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

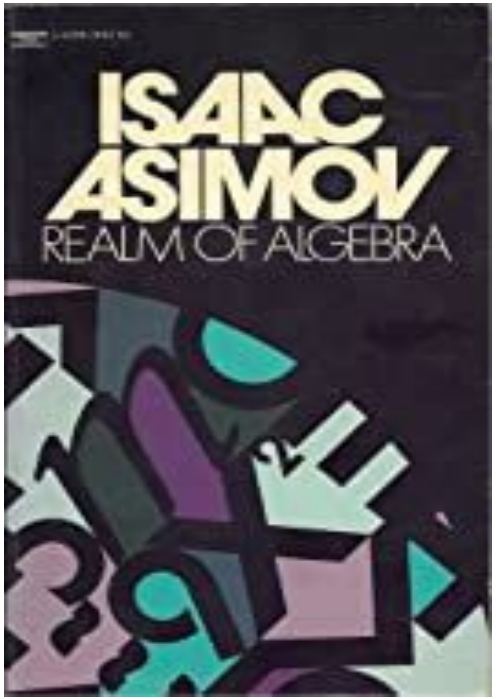
*	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

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

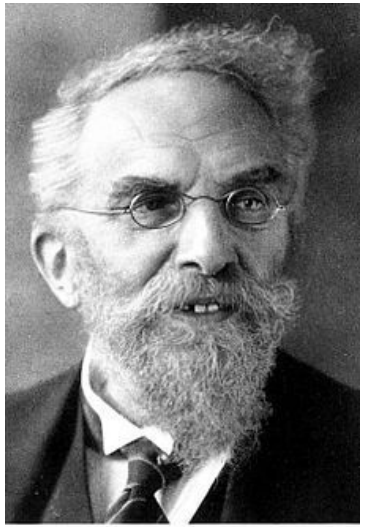
Became convinced that he could find a number system out there, just beyond the reals and complexes. This became a devouring obsession.

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

The Great Algebraic Gene Splicer

by Felix Dilke

a sequel to “Building your own number systems for fun and profit”, this is about an interesting construction I stumbled on as a result

If that showed the fun side of math, this episode will show the uncanny, inhuman side of the subject…

But always in a spirit of objectivity, innovation and discovery. Also I hope you like the pictures.

Pop culture reference: “The Fly” (1986)

In this film, an inventor trying to build a teleportation device finds that his technology can combine multiple living creatures “at the molecular level”.

The results are interesting, but not what he originally had in mind.

Warning: the film is icky.

Anyway, what I’m about to describe is kind of an algebraic version of that.

The previous episode...

...was 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

+ - * /

Trying to construct fields is fun, but difficult.

With this in mind, I ask an apparently simple question...

Motivating question

Starting with the number system of sequences of real numbers, like this:

$$\mathbf{r} = (r_0, r_1, r_2, \ldots)$$

is it possible to ‘simplify’ this system (by identifying sequences) 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 indices *n*, r_n equals s_n.

You can see how this might work.

Of course I have to say what a “majority” is.

But the 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 (just) 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 numbers **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).

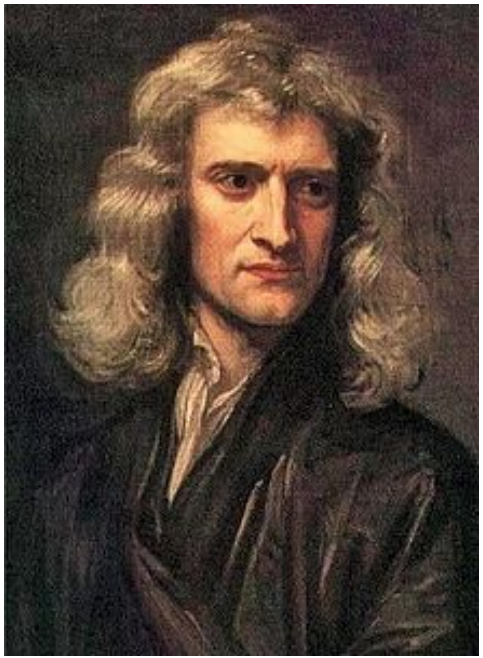
So this gives an alternate way to develop the differential calculus.

Newton’s original formulation of the calculus used infinitesimals, but he “was never able to put this on a rigorous basis” - i.e. 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, 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.

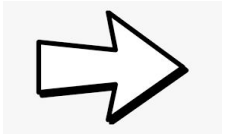
It's almost as if W_1, W_2, … was a sequence converging to the limit $W_{\mathfrak{M}}$.

The gene splicer comes into view

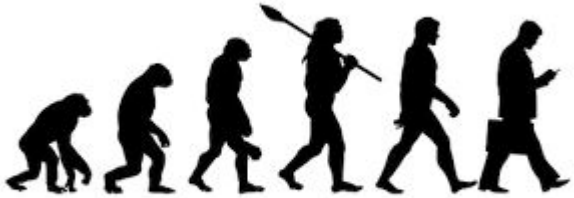
In “The Fly”, artifacts can be combined “at the molecular level”

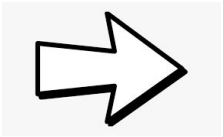
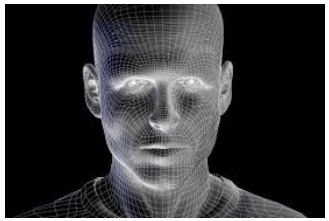
E.g. human subject, housefly, sundry lab equipment included by mistake




Our construction is more like combining an infinite series of steadily more evolved apes to produce a (super)human



Applying the construction

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.

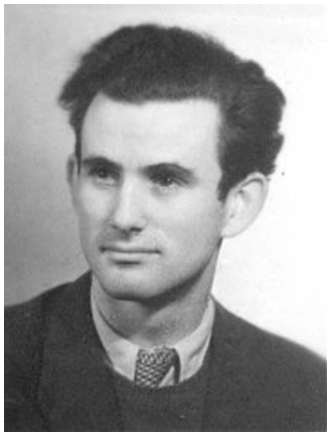
Subject to reasonable conditions, the "majoritarian mega-widget construction" ™ will then combine all the incoming substandard widgets and output the desired widget in response, its first-order properties specified minutely in advance.

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

But...

The bad news

- Some technical baggage is required here. A whole layer of jargon, *model theory*, is needed just to make precise the concept of “generalized widgets” as *models* of a *first order theory* in a *language*.
- Once rigorously expressed, the details of the construction are entirely valid, but if 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 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.

Ultrafilters: touching on the unknowable

- What are these things?
- What else can you do with them?
- Why the deep sense of mystery around the subject?
- And when I tried to construct one...

All this and more next time

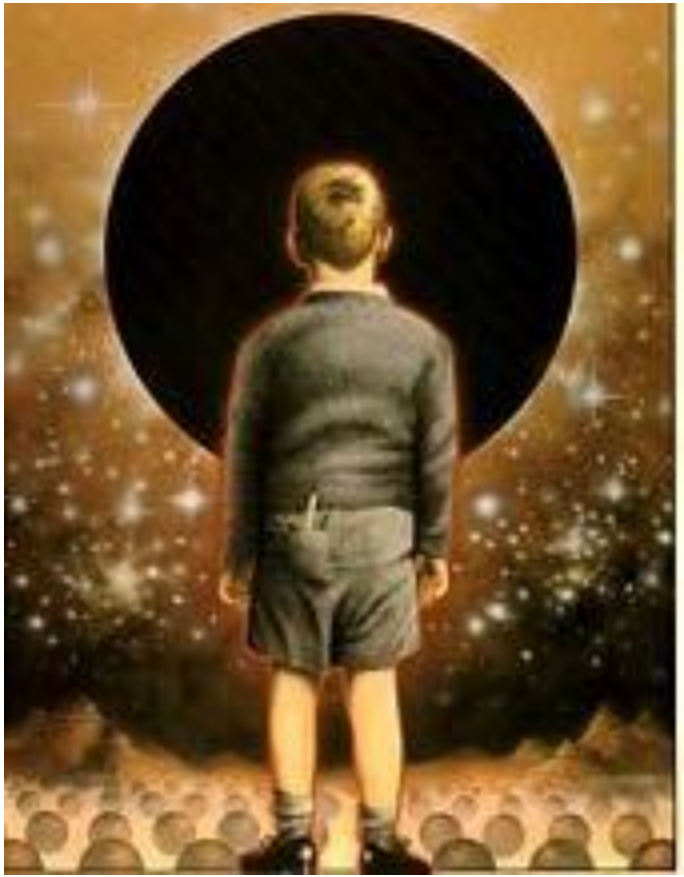
THANK YOU

Facing the unknowable

In the previous talks, I described a construction I stumbled on as a result of trying to build more powerful number systems. It lets you combine many structures of the same type into one, enabling a kind of pick-and-mix “algebraic gene splicing” where you can prescribe in advance the required properties, to a remarkable degree.

But it turns out the most mysterious part of this is the *ultrafilters* - abstruse set-theoretic widgets - used as a key ingredient in the construction.

They exist in profusion, but how to build one?



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. But actually spelling one out appears 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, not 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*”. (Latin for ‘we shall not know’). Was he wrong?

What is an ultrafilter?

Imagine playing “Twenty Questions”, but with any number of questions allowed, and on an infinite set.

You have to guess *x*, supposedly a natural number in the set

N = { 1, 2, 3, … }

You might ask: “Is x > 300?” “Is x prime?” and so on.

Now imagine that, cruelly, your opponent hasn’t really thought of an actual number *x* at all, but has instead devised a system of consistent answers to *all* possible questions. After any finite number of questions, you’ve still only narrowed *x* down to an infinite set.

This (necessarily very elaborate) system of answers is an *ultrafilter*.

No way to win, then. But:

If you played this game instead on the set of all real numbers between 0 and 1,

$$\mathbf{I} = \{ x \in \mathbf{R} : 0 \leq x \leq 1 \}$$

Then perhaps you could win, by repeatedly bisecting the interval to narrow down the location of *x*?

Sort of. You would trap *x* in ever smaller intervals, but they are still infinite sets, and the answer to “Is $x = r$?” for any specific real *r* would always be NO.

You could even determine the exact infinite decimal representation for *x*, to no avail. So *x* does “converge” to some ordinary real number *r*, but $x \mathrel{!}= r$.

The answer to this absurd and nightmarish situation:

Category theory!

Write βX for the set of ultrafilters on X. Then β is a *monad* on the category of sets

and, as I've indicated above, any ultrafilter on the interval **I** = [0, 1] converges to a unique value in **I** infinitely close to it, so we have a mapping

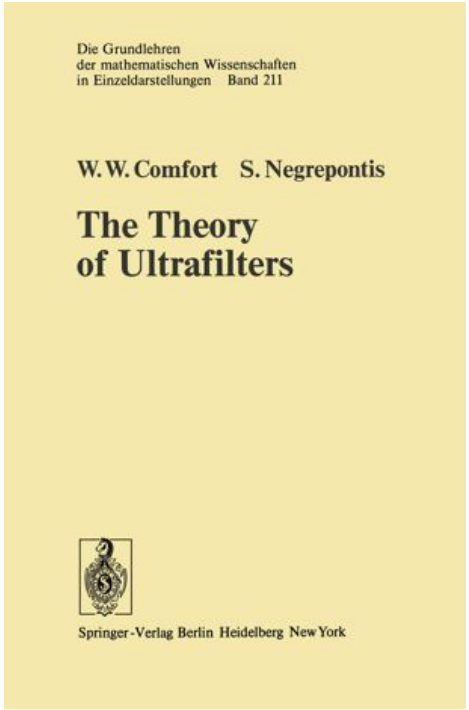
$$\beta \mathbf{I} \to \mathbf{I}$$

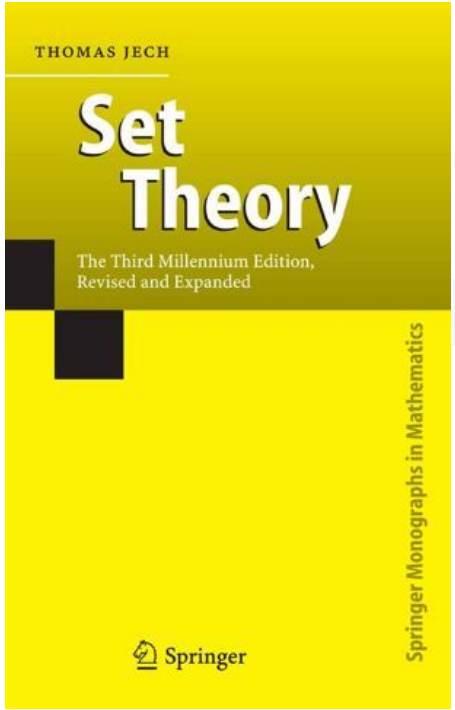
It turns out this makes **I** into an algebra for the monad β, and that this neatly captures the topological structure of the unit interval **I**.

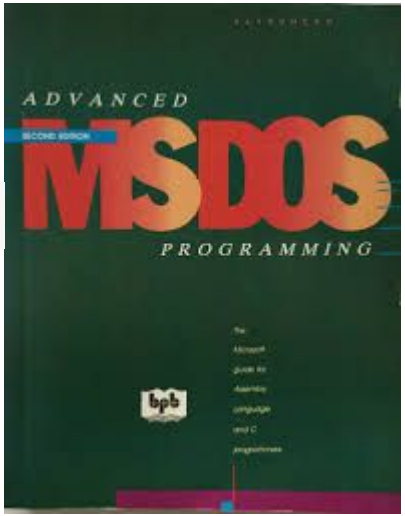
That is: what remains of **I** in a geometry with lengths and angles abstracted away.

Studying ultrafilters within set theory...

A hopeless and heroic task, but people have tried







These are all amazing, magisterial books.

In the end:

You need a better platform.

It turns out we don’t need set theory anyway:

The maths I’ve sketched above can be thought of as a bunch of constructions and theorems carried out in the category of Sets

All this works without essential change in *any* category with sufficiently nice properties, i.e. a topos.

That is, you can construct ultrafilters and ultrapowers in a topos, and all the same ‘gene-splicing’ properties still hold. There’s also an analog of the monad β which shows how to do topology in a topos.

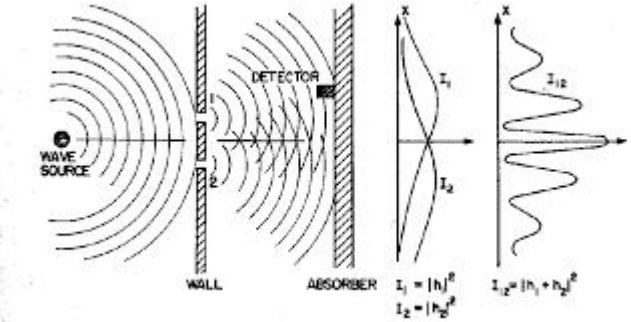
Also the topos itself isn’t required to be a set, so we can operate in a very postmodern fashion “without foundations”. Topoi all the way down.

The catch is...

This viewpoint makes it almost impossible to do conventional math any more, because it points to a complete overhaul of the subject to abolish sets.

It's a bit like the diffraction slit experiment in physics, which (for some) is an apparently simple conundrum whose full resolution requires you to overturn the foundations of the subject, and to posit multiple parallel universes, etc.

As it is, I seem to have pretty much sawed off the branch I was sitting on.



What's left to study?
I will try to answer this next time.

THANK YOU

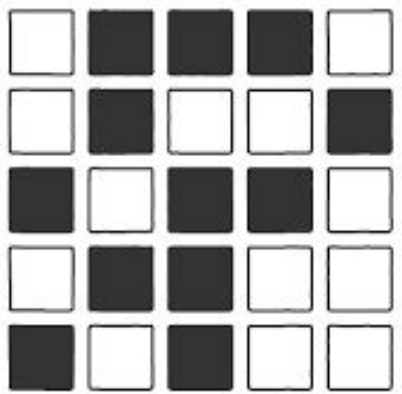
Parity - the next frontier

In the previous talks, I described a chain of events that led to me abandoning set-based math completely.

This is quite a drastic mental shift, an act of renunciation which amounts to throwing out not just the baby but the entire maternity ward and perhaps a wing of the hospital out with the bathwater.

What's left? What can we still study?

A poorly understood concept, *permutation parity*, soon becomes the focus of attention.



Once you stop thinking of everything as a set...

...we see our mathematical structures (groups, rings, graphs, etc) as breathing life into the *dots* and *arrows* of some ambient *category* (a *topos*) which has a carefully selected subset of the properties **Sets (**the category of sets) has.

In other words: it's an abstraction of the category of sets, and you can still do set-like things and apply set-like reasoning, but in a much more general context.

A normal person would ask: why do this?

A mathematician would say: given the power of our familiar set-like reasoning, why not abstract away the irrelevant details and apply it as widely as possible?

But there is still one major unexplained feature of the category **Sets** ...

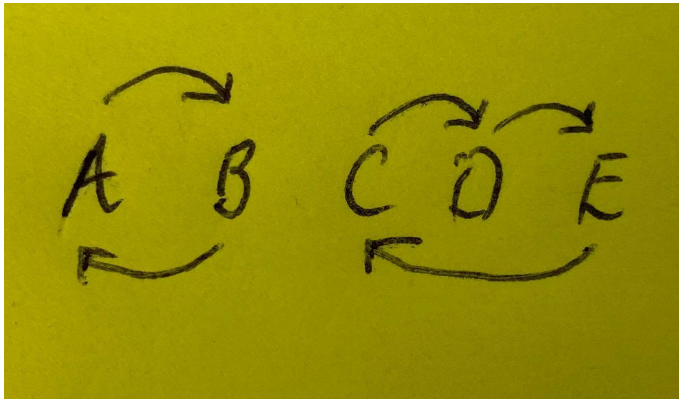
Parity

A *permutation* is a reversible operation on a set that just moves some of its members around. Example…

The most important invariant of a permutation is its *parity*: whether it's even or odd.

The permutation illustrated here is *odd* because it can be achieved in three swaps. But not in an even number of swaps!

One can show: In a precise sense, this is the *only* nontrivial invariant.

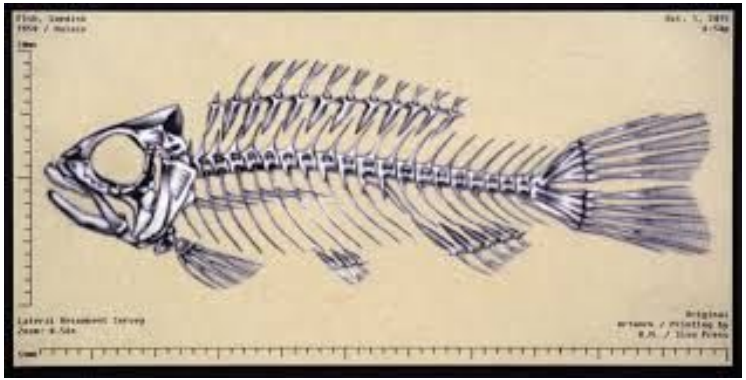


A helpful analogy

So when you permute a finite set (i.e. rearrange its elements) you are also implicitly permuting some invisible two-element set somehow embedded inside it…

Just as, when you flip a fish over in a frying pan, you are implicitly flipping over its skeleton, too.

To permute n is to permute 2.



I should mention the *sporadic triality of the quartet*

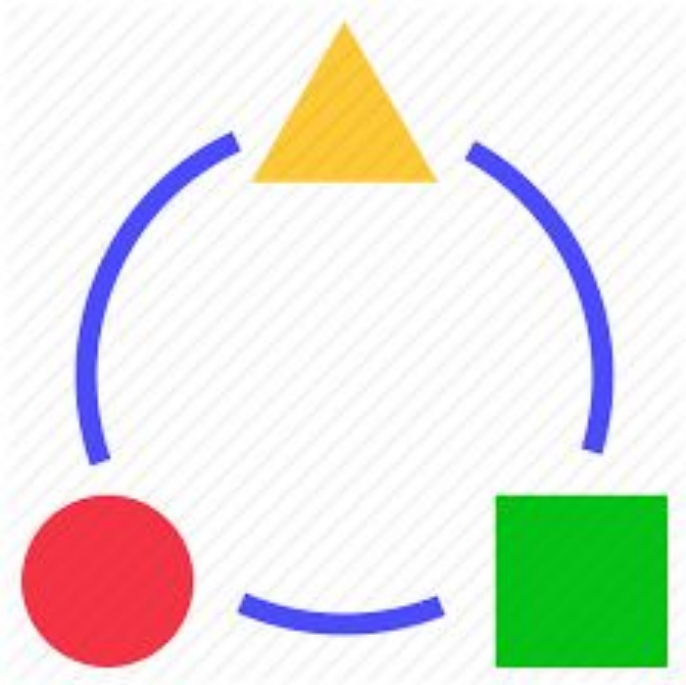
Suppose you permute a 4-element set,

{ A, B, C, D }

You are then implicitly permuting the 3-element set of all “unordered 2-2 partitions” of this set,

{
{ { A, B }, { C, D } },
{ { A, C }, { B, D } },
{ { A, D }, { B, C } }
}

So to permute 4, is to permute 3!



But this is a freak case

It would be nice if there was a similarly canonical description of parity. But I can’t find one. (There is a theory of “model superstructures” which may give pointers, or show why none exists.)

The only correspondences of this form (more precisely, homomorphisms of symmetric groups) are the 4 -> 3 and n -> 2.

You’ll be glad to know that the composite mapping 4 -> 3 -> 2 is just parity, 4 -> 2.

There are some other strikingly odd features of parity:

The theory of parity seems… makeshift

The basic definition and properties of parity are not difficult, but use ad hoc inductive / combinatorial arguments and lack motivation.

As we'll see, it is a fundamental property of sets which seems to lack a convincing general explanation or theory.

There is an interrelationship with the theory of determinants: Given a permutation, we can express it as a matrix of 1s and 0s which rearranges the columns, and then take the determinant of this matrix to calculate parity as +1 or -1. The catch is that you need parity to define determinants in the first place.

There is a similar lack of elegance in developing the theory of determinants. You can do it most smoothly via alternating exterior products … but those are defined via parity, too!

Abstract Parity

In the topos **Set**, the two-element set plays a very special role: it is the *subobject classifier* Ω of the topos. This means that subobjects A -> B are interchangeable with arrows B -> Ω.

So *parity* is an arrow from Aut(X) to Aut(Ω), where Aut(X) is the *internal group object* codifying all bijective arrows from X to itself. The arrow respects the group structure.

Parity only seems to be defined when X is “finite”, another concept that can be a bit slippery to define in a general topos. There are several possible definitions. For us, the most natural one may be “ultrafiniteness”, i.e. that the naturally occurring counit map X -> Ω^Ω^X is bijective.

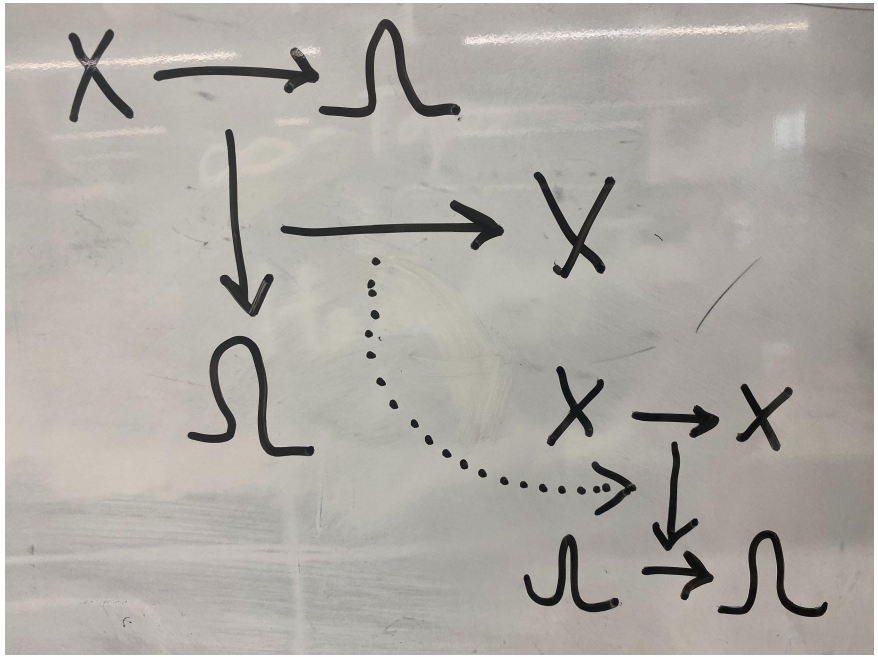
The Goal

So here's what a theory of parity might look like in a general topos:

The left hand side says "X is (ultra)finite"

The right hand side says "X has parity"

It's tantalizing, because on the face of it, there could easily be some sort of canonical mapping between the two.



Getting closer: the transfer

There is an ingenious algebraic construction from group theory, the *transfer* (Issai Schur, 1902) which has always seemed a promising starting point for a proper, invariant definition of parity.

Finally I found a paper which interrelates the transfer with parity-like theories in a general topos (Ferrand 2011). Perhaps the most striking result is:

Let A, B be objects in a topos. If A and B are locally isomorphic, then their automorphism groups have isomorphic abelianizations, $Aut(A)^{ab} \cong Aut(B)^{ab}$.

Unfortunately, *n* and Ω in **Set** are not locally isomorphic. But if we could find a topos where something like this was true, we might now be able to explain parity.

Deep Water

Trying to do math in a general topos can be a little bit daunting, because none of the familiar tools are at hand:

- Everyday concepts like “finiteness” and “the real numbers” are problematic or unavailable
- You have to get to grips with non-Boolean truth values
- The underlying diagram chases are unintuitive and unfamiliar

This is the business we have chosen.

But software tools can help

Modern “theorem provers” (proof assistants) often come with the ability to check proofs in a general topos.

I particularly like Lean (Microsoft Research), which also comes with a large body of code (Project Xena) giving definitions and theorems for “elementary” math.

So, this is something to investigate…

THANK YOU