How topos theory can help algebra

– an invitation –

$\boxed{1}$ **Background on the internal language**

$\boxed{2}$ **Applications in commutative algebra**

$\boxed{3}$ **The mystery of nongeometric sequents**

Ingo Blechschmidt (MPI Leipzig)

Toposes in Como

June 29th, 2018

Motivating testcases

Let A be a ring (commutative, with unit, $1 = 0$ allowed).
Assume that A is reduced: If $x^n = 0$, then $x = 0$.

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

A baby application

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

A child application

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

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

Motivating testcases

Let A be a ring (commutative, with unit, $1 = 0$ allowed).
Assume that A is reduced: If $x^n = 0$, then $x = 0$.

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

A baby application

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

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is surjective over the field $A/\mathfrak{m}$. This is a contradiction to basic linear algebra.

A child application

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

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

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

The displayed proofs, which could have been taken from any standard textbook on commutative algebra, succeed in this reduction quite easily by employing maximal ideals or 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).

It therefore doesn't work in the internal universe of most toposes, and in any case it obscures explicit computational content: Statements so simple as the two displayed ones should admit explicit, computational proofs.

We'll learn how the internal language of a certain well-chosen topos provides a way to perform the reduction in an entirely constructive manner. If so desired, the resulting topos-theoretic proofs can be unwinded to yield fully explicit, topos-free, direct proofs.

Beautiful constructive proofs can also be found in Richman's note on nontrivial uses of nontrivial rings and in the recent textbook by Lombardi and Quitté on constructive commutative algebra.

Motivating testcases

Let A be a ring (commutative, with unit, $1 = 0$ allowed).
Assume that A is reduced: If $x^n = 0$, then $x = 0$.

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

A baby application

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

Proof. Assume not. Then there is a prime ideal $\mathfrak{p}$. The matrix is surjective over the field $\mathrm{Quot}(A/\mathfrak{p})$. This is a contradiction to basic linear algebra.

A child application

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

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

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

The displayed proofs, which could have been taken from any standard textbook on commutative algebra, succeed in this reduction quite easily by employing maximal ideals or 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).

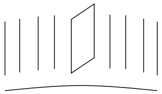
It therefore doesn't work in the internal universe of most toposes, and in any case it obscures explicit computational content: Statements so simple as the two displayed ones should admit explicit, computational proofs.

We'll learn how the internal language of a certain well-chosen topos provides a way to perform the reduction in an entirely constructive manner. If so desired, the resulting topos-theoretic proofs can be unwinded to yield fully explicit, topos-free, direct proofs.

Beautiful constructive proofs can also be found in Richman's note on nontrivial uses of nontrivial rings and in the recent textbook by Lombardi and Quitté on constructive commutative algebra.

Motivating testcases

Let A be a ring (commutative, with unit, $1 = 0$ allowed).
Assume that A is reduced: If $x^n = 0$, then $x = 0$.



Generic freeness

Let B be an A-algebra of finite type ($\cong A[X_1, \ldots, X_n]/\mathfrak{a}$).
Let M be a finitely generated B-module ($\cong B^m/U$).
If $f = 0$ is the only element of A such that

1. $B[f^{-1}]$ and $M[f^{-1}]$ are free modules over $A[f^{-1}]$,
2. $A[f^{-1}] \to B[f^{-1}]$ is of finite presentation and
3. $M[f^{-1}]$ is finitely presented as a module over $B[f^{-1}]$,

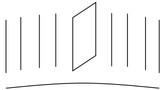
then $1 = 0$ in A.

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.

Motivating testcases

Let A be a ring (commutative, with unit, $1 = 0$ allowed).
Assume that A is reduced: If $x^n = 0$, then $x = 0$.



Generic freeness

Let B be an A-algebra of finite type ($\cong A[X_1, \ldots, X_n]/\mathfrak{a}$).
Let M be a finitely generated B-module ($\cong B^m/U$).
If $f = 0$ is the only element of A such that

1. $B[f^{-1}]$ and $M[f^{-1}]$ are free modules over $A[f^{-1}]$,
2. $A[f^{-1}] \to B[f^{-1}]$ is of finite presentation and
3. $M[f^{-1}]$ is finitely presented as a module over $B[f^{-1}]$,

then $1 = 0$ in A.

Proof. See [Stacks Project, Tag 051Q].

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 (for instance, the proof in the Stacks Project is three pages long) and employ several results in commutative algebra which have not yet been constructivized.

Using the internal language of toposes, we will give a short, conceptual and constructive proof of Grothendieck's generic freeness lemma. Again, if so desired, one can unwind the internal 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.

The internal language of a topos

For any topos $\mathcal{E}$ and any formula φ, we define the meaning of

$$\text{“}\mathcal{E} \models \varphi\text{”} \quad (\text{“}\varphi \text{ holds in the internal universe of } \mathcal{E}\text{”})$$

using (Shulman's extension of) the **Kripke–Joyal semantics**.

$\mathrm{Set} \models \varphi$	$\mathrm{Sh}(X) \models \varphi$	$\mathrm{Eff} \models \varphi$
“φ holds in the usual sense.”	“φ holds continuously.”	“φ holds computably.”

Any topos supports **mathematical reasoning**:

If $\mathcal{E} \models \varphi$ and if φ entails ψ intuitionistically, then $\mathcal{E} \models \psi$.

The internal language of a topos allows to construct objects and morphisms, formulate statements about them and prove such statements in a naive element-based language. From the internal point of view, objects look like sets [more precisely, types]; morphisms look like maps; epimorphisms look like surjections; group objects look like groups; and so on.

To determine whether a statement φ holds in the internal universe of a given topos, one can use the Kripke–Joyal semantics to translate it into an ordinary external statement and then check the validity of the external translation.

For instance, in the effective topos the curious statement “any function $\mathbb{N} \to \mathbb{N}$ is computable” holds, for its external meaning is the triviality “there is a Turing machine which given a Turing machine computing some function $f : \mathbb{N} \to \mathbb{N}$ outputs a Turing machine computing f”. In contrast, the statement “any function $\mathbb{N} \to \mathbb{N}$ is either the zero function or not” does not hold in the effective topos, since its external meaning is “there exists a Turing machine which given a Turing machine computing some function $f : \mathbb{N} \to \mathbb{N}$ decides whether f is the zero function or not”.

The internal language of a topos

For any topos $\mathcal{E}$ and any formula φ, we define the meaning of

$$\text{“}\mathcal{E} \models \varphi\text{”} \quad (\text{“}\varphi \text{ holds in the internal universe of } \mathcal{E}\text{”})$$

using (Shulman's extension of) the **Kripke–Joyal semantics**.

$\mathrm{Set} \models \varphi$ “φ holds in the usual sense.”	$\mathrm{Sh}(X) \models \varphi$ “φ holds continuously.”	$\mathrm{Eff} \models \varphi$ “φ holds computably.”

Any topos supports **mathematical reasoning**:

If $\mathcal{E} \models \varphi$ and if φ entails ψ intuitionistically, then $\mathcal{E} \models \psi$.

no $\varphi \vee \neg\varphi$, no $\neg\neg\varphi \Rightarrow \varphi$, no axiom of choice

Any theorem which has an intuitionistic proof holds in the internal universe of any topos. The restriction to intuitionistic logic is not due to philosophical concerns; it is a fact of life that only very few toposes validate the law of excluded middle (for instance, sheaf toposes over discrete topological space do if the law of excluded middle is available in the metatheory). Luckily, vast amounts of mathematics can be developed in a purely intuitionistic setting.

The internal language machinery itself can be developed in an intuitionistic setting.

The standard internal language of toposes in not enough for our purposes, as it misses unbounded quantification (“for all groups”, “for all rings”) and dependent types. Shulman's stack semantics offers what we need. No knowledge of stacks is necessary to enjoy his paper. Prior work includes Polymorphism is Set Theoretic, Constructively by Pitts and Relating first-order set theories, toposes and categories of classes by Awodey, Butz, Simpson and Streicher (obtained independently and published after Shulman).

The internal language of $\mathrm{Sh}(X)$

Let X be a topological space. We recursively define

$$U \models \varphi \quad (\text{“}\varphi \text{ holds on } U\text{”})$$

for open subsets $U \subseteq X$ and formulas φ. Write “$\mathrm{Sh}(X) \models \varphi$” to mean $X \models \varphi$.

$$\begin{array}{ll}
U \models s = t : F & \text{iff } s|_U = t|_U \in F(U) \\
U \models \varphi \wedge \psi & \text{iff } U \models \varphi \text{ and } U \models \psi \\
U \models \varphi \vee \psi & \text{iff } \cancel{U \models \varphi \text{ or } U \models \psi} \text{ there exists a covering } U = \bigcup_i U_i \text{ s. th.} \\
& \qquad \text{for all } i\text{: } U_i \models \varphi \text{ or } U_i \models \psi \\
U \models \varphi \Rightarrow \psi & \text{iff for all open } V \subseteq U\text{: } V \models \varphi \text{ implies } V \models \psi \\
U \models \forall s : F.\, \varphi(s) & \text{iff for all open } V \subseteq U \text{ and sections } s_0 \in F(V)\text{: } V \models \varphi(s_0) \\
U \models \forall F.\, \varphi(F) & \text{iff for all open } V \subseteq U \text{ and sheaves } F_0 \text{ over } V\text{: } V \models \varphi(F_0) \\
U \models \exists s : F.\, \varphi(s) & \text{iff there exists a covering } U = \bigcup_i U_i \text{ s. th. for all } i\text{:} \\
& \qquad \text{there exists } s_0 \in F(U_i) \text{ s. th. } U_i \models \varphi(s_0) \\
U \models \exists F.\, \varphi(F) & \text{iff there exists a covering } U = \bigcup_i U_i \text{ s. th. for all } i\text{:} \\
& \qquad \text{there exists a sheaf } F_0 \text{ on } U_i \text{ s. th. } U_i \models \varphi(F_0)
\end{array}$$

Many interesting sheaves have few global sections, which is why a definition should as “$U \models \forall s : F.\, \varphi(s)$ iff $U \models \varphi(s_0)$ for all $s_0 \in F(U)$” would miss the point. More precisely, changing the definitions like this would yield the internal language of the topos of presheaves on X.

Here is an explicit example of the translation procedure. Let $\alpha : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves on X. Then:

$$\begin{array}{ll}
& X \models \ulcorner \alpha \text{ is injective} \urcorner \\
\Longleftrightarrow & X \models \forall s, t : \mathcal{F}.\, \alpha(s) = \alpha(t) \Rightarrow s = t \\
\Longleftrightarrow & \text{for all open } U \subseteq X, \text{ sections } s, t \in \mathcal{F}(U)\text{:} \\
& \qquad U \models \alpha(s) = \alpha(t) \Rightarrow s = t \\
\Longleftrightarrow & \text{for all open } U \subseteq X, \text{ sections } s, t \in \mathcal{F}(U)\text{:} \\
& \qquad \text{for all open } V \subseteq U\text{:} \\
& \qquad\qquad \alpha_V(s|_V) = \alpha_V(t|_V) \text{ implies } s|_V = t|_V \\
\Longleftrightarrow & \text{for all open } U \subseteq X, \text{ sections } s, t \in \mathcal{F}(U)\text{:} \\
& \qquad \alpha_U(s|_U) = \alpha_U(t|_U) \text{ implies } s|_U = t|_U \\
\Longleftrightarrow & \alpha \text{ is a monomorphism of sheaves}
\end{array}$$

Internalizing parameter-dependence

Let X be a space. A continuous family $(f_x)_{x \in X}$ of continuous functions (that is, a continuous function $f : X \times \mathbb{R} \to \mathbb{R}$; $f_x(a) = f(x,a)$) induces an endomorphism of the sheaf $\mathcal{C}$ of continuous functions:

$$\bar{f} : \mathcal{C} \longrightarrow \mathcal{C}, \text{ on } U\!: s \longmapsto (x \mapsto f_x(s(x))).$$

- $\mathrm{Sh}(X) \models \ulcorner$The set $\mathcal{C}$ is the set of (Dedekind) reals$\urcorner$.
- $\mathrm{Sh}(X) \models \ulcorner$The function $\bar{f} : \mathbb{R} \to \mathbb{R}$ is continuous$\urcorner$.

- Iff $f_x(-1) < 0$ for all x, then $\mathrm{Sh}(X) \models \bar{f}(-1) < 0$.
- Iff $f_x(+1) > 0$ for all x, then $\mathrm{Sh}(X) \models \bar{f}(+1) > 0$.
- Iff all f_x are increasing, then $\mathrm{Sh}(X) \models \ulcorner\bar{f}$ is increasing$\urcorner$.

- Iff there is an open cover $X = \bigcup_i U_i$ such that for each i there is a continuous function $s : U_i \to \mathbb{R}$ with $f_x(s(x)) = 0$ for all $x \in U_i$, then $\mathrm{Sh}(X) \models \exists s\!:\!\mathbb{R}.\, \bar{f}(s) = 0$.

This slide, unrelated to commutative algebra or algebraic geometry, aims to illustrate one of the basic uses of the internal language of toposes: Upgrading any theorem admitting an intuitionistic proof to a parameter-dependent version.

Constructively, there are several non-equivalent forms of the intermediate value theorem. The following version doesn't admit an intuitionistic proof:

> Let $g : \mathbb{R} \to \mathbb{R}$ be a function between the (Dedekind) reals which is continuous in the usual epsilon/delta sense. Assume $g(-1) < 0 < g(1)$. Then there exists a number $x \in \mathbb{R}$ such that $g(x) = 0$.

If there was an intuitionistic proof, the statement would hold in any topos, so in particular in sheaf toposes over topological spaces. By the translations shown on the slide (the corner quotes "$\ulcorner \ldots \urcorner$" indicate that translation into formal language is left to the reader), this would amount to the following strengthening of the intermediate value theorem: In continuous families of continuous functions, zeros can locally be picked continuously. However, this strengthening is invalid, as this video shows.

Internalizing parameter-dependence

Let X be a space. A continuous family $(f_x)_{x \in X}$ of continuous functions (that is, a continuous function $f : X \times \mathbb{R} \to \mathbb{R}$; $f_x(a) = f(x, a)$) induces an endomorphism of the sheaf $\mathcal{C}$ of continuous functions:

$$\bar{f} : \mathcal{C} \longrightarrow \mathcal{C}, \text{ on } U\text{: } s \longmapsto (x \mapsto f_x(s(x))).$$

- $\mathrm{Sh}(X) \models \ulcorner$The set $\mathcal{C}$ is the set of (Dedekind) reals$\urcorner$.
- $\mathrm{Sh}(X) \models \ulcorner$The function $\bar{f} : \mathbb{R} \to \mathbb{R}$ is continuous$\urcorner$.

- Iff $f_x(-1) < 0$ for all x, then $\mathrm{Sh}(X) \models \bar{f}(-1) < 0$.
- Iff $f_x(+1) > 0$ for all x, then $\mathrm{Sh}(X) \models \bar{f}(+1) > 0$.
- Iff all f_x are increasing, then $\mathrm{Sh}(X) \models \ulcorner\bar{f}$ is increasing$\urcorner$.

- Iff there is an open cover $X = \bigcup_i U_i$ such that for each i there is a continuous function $s : U_i \to \mathbb{R}$ with $f_x(s(x)) = 0$ for all $x \in U_i$, then $\mathrm{Sh}(X) \models \exists s{:}\mathbb{R}.\, \bar{f}(s) = 0$.

In contrast, the following version does admit an intuitionistic proof. We can therefore interpret it in sheaf toposes over topological spaces and thereby obtain the strengthening that in continuous families of strictly increasing continuous functions, zeros can locally be picked continuously. You are invited to prove this strengthening directly, without reference to the internal language.

> Let $g : \mathbb{R} \to \mathbb{R}$ be a function between the (Dedekind) reals which is continuous in the usual epsilon/delta sense and which is strictly increasing ($a < b$ implies $g(a) < g(b)$). Assume $g(-1) < 0 < g(1)$. Then there exists a number $x \in \mathbb{R}$ such that $g(x) = 0$.

The little Zariski topos

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

1. the classifying topos of **local localizations** of A,
2. the classifying locale of **prime filters** 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 $\mathrm{Spec}(A)$.

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: $0 \in \mathfrak{p}$; $x \in \mathfrak{p} \wedge y \in \mathfrak{p} \Rightarrow x + y \in \mathfrak{p}$; $1 \notin \mathfrak{p}$; $xy \in \mathfrak{p} \Leftrightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$

Prime filter: $0 \notin \mathfrak{f}$; $x + y \in \mathfrak{f} \Rightarrow x \in \mathfrak{f} \vee y \in \mathfrak{f}$; $1 \in \mathfrak{f}$; $xy \in \mathfrak{f} \Leftrightarrow x \in \mathfrak{f} \wedge y \in \mathfrak{f}$

Any geometric theory has a classifying topos; 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 prime 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 prime filter and vice versa.

One can also consider the classifying local of prime *ideals* of A. Its associated topological space of points is the the set of prime ideal of A equipped with the *constructible topology*.

In an intuitionistic context, any of the (generalized) spaces of items 1–4 can be adopted as sensible definitions of the spectrum of A. 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, there are rings which are not trivial yet don't have any prime ideals or prime filters. The classical definition yields in this case the empty space.

First steps in the little Zariski topos

Let A be a ring. Let $\mathfrak{f}_0$ be the **generic prime filter** of A; it is a subobject of the constant sheaf $\underline{A}$ of the little Zariski topos.

- The ring $A^\sim := \underline{A}[\mathfrak{f}_0^{-1}]$ is the generic local localization of A.
- Given an A-module M, we have the $A^\sim$-module $M^\sim := \underline{M}[\mathfrak{f}_0^{-1}]$.

The generic prime filter $\mathfrak{f}_0$ can be described in explicit terms. For ring elements f and s, $D(f) \models (s \in \mathfrak{f}_0)$ iff $f \in \sqrt{(s)}$.

First steps in the little Zariski topos

Let A be a ring. Let $\mathfrak{f}_0$ be the **generic prime filter** of A; it is a subobject of the constant sheaf $\underline{A}$ of the little Zariski topos.

- The ring $A^\sim := \underline{A}[\mathfrak{f}_0^{-1}]$ is the generic local localization of A.
- Given an A-module M, we have the $A^\sim$-module $M^\sim := \underline{M}[\mathfrak{f}_0^{-1}]$.

Definition. Let A be a ring and let M be an A-module. We define the *sheaf associated* to M on Spec A, denoted by $\tilde{M}$, as follows. For each prime ideal $\mathfrak{p} \subseteq A$, let $M_\mathfrak{p}$ be the localization of M at $\mathfrak{p}$. For any open set $U \subseteq$ Spec A we define the group $\tilde{M}(U)$ to be the set of functions $s\colon U \to \coprod_{\mathfrak{p} \in U} M_\mathfrak{p}$ such that for each $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in M_\mathfrak{p}$, and such that s is locally a fraction m/f with $m \in M$ and $f \in A$. To be precise, we require that for each $\mathfrak{p} \in U$, there is a neighborhood V of $\mathfrak{p}$ in U, and there are elements $m \in M$ and $f \in A$, such that for each $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = m/f$ in $M_\mathfrak{q}$. We make $\tilde{M}$ into a sheaf by using the obvious restriction maps.

Robin Hartshorne. Algebraic Geometry. 1977.

The generic prime filter $\mathfrak{f}_0$ can be described in explicit terms. For ring elements f and s, $D(f) \models (s \in \mathfrak{f}_0)$ iff $f \in \sqrt{(s)}$.

Our description of $M^\sim$ reveals a precise sense in which $M^\sim$ and M are related: $M^\sim$ is simply a localization of M (first lifted to another universe by the constant sheaf construction). The classical descriptions don't make the relation evident.

First steps in the little Zariski topos

Let A be a ring. Let $\mathfrak{f}_0$ be the **generic prime filter** of A; it is a subobject of the constant sheaf $\underline{A}$ of the little Zariski topos.

- The ring $A^\sim := \underline{A}[\mathfrak{f}_0^{-1}]$ is the generic local localization of A.
- Given an A-module M, we have the $A^\sim$-module $M^\sim := \underline{M}[\mathfrak{f}_0^{-1}]$.

Assuming the Boolean prime ideal theorem, a geometric sequent "$\forall \ldots \forall. (\cdots \Longrightarrow \cdots)$", where the two subformulas may not contain "$\Rightarrow$" and "$\forall$", holds for $M^\sim$ iff it holds for all stalks $M_\mathfrak{p}$.

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

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

$A^\sim$ is a **field** (nonunits are zero).
$A^\sim$ has **$\neg\neg$-stable equality**.
$A^\sim$ is **anonymously Noetherian**.

The generic prime filter $\mathfrak{f}_0$ can be described in explicit terms. For ring elements f and s, $D(f) \models (s \in \mathfrak{f}_0)$ iff $f \in \sqrt{(s)}$.

Our description of $M^\sim$ reveals a precise sense in which $M^\sim$ and M are related: $M^\sim$ is simply a localization of M (first lifted to another universe by the constant sheaf construction). The classical descriptions don't make the relation evident.

One can show, assuming that the little Zariski topos is *overt*, that the module M in Set and the module $\underline{M}$ of the little Zariski topos share all first-order properties. This observation explains the metatheorem displayed at the bottom left. The assumption is satisfied if any element of A is nilpotent or not nilpotent, so it's always satisfied if the law of excluded middle is available. In an intuitionistic context, it's still "morally satisfied". Details are in Section 12.9 of these notes.

As a first approximation, the module $M^\sim$ can be thought of as a reification of all the stalks of M as a single object. The metatheorem makes this precise and also shows the limits of this view: It is only correct for geometric sequents. When considering nongeometric sequents, phenomena appear which are unique to $M^\sim$ in the sense that they are in general not shared by M, its stalks or its quotients.

First steps in the little Zariski topos

Let A be a ring. Let f_0 be the generic prime filter of A; it is a subobject of the constant sheaf $\underline{A}$ of the little Zariski topos.

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 $\mathbf{E} = \mathbf{S}$, 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.

Assuming that A is reduced, the following nongeometric sequents hold in the little Zariski topos (among others):

$A^\sim$ is a field in the sense that zero is the only noninvertible element. This field property was already observed in the 1970s by Mulvey, who didn't know a deeper reason for this property. We now know that it's a shadow of an internal property whose external translation expresses that $A^\sim$ is quasicoherent.

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

$$\mathrm{Spec}(A) \models \forall s\colon A^\sim.\, \neg\neg(s = 0) \Rightarrow s = 0.$$

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. However, in the internal context it is a useful notion: Hilbert's basis theorem holds for it, and we'll put it to good use in our proof of Grothendieck's generic freeness lemma.

First steps in the little Zariski topos

Let A be a ring. Let f_0 be the generic prime filter of A; it is a

Complexity reduction

The external meaning of

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

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.

Are there theorems which can only be proven using the internal language and not be proven without?

No. Just as the translation from internal statements to external statements is entirely mechanical, so is the translation from internal proofs to external proofs. Any proof employing the internal language can be unwinded to yield an external proof not referencing the internal language.

However, depending on the logical complexity of the statements occuring in a given proof, the resulting external proof might be (much) more complex than the internal proof. This is particularly the case if the proof involves double negation, for much the same reason as that in computer science, continuations can twist the control flow in nontrivial ways which are sometimes hard to understand. It is in these cases where we can extract the most value of the internal language, unlocking notions and proofs which might otherwise be hard to obtain.

The slide shows a specific example. The internal statement that $A^{\sim}[X_1, \ldots, X_n]$ is anonymously Noetherian is quite simple; its external translation is quite convoluted.

Revisiting the testcases

Let A be a reduced ring.

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

A baby application

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

Proof. The matrix is surjective over the field $A^\sim$. This is a contradiction to basic linear algebra. Hence $\mathrm{Spec}(A) \models \bot$, thus $1 = 0$ in A.

A child application

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

Proof. The matrix is injective over the field $A^\sim$. This is a contradiction to basic linear algebra. Hence $\mathrm{Spec}(A) \models \bot$, thus $1 = 0$ in A.

Revisiting the testcases

$$\begin{tikzcd} & M \arrow[d, dash, "\text{finitely generated}"] \\ A \arrow[r, "\text{of finite type}"'] & B \end{tikzcd}$$

Let A be a reduced ring.

Generic freeness

Let B be an A-algebra of finite type ($\cong A[X_1, \ldots, X_n]/\mathfrak{a}$).
Let M be a finitely generated B-module ($\cong B^m/U$).
If $f = 0$ is the only element of A such that

1. $B[f^{-1}]$ and $M[f^{-1}]$ are free modules over $A[f^{-1}]$,
2. $A[f^{-1}] \to B[f^{-1}]$ is of finite presentation and
3. $M[f^{-1}]$ is finitely presented as a module over $B[f^{-1}]$,

then $1 = 0$ in A.

Revisiting the testcases

$$\begin{tikzcd} & M \arrow[d, dash, "\text{finitely generated}"] \\ A \arrow[r, "\text{of finite type}"'] & B \end{tikzcd}$$

Let A be a reduced ring.

Generic freeness

Let B be an A-algebra of finite type ($\cong A[X_1, \ldots, X_n]/\mathfrak{a}$).
Let M be a finitely generated B-module ($\cong B^m/U$).
If $f = 0$ is the only element of A such that

1. $B[f^{-1}]$ and $M[f^{-1}]$ are free modules over $A[f^{-1}]$,
2. $A[f^{-1}] \to B[f^{-1}]$ is of finite presentation and
3. $M[f^{-1}]$ is finitely presented as a module over $B[f^{-1}]$,

then $1 = 0$ in A.

Proof. In the little Zariski topos it's **not not** the case that

1. $B^\sim$ and $M^\sim$ are free modules over $A^\sim$,
2. $A^\sim \to B^\sim$ is of finite presentation and
3. $M^\sim$ is finitely presented as a module over $B^\sim$,

by basic linear algebra over the field $A^\sim$. The claim is precisely the external translation of this fact.

Understanding algebraic geometry

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

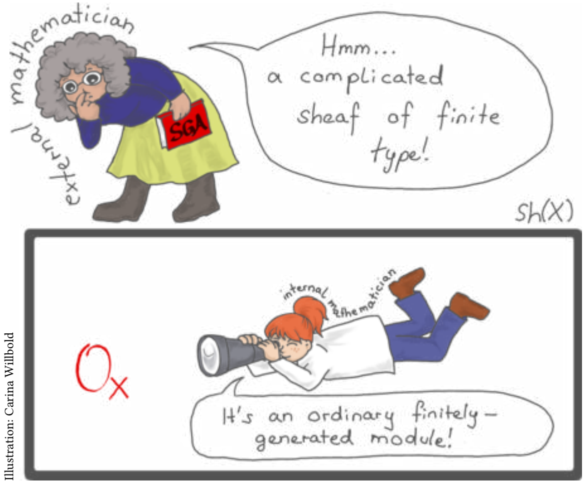


Illustration: Carina Willbold

Understanding 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]
big Zariski topos of X	big Zariski topos of the ring $\mathcal{O}_X$ [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.

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 $\rightarrow$ 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 the internal universe of the **big Zariski topos** of a base scheme.

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

The big Zariski topos

Let S be a fixed base scheme.

Definition

The **big Zariski topos** $\mathrm{Zar}(S)$ of a scheme S is equivalently

1. the topos of sheaves over $(\mathrm{Aff}/S)_{\mathrm{lofp}}$,
2. the classifying topos of local rings over S or
3. the classifying $\mathrm{Sh}(S)$-topos of local $\mathcal{O}_S$-algebras which are local over $\mathcal{O}_S$.

- For an S-scheme X, its functor of points $\underline{X} = \mathrm{Hom}_S(\cdot, X)$ is an object of $\mathrm{Zar}(S)$. It feels like **the set of points** of X.
- In particular, there is the ring object $\underline{\mathbb{A}}^1$ with $\underline{\mathbb{A}}^1(T) = \mathcal{O}_T(T)$.
- This ring object is a **field**: nonzero implies invertible. [Kock 1976]

Synthetic constructions

$\mathbb{A}^n = (\underline{\mathbb{A}}^1)^n = \underline{\mathbb{A}}^1 \times \cdots \times \underline{\mathbb{A}}^1$

$\mathbb{P}^n = \{(x_0, \ldots, x_n) : (\underline{\mathbb{A}}^1)^{n+1} \mid x_0 \neq 0 \vee \cdots \vee x_n \neq 0\}/(\underline{\mathbb{A}}^1)^\times$
$\cong$ set of one-dimensional subspaces of $(\underline{\mathbb{A}}^1)^{n+1}$
(with $\mathcal{O}(-1) = (\ell)_{\ell : \mathbb{P}^n}$, $\mathcal{O}(1) = (\ell^\vee)_{\ell : \mathbb{P}^n}$)

Spec(R) $= \mathrm{Hom}_{\mathrm{Alg}(\underline{\mathbb{A}}^1)}(R, \underline{\mathbb{A}}^1) =$ set of $\underline{\mathbb{A}}^1$-valued points of R

TX $= X^\Delta$, where $\Delta = \{\varepsilon : \underline{\mathbb{A}}^1 \mid \varepsilon^2 = 0\}$

A subset $U \subseteq X$ is **qc-open** if and only if for any $x : X$ there exist $f_1, \ldots, f_n : \underline{\mathbb{A}}^1$ such that $x \in U \iff \exists i.\, f_i \neq 0$.

A **synthetic affine scheme** is a set which is in bijection with Spec(R) for some synthetically quasicoherent $\underline{\mathbb{A}}^1$-algebra R.

A **finitely presented synthetic scheme** is a set which can be covered by finitely many qc-open f.p. synthetic affine schemes U_i such that the intersections $U_i \cap U_j$ can be covered by finitely many qc-open f.p. synthetic affine schemes.

Relations between the Zariski toposes

The big Zariski topos is a topos over the small Zariski topos:

$$\begin{array}{rrcl} \pi: & \mathrm{Zar}(A) & \longrightarrow & \mathrm{Spec}(A) \\ & \text{local } A\text{-algebra } (A \xrightarrow{\alpha} B) & \longmapsto & (A \to A[(\alpha^{-1}[B^\times])^{-1}]) \end{array}$$

This morphism is **connected** (π^{-1} is fully faithful) and **local**, so there is a preinverse

$$\begin{array}{rcl} \mathrm{Spec}(A) & \longrightarrow & \mathrm{Zar}(A) \\ \text{local localization } (A \to B) & \longmapsto & (A \to B) \end{array}$$

which is a subtopos inclusion inducing an idempotent monad $\sharp$ and an idempotent comonad $\flat$ on $\mathrm{Zar}(S)$.

- Internally to $\mathrm{Zar}(S)$, $\mathrm{Spec}(S)$ can be constructed as the **largest subtopos** where $\flat\underline{\mathbb{A}}^1 \to \underline{\mathbb{A}}^1$ is bijective.
- Internally to $\mathrm{Spec}(S)$, $\mathrm{Zar}(S)$ can be constructed as the **classifying topos** of local $\mathcal{O}_S$-algebras which are local over $\mathcal{O}_S$.
- $\mathrm{Zar}(A)$ is the **lax pullback** $(\mathrm{Set} \Rightarrow_{\mathrm{Set}[\mathrm{Ring}]} \mathrm{Set}[\mathrm{LocRing}])$.

Properties of the affine line

- $\underline{\mathbb{A}}^1$ is a local ring:

$$1 \neq 0 \qquad\qquad x + y \text{ inv.} \Longrightarrow x \text{ inv.} \vee y \text{ inv.}$$

- $\underline{\mathbb{A}}^1$ is a field:

$$\neg(x = 0) \Longleftrightarrow x \text{ invertible} \qquad \text{[Kock 1976]}$$
$$\neg(x \text{ invertible}) \Longleftrightarrow x \text{ nilpotent}$$

- $\underline{\mathbb{A}}^1$ satisfies the axiom of microaffinity: Any map $f : \Delta \to \underline{\mathbb{A}}^1$ is of the form $f(\varepsilon) = a + b\varepsilon$ for unique values $a, b : \underline{\mathbb{A}}^1$, where $\Delta = \{\varepsilon : \underline{\mathbb{A}}^1 \mid \varepsilon^2 = 0\}$.
- Any map $\underline{\mathbb{A}}^1 \to \underline{\mathbb{A}}^1$ is a polynomial.
- $\underline{\mathbb{A}}^1$ is anonymously algebraically closed: Any monic polynomial does *not not* have a zero.

Synthetic quasicoherence

Recall $\mathrm{Spec}(R) = \mathrm{Hom}_{\mathrm{Alg}(\underline{\mathbb{A}}^1)}(R, \underline{\mathbb{A}}^1)$ and consider the statement

$$\text{“the canonical map } \begin{array}{rcl} R & \longrightarrow & (\underline{\mathbb{A}}^1)^{\mathrm{Spec}(R)} \\ f & \longmapsto & (\alpha \mapsto \alpha(f)) \end{array} \text{ is bijective”.}$$

- True for $R = \underline{\mathbb{A}}^1[X]/(X^2)$ (microaffinity).
- True for $R = \underline{\mathbb{A}}^1[X]$ (every function is a polynomial).
- True for **any** finitely presented $\underline{\mathbb{A}}^1$-algebra R.

Any known property of $\underline{\mathbb{A}}^1$ follows from this **synthetic quasicoherence**.

the mystery of nongeometric sequents

Classifying toposes in algebraic geometry

(Big) topos	classified theory
Zariski	local rings [Hakim 1972]
étale	separably closed local rings [Hakim 1972, Wraith 1979]
fppf	fppf-local rings (conjecturally: algebraically closed local rings)
ph	?? (conjecturally: algebraically closed valuation rings validating the projective Nullstellensatz)
surjective	algebraically closed geometric fields
$\neg\neg$	?? (conjecturally: algebraically closed geometric fields are integral over the base)
infinitesimal	local algebras together with a nilpotent ideal [Hutzler 2018]
crystalline	??