive inverse of the product.

This rule also concerns both: inverses of *addition* and how *multiplication* operates on them. Again, the distributive law must have something to do with it. It’s the only law tying addition and multiplication together.

Let’s start with what we just found. Multiplying by 0 gives 0, but this time we use an additive inverse to form a zero-sum. Let’s look at `a(b-b) = 0`

$$
\begin{aligned}
a(b-b) &= 0 \\
ab + a(-b) &= 0 && \mid -(ab) && \text{(A9)} \\
a(-b) &= -(ab)
\end{aligned}
$$

`a·(-1) = -a`

Look at our results in the previous section. If we pick 1 for b, we get `a·(-1) = -(a·1) = -a` . to form an additive inverse, we can just multiply by -1. Who would have thought? Let’s keep that in mind for the next section.

`(-a)(-b) = ab`

Multiplying additive inverses is equal to the product of the original numbers.

We’re about to find out why a negative times a negative is a positive. I remember 12-year old me being utterly confused by these things. Let’s get to the bottom of this.

Let’s start with what we learned in the previous section: `a(-b) = -(ab)`

$$
\begin{aligned}
a(-b) &= -(ab) && \mid \cdot (-1) \\
(-1)a(-b) &= (-1)(-ab) \\
(-a)(-b) &= ab && (-1 \cdot a = -a)
\end{aligned}
$$

We’re using the fact that multiplying by -1 produces the additive inverse of a number.

Would 12-year old me have understood that multiplying by a negative effectively mirrors the result across zero to the other side of the axis? And doing it twice gets you to where you started from? Not sure. I wish I was 12 again, so I could think about it.

If a product is zero, at least one of the factors is zero

In symbols: `ab = 0 => a=0 v b=0`. When we encounter a product that is zero, we can conclude that at least one of the factors is zero. We've already established the other direction: multiplying by zero always produces zero.

Now the question is whether there is any way we can multiply two non-zero numbers, and still arrive at zero. Let's see where we end up when we assume such a thing is possible: Let's assume ab = 0 and a≠0 and b≠0.

$$
\begin{aligned}
ab &= 0 && \quad \mid \cdot a^{-1} \cdot b^{-1} \quad a \neq 0, b \neq 0 \\
a^{-1}b^{-1}ab &= 0 \\
(a^{-1}a)(b^{-1}b) &= 0 \\
1 \cdot 1 &= 0 \\
1 &= 0
\end{aligned}
$$

Ups, we're in trouble. Our axiom A6 explicitly says 1≠0. Our assumption that there is a product of 0 where both factors are non-zero leads to a contradiction. The opposite must be true. When a product is 0, at least one factor is necessarily 0.

The arithmetic of fractions

Let's recognize that a fraction like `2/3` is just a shorthand notation for `2·(1/3)`. Numerator times multiplicative inverse of the denominator. Let's see if we can derive the rules of faction arithmetic from this alone.

Adding fractions

Remember how fraction addition works? What's `2/3 + 4/5`? We expand the fractions to a common denominator, then add the numerators. For our example we get something like this: `(2·5 + 4·3)/(3·5) = 22/15`

Let's see what happens when we work solely from our premises, defining fractions `a/b` as `a(1/b)` with `b≠0`.

$$
\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= ab^{-1} + cd^{-1} && \qquad b \neq 0, d \neq 0 \\
&= (ab^{-1} + cd^{-1})(bd)(bd)^{-1} && \qquad (bd)^{-1}(bd) = 1 \\
&= (ab^{-1}bd + cd^{-1}bd)(bd)^{-1} \\
&= (ad + cb)(bd)^{-1} \\
&= \frac{ad + cb}{bd}
\end{aligned}
$$

That looks remarkably like our example

$$\frac{2}{3}+\frac{4}{5}=\frac{2\cdot 5+4\cdot 3}{3\cdot 5}=\frac{22}{15}$$

The formula for adding fractions emerges almost by definition alone. We perform fraction expansion as multiplication with 1 in the form of `(bd)/(bd)`, and we're done.

Multiplying fractions

How about `2/3 · 4/5` ? That's `(2·4)/(3·5) = 8/15` right? Let's see if we can get that from our definitions.

$$\begin{aligned}\frac{a}{b}\cdot\frac{c}{d} &= ab^{-1}\cdot cd^{-1} \quad b\neq 0, d\neq 0\\ &= ac\cdot b^{-1}d^{-1}\\ &= ac\cdot (bd)^{-1}\\ &= \frac{ac}{bd}\end{aligned}$$

The only thing that we did, was to rearrange the factors and reapply our definition for fraction notation.

Dividing fractions

OK, how about `(2/3)/(4/5)` ? That's `(2·5)/(3·4) = 10/12 = 5/6` right? Remember, dividing by something is to multiply with its inverse. Let's see where we end up:

$$\begin{aligned}\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\cdot(\frac{c}{d})^{-1} &= ab^{-1}\cdot(cd^{-1})^{-1} \quad b\neq 0, d\neq 0\\ &= ab^{-1}\cdot c^{-1}(d^{-1})^{-1}\\ &= ab^{-1}\cdot c^{-1}d\\ &= ad\cdot(bc)^{-1}\\ &= \frac{ad}{bc}\end{aligned}$$

We arrive at the conventional formula for dividing fractions.

So what did we gain through abstraction?

We've found out a lot about real numbers by looking at their structure. It's interesting that we haven’t even gotten to what makes real numbers unique: we’ve used only properties that all Field structures have in common.

Rational numbers, Real numbers, Complex numbers, all of them share this structure. The propositions we’ve proven today apply to all of them.

Take Complex numbers for example. We know they’re weird in their multiplications, right? They allow square roots of negative numbers like `i=sqrt(-1)`. However: you don’t have to wonder whether there are non-zero complex numbers that multiplied together result in zero. We’ve proven that it’s not the case for Field structures, and once you know that Complex numbers are a Field structure -by verifying that the axioms hold- you can immediately use all of our deductions.

That’s neat, isn’t it?

Can we please stop fetishising Warren Buffett?

Just because he’s frugal, it doesn’t mean he’s anything like you — If there’s one person that self help and success writers love to use for fodder, it’s Warren Buffett. How could it not be? That humble, kindly looking old ma…

Work 5 min read

Haixun Wang · Jan 2, 2020 ★

The Data Science Behind the Man Who Solved the Market

My holiday reading this year was Gregory Zuckerman’s The Man Who Solved the Market, which I finished in one long sitting on Christmas Eve. …

Machine Learning 10 min read

11 Kalli · Jan 2, 2020 ★

Increase Your Productivity This Year

Reduce social media use and stop Netflix binge-watching — With the Western New Year, I keep thinking about two of the most important things I need to do if I really want to achieve my yearly goals and create greater…

Productivity 6 min read

Ben Scheer · Jan 2, 2020 ★

Answer These 8 Questions Before Your Next Interview

Shape your stories and make them shine. — When it comes down to it, interviewing is like storytelling. In fact, interviews are essentially conversations through which people share ideas, passions, and…

Startup 11 min read

Read more from The Startup

Recommended from Medium

Maximilian Rehn

We misunderstand math the same way we misunderstand religion

Is This Racist?

Math

dearC in Towards Data Science

Log Book — AdaBoost, the math behind the algorithm

Dino Cajic in Dev Genius

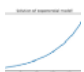
Maximum Independent Set Visually Explained

Michael Lennon in smucs

An Overview of the Graham Scan

Sanyukta Suman in The Startup

Design and Analysis of Firefly Response to the Stimulus



Mohammed Munir Ahmed

Hanoi’s Tower — Real Life Computer Science Lessons

Prateek Saini

Prime Numbers 1!