20th century working methods, continued

A. Putting it all together: the Weil conjectures, Serre, and Grothendieck

B. Category theory as a theory

C. Working mathematical ontology today

Putting it all together: the Weil conjectures, Serre, and Grothendieck

Hendrik Lenstra twenty years ago was firm in his conviction that he did want to solve Diophantine equations, and did not not wish to represent functors—and now he is amused to discover himself representing functors in order to solve Diophantine equations! (Barry Mazur)

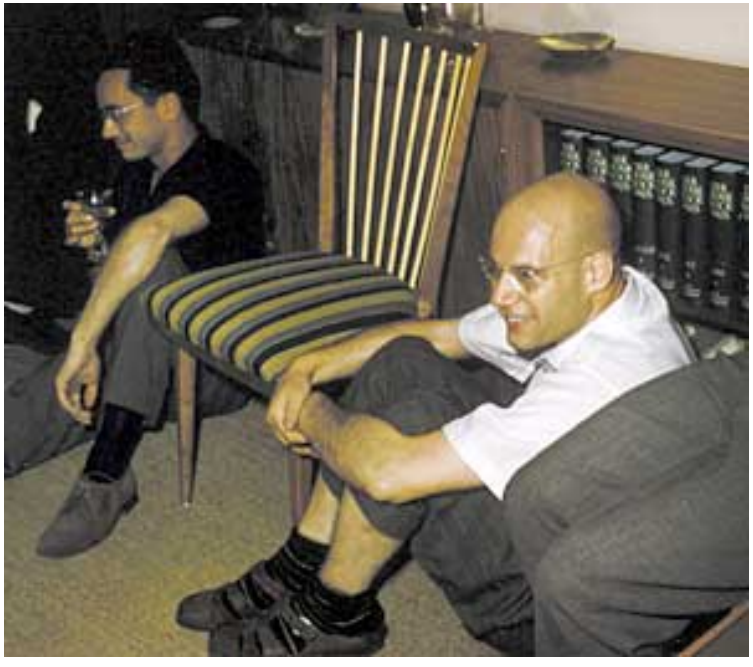
The Weil conjectures:

Number theory that would have amazed Gauss.

Stated using topology from Riemann and Betti.

To be proved (maybe?) by the latest cohomology.

No one had the least idea how to define [a Weil] cohomology and I am not sure anyone but Serre and I, not even Weil if that is possible, was deeply convinced such a thing must exist. (Grothendieck)



The number theory:

Are there integers X, Y with $X^3 - Y^3 = 5$?

There are mod 3:

$$2^3 + 3^3 \;=\; 35 \;\equiv 2 \pmod 3 \quad \text{and} \quad 5 \equiv 2 \pmod 3$$

But there are not modulo 9. Just check all 81 possibilities.

Diophantine equations are hard. Modulo n, not so hard.

Chinese remainder theorem (孙子 3rd c. AD) shows we only need consider prime powers $n = p^k$.

For any finite system Σ of diophantine equations, in variables $X_1, \ldots, X_n$, and any prime p, let N_k be the number of solutions to Σ modulo the power p^k.

Obviously $0 \leq N_k \leq p^{nk}$.

For *nice* systems Σ, Weil gave incredibly beautiful, easy to calculate, estimates of how N_k grows as k goes to infinity.

Most amazing:

Betti The estimates only depend on the Betti numbers of the manifold defined by Σ as equations on complex numbers.

Lefschetz A simple use of the Lefschetz fixed point theorem, *if* you have a cohomology theory for arithmetic spaces.

No one had the least idea how to define such a cohomology and I am not sure anyone but Serre and I, not even Weil if that is possible, was deeply convinced such a thing must exist.
(Grothendieck)

Not only the cohomology had to be discovered.

No one even knew what spaces could express this arithmetic!

> *This truly revolutionary idea thrilled the mathematicians of the time, as I can testify at first hand.*
>
> (Jean-Pierre Serre)

Everything would have to be re-invented.

Relevant to philosophy of math: universe, topos, and scheme.

> *Grothendieck did not believe in universes. He believed in toposes and schemes.* Cartier and Bénabou

For Grothendieck, schemes and toposes are the special and general cases of "the new style of space."

Universes are sets too big for ZFC to prove they exist. A technical device.

Conceptually: a scheme and a topos are both spaces.

Logically each is a category as big as the universe of all ZFC sets.

> *To approach these categories from a 'naïve' point of view, [and] to avoid certain logical difficulties, we accept the notion of a Universe, a set 'large enough' that the habitual operations of set theory do not go outside it.* Grothendieck

But this was a technicality for Grothendieck. Not actually interesting.

What is a scheme?

1. Whatever works for the Weil conjectures.
2. a ringed topological space – standard official definition today.
3. a functor on rings – the "functor of points."
4. for Grothendieck, a topos (étale ringed topos).

It is better not to ask what a scheme *is*, but how schemes *relate to* each other.

> *The points . . . have no ready to hand geometric sense. . . . When one needs to construct a scheme one generally does not begin by constructing the set of points. . . . [While the definition] gives standing to bizarre schemes, allowing it gives a category of schemes with nice properties.* (Pierre Deligne)

Schemes relate to each other the way lines, and spheres, and surfaces of genus n, and more should.

Plus specific new examples specific to arithmetic.

What is a (Grothendieck) topos?

It is like a topological space, but (radically) more general.

Conceptually, it is whatever has cohomology!

So it could be a topological space, or it could be a group.

And Grothendieck developed the ideas so that a topos could be a scheme!

Let us look at it another way.

From inside, a topos looks like a universe of sets.

You can do all of ordinary mathematics inside any topos. But it will not always work out just like in ordinary sets.

Math in the topos $\mathcal{E}_T$ of a topological space T reflects the topology of T.

Math in the topos $\mathcal{E}_G$ of a group G reflects algebra in G.

Math in the topos $\mathcal{E}_{\mathcal{S}}$ of a scheme $\mathcal{S}$ reflects the arithmetic of $\mathcal{S}$.

For a start, simple group theory done inside the topos $\mathcal{E}_T$ (or $\mathcal{E}_G$, or $\mathcal{E}_{\mathcal{S}}$) will give the cohomology groups of T (or G or $\mathcal{S}$).

Well, the topos *defines* the cohomology of $\mathcal{S}$, since that had no prior meaning!

But in the other cases the topos cohomology agrees with the classical cohomology.

When T and G and $\mathcal{S}$ are *singletons*, then $\mathcal{E}_T$ and $\mathcal{E}_G$ and $\mathcal{E}_\mathcal{S}$ are all (isomorphic to) the ordinary category of sets.

In fact Grothendieck was quite surprised at how much of ordinary mathematics you can do in a topos.

He spent at least 15 years absorbing this idea.

This is one of the reasons why he says:

> *Certainly, for more than one aspect of this new geometry (if not for all) no one, on the very eve of the day it appeared, could have dreamed of it—the worker himself no more than others.*

For Grothendieck, "a rebirth of geometry."

Grothendieck himself proved most of the steps in the Weil conjectures using his *étale cohomology*.

The last, and greatest step (the "Riemann hypothesis over finite fields") remained a challenge.

Grothendieck posed "standard conjectures" to complete itf.

Deligne completed the proof by a very clever trick, using étale cohomology but bypassing the standard conjectures.

Grothendieck was very disappointed with this.

As to the larger picture.

Many mathematicians currently prefer to bypass toposes.

But Grothendieck's approach to cohomology, introduced in his paper called *Tōhoku*, is the reason why one noted number theorist says:

> *One now instinctively assumes all obstructions are best described in terms of cohomology groups.*
>
> (Swinnerton Dyer)

Category theory as a theory

Category has been defined in order to be able to define functor, and functor has been defined in order to be able to define natural transformation.

(Peter Freyd)

One philosophic motive for learning this: Category theory is a powerful, widely used, format for organizing vast information.

The first-order Eilenberg-Mac Lane category axioms.

These axioms have trivial consistency strength.

They all follow from

$$\forall x \forall y \ (\ x = y \ ).$$

But that is not an *interesting* interpretation.

Categorical *foundations for mathematics* will assume *much more* than just the elementary category axioms.

There are objects $A, B, C, \ldots$, and arrows $f, g, h, \ldots$.

Each arrow goes from some object to some object, $f : A \to B$.

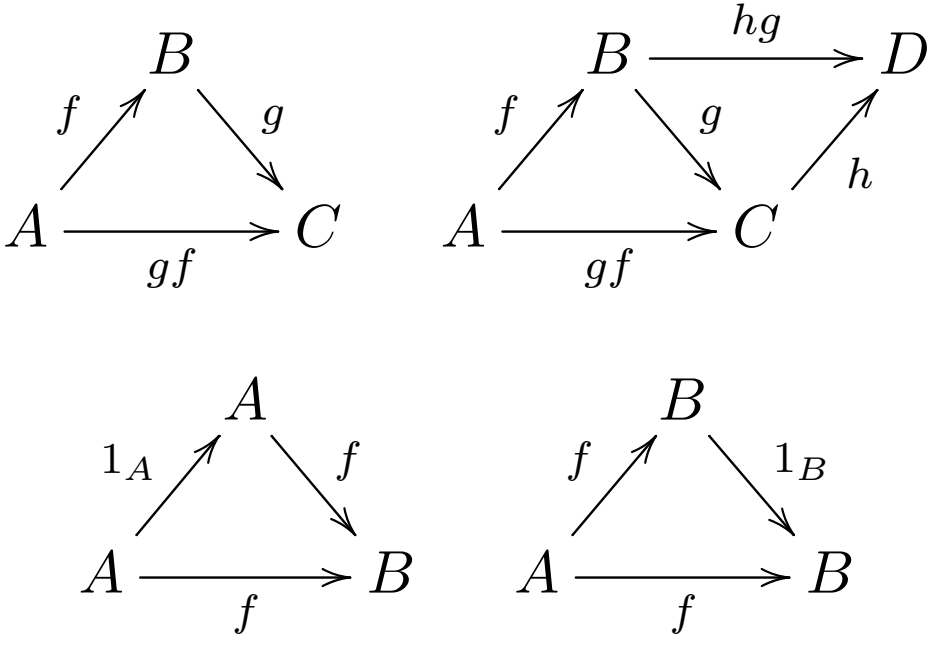
Each object A has an *identity arrow* $1_A : A \to A$.

And when arrow match up $f : A \to B$ and $g : B \to C$ they have a *composite* $gf : A \to C$.

Composition is associative and has identities:

$$h(gf) = (hg)f \quad \text{and} \quad f1_a = 1_B f = f.$$

In pictures:



Types: $A, B, C \ldots$ for objects, and $f, g, h \ldots$ for arrows.

Operators:

Dom takes arrows to objects, read "domain of."

Cod takes arrows to objects, read "codomain of."

1_ takes objects to arrows, read "identity arrow of."

Relation: $C(x, y; z)$ applies to arrows, read "z is the composite of x and y."

Axioms (free variables A,f,g,h):

$\mathrm{Cod}\, f = \mathrm{Dom}\, g$ if and only if $\exists!\ h\ C(f, g; h)$.

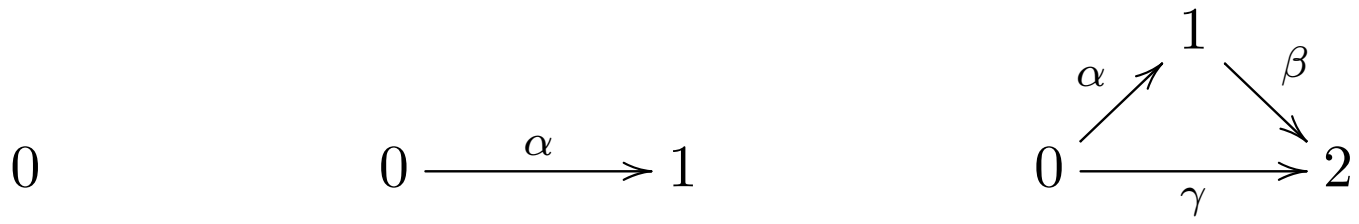
If $C(f, g; h)$ then $(\mathrm{Dom}\, f = \mathrm{Dom}\, h\ \&\ \mathrm{Cod}\, g = \mathrm{Cod}\, h)$.

$\mathrm{Dom}\, 1_A = \mathrm{Cod}\, 1_A = A$.

$C(1_{(\mathrm{Dom}\, f)}, f; f)$ and $C(f, 1_{(\mathrm{Cod}\, f)}; f)$.

If $C(f, g; i)$ and $C(g, h; j)$ and $C(f, j; k)$, then $C(i, h; k)$.

Some finite examples have technical uses:



1 **2** **3**

Some large (proper class) examples: the category **Set** of sets and functions, the category **Grp** of groups and group homomorphisms.

Intermediate sized: **Riemann** the category of Riemann surfaces and holomorphic maps.

The categorical definition of *isomorphism* immediately spread across all of mathematics.

People had long known two different spaces can have "the same topology" (say, a disk and a square). Such spaces were called homeomorphic (among other things).

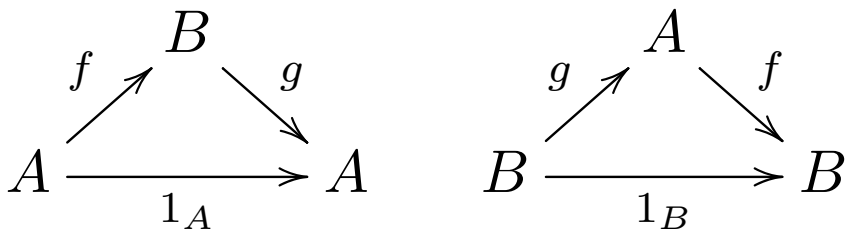
Two different groups can have "corresponding group laws," and there were various terms for that.

But why should one definition of "the same structure" work for both topological spaces and groups?

One does.

An arrow $f : A \to B$ is an *isomorphism* if it has an *inverse*, that is an arrow $g : B \to A$ with $gf = 1_A$ and $fg = 1_B$.

Objects A, B are *isomorphic* if there is some isomorphism $f : A \to B$.

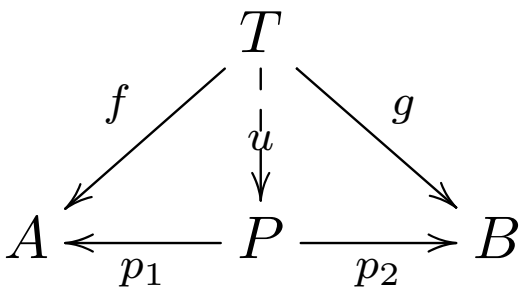


Think g and f "undo" each other.

A *product* of object A, B is an object and two arrows

$$A \xleftarrow[p_1]{} P \xrightarrow[p_2]{} B$$

Such that for any object and two arrows T, f, g there is unique arrow u with $p_1 u = f$ and $p_2 u = g$;



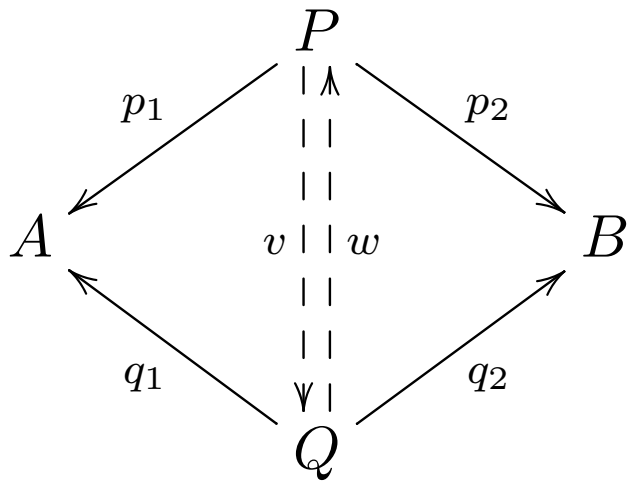
In the category **Set** of sets, the cartesian product $A \times B$ is a product, with

$$p_1\langle x, y\rangle = x \text{ and } p_2\langle x, y\rangle = y \text{ and } u(t) = \langle f(t), g(t)\rangle.$$

But

1. this is stated in any category,
2. in some categories products are quite different from cartesian, or do not exist;
3. and this is only defined *up to isomorphism*.

If you have two products for A, B, say P, p_1, p_2 and Q, q_1, q_2 then there are unique v, w:



And it follows that v, w are inverse. So P, Q are isomorphic.

Categorical definitions always, automatically, are just *up to isomorphism*.

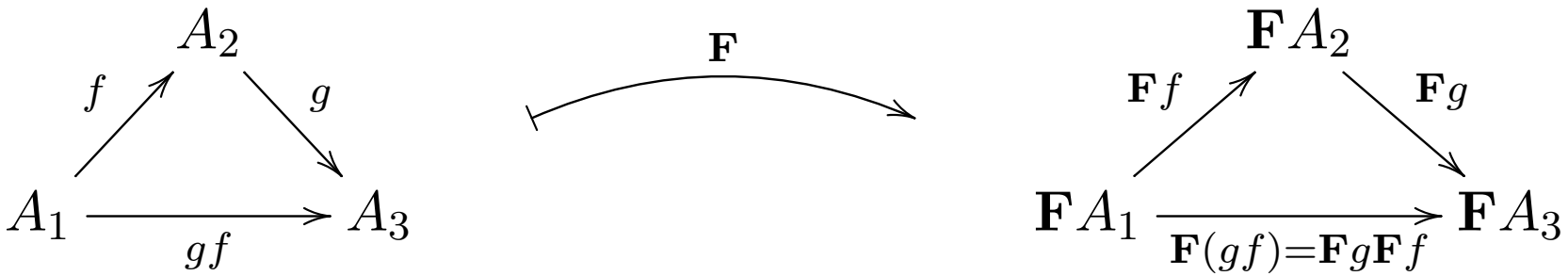
In ZFC there are any different definitions of ordered pair, and so of the cartesian product $A \times B$.

People say it does nto matter which you take since all give isomorphic versions of $A \times B$.

The categorical definition skips all that in the first place.

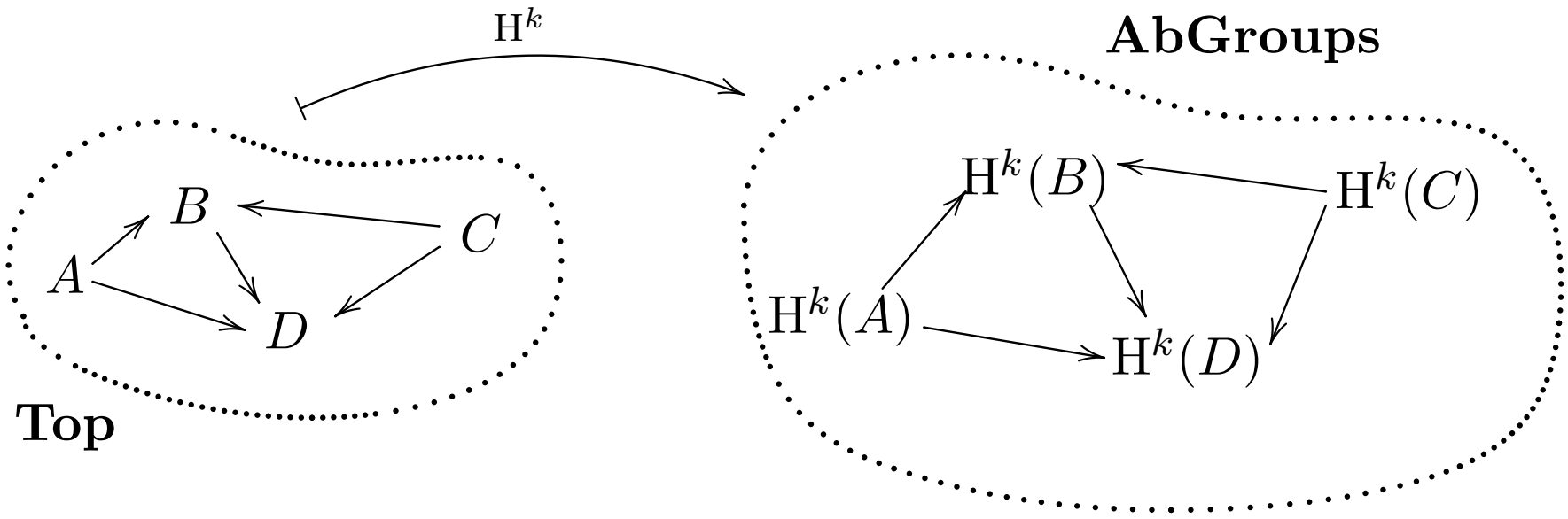
A *functor* $\mathbf{F}: \mathbf{A} \to \mathbf{B}$, assigns to each object A of $\mathbf{A}$ an object $\mathbf{F}A$ of $\mathbf{B}$, and assigns to each arrow $f: A \to A'$ of $\mathbf{A}$ an arrow $\mathbf{F}f: \mathbf{F}A \to \mathbf{F}A'$ of $\mathbf{B}$, so that it preserves domain, codomain, identity arrows, and composition.

To put it in a diagram:

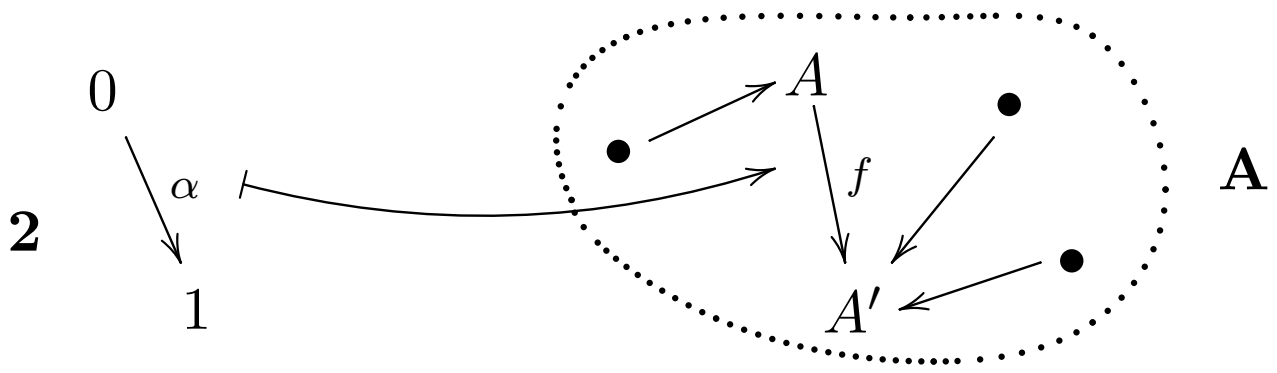


So $\mathbf{F}$ maps the whole network of arrows in $\mathbf{A}$, to the network of arrows n $\mathbf{B}$.

The k-th homology functor:



A cleaner more foundational example:



A functor from **2** to **A** just picks out an arrow of **A**.

A very important class of functors.

The *forgetful functor* or *underlying set* functor $\mathbf{U}: \mathbf{Grp} \to \mathbf{Set}$ takes each group G and gives just the set $\mathbf{U}(G)$ of its elements.

We say we "forget the group operations."

Many structures, including topological spaces have underlying set functors. But there are important examples that do not.

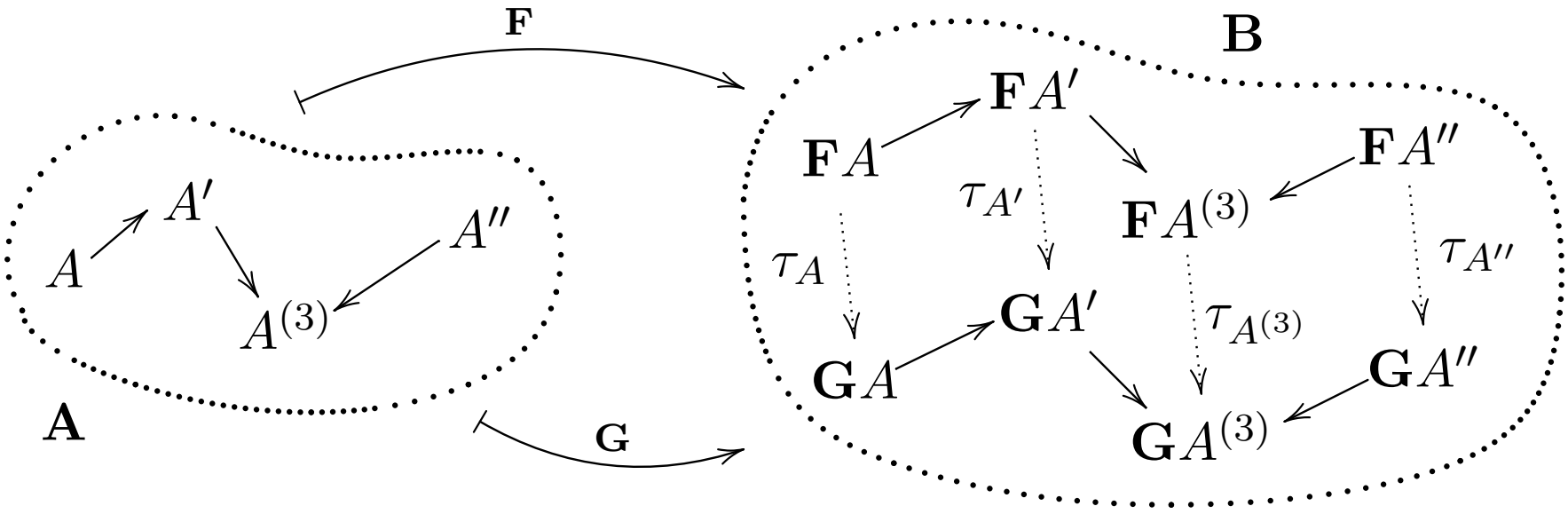
A *natural transformation* $\tau : \mathbf{F} \to \mathbf{G}$, is a family of arrows in $\mathbf{B}$ which roughly speaking carry values of $\mathbf{F}$ over to values of $\mathbf{G}$.

It assigns to each object A of $\mathbf{A}$ an arrow $\tau_A : \mathbf{F}A \to \mathbf{G}A$, meeting the *naturality condition*:

$$(\mathbf{G}f)(\tau_A) = (\tau_{A'})(\mathbf{F}f)$$

In a diagram:

$$\begin{array}{c} A \\ {\scriptstyle f}\downarrow \\ A' \end{array} \qquad\qquad \begin{array}{ccc} \mathbf{F}A & \xrightarrow{\tau_A} & \mathbf{G}A \\ {\scriptstyle \mathbf{F}f}\downarrow & & \downarrow{\scriptstyle \mathbf{G}f} \\ \mathbf{F}A' & \xrightarrow[\tau_{A'}]{} & \mathbf{G}A' \end{array}$$



When all the arrows τ_A are isomorphisms, we say $\mathbf{F}$ and $\mathbf{G}$ are *naturally isomorphic*.

The two functors do practically the same thing.

They are the same *up to isomorphism*.

The term *category theory* did not exist in 1957.

Categories and functors were tools to use in theories. They did not make up an independent subject.

"Category theory" was coined by the mathematical biologist Robert Rosen in 1958.

The term was accepted by category theorists because of Grothendieck.

But also, because of Daniel Kan inventing *adjoint functors*.

I will warn that some mathematicians dislike the term "category theory" since they think it should mean paying *too much* attention to foundational issues.

Some dislike *logic* and *set theory* in the same way.

That's not a problem to me.

Whatever you call it, working mathematics today uses a lot of categories and functors, and adjunctions.

You can do a lot of group theory just looking at homomorphisms $f : G \to H$ between groups.

This is what Emmy Noether emphasized.

But sometimes you want to look at the set of elements of G.

To be precise, we use the underlying set functor $\mathbf{U} : \mathbf{Grp} \to \mathbf{Set}$.

A powerful way to organize this is to relate it to the *free group functor* $\mathbf{F} : \mathbf{Set} \to \mathbf{Grp}$.

Think of a set A as a set of letters: $A = \{a, b, c, d \dots\}$.

Say a *word* on this set is any string of letters and inverse letters:

$$db^{-1}ca^{-1}b \quad \text{or } acd^{-1}bd$$

Multiply them by just putting them together

$$db^{-1}ca^{-1}bacd^{-1}bd$$

The only detail that if you have a letter next to its inverse, like $c^{-1}c$ you cancel them out.

This gives a group, called the *free group* on A, $\mathbf{F}A$. The unit element is the empty string.

This is actually a functor $\mathbf{F} : \mathbf{Set} \to \mathbf{Grp}$.

It has a close connection to the underlying set functor $\mathbf{U} : \mathbf{Grp} \to \mathbf{Set}$.

A function $f : A \to \mathbf{U}G$ from any set A to the set of elements of any group G is practically the same thing as a group homomorphism $h : \mathbf{F}A \to G$ from the free group on A.

People had long known this somehow.

Saying it clearly led to huge progress in many fields.

Working mathematical ontology today

For some time mathematicians have emphasized that mathematics is concerned with structures involving mathematical objects and not with the "internal" nature of the objects themselves. They have recognized that we are not given mathematical objects in isolation but rather in structures. (Michael Resnik)

Some issues in philosophy of mathematics are purely philosophical.

But many are in fact pressing daily issues in mathematics – and so, mathematicians have answers that work.
This lecture is about some of those.

Three things drive mathematicians to ever stronger, more agile organizing tools.

Insight Clearing away the details can make a solution stand out.

Teaching There is a constant drive for better, clear, up to date textbooks.

Proofs Current proofs are often extremely long

For example Andrew Wiles' proof of Fermat's Last Theorem cites several dozen advanced theorems that even experts cannot be expected to know in full offhand.

Those theorems also have very long proofs!

He has to be able to use theorems, which have been proved, but without looking at the proofs themselves.

Hegel's ideal is a practical necessity:

> *In the result, the proof is over and done with and has vanished.*

Understand, in much current mathematics it is completely out of the question for one book to give a major proof in full starting from just concepts and theorems found in graduate textbooks.

Each cited theorem must be concise, explicit, and fully reliable outside its original context.

Theorems must be stated structurally.

Homology theory today would be infeasible if each author had to check every other author's specific ZFC construction of homology groups.

Methods must handle structures at every level from natural numbers to functors by comparable means that readily relate any two levels.

Today I will look at two practical issues at a textbook level. In Resnik's terms:

1. Cross-structure identity. If real numbers, for example, as just points in the real number structure, then how they also be complex numbers?
2. Structures as points in structures. If the ring of real polynomials $\mathbb{R}[X]$ is a structure with points in it, then how can it also be just a point in a larger structure?

Daily working mathematics handles these issues by routine use of categories and functors.

Section refS:begin extends Resnik's structuralism by the standard practice of identifying some structures as parts of others. Certain injections $\mathbb{S}_1 \rightarrowtail \mathbb{S}_2$ of one structure $\mathbb{S}_1$ into another $\mathbb{S}_2$ are taken as *identity preserving* and thus as making $\mathbb{S}_1$ a part of $\mathbb{S}_2$. We use textbook treatments of the real and complex numbers to argue that such identity is not defined by any logical principles but by stipulation or tradition. This opens up a philosophical topic of explaining how particular cases come to be accepted as identity preserving.
Section refS:structuralism pursues the original point of structuralist methods—defining structures as themselves places in patterns of structures rather the way that Resnik describes in his later chapters. It takes polynomials as an example and discusses foundations.

If, for example, real numbers have only relations to each other, how do they gain relations to complex numbers?

> *We suppose you understand the real numbers! The complex numbers are formal expressions* $x_0 + x_1 i$ *with* x_0, x_1 *real, combined by*
>
> $$(x_0 + x_1 i) + (y_0 + y_1 i) = (x_0 + y_0) + (x_1 + y_1)i$$
> $$(x_0 + x_1 i)(y_0 + y_1 i) = (x_0 y_0 - x_1 y_1) + (x_0 y_1 + x_1 y_0)i$$
>
> (Conway and Smith)

If Conway and Smith were ZF set theorists this would mean real numbers cannot be complex numbers.

A real number defined in ZF is not a formal expression made from two real numbers and a letter i.

But Conway and Smith freely equate each real number x with the complex number $x + 0i$.

Virtually all mathematicians do.

Serge Lang:

> *We identify* $\mathbb{R}$ *with its image in* $\mathbb{C}$.

Some important injections are taken as *identity preserving*.

There is no definition of *identity preserving*.

It is just a *stipulation*, a matter of explicit convention.

Mathematicians stipulate which injections are identity preserving only taking care never to stipulate two distinct identity preserving injections between the same patterns.
Nearly everyone takes $\mathbb{R} \rightarrowtail \mathbb{C}$ as identity preserving.
Lang says "it is customary to identify" certain elements of many different algebras with "the integers" or the rational numbers, real numbers et c.

Again, there is no criterion for this. It is stipulation.

Philosopher Fraser MacBride (like many others, I believe) says "the notion of 'identity by fiat' makes dubious sense."

But he gives no further argument.

It makes sense to tens of thousands of mathematicians every year. And to me.

Until MacBride or others express a more specific objection, I will say the standard working solution is a good one.

A possible project.

As to structures in structures, I quote Resnik again:

> *Patterns themselves are (. . .) identified with positions of another pattern, which allows us to obtain results about patterns which were not even previously statable. It is [this] sort of reduction which has significantly changed the practice of mathematics.*

We can look at how this is actually done with polynomials, rings, and the category of rings.

A *commutative ring* R is a structure with 0,1, addition, subtraction, and multiplication following the familiar formal rules.

A *ring morphism* $f : R \to Q$ is a function which preserves 0,1, and the ring operations:

$$f(0) = 0 \qquad f(x - y) = f(x) - f(y) \qquad \text{etc.}$$

We will say "ring" to mean commutative ring.

Intuitively, a real polynomial $p(X)$ is a sum of powers if X:

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \qquad \text{with all } a_i \in \mathbb{R}$$

But what *is* a sum of powers?

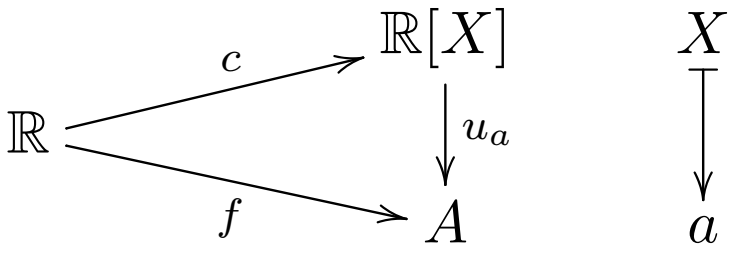
Is it some kind of set? Is it a string of symbols?

Lang says there are "several devices" for this, does not pick one answer.

Let us see how Lang precisely describes the ring of polynomials.

Lang states: $\mathbb{R}[X]$ is a ring with element $X \in \mathbb{R}[X]$ and a morphism $c : \mathbb{R} \to \mathbb{R}[X]$ called the insertion of constants.

For each ring homomorphism $f : \mathbb{R} \to A$ and element $a \in A$, there is a unique homomorphism $u_a : \mathbb{R}[X] \to A$



with $u_a(X) = a$ and agreeing with f on constants.

Do not worry about the details.

The point is Lang defines polynomials, not by saying what each one is, but by saying what the ring of them is.

He describes that ring by its place in the category of rings.

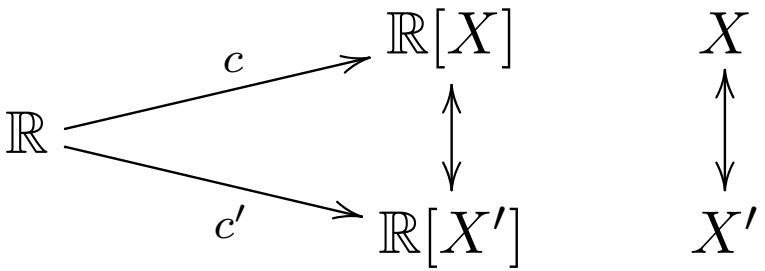
Suggests two set theoretic definitions of polynomials in different books. Neither one precise. Avoids using either one.

He just uses the above precise fact in proofs.

This is how structural mathematics is done. How most mathematics today is done.

Lang's fact does not uniquely specify $\mathbb{R}[X]$, but defines it *up to isomorphism*.

Suppose a ring $\mathbb{R}[X]$ and function c satisfy the fact, and so do another $\mathbb{R}[X']$ and c'. Then there is a unique ring isomorphism $u : \mathbb{R}[X] \to \mathbb{R}[X']$ such that $u(X) = X'$ and $uc = c'$.



We categorical foundationalists like definitions up to isomorphism, so we use that fact to define $\mathbb{R}[X]$, – but right now I am talking about working methods, not foundations.

Further, a standard research tool, not yet standard in textbooks, can describe the whole category **Ring** of rings without saying a ring has a set of elements.

This describes **Ring** up to isomorphism in the category of categories, or even just *up to equivalence*, depend on exactly how you do it.

Define a functor $\mathbf{T}\colon \mathbf{Set} \to \mathbf{Set}$ taking each set A to the set of all *ring theoretic words* on A.

That is, think of a set A as a set of letters: $A = \{a, b, c, d \dots\}$. A *ring theoretic word* on A is any string of letters, and letters 0,1, linked by plus and times:

$$(db + a)(c + 1) \quad \text{or } (a + 0) + cd$$

Add and Multiply them by just putting them together

$$((db+a)(c+1))+((a+0)+cd) \quad \text{or } ((db+a)(c+1))((a+0)+cd)$$

Now, consider two words equal if and only if the ring axioms would imply they are the same.

This functor has natural transformations $\eta : 1_{\mathbf{Set}} \to \mathbf{T}$ and $\mu : \mathbf{T}^2 \to \mathbf{T}$ forming a *triple* or *monad* on **Set**.

Again do not worry about the details.

For some purposes it is actually useful (not only possible in principle) to define **Ring** as the *Eilenberg-Moore* category of the triple $\mathbf{T}, \eta, \mu$.

This can be done up to isomorphism of categories, or up to equivalence, depending on details.

Either way it immediately gives an adjunction whose parts are the free ring functor $\mathbf{F} : \mathbf{Set} \to \mathbf{Ring}$ and underlying set functor functor $\mathbf{U} : \mathbf{Ring} \to \mathbf{Set}$functor $\mathbf{F} : \mathbf{Set} \to \mathbf{Ring}$

To be completely structuralist, we would do all of this in the Category of Categories as Foundation.

But that is an issue of foundations.