Grothendieck's approach to equality

K. Buzzard, Imperial College London

6th May 2022, Grothendieck conference, Chapman University.

Before we start

Two things before we start:

1) Thank you *very much* to the organising committee for the invitation, and thanks to you all for coming!

2) I'm sorry I'm not there in person – I found it too difficult to justify yet another transatlantic flight.

A cool fact

Here's a mathematical fact:

If a is a positive integer which ends in 7, and b is a positive integer which ends in 4, then the product $a \times b$ will end in 8.

When we are young, we are taught an *algorithm* for multiplying positive integers ("column multiplication"). You can prove the above theorem by looking at the algorithm.

The integers modulo 10

Later on, we learn that there's something called "the integers modulo 10".

It is a finite "system of numbers".

A "pre-university" model for it is the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

There is a "reduction modulo 10" map from the positive integers to this set, defined by "divide by 10 and take the remainder", or simply "take the last digit".

For example, the integer 37 gets mapped to 7.

The integers modulo 10

The integers modulo 10: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

The integers modulo 10 have an addition and a multiplication of their own!

It's defined by "if you go off the top, you appear again at the bottom". For example $9 + 1 = 0$, $9 + 2 = 1$, and $7 \times 4 = 28 = 18 = 8$.

Alternative definition: "Do the calculation in the regular integers, and then divide by 10 and take the remainder."

The integers modulo 10

Philosophical objection: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is a subset of the integers. We *already defined* 7×4 to be 28; we are now *redefining* 7×4 to be 8.

At university, we are taught the “correct” way to do it.

The integers modulo 10

The "correct" model for the integers modulo 10 is the quotient ring $\mathbb{Z}/10\mathbb{Z}$, that is, the set

$$\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9]\}.$$

The object [7] is an *equivalence class*, and it is itself an infinite set: it is the numbers $\{\ldots,7,17,27,37,47,\ldots\}$.

The integers modulo 10

How to multiply [7] by [4] in the "correct" integers modulo 10:

First, choose an arbitrary element of [7], for example 37.

Then choose an arbitrary element of [4], for example 204.

Then you multiply them together in the usual way, getting 7548.

This number ends in 8.

So it's in $[8] = \{\ldots, 8, 18, 28, \ldots, 7538, 7548, \ldots, \}$.

So this means $[7] \times [4] = [8]$.

Problems with this definition:

A theoretical problem with this definition:

We need to check that multiplication of [7] and [4] is "well-defined".

What if I had chosen 31415926535897 and 27182818284?

You still get [8] – for example, because of the analysis of the algorithm.

The practical problem with this definition:

Undergraduates can get completely confused about why we are doing it in such a complicated way, with all this "well-defined" nonsense, when the $\{0, 1, 2, \ldots, 9\}$ model *works perfectly well!*

Quotients

The whole idea of a quotient is that we have a set (like the integers), but we want to put a new notion of equality on its elements (an equivalence relation).

For example, if we only care about the last digit of a number, we might want to treat 7 and 37 and 31415926535897 as "the same", even though they're not.

We can do it the "subset way" (choose an element in each equivalence class once and for all), or the "quotient way" (sets of equivalence classes, or other models for quotients).

Are these two ways "equal"?

Equality

Is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ equal to $\{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$?

Well, yes and no.

A set theorist might tell you that they were not equal.

A smart undergraduate might tell you they were "isomorphic as rings".

A PhD student might tell you that they were even "canonically isomorphic as rings".

Probably everyone would agree that they "represent the same mathematical idea".

A student of homotopy type theory might tell you that they really *were* equal.

What do we want from equality?

A student of set theory might tell you that *everything is a set*.

They might go on to tell you that two sets are equal if and only if they have the same elements.

With this viewpoint, $\{0,1,2,3,4,5,6,7,8,9\}$ and $\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9]\}$ are definitely *not equal*.

They are different *models* of the integers modulo 10 within set theory.

What do we want from equality?

A key property that mathematicians want from equality is the *substitution property*:

If A and B are two mathematical objects and $A = B$, and if P is any statement about mathematical objects such that $P(A)$ is true, then $P(B)$ must also be true.

What is a "statement about mathematical objects" though?

Precisely what is allowed will depend on your foundations. Homotopy type theorists allow more equalities than set theorists, but they also allow fewer statements.

Of course most working mathematicians just trust their intuition.

On to Grothendieck

Grothendieck uses set-theoretic language in his algebro-geometric works from the 60s.

However his use of equality does *not* conform to the set-theoretic language.

No doubt this was well-known for a long time.

I certainly didn't notice when I was reading his work when doing my PhD.

I discovered this fact the hard way – when trying to apply the principle of substitution to two rings which Grothendieck was claiming were equal, in Lean, a computer theorem prover.

Here is the mathematical background.

Localisation

Let's say we have the positive integers $\{1, 2, 3, 4, \ldots\}$, but we want to do *division*.

How do we *build* $1/2$, or more generally the set of all positive rationals?

We could make a *preliminary definition*: a positive rational is an ordered pair (n, d) with n (the numerator) and d (the denominator) being positive integers. Let's use the standard notation n/d instead of (n, d).

The problem with the preliminary definition: $1/2 \neq 2/4$. The ordered pairs $(1, 2)$ and $(2, 4)$ are not the same ordered pair.

Localisation

The problem: defining n/d to be the pair (n, d) gives us $1/2 \neq 2/4$.

The fix: quotient!

Say that ordered pairs (a, b) and (c, d) are *equivalent* if $ad = bc$ (for example $1 \times 4 = 2 \times 2$), and define the positive rationals to be the equivalence classes.

This works!

Duality between geometry and algebra

Given a space, the functions on it form a commutative ring (addition, negation, multiplication).

Grothendieck did the converse: given a commutative ring R, he made a space $\mathsf{Spec}(R)$, such that the functions on $\mathsf{Spec}(R)$ were the ring R again.

In fact, Grothendieck equipped the space with a *sheaf of rings*, meaning that for every open set in $\mathsf{Spec}(R)$ he could tell you what the functions on that open set were.

Let's take a look at Grothendieck's formula.

Functions on an open set

The functions on $\mathrm{Spec}(R)$ are the ring R.

Now imagine $f \in R$, so f is a function on $\mathrm{Spec}(R)$.

Consider the subset $D(f)$ of $\mathrm{Spec}(R)$ where $f \neq 0$.

We want to allow R and $1/f$ to be functions on $D(f)$. And $23/f^{37}$. So we need to force the existence of division by f, and we know how to do this!

Let's define the functions on $D(f)$ to be $R[1/f]$, i.e., functions of the form r/f^n, with $r \in R$ and $n = 0, 1, 2, 3, \ldots$.

Formally, this is a quotient of $R \times \{1, f, f^2, f^3, \ldots\}$.

Here's the problem.

What if you have two different functions $f \neq g$ with the same zeros?

This can happen! For example the polynomial functions $(T-23)(T-37)^2$ and $(T-23)^3(T-37)$ both vanish only at 23 and 37.

In this case, $D(f)$ (the space where f doesn't vanish) equals $D(g)$.

Then Grothendieck wants to define the functions on the region $D(f) = D(g)$ where they don't vanish to be $R[1/f]$ *and* $R[1/g]$.

One is a quotient of $R \times \{1, f, f^2, \ldots\}$, one is a quotient of $R \times \{1, g, g^2, g^3, \ldots\}$.

So a set theorist would say these rings were not equal. But they are isomorphic.

Here's the problem

This looks like it is a serious logical issue. Grothendieck's "definition" is not well-defined!

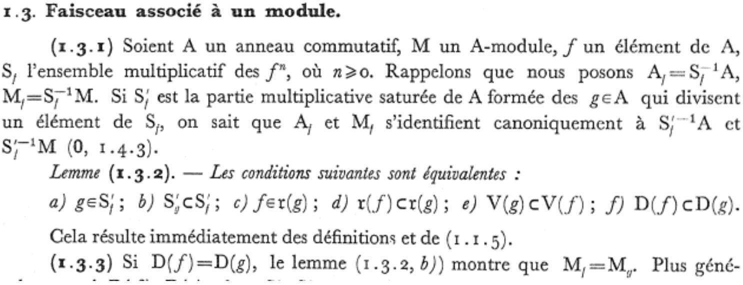
We have: the functions on $D(f)$ are $R[1/f]$, the functions on $D(g)$ are $R[1/g]$, and $D(f) = D(g)$, but $R[1/f] \neq R[1/g]$.

So this formally breaks the principle of substitution.

Let $P(X)$ be the statement "X is a space, and the functions on X are equal to $R[1/f]$"; then $P(D(f))$ is true but $P(D(g))$ is false.

Grothendieck noticed this back in 1960.

Excerpt from EGA1



1.3. Faisceau associé à un module.

(**1.3.1**) Soient A un anneau commutatif, M un A-module, f un élément de A, S_f l'ensemble multiplicatif des f^n, où $n \geqslant 0$. Rappelons que nous posons $A_f = S_f^{-1}A$, $M_f = S_f^{-1}M$. Si S'_f est la partie multiplicative saturée de A formée des $g \in A$ qui divisent un élément de S_f, on sait que A_f et M_f s'identifient canoniquement à $S_f'^{-1}A$ et $S_f'^{-1}M$ (0, 1.4.3).

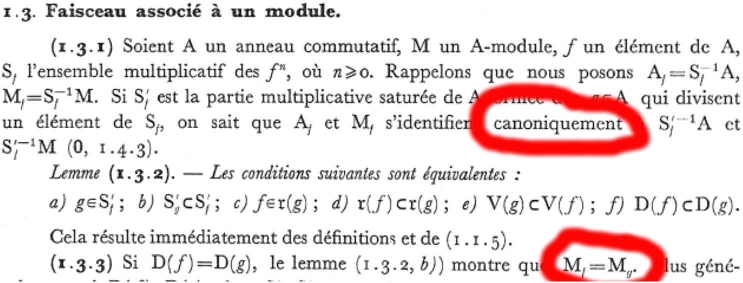
Lemme (**1.3.2**). — *Les conditions suivantes sont équivalentes :*

a) $g \in S'_f$; *b)* $S'_g \subset S'_f$; *c)* $f \in \mathfrak{r}(g)$; *d)* $\mathfrak{r}(f) \subset \mathfrak{r}(g)$; *e)* $V(g) \subset V(f)$; *f)* $D(f) \subset D(g)$.

Cela résulte immédiatement des définitions et de (1.1.5).

(**1.3.3**) Si $D(f)=D(g)$, le lemme (1.3.2, *b)*) montre que $M_f = M_g$. Plus géné-

Excerpt from EGA1



1.3. Faisceau associé à un module.

(**1.3.1**) Soient A un anneau commutatif, M un A-module, f un élément de A, S_f l'ensemble multiplicatif des f^n, où $n \geqslant 0$. Rappelons que nous posons $A_f = S_f^{-1}A$, $M_f = S_f^{-1}M$. Si S'_f est la partie multiplicative saturée de A formée des $g \in A$ qui divisent un élément de S_f, on sait que A_f et M_f s'identifient canoniquement à $S_f'^{-1}A$ et $S_f'^{-1}M$ (0, 1.4.3).

Lemme (**1.3.2**). — *Les conditions suivantes sont équivalentes :*

a) $g \in S'_f$; *b)* $S'_g \subset S'_f$; *c)* $f \in \mathfrak{r}(g)$; *d)* $\mathfrak{r}(f) \subset \mathfrak{r}(g)$; *e)* $V(g) \subset V(f)$; *f)* $D(f) \subset D(g)$.

Cela résulte immédiatement des définitions et de (1.1.5).

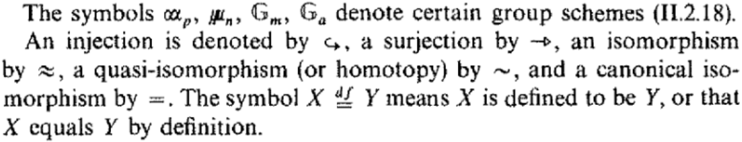
(**1.3.3**) Si $D(f) = D(g)$, le lemme (1.3.2, *b)*) montre que $M_f = M_g$. Plus géné-

Canonical

So Grothendieck says that it's OK because even if the rings aren't *equal*, they are *canonically isomorphic*.

Milne in his book on étale cohomology, the cohomology theory defined by Grothendieck in order to prove the Weil conjectures, decides that this all sounds fine:

Milne's etale cohomology.



The symbols α_p, μ_n, $\mathbb{G}_m$, $\mathbb{G}_a$ denote certain group schemes (II.2.18).

An injection is denoted by $\hookrightarrow$, a surjection by $\twoheadrightarrow$, an isomorphism by $\approx$, a quasi-isomorphism (or homotopy) by $\sim$, and a canonical isomorphism by $=$. The symbol $X \overset{\mathrm{df}}{=} Y$ means X is defined to be Y, or that X equals Y by definition.

"a canonical isomorphism [is denoted by] $=$."

Canonical

But what does this word "canonical" mean?

Well let's look at Wikipedia's page on Canonical Maps.

Definition of "canonical map" from Wikipedia page on canonical maps

"In mathematics, a *canonical map*, also called a natural map, is a map or morphism between objects that arises naturally from the definition or the construction of the objects. In general, it is the map which preserves the widest amount of structure, and it tends to be unique. In the rare cases where latitude in choices remains, the map is either conventionally agreed upon to be the most useful for further analysis, or sometimes the most elegant map known to date."

In my opinion, we have now degenerated into waffle. You cannot type this definition into a computer theorem prover.

A true story

The main theorem of global class field theory is a theorem saying that given a global field, two abelian groups associated to the field are "canonically" isomorphic.

In fact there are two distinct "canonical" isomorphisms, one due to Artin (used extensively by the Heegner point community), and one due to Deligne (used extensively by the Shimura variety community). They are both widely used, and differ by a minus sign.

So much for "conventionally agreed upon".

So what is going on?

It seems to me that Grothendieck is *sweeping something under the carpet*.

However, historically mathematicians have been doing this for a lot longer!

For example, there's something fishy about our definition of the real numbers.

The real numbers

Gauss and Euler and Riemann spoke unambiguously about "the real numbers".

Later on, people tried to make them. There are now several known constructions.

Are the real numbers as defined by Cauchy *equal to* the real numbers as defined by Dedekind? Not if you're a set theorist! They are *models* for the real numbers.

But this does not cause problems, because of the *mathematician's manifesto for real numbers*:

"Don't ask what they're made of, just assume they're a complete ordered field".

The real numbers

"Don't ask what they're made of, just assume they're a complete ordered field".

The common convention in mathematics is that we *restrict* the language we use when speaking about the real numbers.

We are not allowed to talk about elements of elements of "the" set of real numbers, because there is more than one answer!

By *restricting* what we allow as a valid statement about the real numbers, we can have *more* leeway in how we treat equality, without violating the principle of substitution.

For example, we can assume that the Cauchy reals and the Dedekind reals are *equal*.

Unwritten conventions

Similarly, there are restrictions in what we can say about sheaves of functions in mathematics – "unwritten conventions" which are obvious to every algebraic geometer.

These unwritten conventions are subtle to explain to a computer theorem prover written in set theory, simple type theory, or dependent type theory.

These systems have a definition of equality which is *weaker* than Grothendieck's.

As a result, such systems have to *work hard* to apply Grothendieck's substitution principle; the inbuilt one is *too weak*.

Homotopy type theory.

Homotopy type theory forgets about "canonical" and decrees that *all* isomorphisms are equalities.

So it looks like we can recover Grothendieck's substitution principle.

However, in homotopy type theory, things can be *equal in more than one way*; whatever a "canonical" isomorphism really is, homotopy theory type theory also allows equality corresponding to "noncanonical isomorphisms" (e.g. $\mathbb{N} = \mathbb{Z}$).

So this approach has gone too far! It also does not capture what Grothendieck wanted.

Conclusion

Axiomatically modelling Grothendieck's concept of equality seems to me to be an unsolved problem.

Thank you very much for your attention.