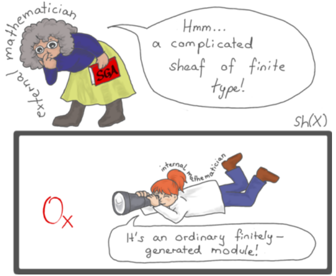


New reduction techniques in commutative algebra driven by logical methods

– an invitation –

Ingo Blechschmidt
Università di Verona

Logic Seminar Padova
December 5st, 2018

We can associate to any reduced ring A a *forcing model* $A^\sim$.

- The forcing model has the pleasant property that it is a field.
- Reasoning about it requires that we restrict ourselves to intuitionistic logic.

Details are on the following slides.

Summary

A baby example

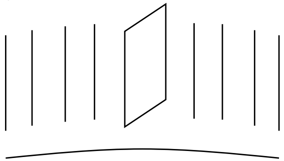
Let M be an injective matrix with more columns than rows over a reduced ring A. Then $1 = 0$ in A.

$$\begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Generic freeness

Generically, any finitely generated module over a reduced ring is free.

(A ring is reduced iff $x^n = 0$ implies $x = 0$.)



The two displayed statements are trivial for fields. It is therefore natural to try to reduce the general situation to that of fields.

Summary

A baby example

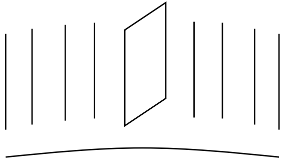
Let M be an injective matrix with more columns than rows over a reduced ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a minimal prime ideal $\mathfrak{p} \subseteq A$. The matrix is injective over the field $A_\mathfrak{p} = A[(A \setminus \mathfrak{p})^{-1}]$; contradiction to basic linear algebra.

Generic freeness

Generically, any finitely generated module over a reduced ring is free.

(A ring is reduced iff $x^n = 0$ implies $x = 0$.)



The displayed proof, which could have been taken from any standard textbook on commutative algebra, succeeds in this reduction by employing proof by contradiction and minimal prime ideals. However, this way of reducing comes at a cost: It requires the Boolean Prime Ideal Theorem (for ensuring the existence of a prime ideal and for ensuring that stalks at minimal prime ideals are fields) and even the full axiom of choice (for ensuring the existence of a minimal prime ideal).

We should hope that such a simple statement admits a more informative, explicit, computational proof not employing transfinite methods: There should be an explicit method for transforming the given conditional equations expressing injectivity into the equation $1 = 0$. And indeed there is: Beautiful constructive proofs can be found in Richman's note on nontrivial uses of trivial rings and in the recent textbook by Lombardi and Quitté on constructive commutative algebra.

The new reduction technique presented in this talk provides a way of performing the reduction in an entirely constructive manner, avoiding the axiom of choice. If so desired, resulting topos-theoretic proofs can be unwound to yield fully explicit, topos-free, direct proofs.

Summary

A baby example

Let M be an injective matrix with more columns than rows over a reduced ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a minimal prime ideal $\mathfrak{p} \subseteq A$. The matrix is injective over the field $A_\mathfrak{p} = A[(A \setminus \mathfrak{p})^{-1}]$; contradiction to basic linear algebra.

Generic freeness

Generically, any finitely generated module over a reduced ring is free.

Proof. See [Stacks Project].

The baby example demonstrates that the reduction technique of this talk is of interest to constructive commutative algebra. What about classical commutative algebra? This is what the second example aims at. Grothendieck's generic freeness lemma is an important theorem in algebraic geometry, where it is usually stated in the following geometric form:

> Let X be a reduced scheme. Let $\mathcal{B}$ be an $\mathcal{O}_X$-algebra of finite type. Let $\mathcal{M}$ be a $\mathcal{B}$-module of finite type. Then over a dense open,
>
> (a) $\mathcal{B}$ and $\mathcal{M}$ are locally free as sheaves of $\mathcal{O}_X$-modules,
> (b) $\mathcal{B}$ is of finite presentation as a sheaf of $\mathcal{O}_X$-algebras and
> (c) $\mathcal{M}$ is of finite presentation as a sheaf of $\mathcal{B}$-modules.

All previously known proofs proceed in a series of reduction steps, finally culminating in the case where A is a Noetherian integral domain. They are somewhat convoluted (spanning several pages) and require nontrivial prerequisites in commutative algebra.

Using the new reduction technique, there is a short (one-paragraph) and conceptual proof of Grothendieck's generic freeness lemma. It is constructive as a bonus; and if desired, one can unwind the resulting proof to obtain a constructive proof which doesn't reference topos theory. The proof obtained in this way is still an improvement on the previously known proofs, requiring no advanced prerequisites in commutative algebra, and takes about a page.

Summary

- For any reduced ring A, there is a ring $A^\sim$ in a certain topos with

$$\models \big(\forall x : A^\sim .\, \neg(\exists y : A^\sim .\, xy = 1) \Rightarrow x = 0\big).$$

- This semantics is sound with respect to intuitionistic logic.
- It has uses in classical and constructive commutative algebra.

A baby example

Let M be an injective matrix with more columns than rows over a reduced ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a minimal prime ideal $\mathfrak{p} \subseteq A$. The matrix is injective over the field $A_\mathfrak{p} = A[(A \setminus \mathfrak{p})^{-1}]$; contradiction to basic linear algebra.

Generic freeness

Generically, any finitely generated module over a reduced ring is free.

Proof. See [Stacks Project].

Instead of passing from a given ring A to one of its stalks $A_\mathfrak{p}$ or quotient rings $A/\mathfrak{a}$, the reduction technique presented in this talk passes from A to a *forcing model* $A^\sim$.

Unlike stalks or quotient rings, which are honest rings, the forcing model $A^\sim$ is not a ring in the strict sense of the word: It doesn't have an underlying *set* of elements, but instead an underlying *sheaf* of elements. It is a *ring object* in a certain category, the *little Zariski topos* of A. But as long as we restrict to intuitionistic reasoning, this difference is immaterial. A metatheorem displayed on a later slide states that any intuitionistic theorem about rings applies to $A^\sim$ just as if A were a proper, ordinary ring.

Studying $A^\sim$ is in fact the same as studying A from a certain different, *local* point of view. The precise meaning of this statement will be explained on slide 3.

Summary

- For any reduced ring A, there is a ring $A^\sim$ in a certain topos with
$$\models \big(\forall x : A^\sim.\ \neg(\exists y : A^\sim.\ xy = 1) \Rightarrow x = 0\big).$$
- This semantics is sound with respect to intuitionistic logic.
- It has uses in classical and constructive commutative algebra.

A baby example

Let M be an injective matrix with more columns than rows over a reduced ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a minimal prime ideal $\mathfrak{p} \subseteq A$. The matrix is injective over the field $A_\mathfrak{p} = A[(A \setminus \mathfrak{p})^{-1}]$; contradiction to basic linear algebra.

Generic freeness

Generically, any finitely generated module over a reduced ring is free.

Proof. See [Stacks Project].

Intuitionistic logic is the same as classical logic, but without:

- the law of excluded middle: $\varphi \vee \neg\varphi$
- the law of double negation elimination: $\neg\neg\varphi \Rightarrow \varphi$
- the axiom of choice

If one is unfamiliar with constructive mathematics, then doing without these three laws seems unmotivated, rather peculiar and overtly restrictive. Here, the restriction to intuitionistic logic is not by some philosophical choice. Rather, it's by mathematical necessity. It's just a fact that in general, the laws of classical logic don't apply to $A^\sim$. (Assuming a classical metatheory and assuming A to be Noetherian, they do iff A is of Krull dimension ≤ 0.)

Luckily, vast amounts of commutative algebra work in the intuitionistic setting, as for instance evidenced by the recent 1000^+-page textbook by Lombardi and Quitté. This claim extends to statements which are usually proven using maximal ideals or minimal ideal prime ideals and hence require Zorn's lemma. Indeed, the technique presented in this talk allows to constructivize some results of this kind.

Background on constructive mathematics can for instance be found in a talk by Andrej Bauer (written notes). The standard proof that $\sqrt{2}$ is not rational is perfectly fine in constructive mathematics.

Motivating the semantics

A ring is **local** iff $1 \neq 0$ and if $x + y = 1$ implies that x is invertible or y is invertible.

Examples: $k,\ k[[X]],\ \mathbb{C}\{z\},\ \mathbb{Z}_{(p)}$

Non-examples: $\mathbb{Z},\ k[X],\ \mathbb{Z}/(pq)$

Locally, any ring is local.

Let $x + y = 1$ in a ring A. Then:

- The element x is invertible in $A[x^{-1}]$.
- The element y is invertible in $A[y^{-1}]$.

(Recall $A[f^{-1}] = \{ \frac{u}{f^n} \mid u \in A, n \in \mathbb{N} \}$.)

In topos theory, we have lots of experience of *changing universes* in order to *force* some statements to become true. However, because the field condition we are aiming at is not a *geometric sequent*, these techniques do not work here. Hence we'll take it more slowly and only devise a semantics which forces the given ring to be local.

The displayed definition of a local ring is, in the presence of the axiom of choice, equivalent to the more common one (ring with exactly one maximal ideal). In constructive mathematics, the displayed definition usually works better.

The key insight is that *locally* (in the sense of topology/geometry), any ring is a local ring. That is, we may pretend that any given ring is local if we are prepared to pass to numerous localizations during the course of an argument. The semantics displayed on the next slide manages this localization-juggling for us.

By $A[f^{-1}]$, we mean the localization of A away from f. This construction makes sense even if f is a zero divisor, in which case $A[f^{-1}]$ is the zero ring.

The Kripke–Joyal semantics

Let A be a ring (commutative, with unit). We recursively define

$$f \models \varphi \quad (\text{“}\varphi \text{ holds away from the zeros of } f\text{”})$$

for elements $f \in A$ and statements φ. Write “$\models \varphi$” to mean $1 \models \varphi$.

$f \models \top$	is	true
$f \models \bot$	iff	f is nilpotent
$f \models x = y$	iff	$x = y \in A[f^{-1}]$
$f \models \varphi \wedge \psi$	iff	$f \models \varphi$ and $f \models \psi$
$f \models \varphi \vee \psi$	iff	there exists a partition $f^n = fg_1 + \cdots + fg_m$ with, for each i, $fg_i \models \varphi$ or $fg_i \models \psi$
$f \models \varphi \Rightarrow \psi$	iff	for all $g \in A$, $fg \models \varphi$ implies $fg \models \psi$
$f \models \forall x : A^{\sim}.\, \varphi$	iff	for all $g \in A$ and all $x_0 \in A[(fg)^{-1}]$, $fg \models \varphi[x_0/x]$
$f \models \exists x : A^{\sim}.\, \varphi$	iff	there exists a partition $f^n = fg_1 + \cdots + fg_m$ with, for each i, $fg_i \models \varphi[x_0/x]$ for some $x_0 \in A[(fg_i)^{-1}]$

The clause for “$\vee$” is made exactly in such a way as to ensure, if $x + y = 1$, that $1 \models ((\exists z : A^{\sim}.\, xz = 1) \vee (\exists z : A^{\sim}.\, yz = 1))$.

The definition of the semantics is reminiscent of Kripke and Beth models. Indeed, it is a fragment of the Kripke–Joyal semantics of the *internal language of a topos*, and this general semantics encompasses Kripke and Beth models as special cases.

The Kripke–Joyal semantics

Write "$\models \varphi$" to mean $1 \models \varphi$.

$$
\begin{array}{lll}
f \models x = y & \text{iff} & x = y \in A[f^{-1}] \\
f \models \varphi \wedge \psi & \text{iff} & f \models \varphi \text{ and } f \models \psi \\
f \models \varphi \vee \psi & \text{iff} & \text{there exists a partition } f^n = fg_1 + \cdots + fg_m \text{ with,} \\
& & \quad \text{for each } i,\ fg_i \models \varphi \text{ or } fg_i \models \psi
\end{array}
$$

Monotonicity

If $f \models \varphi$, then also $fg \models \varphi$.

Locality

If $f^n = fg_1 + \cdots + fg_m$ and $fg_i \models \varphi$ for all i, then also $f \models \varphi$.

Soundness

If $\varphi \vdash \psi$ and $f \models \varphi$, then $f \models \psi$.

Forced properties

$\models \ulcorner A^\sim$ is a local ring$\urcorner$.

The soundness lemma states: If $f \models \varphi$, and if φ intuitionistically entails a further statement ψ, then also $f \models \psi$. In this way we can *reason* with the forcing model, similarly as if $A^\sim$ would actually exist as a ring instead of merely being a convenient syntactic fiction.

If we want $A^\sim$ to actually exist, not just as a figure of speech, then we have to broaden our notion of existence and accept ring objects in toposes. More on this on the next slide.

The four lemmas displayed on this slide, as well as all the claims on further slides, can be proven in very weak intuitionistic metatheories.

The Kripke–Joyal semantics

Write "$\models \varphi$" to mean $1 \models \varphi$.

$$
\begin{array}{lll}
f \models x = y & \text{iff} & x = y \in A[f^{-1}] \\
f \models \varphi \wedge \psi & \text{iff} & f \models \varphi \text{ and } f \models \psi \\
f \models \varphi \vee \psi & \text{iff} & \text{there exists a partition } f^n = fg_1 + \cdots + fg_m \text{ with,} \\
& & \quad \text{for each } i,\ fg_i \models \varphi \text{ or } fg_i \models \psi
\end{array}
$$

Monotonicity

If $f \models \varphi$, then also $fg \models \varphi$.

Locality

If $f^n = fg_1 + \cdots + fg_m$ and $fg_i \models \varphi$ for all i, then also $f \models \varphi$.

Soundness

If $\varphi \vdash \psi$ and $f \models \varphi$, then $f \models \psi$.

Forced properties

$\models \ulcorner A^\sim$ is a local ring$\urcorner$.

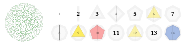
Irrespective of whether A is a local ring, its mirror image $A^\sim$ is always a local ring (that is, the axioms of what it means to be a local ring hold under the translation rules specified by the semantics). A basic application of this forcing model are local-to-global principles. For instance:

- The statement "the kernel of a surjective matrix over a local ring is finite free" admits a constructive proof. It therefore holds for $A^\sim$. Its external meaning is that the kernel of a surjective matrix M over A is finite locally free (there exists a partition $1 = f_1 + \cdots + f_n$ such that for each i, the localized module $(\ker M)[f_i^{-1}]$ is finite free).
- The ring A is a Prüfer domain if and only if $A^\sim$ is a Bézout domain. Therefore any constructive theorem about Bézout domains entails a corresponding theorem about Prüfer domains. Bézout domains are quite rare, while Prüfer domains abound (for instance the ring of integers of any number field is a Prüfer domain, even constructively so).

A universal property

The displayed semantics is the first-order fragment of the **higher-order internal language** of the **little Zariski topos**.

Set

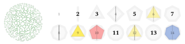


The usual laws of logic hold.

Sh X

The intermediate value theorem fails.

Eff



Every function is computable.

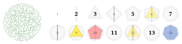
A topos is a special kind of category. Every topos has an associated *internal language* which can be used to do mathematics *internally to the topos*.

The prototypical example of a topos is the category Set. Doing mathematics internally to Set amounts to just doing mathematics in the usual sense. A primer on the topos-theoretic landscape is contained in these slides. These slides also explain the geometric reason why the intermediate value theorem fails in most toposes of sheaves, and why in the effective topos any function $\mathbb{N} \to \mathbb{N}$ is computable.

A universal property

The displayed semantics is the first-order fragment of the **higher-order internal language** of the **little Zariski topos**.

Set

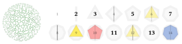


The usual laws of logic hold.

Sh X

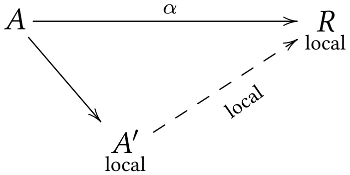
The intermediate value theorem fails.

Eff



Every function is computable.

Is there a **free local ring** $A \to A'$ over A?



For a fixed ring R, the localization $A' := A[S^{-1}]$ with $S := \alpha^{-1}[R^\times]$ would do the job. (S is a *filter*.)

Hence we need the **generic filter**.

A free local ring A' over A is a local ring A' together with a ring homomorphism $A \to A'$ such that any ring homomorphism $A \to R$ to a local ring uniquely factors over a local ring homomorphism $A' \to R$. (A ring homomorphism is *local* iff it reflects invertibility.)

Assuming the Boolean Prime Ideal Theorem, one can show that there is a free local ring over A if and only if A has exactly one prime ideal. In this case A is already local, and we can take $A' := A$. If we want every ring to possess a free local ring over it, we need to accept ring objects of different toposes than Set.

The little Zariski topos contains the *generic filter* of A. Localizing A at this filter yields the desired free local ring. It is precisely what was called $A^\sim$ before. It is also known as the structure sheaf of Spec(A).

The little Zariski topos

Let A be a ring. Its **little Zariski topos** is equivalently

1. the classifying locale of **prime filters** of A,
2. the classifying topos of **local localizations** of A,
3. the locale given by the frame of **radical ideals** of A,
4. the topos of sheaves over the poset A with $f \preceq g$ iff $f \in \sqrt{(g)}$ and with $(f_i \to f)_i$ deemed covering iff $f \in \sqrt{(f_i)_i}$ or
5. the topos of sheaves over $\operatorname{Spec}(A)$.

Its associated topological space of points is the **classical spectrum**

$$\{\mathfrak{f} \subseteq A \mid \mathfrak{f} \text{ prime filter}\} + \text{Zariski topology}.$$

It has **enough points** if the Boolean Prime Ideal Theorem holds.

Prime ideal: $0 \in \mathfrak{p}$; $x \in \mathfrak{p} \wedge y \in \mathfrak{p} \Rightarrow x + y \in \mathfrak{p}$; $1 \not\in \mathfrak{p}$; $xy \in \mathfrak{p} \Leftrightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$

Prime filter: $0 \not\in \mathfrak{f}$; $x + y \in \mathfrak{f} \Rightarrow x \in \mathfrak{f} \vee y \in \mathfrak{f}$; $1 \in \mathfrak{f}$; $xy \in \mathfrak{f} \Leftrightarrow x \in \mathfrak{f} \wedge y \in \mathfrak{f}$

Any geometric theory has a *classifying topos* which contains the *generic model* of that theory (any model in any topos is uniquely the pullback of the generic one); if the theory under consideration is propositional (doesn't have any sorts), then its classifying topos can be chosen to be the topos of sheaves over a locale. One can also give a direct account of classifying locales, as a pedagogical stepping stone to the full theory of classifying toposes.

The slide contains a small lie: The classical definition of the spectrum of a ring is via the set of prime ideals of A, not filters. If the law of excluded middle is available, there is no difference between these definitions since the complement of a prime ideal is a filter and vice versa. One can also consider the classifying locale of prime ideals of A. Its associated topological space of points is the set of prime ideals of A equipped with the *constructible topology*.

In an intuitionistic (but still impredicative) context, any of the (generalized) spaces of items 1–4 can be adopted as sensible definitions of the spectrum. Item 5 is then a tautology. The classical definition of the spectrum as a topological space doesn't work very well, because verifying the universal property one expects of it requires the Boolean Prime Ideal Theorem. Most dramatically, in some toposes there are rings which are not trivial yet have neither prime ideals nor filters. The classical definition yields in this case the empty space.

Investigating the forcing model

The **little Zariski topos** of a ring A is equivalently

- the topos of sheaves over $\mathrm{Spec}(A)$,
- the locale given by the frame of radical ideals of A,
- the classifying locale of filters of A

and contains a **mirror image** of A, the sheaf of rings $A^\sim$.

Assuming the Boolean Prime Ideal Theorem, a first-order formula "$\forall \ldots \forall. (\cdots \Longrightarrow \cdots)$", where the two subformulas may not contain "$\Rightarrow$" and "$\forall$", holds for $A^\sim$ iff it holds for all stalks $A_\mathfrak{p}$.

$A^\sim$ inherits any property of A which is **localization-stable**.

If A is reduced ($x^n = 0 \Rightarrow x = 0$):

$A^\sim$ is a **field**.
$A^\sim$ has **$\neg\neg$-stable equality**.
$A^\sim$ is **anonymously Noetherian**.

For working with $A^\sim$, it's important to know how properties of A relate to properties of $A^\sim$.

The first displayed metatheorem justifies that, to a first approximation, the forcing model $A^\sim$ is a reification of all the stalks of A into a single coherent entity. But crucially, this slogan is only correct for properties which can be put in the displayed syntactical form (called *geometric sequents*). The reductive power of passing from A to $A^\sim$ results from surprising non-geometric sequents which are satisfied by $A^\sim$ and not shared by A, its localizations or its quotients.

A slight generalization of the second metatheorem soups up a number of basic lemmas of algebraic geometry, there stated in geometric language. For instance, if M is finitely generated, then $M^\sim$ is of finite type. If M is finitely presented, then $M^\sim$ is of finite presentation. If M is coherent, then $M^\sim$ is coherent.

Investigating the forcing model

The **little Zariski topos** of a ring A is equivalently

- the topos of sheaves over $\mathrm{Spec}(A)$,
- the locale given by the frame of radical ideals of A,
- the classifying locale of filters of A

and contains a **mirror image** of A, the sheaf of rings $A^\sim$.

Assuming the Boolean Prime Ideal Theorem, a first-order formula "$\forall \ldots \forall. (\cdots \implies \cdots)$", where the two subformulas may not contain "$\Rightarrow$" and "$\forall$", holds for $A^\sim$ iff it holds for all stalks $A_\mathfrak{p}$.

$A^\sim$ inherits any property of A which is **localization-stable**.

If A is reduced ($x^n = 0 \Rightarrow x = 0$):

$A^\sim$ is a **field**.
$A^\sim$ has **$\neg\neg$-stable equality**.
$A^\sim$ is **anonymously Noetherian**.

Surprisingly and significantly, in case that A is reduced, there are a number of non-geometric sequents validated by $A^\sim$. These are unique features of the forcing model.

$A^\sim$ is a field in the sense that zero is the only noninvertible element.

$A^\sim$ has $\neg\neg$-stable equality in the sense that

$$\models \forall x : A^\sim. \forall y : A^\sim. \neg\neg(x = y) \Rightarrow x = y.$$

Classically, every set has $\neg\neg$-stable equality; intuitionistically, this is a special property of some sets. It's quite useful, as some theorems of classical commutative algebra can only be proven intuitionistically when weakened by double negation. The stability then allows, in some cases, to obtain the original conclusion.

$A^\sim$ is *anonymously Noetherian* in the sense that any of its ideals is *not not* finitely generated. A philosophically-motivated constructivist might be offended by this notion, since it runs counter to the maxim that constructive mathematics should be informative, telling us only that there can't not be finite generating families. However, in the forcing context it is a useful notion: Hilbert's basis theorem holds for it, and it can be put to good use in the proof of (the general case of) Grothendieck's generic freeness lemma.

Investigating the forcing model

The little Zariski topos of a ring A is equivalently

- the topos of sheaves over Spec(A),

and

> **ON THE SPECTRUM OF A RINGED TOPOS** **209**
>
> For completeness, two further remarks should be added to this treatment of the spectrum. One is that in **E** the canonical map $A \to \Gamma_*(LA)$ is an isomorphism—i.e., the representation of A in the ring of "global sections" of LA is complete. The second, due to Mulvey in the case **E** = **S**, is that in Spec(**E**, A) the formula
>
> $$\neg(x \in U(LA)) \Rightarrow \exists n(x^n = 0)$$
>
> is valid. This is surely important, though its precise significance is still somewhat obscure—as is the case with many such nongeometric formulas. In any case, calculations such as these are easier from the point of view of the Heyting algebra of radical ideals of A, and hence will be omitted here.

Miles Tierney. On the spectrum of a ringed topos. 1976.

$A^\sim$ inherits any property of A which is localization-stable.

The field property was already observed in the 1970s by Mulvey, but apparently back then its significance for applications was overlooked and no deeper reason for this property was known. We now know that it's a shadow of a forced higher-order property whose external translation expresses that $A^\sim$ is quasicoherent (details are in Section 3.3 of these notes).

Investigating the forcing model

The **little Zariski topos** of a ring A is equivalently

The external meaning of

$$\models \ulcorner A^\sim[X_1, \ldots, X_n] \text{ is anonymously Noetherian} \urcorner$$

is:

For any element $f \in A$ and any (not necessarily quasicoherent) sheaf of ideals $\mathcal{J} \hookrightarrow A^\sim[X_1, \ldots, X_n]|_{D(f)}$: If

for any element $g \in A$ the condition that

the sheaf $\mathcal{J}$ is of finite type on $D(g)$

implies that $g = 0$,

then $f = 0$.

which is **localization-stable**.

Some properties of the forcing model, which are easy to state and prove as properties about $A^\sim$, have quite complex meanings when unravelled to refer directly to A. In this way the forcing model unlocks observations which might otherwise be too unwieldy to manage.

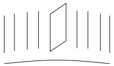
Revisiting the test cases

Let A be a reduced commutative ring ($x^n = 0 \Rightarrow x = 0$).
Let $A^\sim$ be its mirror image in the little Zariski topos.

A baby example

Let M be an injective matrix over A with more columns than rows. Then $1 = 0$ in A.

Proof. M is also injective as a matrix over $A^\sim$. Since $A^\sim$ is a field, this is a contradiction by basic linear algebra. Thus $\models \bot$. This amounts to $1 = 0$ in A.



Generic freeness

Let M be a finitely generated A-module. If $f = 0$ is the only element of A such that $M[f^{-1}]$ is a free $A[f^{-1}]$-module, then $1 = 0$ in A.

Proof. The claim amounts to $\models$ "$M^\sim$ is **not not** free". Since $A^\sim$ is a field, this follows from basic linear algebra.

With the baby example, we see that the new reduction technique presented in this talk allows to reinterpret the core content of the classical proof shown on slide 1 in a constructive fashion. Since the forcing model was set up in a constructive way, we could mechanically extract an explicit procedure from the new proof.

For the second example, a remark might be in order. A basic theorem of undergraduate linear algebra is that any finitely generated vector space has a basis. In this form, the theorem cannot quite be proven intuitionistically. Indeed, the standard proof uses the law of excluded middle in the first step:

> Let $(x_1, \ldots, x_n)$ be a given finite generating family. It might be the case that one of the vectors x_i can be expressed as a linear combination of the others, or not. In the second case, the family is linearly independent and thus the vector space is shown to have a basis. In the first case, we continue with the smaller generating family $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ in an inductive fashion.

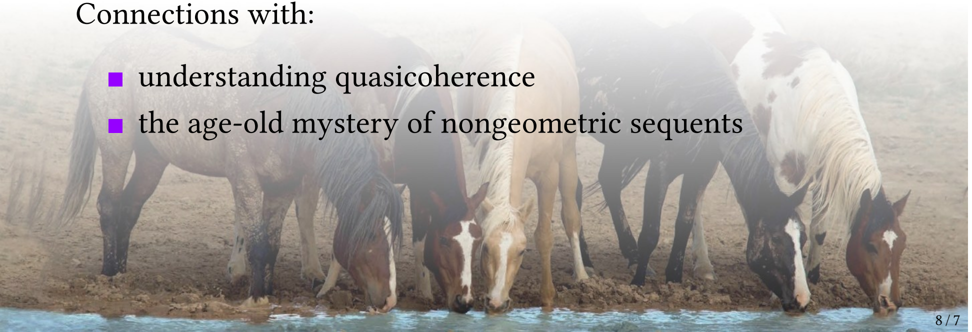
Intuitionistically, the law of excluded middle is not available; however its double negation ($\neg\neg(\varphi \vee \neg\varphi)$) is. Threading the double negation through the rest of the proof yields the following theorem of intuitionistic linear algebra: Any finitely generated vector space is *not not* free. It is this theorem which the proof on the slide refers to.

The Zariski topos and related toposes have applications in:

- classical algebra and classical algebraic geometry
- constructive algebra and constructive algebraic geometry
- synthetic algebraic geometry ("schemes are just sets")

Connections with:

- understanding quasicoherence
- the age-old mystery of nongeometric sequents



Summarizing, we can associate to any reduced ring A the forcing model $A^\sim$.

- The forcing model has the pleasant property that it is a field.
- Reasoning about it requires that we restrict ourselves to intuitionistic logic.

Depending on the application, this trade-off can not be useful at all, or be quite valuable. It certainly is so for proving Grothendieck's generic freeness lemma, simplifying a multi-page argument to a single and conceptual paragraph. (The previous slide only showed a fragment of the general statement of Grothendieck's generic freeness lemma. The technique outlined in these slides is amenable to the full version. Details are in Section 11.5 of these notes.)

The ideas underlying this new reduction technique can also be used for different purposes: for understanding, in a rigorous way, notions of algebraic geometry as notions of algebra, and for developing a synthetic account of algebraic geometry. This is very briefly touched upon on the next two slides.

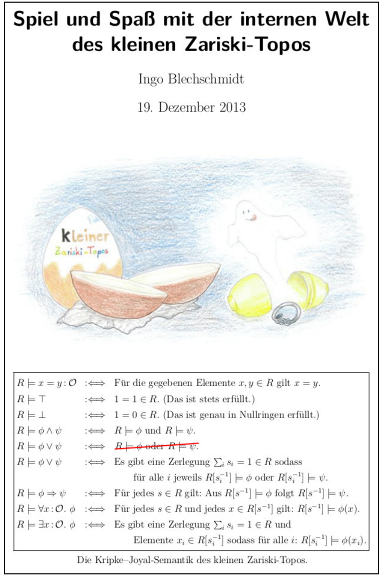
The Zariski topos and related toposes have applications in:

- classical algebra and classical algebraic geometry
- constructive algebra and constructive algebraic geometry
- synthetic algebraic geometry ("schemes are just sets")

Connections with:

- understanding quasicoherence
- the age-old mystery of nongeometric sequents

Further reading



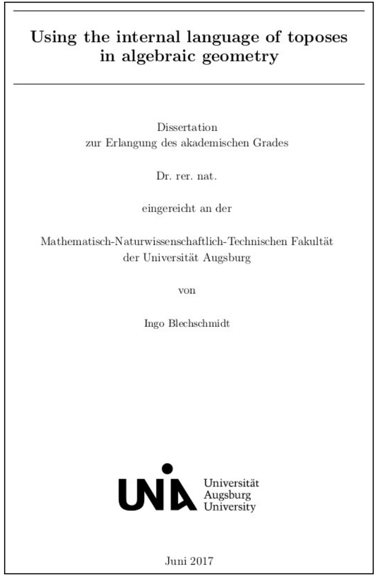
Spiel und Spaß mit der internen Welt des kleinen Zariski-Topos

Ingo Blechschmidt

19. Dezember 2013

$R \models x = y : \mathcal{O}$	$:\Longleftrightarrow$	Für die gegebenen Elemente $x, y \in R$ gilt $x = y$.
$R \models \top$	$:\Longleftrightarrow$	$1 = 1 \in R$. (Das ist stets erfüllt.)
$R \models \bot$	$:\Longleftrightarrow$	$1 = 0 \in R$. (Das ist genau in Nullringen erfüllt.)
$R \models \phi \wedge \psi$	$:\Longleftrightarrow$	$R \models \phi$ und $R \models \psi$.
$R \models \phi \vee \psi$	$:\Longleftrightarrow$	~~$R \models \phi$ oder $R \models \psi$.~~
$R \models \phi \vee \psi$	$:\Longleftrightarrow$	Es gibt eine Zerlegung $\sum_i s_i = 1 \in R$ sodass für alle i jeweils $R[s_i^{-1}] \models \phi$ oder $R[s_i^{-1}] \models \psi$.
$R \models \phi \Rightarrow \psi$	$:\Longleftrightarrow$	Für jedes $s \in R$ gilt: Aus $R[s^{-1}] \models \phi$ folgt $R[s^{-1}] \models \psi$.
$R \models \forall x : \mathcal{O}.\ \phi$	$:\Longleftrightarrow$	Für jedes $s \in R$ und jedes $x \in R[s^{-1}]$ gilt: $R[s^{-1}] \models \phi(x)$.
$R \models \exists x : \mathcal{O}.\ \phi$	$:\Longleftrightarrow$	Es gibt eine Zerlegung $\sum_i s_i = 1 \in R$ und Elemente $x_i \in R[s_i^{-1}]$ sodass für alle i: $R[s_i^{-1}] \models \phi(x_i)$.

Die Kripke–Joyal-Semantik des kleinen Zariski-Topos.



Using the internal language of toposes in algebraic geometry

Dissertation
zur Erlangung des akademischen Grades

Dr. rer. nat.

eingereicht an der

Mathematisch-Naturwissenschaftlich-Technischen Fakultät
der Universität Augsburg

von

Ingo Blechschmidt

Universität Augsburg University

Juni 2017

Applications in algebraic geometry

Understand **notions of algebraic geometry** over a scheme X as **notions of algebra** internal to $\mathrm{Sh}(X)$.

externally	internally to $\mathrm{Sh}(X)$
sheaf of sets	set
sheaf of modules	module
sheaf of finite type	finitely generated module
tensor product of sheaves	tensor product of modules
sheaf of rational functions	total quotient ring of $\mathcal{O}_X$
dimension of X	Krull dimension of $\mathcal{O}_X$
spectrum of a sheaf of $\mathcal{O}_X$-algebras	ordinary spectrum [with a twist]
higher direct images	sheaf cohomology

Let $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ be a short exact sequence of sheaves of $\mathcal{O}_X$-modules. If $\mathcal{F}'$ and $\mathcal{F}''$ are of finite type, so is $\mathcal{F}$.

$\Longleftarrow$

Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of modules. If M' and M'' are finitely generated, so is M.

One doesn't need to be an expert in topos theory in order to know that many notions in algebraic geometry are inspired by notions in algebra and that proofs in algebraic geometry often proceed by reducing to algebra.

If X is a scheme, the internal language of the topos $\mathrm{Sh}(X)$ is a way of making this connection precise: In many cases, the former are simply interpretations of the latter internal to $\mathrm{Sh}(X)$. Because this connection is precise instead of informal, additional value is gained: We can skip many basic proofs in algebraic geometry because they're just externalizations of proofs in algebra carried out internally to $\mathrm{Sh}(X)$.

Applications in algebraic geometry

Understand **notions of algebraic geometry** over a scheme X as **notions of algebra** internal to $\mathrm{Sh}(X)$.

externally	internally to $\mathrm{Sh}(X)$
sheaf of sets	set
sheaf of modules	module
sheaf of finite type	finitely generated module
tensor product of sheaves	tensor product of modules
sheaf of rational functions	total quotient ring of $\mathcal{O}_X$
dimension of X	Krull dimension of $\mathcal{O}_X$
spectrum of a sheaf of $\mathcal{O}_X$-algebras	ordinary spectrum [with a twist]
higher direct images	sheaf cohomology

Let $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ be a short exact sequence of sheaves of $\mathcal{O}_X$-modules. If $\mathcal{F}'$ and $\mathcal{F}''$ are of finite type, so is $\mathcal{F}$.

$\Longleftarrow$

Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of modules. If M' and M'' are finitely generated, so is M.

A basic example is as follows. A short exact sequence of sheaves of modules looks like a short exact sequence of plain modules from the internal point of view of $\mathrm{Sh}(X)$. If the two outer sheaves are of finite type, then from the internal point of view, the two outer modules will look like finitely generated modules. Because the standard proof of the proposition quoted on the lower right is intuitionistically valid, it follows that, from the internal point of view, the middle module is too finitely generated. Consulting the dictionary a second time, this amounts to saying that the middle sheaf is of finite type.

A more advanced example is: The theorem "any finitely generated vector space does *not not* have a basis" of constructive linear algebra entails, by interpretation in $\mathrm{Sh}(X)$, that any sheaf of finite type over a reduced scheme is finite locally free on a *dense open subset*.

More details on this research program can be found in these notes, partly reported on at the 2015 IHÉS topos theory conference. Even though many important dictionary entries are still missing (for instance pertaining to derived categories and intersection theory), I believe that it is already in its current form useful to working algebraic geometers.

The next slide illustrates a further, different way of approaching algebraic geometry using topos theory.

Synthetic algebraic geometry

Usual approach to algebraic geometry: **layer schemes above ordinary set theory** using either

- locally ringed spaces

  set of prime ideals of $\mathbb{Z}[X, Y, Z]/(X^n + Y^n - Z^n)$ + Zariski topology + structure sheaf

- or Grothendieck's functor-of-points account, where a scheme is a functor Ring $\to$ Set.

$$A \longmapsto \{(x, y, z) \in A^3 \mid x^n + y^n - z^n = 0\}$$

At the Secret Blogging Seminar, there was an insightful long-running discussion on the merits of the two approaches to algebraic geometry. Two disadvantages of the approach using locally ringed spaces is that the underlying topological spaces don't actually parametrize "honest", "geometric" points, but the more complex notion of irreducible closed subsets; and that they don't work well in a constructive setting. (For this, they would have to be replaced by locally ringed locales.)

The functorial approach is more economical, philosophically rewarding, and works constructively. Given a functor $F : \text{Ring} \to \text{Set}$, we imagine $F(A)$ to be the set of "A-valued points" of the hypothetical scheme described by F, the set of "points with coordinates in A". These sets have direct geometric meaning. However, typically only field-valued points are easy to describe. For instance, the functor representing projective n-space is given on fields by

$$K \longmapsto \text{the set of lines through the origin in } K^{n+1} \cong \{[x_0 : \cdots : x_n] \mid x_i \neq 0 \text{ for some } i\},$$

whereas on general rings it is given by

$$A \longmapsto \text{the set of quotients } A^{n+1} \twoheadrightarrow P, \text{ where } P \text{ is projective, modulo isomorphism.}$$

It is these more general kinds of points which impart a sense of cohesion on the field-valued points, so they can't simply be dropped from consideration.

Synthetic algebraic geometry

Usual approach to algebraic geometry: **layer schemes above ordinary set theory** using either

- locally ringed spaces

  $$\text{set of prime ideals of } \mathbb{Z}[X, Y, Z]/(X^n + Y^n - Z^n) + \text{Zariski topology} + \text{structure sheaf}$$

- or Grothendieck's functor-of-points account, where a scheme is a functor Ring $\to$ Set.

  $$A \longmapsto \{(x, y, z) \in A^3 \mid x^n + y^n - z^n = 0\}$$

Synthetic approach: model schemes **directly as sets** in a certain nonclassical set theory, the internal universe of the **big Zariski topos** of a base scheme.

$$\{(x, y, z) : (\underline{\mathbb{A}}^1)^3 \mid x^n + y^n - z^n = 0\}$$

This tension is resolved by observing that the category of functors Ring $\to$ Set is a topos (the *big Zariski topos* of Spec($\mathbb{Z}$)) and that we can therefore employ its internal language. This language takes care of juggling stages behind the scenes. For instance, projective n-space can be described by the naive expression

$$\{(x_0, \ldots, x_n) : (\underline{\mathbb{A}}^1)^{n+1} \mid x_0 \neq 0 \vee \cdots \vee x_n \neq 0\}/(\underline{\mathbb{A}}^1)^\times.$$

This example illustrates the goal: to develop a synthetic account of algebraic geometry, in which schemes are plain sets and morphisms between schemes are maps between those sets. It turns out that there are many similarities with the well-developed synthetic account of differential geometry, but also important differences, and it also turns out that synthetic algebraic geometry has close connections to a certain age-old unsolved problem in topos theory, the *mystery of nongeometric sequents*.

Details are in this set of slides.