Building your own number systems for fun and profit

Felix Dilke

I’ve always liked mucking around with numbers and symbols

Number systems are useful workspaces for science and engineering, but they can also be imaginative playgrounds where we can discover and invent new stuff.

Particularly if you jump a level and try to build number systems of your own.

There is a long and proud tradition of this, and I’ll try to describe how my own adventures draw on it.

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

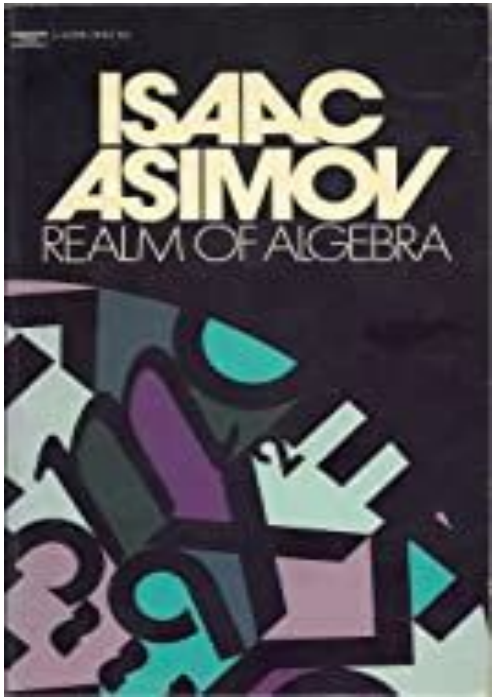
*	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

As a kid, I read lots of books about algebra

But especially, these ones:

The first touched my imagination by describing some of the impossibly romantic figures who have shaped this subject.

The second shows you how to construct your own number systems.



Impossibly Romantic Figure #1

Evariste Galois (1811-1832). Note the dates!

Galois created some amazing mathematics, and no doubt would have done more if he hadn't got involved in post-Napoleonic revolutionary politics, thereby turning his life into a deleted scene from The Three Musketeers. He was tricked into fighting a duel, and died in a ditch age 20. As it was, he still belongs in the subject's grand hall of fame.

This makes him pretty much the poster boy for "genius who tragically died young".

Galois pioneered the study of fields

A *field* is a four-function number system, i.e. a collection of values that admit the arithmetic operations +,-,*,/, subject to the usual rules.

Example: the real numbers

Example: the complex numbers

Non example: 2 x 2 matrices, because AB != BA and also you can't always divide.

Perhaps the first really intriguing example: integers modulo 5

Because 2 * 3 = 6 = 1 mod 5, and so ½ = 3 and ⅓ = 2. Also ¼ = 4.

I’ll just touch on the theory of *finite fields*

So a finite field is a pocket-sized four function number system with only finitely many elements… Like the integers mod 5, { 0, 1, 2, 3, 4 }.

If you can construct addition and multiplication tables that obey the rules, you too can create a finite field.

It turns out there is exactly one field of size q, for any number q that is a power of a prime number!

Among other things, these fields are great for constructing codes, particularly if q is a power of 2. They are also the starting point for all kinds of combinatorial and number-theoretic tricks.

Impossibly Romantic Figure #2

William Rowan Hamilton (1805-1865) - Royal Astronomer of Ireland

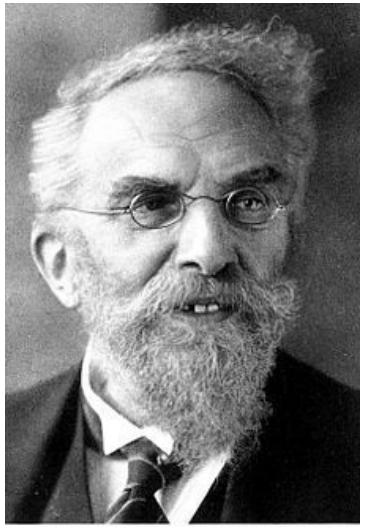
Became convinced that he could find a number system out there, just beyond the reals and complexes. This became a devouring obsession.

To concentrate on the problem, Hamilton locked himself in his study, where his long suffering wife would bring him plates of food. Often the furiously scribbling Hamilton would simply ignore these, and they would be found months later in a mummified state crushed under piles of manuscripts.

This apparently hopeless quest went on for years.

Finally came a Eureka moment when Hamilton was out walking by the river and discovered the quaternions, which are like a field but not commutative! (AB != BA). He immediately inscribed the equations for them on Broom Bridge in Dublin. (There's now a mini-monument on the spot).

Another field: the p-adic numbers (Kurt Hensel, 1897)



Real numbers generally look like this:

Pi = 3.1415926…

Let’s do that in bicimal (base 2 rather than 10):

Pi = 11.0010010000…

So they’re just rightward-infinite sequences of digits. Let’s instead consider leftward-infinite bicimal expressions:

Q = ...0000100100.11

These can be made into a field, with fairly straightforward definitions of +/-/*//. You can actually do this for any prime base, not just 2, and the resulting system is a warped number-theoretic playground which is sort of like the complex numbers, with its own concepts of limits, Taylor series and path integration.

So… I became interested in constructing fields

The real and complex numbers are of course indispensable as workspaces for physicists and engineers. But… what other fields are there?

It is not easy. You can't just write down a bunch of symbols and expect them to obey the rules of arithmetic.

Typically, division (/) is the hardest. Of course, before this can even be a possibility, you have to avoid situations where AB = 0 without A or B being 0.

Somehow, then, I ended up focusing on the following problem...

Let’s construct a field

Consider the set of sequences of real numbers:

r = (r0, r1, r2, …)

Obviously, we can add/subtract/multiply these, but not divide them.

Is it possible to *identify sequences* - i.e. find a ‘similarity relation’ **~**, such that if we consider sequences **r** and **s** “the same” whenever **r ~ s**, the resulting system is consistent, nontrivial, obeys all the rules of arithmetic, has division, and is a field?

Is it possible…?

YES

and this opened up a rabbit hole of unforeseen dimensions which I shall tell you about next time

To be continued

THANK YOU

Journey into Math, part 2

by Felix Dilke

a sequel to “Building your own number systems for fun and profit”

If that showed the fun side of math, this episode will show the uncanny, inhuman side of the subject… You have been warned.

The story so far: I ask an apparently question about constructing *fields* … that is, four-function number systems like the real numbers

It’s a field if: you can have a pocket calculator of it

Motivating question

Is it possible to ‘simplify’ (by identifying elements) the number system of real sequences,

r = (r_0, r_1, r_2, …)

so that it becomes a field, with four function arithmetic (+ - * /)? Yes.

Like this: Consider two sequences **r** and **s** “similar”, **r** ~ **s**, if:

for a majority of numbers *n*, r_n equals s_n.

You can see how this might work. Of course I have to say what a “majority” is.

By (more or less) routine calculation...

… this construction works and defines a field, with full-service four function arithmetic, PROVIDED we have a “system of majorities” (sets of integers) for which the following reasonable-sounding conditions on “majorities” are true:

The empty set is not a majority.

Any superset of a majority is a majority.

The intersection of two majorities is a majority.

For any set A, either A or its complement is a majority.

It’s possible, if not entirely straightforward, to find a “system of majorities” $\mathfrak{M}$ that does all this.

OK, we have a field. What is it like?

This is the field **R*** of *hyperreal numbers* (Abraham Robinson, ~ 1960)

It's basically a (very) big brother to the real number system **R**.

very big:

in that its size is a strictly larger level of infinity than **R**'s

brother:

in that it has very similar properties to R:

First order logic cannot tell them apart.

What can we do in this big “hyperreal” number field?

Among other things, it contains true infinitesimals (infinitely tiny values smaller than any positive real number).

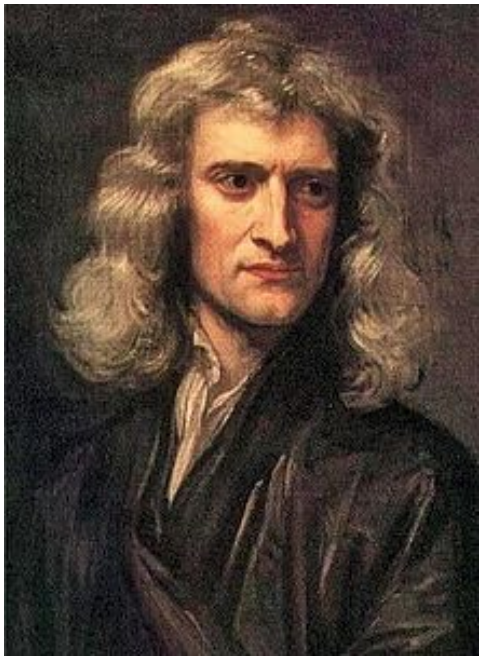
So this gives an alternate way to develop the differential calculus.

Newton’s original formulation of the calculus used infinitesimals, but he was never able to put this on a rigorous basis - that’s a polite way of saying that strictly speaking, and with all due respect to him, Sir Isaac was talking nonsense - and the theory had to be redeveloped later on more solid foundations. Now, at last, we can finally realize his true vision: Newton remastered.

This also leads to a whole new branch of math, “nonstandard analysis”.

So far, not a bad payoff from my apparently simple initial question.

But, we are just getting started - it gets deeper and darker yet...



Into the expanding rabbit hole

The construction is quite general. It doesn't just work with the real numbers. Given *any* field F, the same construction will give a big brother F* of F. (Curiously, it's no good with finite fields: F* = F in that case.)

It doesn't even have to be a field - everything still works with any reasonable algebraic/relational theory. So for a wide range of concepts of "widget" (graph / monoid / vector space / etc) we can take any widget **W** and produce a new big brother widget **W***.

Next, we don't have to use the same widget over and over in the sequence. We can take a sequence of possibly different widgets

W_1, W_2, …

and multiply them up (via the identification scheme) to produce a mega-widget W_𝔐, where I've written 𝔐 for the system of majorities.

What can we say about the mega-widget $W_{\mathfrak{M}}$?

Actually there's a theorem that describes its properties very precisely:

A statement ϕ of first order logic is true in $W_{\mathfrak{M}}$ if and only if it is true in W_n for a majority of indices n.

So this is a kind of genetic engineering of algebraic structures! Given a bunch of widgets which collectively almost have some property we want, we can use the construction to combine them into a mega-widget which ticks all the boxes.

It's almost as if W_1, W_2, … was a sequence converging to the limit $W_{\mathfrak{M}}$.

The story so far, then:

Suppose you are an ordinary hard-nosed mathematician studying the theory of widgets. Your quest is to construct the perfect widget.

You have a bunch of widgets W_1, W_2, … (they don't actually have to form a countable sequence) which approximate to having the property you want.

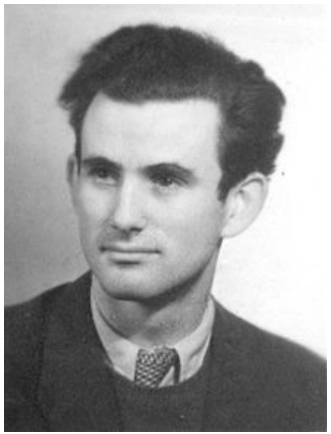
Subject to reasonable conditions, the "majoritarian mega-widget construction" ™ will then combine all the incoming substandard widgets and output the perfect widget in response, its first-order properties specified minutely in advance.

This sounds like a bogglingly powerful and general construction, and it is.

Now for the bad news...

The bad news

- There is a certain amount of technical baggage required here. In fact a whole branch of math, *model theory*, is needed just to make precise the concept of “generalized widgets” as *models* of a *first order theory* in a *language*.
- The details of the construction do all go through and are entirely valid, but in case I thought I had discovered something new and amazing here, this was all originally discovered by Polish logician Jerzy Łoś in 1957.



- He called his construction the *ultraproduct*, or if you’re multiplying up identical things, the *ultrapower*.
- The “majority systems” used in the construction are called *ultrafilters*. Of which much more anon.

The Łoś ultraproduct theorem

(which I had rediscovered)… is like some weird alien artifact fallen to earth.

There are certainly applications. But it turns out that they don't really require ultraproducts at all. As one textbook rather brutally puts it: "In the end, ultraproducts are only useful for proving theorems about ultraproducts."

Mostly, there are simpler constructions from model theory which are more straightforward to define, and easier to use. They also don't require such powerful axioms of set theory (the Łoś theorem relies heavily on AC).

What about the ultrafilters (aka "majority systems") themselves?

We could start by trying to construct one.

The executive summary: You can’t.

It’s fair to say that I tried pretty hard to construct a (non-principal) ultrafilter.

Others have tried too. It seems to be fundamentally impossible.

Although as noted, there are theorems ensuring an adequate supply of them. It’s just that actually spelling one out appears to be beyond the wit of man.

The closest you can get is that there are alternative versions of set theory (specifically, using the Axiom of Determinacy, which isn’t consistent with AC) in which an explicit construction is possible. But this is no good for mainstream math.

If you believe in an orderly universe, this is a pretty bitter pill to swallow. After all, In his 1900 address to the International Congress of Mathematicians, David Hilbert proclaimed: “In mathematics there is no *ignorabimus*”. (That’s Latin for ‘we shall not know’). Was he wrong?

Ultrafilters: touching on the unknowable

- What are these things?
- What else can you do with them?
- Why does it seem to be impossible to construct one?
- Why does the mere thought of them induce a weird, spinning sensation?

All this and more next time

THANK YOU